175

Грабе. †

Элементарный
курс
теории чисел.

†Принял изд. (1863–1939) 1913 г.

Киев
1913

Элементарный курсъ теоріи чиселъ.

ГЛАВА I.

О дѣлимости чиселъ.

§ 1. Мы будемъ разсматривать въ первой главѣ исключительно числа цѣлыя положительныя, а потому будемъ такія числа называть просто числами.

§ 2. Если число a есть произведеніе двухъ чиселъ b и c, $a = b \cdot c$, то число a мы будемъ называть *кратнымъ* числа b, причемъ будемъ говорить, что число a дѣлится на b; съ другой стороны, число b мы будемъ называть *дѣлителемъ* или *множителемъ* числа a. Будемъ также говорить, что b входитъ множителемъ въ число a.

§ 3. Очевидно, что *если число a есть кратное b, и b—кратное c, то число a есть кратное c*, ибо два равенства $a = mb$, $b = nc$ влекутъ, какъ слѣдствіе, равенство $a = (mn)c$. Это свойство можетъ быть распространено на какое угодно число чиселъ, а именно, *если имѣется рядъ чиселъ, изъ которыхъ каждое предыдущее есть кратное каждаго непосредственно за нимъ слѣдующаго, то каждое изъ этихъ чиселъ будетъ кратнымъ относительно всѣхъ слѣдующихъ.*

§ 4. *Если два числа a и b суть кратныя третьяго числа c, то кратными этого числа будутъ сумма $a + b$ и разность $a - b$.*

Въ самомъ дѣлѣ, два равенства: $a = mc$ и $b = nc$ влекутъ, какъ слѣдствіе, равенство $a \pm b = (m \pm n)c$.

§ 5. Одной изъ важнѣйшихъ задачъ теоріи чиселъ является нахожденіе всѣхъ общихъ дѣлителей двухъ чиселъ a, b.

Для рѣшенія этой задачи предложенъ еще *Эвклидомъ* весьма важный по своимъ приложеніямъ *алгоритмъ*[1]). Этотъ алгоритмъ состоитъ въ слѣдующемъ.

Дѣлимъ большее изъ чиселъ, напр. a, на меньшее b. Если дѣленіе совершается безъ остатка, то всякій дѣлитель числа b будетъ дѣлителемъ числа a. Въ этомъ случаѣ, слѣдовательно, задача нахожденія всѣхъ общихъ дѣлителей чиселъ a и b приводится къ задачѣ нахожденія всѣхъ дѣлителей числа b.

Обращаемся къ случаю, когда a не дѣлится на b. Производя дѣленіе по правиламъ элементарной ариѳметики, приходимъ къ нѣкоторому частному q_1 и остатку r_1. Тогда получимъ равенство:

$$a = bq_1 + r_1 . \qquad (1)$$

Меньшее число b будемъ дѣлить на первый остатокъ r_1 и обозначимъ черезъ q_2 и r_2 частное и остатокъ этого дѣленія. Получаемъ

$$b = r_1 q_2 + r_2 . \qquad (2)$$

Продолжая первый остатокъ дѣлить на второй остатокъ, приходимъ къ равенству

$$r_1 = r_2 q_3 + r_3 , \qquad (3)$$

гдѣ r_3 — новый остатокъ.

Остатки r_1, r_2, r_3, ... при такомъ послѣдовательномъ дѣленіи слѣдуютъ убывая. Такъ какъ чиселъ цѣлыхъ положительныхъ, меньшихъ числа r_1, конечное число, то послѣ конечнаго ряда послѣдовательныхъ дѣленій мы придемъ къ остатку, равному нулю, такъ что получимъ

$$r_{n-1} = r_n q_{n+1} \qquad (n+1),$$

такъ какъ $r_{n+1} = 0$.

На основаніи равенства (1) каждый общій дѣлитель α чиселъ a и b будетъ дѣлителемъ числа r_1, ибо дѣлитель числа b будетъ дѣлителемъ числа bq_1 (см. § 3), а кромѣ того, число α, будучи общимъ дѣлителемъ чиселъ a и bq_1, будетъ дѣлителемъ числа $a - bq_1$, равнаго остатку r_1.

Итакъ, общій дѣлитель α двухъ чиселъ a и b будетъ общимъ дѣлителемъ чиселъ b и r_1, а слѣдовательно, на основаніи равенства (2) будетъ дѣлителемъ числа r_2. Продолжая наше разсужденіе, мы замѣтимъ, что всякій общій дѣлитель α чиселъ a и b будетъ дѣлителемъ послѣдняго остатка r_n.

Очевидно, что и обратно: всякій дѣлитель остатка r_n будетъ дѣлителемъ всѣхъ предыдущихъ остатковъ и общимъ дѣлителемъ чиселъ a и b.

---

[1]) Алгоритмомъ называется всякая послѣдовательность дѣйствій, выполняя которыя мы рѣшаемъ какую нибудь задачу.

Такимъ образомъ мы видимъ, что *задача нахожденія всѣхъ общихъ дѣлителей двухъ чиселъ a и b равносильна задачѣ нахожденія всѣхъ дѣлителей послѣдняго изъ остатковъ r_n въ алгоритмѣ Эвклида.*

Среди дѣлителей числа r_n находится, очевидно, само число r_n, причемъ это число будетъ, очевидно, наибольшимъ изъ всѣхъ дѣлителей; поэтому, послѣдній остатокъ r_n есть не что иное, какъ *наибольшій дѣлитель* двухъ заданныхъ чиселъ a и b. Если этотъ послѣдній остатокъ равенъ единицѣ, то очевидно, что въ этомъ случаѣ числа a и b не могутъ имѣть общихъ дѣлителей, отличныхъ отъ единицы. Подобныя числа носятъ названіе *взаимно простыхъ чиселъ*.

§ 6. Алгоритмъ Эвклида представляетъ изъ себя начало, на основаніи котораго могутъ быть съ удобствомъ доказываемы самыя разнообразныя предложенія теоріи чиселъ.

Какъ примѣръ, приведемъ рядъ доказательствъ простѣйшихъ теоремъ.

§ 7. *Если числа a и b взаимно простыя, то всѣ общіе дѣлители чиселъ ak и b будутъ общими дѣлителями чиселъ k и b.*

Въ самомъ дѣлѣ, въ этомъ случаѣ алгоритмъ Эвклида приводится къ равенствамъ:

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_2 + r_2 \\ &\cdots\cdots\cdots \\ r_{n-2} &= r_{n-1}q_n + 1, \end{aligned} \qquad (1)$$

ибо $r_n = 1$.

Умножая равенства (1) на k, получимъ:

$$\begin{aligned} ka &= bkq_1 + kr_1 \\ kb &= kr_1q_2 + kr_2 \\ &\cdots\cdots\cdots \\ kr_{n-2} &= kr_{n-1}q_n + k. \end{aligned} \qquad (2)$$

Равенства (2) показываютъ, что общій дѣлитель чиселъ ka и b будетъ дѣлителемъ числа kr_1.

Общій дѣлитель чиселъ b и kr_1 будетъ дѣлителемъ числа kr_2.

Продолжая разсужденія далѣе, замѣтимъ, что общій дѣлитель первыхъ чиселъ ka и b будетъ дѣлителемъ чиселъ kr_{n-2} и kr_{n-1}, а слѣдовательно, и числа k, откуда слѣдуетъ справедливость высказанной теоремы.

§ 8. *Если a и k суть числа взаимно простыя съ b, то и произведеніе ихъ ak должно быть простымъ съ b.*

Справедливость этого предложенія вытекаетъ какъ слѣдствіе изъ теоремы предыдущаго §-фа. Въ самомъ дѣлѣ, на основаніи предыдущаго общій наибольшій дѣлитель у чиселъ ak и b будетъ такой же, какъ у чиселъ k и a; но эти послѣднія взаимно простыя; слѣдовательно, этотъ наибольшій дѣлитель равенъ единицѣ, а слѣдовательно взаимно простыя и числа ak и b.

§ 9. *Если a и b взаимно простыя, но ak дѣлится на b, то k дѣлится на b.*

Теорема эта есть слѣдствіе теоремы § 7. Въ этомъ случаѣ число b есть общій наибольшій дѣлитель чиселъ ak и b.

§ 10. Теорема § 8 можетъ быть обобщена слѣдующимъ образомъ. Разсмотримъ два ряда чиселъ

$$a,\ b,\ c,\ \ldots \qquad (1)$$

$$\alpha,\ \beta,\ \gamma,\ \ldots \qquad (2)$$

Положимъ, что каждое изъ чиселъ ряда (1) взаимно простое съ каждымъ изъ чиселъ ряда (2); тогда произведеніе всѣхъ чиселъ перваго ряда $a.b.c.\ldots$ будетъ взаимно простымъ съ произведеніемъ $\alpha.\beta.\gamma\ldots$ второго ряда.

Въ самомъ дѣлѣ, числа a и b простыя съ числомъ α, слѣдовательно и ихъ произведеніе ab будетъ также взаимно простое съ α. Но такъ какъ далѣе и число c также простое съ α, то произведеніе $(ab)c$ будетъ также простое съ α.

Продолжая такое же разсужденіе, мы замѣтимъ, что и произведеніе всѣхъ чиселъ

$$a.b.c\ldots \qquad (3)$$

будетъ взаимно простое съ α.

Но такъ какъ число (3) окажется взаимно простымъ не только съ α, но и со всѣми числами ряда (2), то, слѣдовательно, это число (3) будетъ взаимно простымъ съ произведеніемъ $\alpha.\beta.\gamma\ldots$ чиселъ второго ряда, что и требовалось доказать.

§ 11. Если мы всѣ числа ряда (1) предыдущаго §-фа, число которыхъ пусть будетъ m, будемъ предполагать равными между собою и равными числу a, а всѣ числа ряда (2), числомъ n, равными α, то приходимъ къ такому свойству чиселъ:

Если два числа a и α суть числа взаимно простыя, то будутъ также взаимно простыми произвольныя ихъ степени a^m и α^n.

§ 12. Теорема предыдущаго §-фа даетъ возможность показать, что *корень любой степени m изъ цѣлаго числа A будетъ число или ирраціональное, или цѣлое.*

Въ самомъ дѣлѣ, допустимъ, что этотъ корень будетъ числомъ раціональнымъ

$$\frac{a}{b},$$

гдѣ a и b—числа взаимно простыя.

Получаемъ равенство

$$a^m = Ab^m. \qquad (1)$$

Оказывается, съ одной стороны, что число a^m должно быть взаимно простымъ съ числомъ b^m (см. § 11); съ другой стороны a^m дѣлится на b^m на основаніи равенства (1). Оба эти требованія могутъ быть удовлетворены только положеніемъ: $b^m = 1$, откуда $b = 1$, что и требовалось доказать.

§ 13. Разсмотримъ теперь общихъ дѣлителей ряда чиселъ

$$a, b, c, \ldots \qquad (1)$$

число которыхъ больше двухъ.

Находимъ по правилу Эвклида общій наибольшій дѣлитель первыхъ двухъ чиселъ a и b. Пусть этотъ дѣлитель будетъ δ_1; тогда общій дѣлитель первыхъ трехъ чиселъ ряда долженъ быть дѣлителемъ числа δ_1 и третьяго числа c. Найдемъ общій наибольшій дѣлитель δ_2 чиселъ δ_1 и c. Очевидно, что общіе дѣлители первыхъ трехъ чиселъ ряда (1) будутъ въ то же время дѣлителями числа δ_2 и обратно.

Общіе дѣлители первыхъ четырехъ чиселъ ряда найдутся, если разсматривать общіе дѣлители числа δ_2 и четвертаго числа нашего ряда.

Продолжая такимъ образомъ вычисленіе наибольшихъ общихъ дѣлителей для ряда паръ чиселъ, мы придемъ, наконецъ, къ такому числу δ, что всякій общій дѣлитель всѣхъ чиселъ ряда будетъ дѣлителемъ этого числа δ, и обратно, всякій дѣлитель числа δ будетъ общимъ дѣлителемъ всѣхъ чиселъ ряда.

Очевидно, что само число δ будетъ наибольшимъ общимъ дѣлителемъ всѣхъ чиселъ разсматриваемаго ряда.

§ 14. Если общій дѣлитель всѣхъ чиселъ ряда равенъ единицѣ, то мы будемъ называть такія числа *не имѣющими общаго дѣлителя*. Названіе же взаимно простыхъ мы будемъ придавать числамъ, когда число ихъ больше двухъ, только въ томъ случаѣ, если каждыя два изъ этихъ чиселъ попарно взаимно простыя. Отсюда, очевидно, слѣдуетъ, что *взаимно простыя числа суть также числа безъ общаго дѣлителя*, но обратно можно указать числа безъ общаго дѣлителя, которыя не будутъ взаимно простыми, напр. 2, 6, 9.

§ 15. Поставимъ теперь задачей найти всѣ числа, кратныя нѣсколькихъ чиселъ a, b, c, . . .

Разсмотримъ сначала два числа a и b.

Обозначимъ черезъ δ общаго наибольшаго дѣлителя этихъ чиселъ, такъ что будетъ $a = \delta a_1$, $b = \delta b_1$, гдѣ a_1 и b_1 взаимно простыя числа.

Всякое кратное числа a будетъ имѣть видъ

$$sa = s\delta a_1 . \qquad (1)$$

Если мы желаемъ, чтобы это кратное было также кратнымъ b, то необходимо подобрать число s такимъ образомъ, чтобы $s\delta a_1$ дѣлилось на δb_1: другими словами, чтобы sa_1 дѣлилось на b_1; числа a_1 и b_1 взаимно простыя, слѣдовательно, s должно быть кратнымъ b_1, и мы получаемъ $s = tb_1$.

Итакъ, подставляя въ формулу (1), получаемъ общій видъ $t\delta a_1 b_1$ числа, кратнаго двухъ заданныхъ a и b.

Очевидно, что наименьшимъ кратнымъ будетъ число, получаемое при наименьшемъ значеніи t, т. е. при $t = 1$. Обозначая наименьшее кратное чиселъ a и b черезъ μ, получимъ:

$$\mu = \delta a_1 b_1 = \frac{ba}{\delta} . \qquad (2)$$

Получаемъ теорему:

Наименьшее кратное двухъ чиселъ равняется ихъ произведенію, дѣленному на наибольшаго общаго дѣлителя.

Очевидно, что задача нахожденія наименьшаго кратнаго ряда чиселъ: a, b, c, . . . приведется къ нахожденію наименьшаго кратнаго чиселъ: μ, c, . . . Ищемъ слѣдовательно, наименьшее кратное чиселъ μ и c и продолжаемъ нахожденіе послѣдовательное наименьшихъ кратныхъ чиселъ по два, до тѣхъ поръ, пока не дойдемъ до числа ω, представляющаго наименьшее кратное всѣхъ чиселъ ряда.

§ 16. Не трудно видѣть, что, если числа ряда a, b, c . . . взаимно простыя, то наименьшее кратное ихъ равно ихъ произведенію $a . b . c$ . . Въ самомъ дѣлѣ, въ этомъ случаѣ общій наибольшій дѣлитель δ чиселъ a и b равенъ единицѣ; значитъ $\mu = ab$.

Далѣе, число μ оказывается взаимно простымъ съ третьимъ числомъ c, слѣдовательно, наименьшее кратное трехъ чиселъ a, b, c будетъ равно произведенію $\mu c = abc$ и т. д.

§ 17. Въ предыдущихъ §-хъ мы видѣли, что задача нахожденія всѣхъ общихъ дѣлителей нѣсколькихъ чиселъ приводится къ задачѣ нахожденія всѣхъ дѣлителей нѣкотораго числа. Этой послѣдней задачей мы теперь и займемся.

Если нѣкоторое число p имѣетъ, кромѣ единицы, только одного дѣлителя, а именно, самого себя, то такое число называется *простымъ*.

Не трудно убѣдиться въ слѣдующихъ свойствахъ простыхъ чиселъ:

I. Если p простое число, а a другое число, то p или входитъ множителемъ въ число a, или взаимно простое съ нимъ.

Въ самомъ дѣлѣ, общимъ наибольшимъ дѣлителемъ чиселъ a и p можетъ быть или единица, или p.

II. Если произведеніе нѣсколькихъ чиселъ дѣлится на простое число p, то на него дѣлится, по крайней мѣрѣ, одно изъ этихъ чиселъ, ибо, если бы всѣ множители не дѣлились на p, то и произведеніе по теоремѣ § 10 не дѣлилось бы на p.

§ 18. Если нѣкоторое число a, кромѣ самого себя и единицы, имѣетъ дѣлителя b, то оно называется числомъ *составнымъ*.

Относительно составныхъ чиселъ имѣетъ мѣсто теорема:

Всякое составное число разлагается однимъ только способомъ на простые множители.

Возьмемъ произвольное число a. Можетъ произойти одно изъ двухъ: или это число окажется простымъ, или же оно будетъ имѣть нѣкотораго отличнаго отъ единицы дѣлителя b. Если b число не простое, то оно имѣетъ нѣкотораго дѣлителя c, отличнаго отъ единицы: если дѣлитель c не простой, то можно указать новаго его дѣлителя d. Продолжая такимъ образомъ далѣе и замѣчая, что дѣлители b, c, d, ... идутъ убывая, мы дойдемъ такимъ образомъ до дѣлителя p, который будетъ простымъ числомъ.

Мы получимъ слѣдующее разложеніе нашего числа: $a = pa_1$.

Если число a_1 простое, то разложеніе на простые множители окончено; если же число a_1 составное, то примѣняя къ нему предыдущее разсужденіе, мы придемъ къ нѣкоторому простому его множителю p_1; будетъ $a_1 = p_1 a_2$ или $a = pp_1 a_2$. Продолжая далѣе выдѣленіе простыхъ множителей въ числѣ a_2, мы разложимъ число a на простыхъ множителей $a = pp_1 p_2 \ldots$

Не трудно убѣдиться, что такое разложеніе совершается однимъ способомъ.

Въ самомъ дѣлѣ, если допустимъ другое разложеніе: $a = qq_1 q_2 \ldots$, получаемъ равенство

$$pp_1 p_2 \ldots = qq_1 q_2 \ldots \qquad (1)$$

На основаніи свойства II предыдущаго параграфа простое число p должно дѣлить одного изъ множителей q, q_1, q_2, ... второй части. Пусть этотъ множитель, дѣлящійся на p есть q, тогда должно быть $q = p$, ибо q простое число.

Можемъ сократить на одинъ множитель равенство (1) и тогда получимъ равенство $p_1 p_2 \ldots = q_1 q_2 \ldots$ Разсуждая подобно предыдущему, получимъ $p_1 = q_1$ и т. д. Итакъ мы видимъ, что два разложенія $pp_1 p_2 \ldots$ и

$qq_1q_2\ldots$ должны состоять изъ однихъ и тѣхъ же множителей и могутъ отличаться только порядкомъ ихъ расположенія.

§ 19. Среди простыхъ дѣлителей составного числа въ его разложеніи на простые множители могутъ быть нѣсколько одинаковыхъ, а потому всякое составное число m можетъ быть представлено въ такомъ видѣ:

$$m = p^{l} p_1^{l_1} p_2^{l_2} \ldots p_n^{l_n},$$

гдѣ p, p_1, p_2, $\ldots$, p_n различныя простыя числа, входящія въ составъ числа m, а l, l_1, l_2, $\ldots$, l_n нѣкоторые цѣлые положительные ихъ показатели.

§ 20. Уже Эвклидомъ показано, что *рядъ простыхъ чиселъ:*

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots$$

продолженный неопредѣленно, не можетъ состоять изъ конечнаго числа чиселъ, т. е. другими словами, что *число простыхъ чиселъ безконечно велико.* Въ самомъ дѣлѣ, допустимъ обратное, что рядъ простыхъ чиселъ обрывается на нѣкоторомъ числѣ p; тогда число $N = (2 . 3 . 5 \ldots p) + 1$ должно было быть:

1) или простымъ,

2) или имѣть простого дѣлителя, превосходящаго p.

Обѣ эти возможности надо откинуть какъ противорѣчащія предположенію.

Доказанное Эвклидомъ предложеніе есть частный случай другого, болѣе общаго, а именно, что *во всякой ариѳметической прогрессіи, составленной изъ цѣлыхъ чиселъ вида $ax + b$, гдѣ a и b числа взаимно простыя, заключается безчисленное множество простыхъ чиселъ.*

Это предложеніе было доказано L. Dirichlet [1]).

Оказалось, что предложеніе, такъ просто доказываемое въ случаѣ $a = 1$, потребовало въ общемъ случаѣ приложенія соображеній интегральнаго исчисленія.

§ 21. Размотримъ задачу нахожденія всѣхъ дѣлителей числа

$$m = p^{l} p_1^{l_1} p_2^{l_2} \ldots p_n^{l_n}.$$

Не трудно видѣть, что дѣлителемъ числа m можетъ быть только число вида

$$p^{\lambda} p_1^{\lambda_1} p_2^{\lambda_2} \ldots p_n^{\lambda_n}$$

при условіи $0 \leqq \lambda \leqq l$, $0 \leqq \lambda_1 \leqq l_1$, $\ldots$, $0 \leqq \lambda_n \leqq l_n$.

---

[1]) См. Д. Граве. Ариѳметическая теорія алгебраическихъ величинъ. Томъ I. Квадратичная область, Стр. 219.

Если дѣлитель отличенъ отъ самого числа, то мы будемъ его называть *настоящимъ* дѣлителемъ.

Если мы разсмотримъ выраженія

$$P = 1 + p + p^2 + \ldots + p^{l}$$
$$P_1 = 1 + p_1 + p_1^2 + \ldots + p_1^{l_1}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$P_n = 1 + p_n + p_n^2 + \ldots + p_n^{l_n},$$

и если мы произведемъ перемноженіе членовъ въ произведеніи многочленовъ

$$PP_1P_2 \ldots P_n, \qquad (1)$$

то получится многочленъ, каждый изъ членовъ котораго будетъ дѣлителемъ числа m. Кромѣ того, всякій дѣлитель числа m встрѣтится одинъ разъ среди членовъ этого произведенія.

Слѣдовательно, произведеніе (1) представляетъ изъ себя не что иное, какъ сумму всѣхъ дѣлителей числа m.

Итакъ, мы видимъ, что сумма всѣхъ дѣлителей числа m выражается формулой

$$\frac{p^{l+1}-1}{p-1} \cdot \frac{p_1^{l_1+1}-1}{p_1-1} \cdot \ldots \cdot \frac{p_n^{l_n+1}-1}{p_n-1}.$$

Число всѣхъ дѣлителей числа m будетъ равняться, очевидно, числу всѣхъ членовъ въ произведеніи (1). Но такъ какъ

въ полиномѣ P число-членовъ есть $l+1$,

„ „ P_1 „ „ „ l_1+1,

. . . . . .

„ „ P_n „ „ „ l_n+1,

то число дѣлителей числа m выразится такъ:

$$(l+1)(l_1+1) \ldots (l_n+1).$$

§ 22. Для составленія таблицы простыхъ чиселъ до извѣстнаго предѣла былъ данъ еще Эратосѳеномъ (276—194 до Р. Х.) пріемъ, носящій до сихъ поръ названіе *Эратосѳенова рѣшета* и состоящій въ слѣдующемъ: выписываютъ до требуемаго предѣла всѣ по порядку натуральныя нечетныя числа и затѣмъ вычеркиваютъ кратныя числа 3, оставляя число 3; первымъ послѣ 3 невычеркнутымъ числомъ оказывается простое 5, вычеркива-

ютъ кратныя этого числа; послѣ числа 5 оказывается первымъ не вычеркнутымъ числомъ слѣдующее простое 7, вычеркиваютъ далѣе кратныя его и продолжаютъ описанный процессъ до тѣхъ поръ, пока не останутся исключительно числа простыя.

§ 23. Равносильную по трудности задачу представляетъ разложеніе чиселъ на простые множители. Для рѣшенія этой задачи приходится пробовать дѣлить заданное число A на всѣ по порядку простыя числа не превосходящія $\sqrt{A}$. Этотъ извѣстный уже съ древности пріемъ остается до сихъ поръ единственнымъ путемъ для рѣшенія задачи, причемъ приходится считать задачу разложенія очень большихъ чиселъ на простые множители задачей трудною.

Существенныя добавленія сдѣланы Euler'омъ [1]) и Чебышевымъ [2]), хотя эти добавленія относятся *не къ видоизмѣненію* метода, а лишь касаются уменьшенія числа пробъ дѣленій.

Для облегченія разложенія чиселъ на множители въ настоящее время имѣются очень большія таблицы дѣлителей. Основной принципъ построенія этихъ таблицъ состоитъ въ томъ, что для каждаго числа дается въ таблицѣ наименьшій простой его дѣлитель.

Таблица *Z. Chernac.* подъ названіемъ *Cribrum arithmeticum* Deventer 1811 идетъ до числа 1020000.

Для чиселъ первыхъ трехъ милліоновъ имѣется хорошая таблица *L. Ch. Burckhardt.* Tables des diviseurs pour tous les nombres des 1-e, 2-e, et 3-e million, ou plus exactement, depuis la 3036000 avec les nombres premiers qui s'y trouvent. Paris 1814—17.

Небольшое извлеченіе изъ этой таблицы (отъ 1 до 107999) я даю въ концѣ этой книги съ указаніемъ правила пользованія таблицей.

Таблица Burckhardt'a продолжена Glaisher'омъ для 4-го, 5-го и 6-го милліона и Dase для 7-го и 8-го.

§ 24. Старые математики пытались подвести законъ ряда простыхъ чиселъ подъ какую нибудь общую формулу. Такъ, напримѣръ, Euler далъ три формулы

$$x^2 + x + 17,$$

$$2x^2 + 29,$$

$$x^2 + x + 41,$$

которыя при подстановкѣ вмѣсто x натуральнаго ряда чиселъ 0, 1, 2, 3, ... даютъ большое число простыхъ чиселъ.

---

[1]) Euler. Commentationes Arithmeticae collectae. T. 1. p. 379. T. 2. p. 270.

[2]) Чебышевъ. Теорія сравненій. Глава VIII.

Но не трудно видѣть, что полиномъ съ цѣлыми коэффиціентами

$$a + bx + cx^2 + dx^3 + \ldots$$

не можетъ представлять постоянно (при всѣхъ цѣлыхъ значеніяхъ x) только простыя числа.

Въ самомъ дѣлѣ, пусть при нѣкоторомъ цѣломъ значеніи x_0 полиномъ даетъ простое число p, т. е.

$$p = a + bx_0 + cx_0^2 + dx_0^3 + \ldots$$

Очевидно, что при $x = x_0 + py$ будетъ получаться значеніе

$$a + bx_0 + cx_0 + dx_0^3 + \ldots + p.P = p(1 + P)$$

полинома, дѣлящееся на p, какое бы цѣлое значеніе ни принимала буква y, поэтому нашъ полиномъ не будетъ всегда давать простое число.

§ 25. Знаменитый математикъ Fermat (1601—1665) думалъ, что числа вида

$$2^{2^n} + 1 \qquad (1)$$

всегда простыя и, дѣйствительно, для первыхъ значеній $n = 0, 1, 2, 3, 4$ получаются простыя числа 2, 5, 17, 257, 65537.

Но уже Euler (1707—1783) показалъ, что при $n = 5$ формула (1) даетъ число дѣлящееся на 641.

Landry показалъ, что при $n = 6$ число будетъ дѣлиться на 274177. Извѣстный русскій математикъ священникъ отецъ Первушинъ нашелъ дѣлителей при $n = 12$ и $n = 23$, эти дѣлители суть

при $n = 12$	114689
при $n = 23$	167772161

Наконецъ, Lucas указываетъ дѣлителя 2748779069441 для случая $n = 36$.

§ 26. Можно думать, что числа вида

$$2 + 1.\ 2^2 + 1,\ 2^{2^2} + 1,\ 2^{2^{2^2}} + 1,\ 2^{2^{2^{2^2}}} + 1, \ldots$$

суть простыя.

Eisenstein высказалъ теорему, для которой быть можетъ онъ имѣлъ доказательство:

Существуетъ безчисленное множество простыхъ чиселъ вида

$$2^{2^n} + 1.$$

До сихъ поръ не найдено доказательствъ этихъ двухъ предложеній.

Вообще говоря, самъ законъ распредѣленія простыхъ чиселъ, законъ ихъ слѣдованія другъ за другомъ представляетъ рядъ задачъ громадной трудности не рѣшенныхъ до настоящаго времени.

Русская наука можетъ гордиться замѣчательнымъ изслѣдованіемъ Чебышева о простыхъ числахъ. Эти изслѣдованія были продолжены геніальнымъ нѣмецкимъ математикомъ Riemann'омъ.

E. Landau, профессоръ университета въ Гёттингенѣ, лучшій знатокъ аналитической теоріи чиселъ, написалъ о простыхъ числахъ большое (два тома) сочиненіе подъ заглавіемъ: Handbuch der Lehre von der Verteilung der Primzahlen 1909. Всякій желающій познакомиться съ современнымъ положеніемъ вопросовъ о простыхъ числахъ найдетъ въ книгѣ Landau прекрасное руководство.

Въ блестящей рѣчи, произнесенной на общемъ собраніи 23 Августа 1912 Международнаго Конгресса Математиковъ въ Cambridge'ѣ, профессоръ Landau подчеркнулъ рядъ вопросовъ о простыхъ числахъ, представляющихъ до сихъ поръ непреодолимыя трудности:

1. Представляетъ ли функція n^2+1 при цѣлыхъ значеніяхъ n безчисленное число простыхъ чиселъ?

2. Имѣетъ ли уравненіе $m=p+p'$ для всякаго четнаго $m>2$ рѣшеніе въ простыхъ числахъ p и p'?

3 Имѣетъ ли уравненіе $2=p-p'$ безчисленное число рѣшеній въ простыхъ числахъ?

4. Лежитъ ли между n^2 и $(n+1)^2$ при всякомъ цѣломъ n по крайней мѣрѣ одно простое число?

§ 27. Обращаясь къ вопросу о дѣлителяхъ чиселъ, мы должны упомянуть о нѣкоторыхъ вопросахъ теоріи чиселъ, которые нѣкогда играли большую ролъ и занимали вниманіе самыхъ выдающихся математиковъ. Въ настоящее время эти вопросы считаются устарѣвшими и ими мало интересуются.

Такая перемѣна отношенія ученыхъ къ объекту изученія объясняется желаніемъ рѣшать задачи „важныя и необходимыя“ для движенія науки впередъ.

Одного обстоятельства, что данный вопросъ „интересенъ и любопытенъ“ еще не достаточно, чтобы на него обратили вниманіе серьезные ученые.

Къ числу такихъ устарѣвшихъ задачъ принадлежитъ задача нахожденія чиселъ *совершенныхъ* (numeri perfecti) и *дружественныхъ* (numeri amicabiles).

§ 28. Совершеннымъ называется число, сумма *настоящихъ* дѣлителей котораго равна этому числу.

Если мы будемъ разсматривать сумму $\sigma(n)$ *всѣхъ* дѣлителей числа n, то совершенное число опредѣлится равенствомъ

$$\sigma(n) = 2n \tag{1}$$

Такими совершенными числами являются напр.

$$6,\ 28,\ 496,\ 8128,\ \ldots \tag{2}$$

Въ самомъ дѣлѣ,

$$6 = 1 + 2 + 3\ ;\ 28 = 1 + 2 + 4 + 7 + 14\ ;\ \ldots$$

До сихъ поръ не извѣстно ни одного нечетнаго совершеннаго числа.

Эвклидъ далъ единственную извѣстную методу для нахожденія чиселъ совершенныхъ.

Разсмотримъ числа вида

$$n = 2^{\alpha}p\,, \tag{3}$$

гдѣ p число простое, тогда сумма дѣлителей будетъ

$$\sigma(n) = (2^{\alpha+1} - 1)\ (p + 1)$$

Уравненіе (1) даетъ

$$(2^{\alpha+1} - 1)(p + 1) = 2^{\alpha+1}p$$

Откуда

$$p = 2^{\alpha+1} - 1 \tag{4}$$

Итакъ, совершенныя числа получаются по формулѣ (3) и (4) при такихъ значеніяхъ α, которыя обращаютъ выраженіе $2^{\alpha+1} - 1$ въ простое число.

Очевидно, что число $\alpha+1$ должно быть простымъ, ибо, если $\alpha+1=q^r$, то выраженіе $2^{q^r} - 1$ очевидно дѣлится на $2^q - 1$. Это условіе, будучи необходимымъ, однако не достаточно, ибо $2^{11} - 1 = 23 \cdot 89$.

Полагая $\alpha + 1 = 2,\ 3,\ 5,\ 7$ получаемъ совершенныя числа, указанныя въ рядѣ (2).

§ 29. *Не существуетъ другихъ четныхъ совершенныхъ чиселъ кромѣ получаемыхъ по методѣ Эвклида.*

Въ самомъ дѣлѣ, пусть четное совершенное число n имѣетъ видъ $n = 2^{\lambda}p^{\mu}q^{k} \ldots$

Тогда по опредѣленію совершеннаго числа имѣемъ

$$2^{\lambda+1}p^{\mu}q^{k} \ldots = (2^{\lambda+1} - 1)\frac{p^{\mu+1} - 1}{p - 1} \cdot \frac{q^{k+1} - 1}{q - 1} \ldots$$

или иначе

$$p^\mu q^k \ldots + \frac{p^\mu q^k \ldots}{2^{\lambda+1}-1} = (1 + p + \ldots p^\mu)(1 + q + q^2 + \ldots + q^k) \ldots \quad (1)$$

Мы замѣчаемъ прежде всего, что число $\frac{p^\mu q^k}{2^{\lambda+1}-1}$ должно быть цѣлымъ и должно имѣть видъ $p^{\mu'} q^{k'} \ldots$ Равенство (1) невозможно, если послѣ раскрытія скобокъ во второй части будетъ болѣе двухъ членовъ. Значитъ задача возможна только въ случаѣ $2 = (\mu + 1)(k + 1) \ldots$ или $\mu = 1$, $k = 0, \ldots$ то есть $n = 2^\lambda p$.

Резюмируя сказанное мы замѣчаемъ, что совершенныя числа, до сихъ поръ извѣстныя, получаются по формулѣ $2^{p-1}(2^p - 1)$ при простыхъ значеніяхъ $p : 2, 3, 5, 7, 13, 17, 19, 31, 61, \ldots$

§ 20. Числа называются дружественными (n. amicabiles), если сумма *настоящихъ* дѣлителей каждаго изъ нихъ равна другому. Два такихъ числа m и n опредѣляются уравненіемъ $\sigma(m) = \sigma(n) = m + n$.

Таковыми числами являются слѣдующія пары чиселъ

$$284 = 2^2 . 71 \qquad 220 = 2^2 . 5 . 11$$

$$18416 = 2^4 . 1151 \qquad 17296 = 2^4 23 . 47 .$$

Euler далъ таблицу 61 пары дружественныхъ чиселъ.

§ 31. Мы упомянемъ здѣсь еще объ одномъ старомъ вопросѣ, о такъ называемыхъ *фигурныхъ* числахъ.

Разсмотримъ рядъ ариѳметическихъ прогрессій, начинающихся съ 1 и разности которыхъ суть числа натуральнаго ряда $1, 2, 3, 4, \ldots$

$$1, 2, 3, 4, \ldots n, \ldots$$

$$1, 3, 5, 7, \ldots 2n-1, \ldots$$

$$1, 4, 7, 10, \ldots 3n-2, \ldots$$

$$1, 5, 9, 13, \ldots 4n-3, \ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

Суммы n первыхъ членовъ этихъ прогрессій представляютъ изъ себя такъ называемыя: *треугольныя, квадратныя, пятиугольныя, шестиугольныя* ... числа порядка n.

Итакъ, q-угольное число порядка n есть не что иное какъ сумма n первыхъ членовъ ариѳметической прогрессіи съ разностью $q - 2$, а именно

$$1 + [1 + (q-2)] + [1 + 2(q-2)] + \ldots + [1 + (n-1)(q-2)] .$$

Если мы обозначимъ это число черезъ $P_n^{(q)}$, то мы получимъ

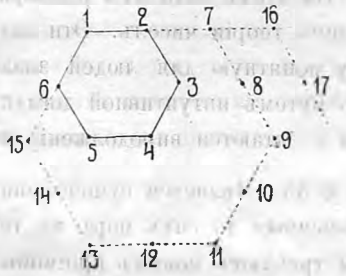
$$P_n^{(q)} = n + (q-2)\frac{n(n-1)}{2}.$$

Названіе такихъ многоугольныхъ чиселъ происходитъ отъ нѣкотораго геометрическаго построенія, которое пояснимъ на числахъ шестиугольныхъ

$$P_n^{(6)} = n + 2(n^2 - n) = 2n^2 - n$$

$$P_1^{(6)} = 1\,,\ P_2^{(6)} = 6\,,\ P_3^{(6)} = 15\,,\ P_4^{(6)} = 28\,.$$

Строимъ рядъ шестиугольниковъ подобныхъ и подобно расположенныхъ съ центромъ подобія въ вершинѣ одного изъ нихъ (общей для всѣхъ ихъ) при чемъ длина стороны возрастаетъ въ ариѳметической прогрессіи. Если мы на этихъ шестиугольникахъ расположимъ натуральныя числа въ указанномъ порядкѣ, то по одной сторонѣ общей всѣмъ шестиугольникамъ получимъ шестиугольныя числа. Подобные же чертежи относятся къ многоугольникамъ съ другимъ числомъ сторонъ.



§ 32. Фигурныя числа получили особенное значеніе послѣ теоремы, высказанной безъ доказательства Fermat'омъ.

Теорема. Всякое натуральное число есть сумма трехъ треугольныхъ, четырехъ квадратныхъ, пяти пятиугольныхъ, шести шестиугольныхъ и т. д.

Въ продолженіи двухъ столѣтій несмотря на усилія самыхъ выдающихся математиковъ теорема не была доказана въ общемъ ея видѣ и только въ 19-мъ столѣтіи Cauchy доказалъ ее, видоизмѣнивъ ея формулировку.

§ 33. Waring[1]) высказалъ предположеніе, которое можно разсматривать до нѣкоторой степени какъ обобщеніе приведенной выше теоремы Fermat. Это предположеніе относится къ представленію натуральнаго числа въ видѣ суммы одинаковыхъ степеней другихъ чиселъ, т. е. къ представ-

[1]) Meditationes arithmeticae ed. 3. Cambridge 1782. p. 340—350.

ленію числа n въ видѣ

$$n = a^p + b^p + c^p + \ldots \qquad (1)$$

Waring утверждалъ, что для каждаго числа p существуетъ минимальное число N_p членовъ второй части уравненія (1), причемъ всякое число n распадается на N_p p-ыхъ степеней и не всякое можетъ быть представлено въ видѣ суммы p-хъ степеней съ меньшимъ чѣмъ N_p числомъ членовъ.

Лишь въ послѣднее время удалось Hilbert'у доказать [1]) теорему Waring'a.

§ 34. Излагая основныя свойства дѣлимости чиселъ, я обратилъ вниманіе читателя на знаменитыя въ исторіи теоріи чиселъ задачи.

На этихъ задачахъ рельефно выступаетъ общій характеръ вопросовъ и задачъ теоріи чиселъ. Эти задачи допускаютъ элементарную формулировку понятную для людей знающихъ только ариѳметику, и полученныя часто путемъ интуитивной догадки онѣ представляютъ громадныя затрудненія и остаются впродолженіе вѣковъ нерѣшенными.

§ 35. Является существеннымъ вопросъ: дѣйствительно ли задачи, нерѣшенныя до сихъ поръ въ теоріи чиселъ, не имѣютъ простого рѣшенія и требуютъ новыхъ пріемовъ и методовъ изслѣдованія, или же рѣшеніе этихъ задачъ не трудно, но случайно ускользаетъ отъ догадокъ ученыхъ.

Бывали случаи, что, дѣйствительно, совершенно элементарныя соображенія долго не были замѣчены математиками. Одинъ изъ такихъ примѣровъ въ исторіи математики я приведу. Послѣдователи Fermat'a разсматривали разложеніе на множители чиселъ вида $2^n \pm 1$. Landry далъ таблицу разложеній до $n \leqslant 64$, причемъ прибавляетъ, что наибольшее затрудненіе представляло разложеніе

$$2^{58} + 1 = 5 \cdot 107367629 \cdot 536903681 . \qquad (1)$$

Потомъ оказалось, какъ показалъ одинъ изъ мало извѣстныхъ математиковъ Aurifeuille, что формула (1) непосредственно слѣдуетъ изъ тождества

$$2^{4n+2} + 1 = \left(2^{2n+1} + 2^{n+1} + 1\right)\left(2^{2n+1} - 2^{n+1} + 1\right) \text{ при } n = 14 .$$

Примѣры, подобные указанному однако настолько малочисленны, что приходится держаться мнѣнія обратнаго, а именно, что, если задача прошла нерѣшенною черезъ усилія наиболѣе талантливыхъ математиковъ, то мало надежды на простое ея рѣшеніе.

---

[1]) Nachrichten der Gött. Ges. d. W. 6. 2. 1909.

Попытки искать новые пріемы рѣшенія трудныхъ задачъ приводили обыкновенно къ важнымъ научнымъ открытіямъ.

Такъ было дѣло съ доказательствомъ теоремы Fermat'a, получившей названіе *„великой теоремы Fermat'a"*. Эта теорема состоитъ въ слѣдующемъ.

Уравненіе $x^n + y^n = z^n$ *не можетъ быть удовлетворено ни при какихъ цѣлыхъ значеніяхъ* x, y, z, *если цѣлое число* n *больше* 2.

Эту теорему Fermat сообщилъ на полѣ принадлежавшаго ему сочиненія Діофанта, причемъ Fermat присовокупляетъ:

„Я нашелъ замѣчательное доказательство этого предложенія, но поле книги слишкомъ узко, чтобы его написать".

Съ тѣхъ поръ въ продолженіе почти трехсотъ лѣтъ эта задача не рѣшена, несмотря на то, что едва ли найдется кромѣ квадратуры круга другая задача, которая привлекала бы большее вниманіе математиковъ. Теорема Fermat'a раздѣлила участь квадратуры круга также по громадному числу ошибочныхъ доказательствъ, данныхъ различными авторами.

Несмотря на это, очень многое уже сдѣлано для доказательства теоремы Fermat'a.

Euler доказалъ теорему для $n = 3$ и 4. Для $n = 5$ было дано доказательство Dirichlet и Legendre'омъ въ 1825—1827 годахъ. Въ 1837 году Lamé доказалъ теорему для $n = 7$.

Особенно замѣчательны изслѣдованія по этой задачѣ знаменитаго нѣмецкаго математика Kummer'a, который посвятилъ ей большую часть своей жизни. Сначала Kummer'у показалось, что онъ рѣшилъ задачу вполнѣ, затѣмъ онъ замѣтилъ въ своемъ доказательствѣ слабый пунктъ. Желая освободить доказательство отъ замѣченныхъ имъ недостатковъ, Kummer пришелъ къ научному открытію первостепенной важности. Онъ ввелъ въ науку новое понятіе, которое онъ назвалъ *идеальнымъ числомъ*. При помощи идеальныхъ чиселъ, онъ сдѣлалъ свое доказательство вполнѣ строгимъ, но зато, къ сожалѣнію, его новое доказательство оказалось пригоднымъ не для всѣхъ цѣлыхъ значеній показателя n. Во всякомъ случаѣ для всѣхъ значеній показателя до 100 теорема доказывается по Kummer'у вполнѣ строго.

§ 35. Итакъ, на примѣрѣ задачи Fermat'a мы видимъ, что движеніе впередъ теоріи чиселъ не можетъ быть совершено элементарными пріемами. Изслѣдователь долженъ быть во всеоружіи созданныхъ его предшественниками общихъ теорій и методъ. Въ виду этого я ставлю цѣлью книги изложеніе тѣхъ общаго характера методъ, которыя сдѣлались классическими и которыя составляютъ азбуку теоріи чиселъ.

ГЛАВА II.

Элементарныя свѣдѣнія изъ аналитической теоріи чиселъ.

§ 1. Въ теоріи чиселъ мы будемъ разсматривать понятіе о *функціи*, проходящее черезъ всю математику. Скажемъ нѣсколько словъ объ этомъ понятіи.

Въ основу мы кладемъ понятіе о *числовомъ множествѣ* или *ансамблѣ*.

Числовымъ ансамблемъ называется такимъ образомъ указанная совокупность чиселъ S, что относительно каждаго числа можно будетъ сказать, принадлежитъ оно къ совокупности или нѣтъ.

Здѣсь мы беремъ общее понятіе о числѣ, данное въ элементарной алгебрѣ, т. е. разсматриваемъ всѣ возможныя какъ вещественныя, такъ и мнимыя числа.

§ 2. Если мы одно изъ чиселъ ансамбля S, *не указывая которое именно*, обозначимъ одной буквой x, то эта буква выразитъ такъ называемую *перемѣнную величину, пробѣгающую данный ансамбль*.

§ 3. Если мы напишемъ $x = a$, гдѣ a есть одно изъ чиселъ ансамбля S, то мы говоримъ, что *перемѣнная приняла частное значеніе* a.

§ 4. Обыкновенно устанавливается нѣкоторый *процессъ измѣненія перемѣнной величины* тѣмъ что указывается, какія значенія перемѣнная принимаетъ раньше и какія позже.

Къ числу такихъ процессовъ измѣненія отмѣтимъ, напримѣръ, *возрастаніе* и *убываніе* перемѣнной.

§ 5. Измѣненіе вещественной перемѣнной x носитъ названіе *непрерывнаго*, если она, принимая два значенія a и b, проходитъ черезъ всѣ промежуточныя значенія.

Если перемѣнная x принимаетъ комплексныя значенія, то непрерывное ея измѣненіе можно геометрически интерпретировать, какъ непрерывное движеніе точки по плоскости.

§ 6. Разсмотрѣніе непрерывныхъ перемѣнныхъ привело къ *анализу безконечно малыхъ*, имѣющему громадныя приложенія въ натуральной философіи.

§ 7. Если двѣ перемѣнныя x и y, пробѣгающія ансамбли S и Σ, таковы, что указаны правила соотвѣтствія частныхъ значеній. ими принимаемыхъ, причемъ, если одна перемѣнная x принимаетъ нѣкоторое произвольно выбранное значеніе изъ ансамбля S, то другая y приметъ уже вполнѣ опредѣленное *соотвѣтственное* значеніе изъ ансамбля Σ; тогда перемѣнную y называютъ *зависимою перемѣнною*, или *функціею* отъ x, которая носитъ названіе *перемѣнной независимой*.

То обстоятельство, что y есть функція отъ x обозначается знакомъ $y = f(x)$ (первая буква слова functio).

Очевидно, что всякая формула, заключающая x, есть всегда нѣкоторая функція отъ x, напримѣръ

$$y = x^2 + x - 3, \quad y = lg\, x, \quad y = \sqrt[3]{x^2 - 1}.$$

Для обозначенія различныхъ функцій можно брать или различныя буквы, или одну и ту же букву снабжать различными значками

$$f_1(x), \; f_2(x), \; f''(x), \; \psi(x), \; F(x), \; \ldots$$

§ 8. Понятіе о функціи одной перемѣнной независимой обобщается на случай многихъ перемѣнныхъ независимыхъ. Такъ, напримѣръ, величина V, опредѣляемая формулой

$$V = \frac{x^2 - y^2}{sin\, z + t}$$

принимаетъ опредѣленное значеніе, когда величины x, y, z, t принимаютъ опредѣленныя значенія.

Величина V будетъ функціей отъ четырехъ перемѣнныхъ независимыхъ x, y, z, t.

§ 9. Часто принято было говорить, что теорія чиселъ характеризуется употребленіемъ *прерывныхъ* перемѣнныхъ и функцій, т. е. такихъ, которыя отступаютъ отъ основного свойства непрерывнаго измѣненія.

Извѣстный русскій математикъ и философъ Бугаевъ любилъ теорію чиселъ, которую онъ называлъ *аримологіей*, противопоставлять анализу безконечно малыхъ и видѣлъ ея главное отличіе въ прерывности разсматриваемыхъ величинъ.

Но современная наука враждебна какимъ либо предвзятымъ симпатіямъ или антипатіямъ. Она старается для достиженія своихъ цѣлей брать все хорошее и удобное, гдѣ бы оно ни находилось, а потому въ настоящее время обнаруживается въ теоріи чиселъ сильное теченіе въ пользу сближенія съ анализомъ безконечно малыхъ.

Образовалась цѣлая наука, которой даютъ названіе *аналитической теоріи чиселъ*, въ которой на каждомъ шагу примѣняются соображенія интегральнаго исчисленія, теоріи рядовъ, теоріи функцій комплекснаго перемѣннаго.

Не надо думать, что аналитическая теорія чиселъ является особеннымъ отдѣломъ теоріи чиселъ.

Сближеніе теоріи чиселъ съ другими частями алгебраическаго и трансцендентнаго анализа все болѣе и болѣе разростается въ грандіозное цѣлое, которому лучше всего дать названіе *чистой математики* въ отличіе отъ математики, имѣющей цѣлью приложенія въ техникѣ и натуральной философіи.

§ 10. Въ этомъ курсѣ я ограничусь очень незначительными свѣдѣніями по аналитической теоріи чиселъ, лишь тѣми свѣдѣніями, которыя имѣютъ большое значеніе для самого курса.

Функція [x].

§ 11. Мы разсмотримъ функцію вещественнаго перемѣннаго x, которая представляетъ изъ себя не что иное, какъ *цѣлую часть вещественнаго числа* x или, иначе сказать, *наибольшее цѣлое число не превосходящее* x.

Для обозначенія этой функціи былъ введенъ Legendre'омъ знакъ *Ex* отъ слова Entier (цѣлая часть).

Мы возьмемъ болѣе употребительное нынче обозначеніе Gauss'a $[x]$.

По опредѣленію функціи мы имѣемъ, напримѣръ,

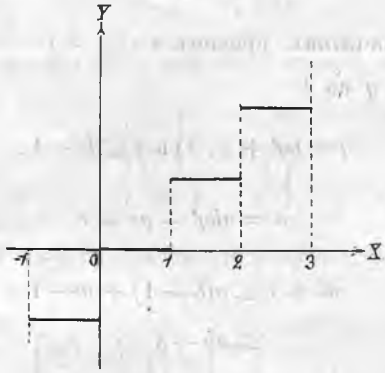
$$[2] = 2\,,\ \left[\frac{17}{3}\right] = 5\,,\ [\sqrt{14}] = 3\,,\ [\sin\pi] = -1\,,\ \left[-\frac{3}{2}\right] = -2\,.$$

§ 12. Не трудно видѣть, что если мы будемъ изображать въ видѣ линіи на плоскости двухъ координатъ x и y уравненіе

$$y = [x]\,,$$

то получимъ не непрерывную линію, а линію прерывную, состоящую изъ

горизонтальныхъ прямолинейныхъ кусковъ длины равной единицѣ и расположенныхъ подобно ступенямъ лѣстницы.



§ 13. По опредѣленію функціи мы имѣемъ неравенства

$$[x] \leqq x < [x] + 1$$

или

$$x - 1 < [x] \leqq x .$$

§ 14. Если $x = y + z + \ldots + t$

то

$$[x] \geqslant [y] + [z] + \ldots + [t] , \qquad (1)$$

ибо

$$y = [y] + y_0 , \; z = [z] + z_0 , \; \ldots \; t = [t] + t_0 , \qquad (2)$$

гдѣ y_0, z_0, $\ldots$ t_0 суть правильныя дроби или нули.

Изъ равенствъ (2) получаемъ

$$x = [y] + [z] + \ldots + [t] + (y_0 + z_0 + \ldots + t_0) ,$$

откуда слѣдуетъ непосредственно неравенство (1).

§ 15. Докажемъ для всякихъ трехъ натуральныхъ чиселъ n, a, b справедливость равенства

$$\left[\frac{n}{ab}\right] = \left[\frac{\left[\frac{n}{a}\right]}{b}\right] = \left[\frac{\left[\frac{n}{b}\right]}{a}\right] .$$

Докажемъ равенство

$$\left[\frac{n}{ab}\right] = \left[\frac{\left[\frac{n}{a}\right]}{b}\right] ,$$

ибо другое будетъ слѣдовать изъ того же доказательства.

Дѣлимъ n на a

$$n = aq + r, \tag{1}$$

гдѣ q частное, а r остатокъ, причемъ $r \leqq a - 1$.

Дѣлимъ далѣе q на b

$$q = bq' + s, \text{ гдѣ } s \leqq b - 1. \tag{2}$$

Получаемъ

$$n = abq' + as + r \tag{3}$$

но

$$\begin{aligned} as + r &\leqq a(b-1) + a - 1 \\ &\leqq ab - 1 \\ &< ab. \end{aligned}$$

Итакъ, на основаніи (3) имѣемъ

$$q' = \left[\frac{n}{ab}\right],$$

но на основаніи (1) и (2)

$$q' = \left[\frac{q}{b}\right] = \left[\frac{\left[\frac{n}{a}\right]}{b}\right],$$

что и требовалось доказать.

§ 16. Обращаемся теперь къ задачѣ *найти, съ какимъ показателемъ входитъ данное простое число p множителемъ въ факторіальное произведеніе*

$$n! = 1 \cdot 2 \cdot 3 \cdot 4 \ldots n;$$

Очевидно, что всѣ множители этого произведенія, которые суть кратные числа p, будутъ имѣть видъ

$$p,\ 2p,\ 3p,\ \ldots\ \left[\frac{n}{p}\right] p.$$

Число этихъ чиселъ есть

$$\left[\frac{n}{p}\right].$$

Итакъ, въ произведеніе $n!$ входитъ степень

$$p^{\left[\frac{n}{p}\right]}$$

и кромѣ того еще такая степень, которая входитъ въ факторіалъ

$$1 . 2 . 3 \ldots \left[\frac{n}{p}\right].$$

Повторяя разсужденія получимъ еще степень съ показателемъ

$$\left[\frac{\left[\frac{n}{p}\right]}{p}\right] = \left[\frac{n}{p^2}\right]$$

и т. д., то есть окончательно показатель степени, съ которою число p входитъ въ факторіалъ $n!$ будетъ

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots \qquad (1)$$

Особенно просто получается показатель (1) если написать число p по системѣ счисленія при основаніи p (p-адическимъ числомъ по терминологіи профессора Hensel'a)

$$n = a + bp + cp^2 + dp^3 + \ldots$$

Нетрудно видѣть, что число (1) равно

$$\frac{n - (a + b + c + \ldots)}{p - 1}.$$

Отсюда получаемъ какъ верхній предѣлъ показателя, съ которымъ p входитъ въ факторіалъ $n!$, число

$$\frac{n}{p - 1}.$$

§ 17. Извѣстна теорема о возвышеніи многочлена въ цѣлую положительную степень, выражающаяся формулой

$$(a + b + c + \ldots + l)^n = \sum \frac{n!}{\alpha!\beta!\ldots\lambda!} a^\alpha b^\beta c^\gamma \ldots l^\lambda,$$

гдѣ сумма показателей въ каждомъ членѣ равна n, причемъ сумма распространяется на всѣ цѣлыя и равныя нулю значенія $\alpha, \beta, \gamma, \ldots \lambda$, удовлетворяющія равенству

$$n = \alpha + \beta + \gamma + \ldots + \lambda.$$

Очевидно, что выраженіе

$$\frac{n!}{\alpha!\,\beta!\,\gamma!\,\ldots\,\lambda!}$$

какъ коэффиціентъ полинома возвышеннаго въ цѣлую ножительную степень есть цѣлою число.

Посмотримъ, нельзя ли убѣдиться, что формула (1) даетъ цѣлое число, независимо отъ того откуда эта формула получена.

Мы имѣемъ равенство

$$\frac{n}{p^k} = \frac{\alpha}{p^k} + \frac{\beta}{p^k} + \frac{\gamma}{p^k} + \ldots \qquad (1')$$

Прилагая неравенство § 14, получимъ

$$\left[\frac{n}{p^k}\right] \geqslant \left[\frac{\alpha}{p^k}\right] + \left[\frac{\beta}{p^k}\right] + \left[\frac{\gamma}{p^k}\right] + \ldots$$

Суммируя по значку $k = 1, 2, 3, \ldots$, получимъ

$$\sum\left[\frac{n}{p^k}\right] \geqslant \sum\left[\frac{\alpha}{p^k}\right] + \sum\left[\frac{\beta}{p^k}\right] + \sum\left[\frac{\gamma}{p^k}\right] + \ldots$$

Но лѣвая часть этого неравенства даетъ показателя, съ которымъ простое число p входитъ въ числителя выраженія (1), а правая часть указываетъ показателя знаменателя.

Слѣдовательно показатель числителя не менѣе показателя знаменателя и теорема относительно цѣлости выраженія (1) доказана.

§ 18. Докажемъ теперь одну формулу, которая была исходной точкой изслѣдованій Чебышева о простыхъ числахъ.

На основаніи § 16 получаемъ

$$1.2.3\ldots n = \Pi p^{\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots}$$

гдѣ произведеніе Π распространяется на всѣ простыя числа, не превосходящія числа n. Прологариѳмировавъ, получаемъ

$$lg\,(1.2.3\ldots n) = \sum\left[\frac{n}{p}\right] lg\,p + \sum\left[\frac{n}{p^2}\right] lg\,p + \ldots$$

Введемъ въ разсмотрѣніе функцію $\theta(x)$, выражающую сумму логариѳмовъ всѣхъ простыхъ чиселъ не превосходящихъ x. Покажемъ спра-

ведливость слѣдующаго равенства

$$\vartheta(n)+\vartheta\left(\frac{n}{2}\right)+\vartheta\left(\frac{n}{3}\right)+\ldots=\sum\left[\frac{n}{p}\right]lg\,p, \qquad (1)$$

гдѣ въ первой части пишутся функціи ϑ до тѣхъ поръ, пока перестаютъ существовать простыя числа, меньшія аргумента функціи; во второй же части сумма распространяется на всѣ простыя числа, не превосходящія n.

Въ самомъ дѣлѣ, разсмотримъ какое нибудь простое число p. Его логариѳмъ будетъ входить во всѣ первыя функціи

$$\vartheta(n),\ \vartheta\left(\frac{n}{2}\right),\ \vartheta\left(\frac{n}{3}\right),\ \ldots$$

до тѣхъ поръ, пока въ рядѣ чиселъ n, $\frac{n}{2}$, $\frac{n}{3}$, ... не появятся меньшія p.

Пусть при нѣкоторомъ числѣ k произойдутъ неравенства

$$\frac{n}{k}\geqslant p>\frac{n}{k+1}, \qquad (2)$$

тогда $lg\,p$ войдетъ въ первую часть k разъ слагаемымъ. Неравенства (2) можно преобразовать такъ:

$$k\leqslant\frac{n}{p}<k+1,$$

т. е. получаемъ

$$k=\left[\frac{n}{p}\right].$$

Итакъ, мы видимъ, что въ первой части равенства (1) логариѳмъ всякаго простого числа p входитъ со множителемъ k, слѣдовательно, равенство (1) справедливо.

Подобнымъ же образомъ покажемъ

$$\vartheta(\sqrt{n})+\vartheta\left(\sqrt{\frac{n}{2}}\right)+\vartheta\left(\sqrt{\frac{n}{3}}\right)+\ldots=\sum\left[\frac{n}{p^2}\right]lg\,p$$

$$\vartheta(\sqrt[3]{n})+\vartheta\left(\sqrt[3]{\frac{n}{2}}\right)+\vartheta\left(\sqrt[3]{\frac{n}{3}}\right)+\ldots=\sum\left[\frac{n}{p^3}\right]lg\,p \qquad (3)$$

. . . . . .

Суммируя равенства (2) и (3), получимъ окончательно формулу

$$lg\,(1\,.\,2\,.\,3\,\ldots\,n) = \theta\,(n) + \theta\left(\frac{n}{2}\right) + \theta\left(\frac{n}{3}\right) + \ldots$$

$$+ \theta\,(\sqrt{n}) + \theta\left(\sqrt{\frac{n}{2}}\right) + \theta\left(\sqrt{\frac{n}{3}}\right) + \ldots$$

$$+ \theta\,(\sqrt[3]{n}) + \theta\left(\sqrt[3]{\frac{n}{2}}\right) + \theta\left(\sqrt[3]{\frac{n}{3}}\right) + \ldots$$

. . . . . .

§ 19. Закончимъ изложеніе свойствъ функціи $[x]$ указаніемъ на одну формулу, имѣющую значеніе въ нѣкоторыхъ вопросахъ теоріи чиселъ.

Разсмотримъ функцію

$$y = f(x)\,, \qquad (1)$$

которую мы для простоты будемъ предполагать обладающею слѣдующими свойствами:

1) она однозначна для всѣхъ значеній въ промежуткѣ $x = 0$, $x = b$,
2) непрерывна во всемъ промежуткѣ,
3) все время возрастаетъ,
4) при $x = 0$; $y = f(0) = 0$.

Пусть требуется вычислить сумму

$$[f(1)] + [f(2)] + [f(3)] + \ldots + [f(b)]\,. \qquad (2)$$

Обозначимъ функцію обратную черезъ $F(x)$, такъ что будетъ

$$x = F(y)\,.$$

Оказывается возможнымъ такъ преобразовать сумму (2), чтобы въ нее входили цѣлыя значенія обратной функціи, то есть величины

$$[F(y)]\,.$$

Для этой цѣли разсмотримъ, сколько членовъ въ рядѣ (2) равны числу

$$\nu = [f(n)]\,.$$

Сначала найдемъ число m членовъ суммы (2) меньшихъ ν.

Должны буемъ написать неравенства

$$[f(m)] < \nu \leqq [f(m+1)]\,.$$

Отсюда

$$f(m) < \nu \leqq f(m+1)$$

Взявъ отъ всѣхъ трехъ частей неравенства функцію $F(x)$, которая также возрастающая, получимъ

$$F(f(m)) < F(\nu) \leqq F(f(m+1))$$

или иначе

$$m < F(\nu) \leqq m+1 .$$

Отсюда получаемъ одно изъ двухъ

или I., $m = [F(\nu)]$

или II., $m = [F(\nu)] - 1 = F(\nu) - 1 .$

Случай II имѣетъ мѣсто, если $F(\nu) = [F(\nu)]$, то есть если на линіи

$$y = f(x)$$

лежитъ точка съ цѣлыми координатами $x = m+1$, $y = \nu$.

Разсмотримъ сначала случай, что на разсматриваемой кривой не существуетъ точекъ съ цѣлыми координатами. Тогда на всемъ протяженіи кривой $y = f(x)$ имѣетъ мѣсто случай I.

Мы получимъ число членовъ суммы (2) равныхъ ν, если изъ числа членовъ меньшихъ $\nu+1$ вычтемъ число членовъ меньшихъ ν. Отсюда получаемъ

$$S = \sum_{n=1}^{n=b} [f(x)] = \sum_{\nu=1}^{\nu=\beta} \nu \{[F(\nu+1)] - [F(\nu)]\} , \tag{3}$$

гдѣ $\beta = [f(b)]$.

Или написавъ подробнѣе

$$S = \beta \{b - [F(\beta)]\} + (\beta - 1)\{[F(\beta)] + [F(\beta-1)]\} + \ldots$$

$$\ldots + 2 . \{[F(3)] - [F(2)]\} + 1 . \{[F(2)] - [F(1)]\} ,$$

такъ что

$$S = \beta b - \sum_{\nu=1}^{\nu=\beta} [F(\nu)] , \tag{4}$$

Сопоставляя (3) и (4), получимъ окончательно

$$\sum_{n=1}^{n=b} [f(n)] + \sum_{\nu=1}^{\nu=\beta} [F(\nu)] = b\beta . \tag{5}$$

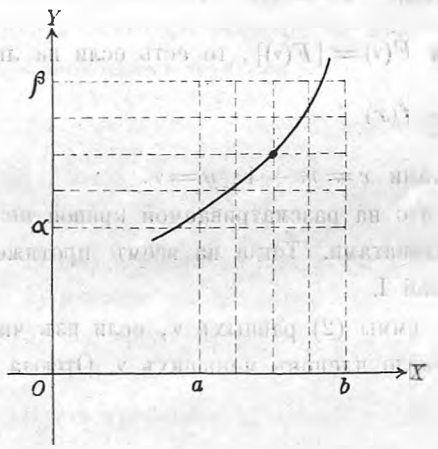
Для $a<b$ и $\alpha=[f(a)]$ будемъ имѣть

$$\sum_{n=1}^{n=a}[f(n)]+\sum_{\nu=1}^{\nu=\alpha}[F(\nu)]=a\alpha\,. \qquad (6)$$

Вычитая (6) изъ (5) получимъ

$$\sum_{n=a+1}^{n=b}[f(n)]+\sum_{\nu=\alpha+1}^{\nu=\beta}F[(\nu)]=b\beta-a\alpha\,. \qquad (7)$$

Послѣдняя формула находится въ полной аналогіи съ извѣстной формулой интегральнаго исчисленія



$$\int_a^b ydx+\int_\alpha^\beta xdy=b\beta-a\alpha \qquad (8)$$

гдѣ $\alpha=f(a)$, $\beta=f(b)$.

Въ формулѣ (7) приходится при вычисленіи суммъ первой части считать число точекъ съ цѣлыми координатами, лежащихъ въ двухъ площадяхъ, аналогичныхъ интеграламъ первой части равенства (8); поэтомумы могли бы получить формулу (7) непосредственно изъ геометрическихъ соображеній.

§ 20. При разсужденіяхъ предыдущаго параграфа мы предполагали, что на разсматриваемой дугѣ кривой $y=f(x)$ не существуетъ точекъ съ цѣлыми координатами. Если же такая точка появляется, то она даетъ лишнюю единицу, ибо её при геометрическомъ выводѣ формулы (7) § 19 придется принимать въ счетъ въ обѣихъ суммахъ

$$\int xdy \quad \text{и} \quad \int ydx\,,$$

откуда получается въ первой части (7) лишняя единица.

Въ этомъ легко убѣдиться изъ слѣдующихъ аналитическихъ соображеній, ибо, если точка съ координатами $(m+1\,,\nu)$ лежитъ на кривой, то придется принять въ разсчетъ случай II § 19, и тогда въ формулѣ

$$S=\Sigma\,\nu\,\{[F(\nu+1)]-[F(\nu)]\}\,.$$

придется вмѣсто $[F(\nu)]$ писать $[F'(\nu)]-1$ и мы будемъ имѣть

$$\ldots(\nu+1)\{[F(\nu+2)]-[F(\nu+1)]\}+\nu\{[F(\nu+1)]-[F'(\nu)]+1\}+$$
$$+(\nu-1)\{[F'(\nu)]-1-F(\nu-1)\}+\ldots$$

Произойдетъ измѣненіе относительно предыдущаго случая на число

$$\nu\cdot 1+(\nu-1)(-1)=1\,.$$

Итакъ, если на дугу между абсциссами a и b (включая вершину предѣла b) попадаютъ ζ точекъ съ цѣлыми координатами, то получаемъ формулу

$$\sum_{n=1}^{n=b}[f(n)]+\sum_{\nu=\alpha+1}^{\nu=\beta}[F(\nu)]=b\beta-a\alpha+\zeta\,.$$

Если мы будемъ называть *ариѳметическою нагрузкой* дуги число ζ лежащихъ на ней точекъ съ цѣлыми координатами, то послѣдняя формула даетъ для такой нагрузки опредѣленное вполнѣ аналитическое выраженіе. Эти соображенія обобщаются безъ труда на случай геометріи большаго числа измѣреній. Въ частности можно получить выраженіе ариѳметической нагрузки куска поверхности.

§ 21. Приложимъ выведенную въ предыдущемъ параграфѣ формулу къ весьма важному случаю [1]), когда линія разсматриваемая есть прямая

$$y=\frac{Q}{P}x\,;\;x=\frac{P}{Q}y\,,$$

а P и Q нечетныя взаимно простыя цѣлыя числа, причемъ $Q<P$.

Пусть $a=0$, $\alpha=0$, кромѣ того $b=\frac{P-1}{2}$, тогда должно быть

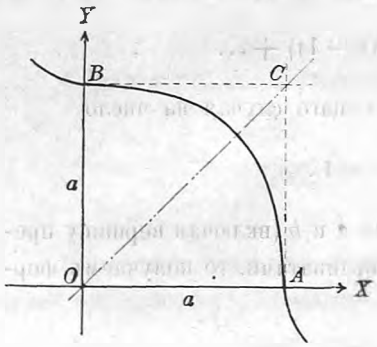
$$\beta=\left[\frac{Q}{P}b\right]=\left[\frac{Q(P-1)}{2P}\right]=\left[\frac{Q-1}{2}+\frac{P-Q}{2P}\right]=\frac{Q-1}{2}$$

и значитъ имѣемъ

$$\sum_{n=1}^{n=\frac{P-1}{2}}\left[\frac{Q}{P}n\right]+\sum_{\nu=1}^{\nu=\frac{Q-1}{2}}\left[\frac{P}{Q}\nu\right]=\frac{P-1}{2}\cdot\frac{Q-1}{2}\,.$$

[1]) *Eisenstein*, Journ. für r. u. ang. Math. 28. 1844, p. 246.

§ 22. Покажемъ еще примѣненіе приводимыхъ соображеній къ знаменитой теоремѣ Fermat'a.



Если будемъ разсматривать кривую линію, опредѣляемую уравненіемъ

$$x^p + y^p = a^p, \qquad (1)$$

гдѣ a нѣкоторое заданное цѣлое число, то доказательство невозможности уравненія (1) при $p > 2$ и при произвольномъ a сведется къ доказательству того, что равна нулю ариѳметическая нагрузка конечнаго куска AB кривой (1) заключеннаго между положительными направленіями осей координатъ, если при этомъ оба конца A и B исключаются изъ разсмотрѣнія.

Мы придемъ къ случаю разобранному нами, если возьмемъ за новое начало координатъ A.

Получаемъ формулу

$$\sum_{x=1}^{x=a-1}\left[a\sqrt[p]{1-\left(\frac{x}{a}\right)^p}\right]+\sum_{x=1}^{x=a-1}\left[a-a\sqrt[p]{1-\left(\frac{x}{a}\right)^p}\right]=(a-1)^2+\zeta,$$

гдѣ ζ искомая нагрузка

Вслѣдствіе симметричности кривой (1) относительно координатъ x и y число ζ не можетъ быть нечетнымъ и, слѣдовательно, наименьшее его значеніе отличное отъ нуля должно быть 2.

Итакъ, доказательство теоремы Fermat'a равносильно съ провѣркой справедливости неравенства

$$\sum_{x=1}^{x=a-1}\left\{\left[\sqrt[p]{a^p-x^p}\right]+\left[a-\sqrt[p]{a^p-x^p}\right]\right\}<(a-1)^2+2,$$

при всякомъ a.

О функціи $\varphi(n)$, выражающей число чиселъ меньшихъ n и взаимнопростыхъ съ n.

§ 23. Слѣдуя Euler'y мы будемъ обозначать число чиселъ меньшихъ n и взаимнопростыхъ съ n знакомъ $\varphi(n)$.

Такъ, напримѣръ, непосредственная провѣрка даетъ

Число n	Числа взаимно простыя съ n	Значеніе $\varphi(n)$
$n=2$	1	$\varphi(2)=1$
$n=3$	1, 2	$\varphi(3)=2$
$n=4$	1, 3	$\varphi(4)=2$
$n=5$	1, 2, 3, 4	$\varphi(5)=4$

и такъ далѣе.

Знакъ $\varphi(n)$ представляетъ замѣчательную по свойствамъ функцію. Эта функція принадлежитъ къ числу такъ называемыхъ *ариѳметическихъ* или *числовыхъ*, ибо она опредѣлена только для цѣлыхъ значеній аргумента n.

§ 24. *Теорема. Если d есть дѣлитель числа n, такъ что $n=d\delta$, то число чиселъ меньшихъ n и имѣющихъ съ n наибольшаго общаго дѣлителя d будетъ $\varphi(\delta)$.*

Въ самомъ дѣлѣ, пусть m число меньшее n и имѣетъ съ n общаго наибольшаго дѣлителя d; тогда $m=d.\varepsilon$, причемъ ε число взаимно простое съ δ. Кромѣ того $\varepsilon<\delta$, ибо по предположенію $m<n$. Итакъ, чиселъ m будетъ какъ разъ столько, сколько существуетъ чиселъ ε меньшихъ δ и взаимно простыхъ съ δ, т. е. $\varphi(\delta)$.

§ 25. Хотя знакъ $\varphi(1)$ не имѣетъ значенія самъ по себѣ, но серьезныя основанія заставляютъ поставить требованіе $\varphi(1)=1$, которое мы будемъ сохранять въ дальнѣйшемъ.

§ 26. *Теорема. Существуетъ равенство*

$$\sum\varphi(\delta)=n, \qquad (1)$$

гдѣ сумма распространена на всѣхъ дѣлителей δ числа n.

Для доказательства теоремы мы можемъ разсуждать такъ. Выпишемъ всѣхъ дѣлителей числа n, пусть они будутъ

$$1, d_1, d_2, \ldots d_k, n, \qquad (2)$$

пусть дополнительные дѣлители будутъ

$$n, \delta_1, \delta_2, \ldots \delta_k, 1 \quad (\delta_i d_i=n). \qquad (3)$$

Будемъ собирать числа не превосходящія n въ группы, причемъ въ каждую группу возьмемъ числа, имѣющія одного и того же общаго наибольшаго дѣлителя съ n. Обозначимъ знакомъ (d_i) группу чиселъ, имѣющихъ съ n общаго наибольшаго дѣлителя d_i.

Получимъ слѣдующій рядъ группъ

$$(1),\ (d_1),\ (d_2),\ \ldots\ (d_k),\ (n); \tag{4}$$

очевидно, на основаніи теоремы § 24, получаемъ въ группахъ (4) слѣдующія числа чиселъ

$$\varphi(n),\ \varphi(\delta_1),\ \varphi(\delta_2),\ \ldots\ \varphi(\delta_k),\ \varphi(1). \tag{5}$$

Такъ какъ всѣ числа $1, 2, 3, \ldots n$ попали по одному въ которую нибудь изъ группъ, то должно получиться

$$\varphi(n) + \varphi(\delta_1) + \varphi(\delta_2) + \ldots + \varphi(\delta_k) + \varphi(1) = n$$

и теорема доказана.

Если рядъ чиселъ (2) представляетъ дѣлителей числа n, расположенныхъ въ возрастающемъ порядкѣ, то рядъ дополнительныхъ дѣлителей (3) даетъ тѣ же числа, но въ обратномъ порядкѣ. Напримѣръ, $n = 12$

$$\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 12$$

ибо

$$1 + 1 + 2 + 2 + 2 + 4 = 12.$$

§ 27. *Теорема. Если a и b два взаимно простыхъ числа, то имѣетъ мѣсто равенство*

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Справедливость этой теоремы провѣряется непосредственно для всѣхъ малыхъ чиселъ ab, не превосходящихъ какого нибудь опредѣленнаго числа, напримѣръ, числа 30.

Такъ, напримѣръ, $\varphi(6) = \varphi(2.3) = \varphi(2)\varphi(3)$; $\varphi(10) = \varphi(2.5) = \varphi(2)\varphi(5)$ и т. д.

Можемъ примѣнить поэтому доказательство по индукціи, то есть доказывать теорему для чиселъ a и b, предполагая ея справедливость для чиселъ меньшихъ.

Пусть α пробѣгаетъ всю совокупность настоящихъ дѣлителей a, а β совокупность настоящихъ дѣлителей числа b; тогда всѣ дѣлители числа a получаются при помощи чиселъ a и α, а всѣ дѣлители числа b при помощи чиселъ b и β. Очевидно, что всѣ дѣлители числа ab будутъ имѣть видъ ab, $a\beta$, αb, $\alpha\beta$, причемъ совокупность чиселъ $a\beta$, αb, $\alpha\beta$ дастъ всѣхъ настоящихъ дѣлителей числа ab.

По теоремѣ § 26 будемъ имѣть

$$a = \varphi(a) + \sum\varphi(\alpha) \tag{1}$$

$$b = \varphi(b) + \sum\varphi(\beta) \tag{2}$$

$$ab = \varphi(ab) + \sum\varphi(a\beta) + \sum\varphi(\alpha b) + \sum\varphi(\alpha\beta). \tag{3}$$

Перемножая (1) и (2), получимъ

$$ab = \varphi(a)\varphi(b) + \sum\varphi(a)\varphi(\beta) + \sum\varphi(\alpha)\varphi(b) + \sum\varphi(\alpha)\varphi(\beta). \qquad (4)$$

Но по предположенію справедливости доказываемой теоремы для чиселъ меньшихъ получаемъ

$$\varphi(a)\varphi(\beta) = \varphi(a\beta),\ \varphi(\alpha)\varphi(b) = \varphi(\alpha b),\ \varphi(\alpha)\varphi(\beta) = \varphi(\alpha\beta)$$

и, слѣдовательно, сравнивая (3) и (4), получимъ

$$\varphi(a)\varphi(b) = \varphi(ab)$$

и теорема доказана.

§ 28. Теорема послѣдняго параграфа даетъ возможность вывести весьма важную формулу для вычисленія функціи $\varphi(n)$.

Пусть будетъ $n = p_1^{\omega_1} p_2^{\omega_2} \ldots p_k^{\omega_k}$,

тогда получаемъ

$$\varphi(n) = \varphi\left(p_1^{\omega_1}\right)\varphi\left(p_2^{\omega_2}\right) \ldots \varphi\left(p_k^{\omega_k}\right). \qquad (1)$$

§ 29. Остается найти выраженіе

$$\varphi(p^\omega),$$

гдѣ p простое число.

Остановимся сначала на случаѣ $\omega=1$. Очевидно, что тогда $\varphi(p)=p-1$, ибо всѣ числа $1, 2, 3, \ldots p-1$ взаимно простыя съ простымъ числомъ p.

Обращаемся теперь къ общему случаю p^ω.

Очевидно, что числа меньшія p^ω и взаимно простыя съ p^ω суть не дѣлящіяся на p, а потому изъ всѣхъ чиселъ

$$1, 2, 3, \ldots p^\omega \qquad (1)$$

придется откинуть всѣ дѣлящіяся на p, то есть числа

$$1.p,\ 2.p,\ 3.p,\ \ldots\ p^{\omega-1}.p. \qquad (2)$$

Такъ какъ число откинутыхъ чиселъ (2) есть $p^{\omega-1}$, то получится окончательно

$$\varphi(p^\omega) = p^\omega - p^{\omega-1} = p^\omega\left(1 - \frac{1}{p}\right). \qquad (3)$$

§ 30. Сравнивая формулу (1) § 28 съ формулой (3) § 29, мы получимъ окончательно слѣдующую формулу для вычисленія $\varphi(n)$ въ самомъ общемъ случаѣ.

Если $n = p_1^{\omega_1} p_2^{\omega_2} \dots p_k^{\omega_k}$,

то

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_k}\right). \qquad (1)$$

Такъ, напримѣръ,

$$n = 24 = 2^3 . 3$$

$$\varphi(24) = 24\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 8,$$

и дѣйствительно существуетъ только 8 чиселъ

$$1, 5, 7, 11, 13, 17, 19, 23$$

меньшихъ 24 и взаимно простыхъ съ 24.

Принципъ Dedekind'a.

§ 31. Формулу (1) предыдущаго параграфа можно переписать въ такомъ видѣ

$$\varphi(n) = n - \sum\frac{n}{p_1} + \sum\frac{n}{p_1 p_2} - \sum\frac{n}{p_1 p_2 p_3} + \dots, \qquad (1)$$

гдѣ суммы распространяются на различныя сочетанія различныхъ простыхъ множителей $p_1, p_2, p_3, \dots$ числа n по одному, по два, по три и т. д.

Формулу (1) можно считать слѣдствіемъ формулы

$$\sum\varphi(\delta) = n \qquad (2)$$

и её можно было бы написать сразу, примѣняя нѣкоторый *„принципъ обращенія“*, указанный *Dedekind'ом*[1]) и *Liouville'ем*[2]) и составляющій весьма важную теорему теоріи чиселъ.

Этотъ принципъ мы разъяснимъ на болѣе общей задачѣ.

Задача. Двѣ функціи $\psi(x)$ и $F(x)$ связаны равенствомъ

$$\sum\psi(\delta) = F(n) \qquad (3)$$

справедливымъ для всякаго цѣлаго n, причемъ сумма въ лѣвой части распространена на всѣхъ дѣлителей числа n. Спрашивается, что можно сказать о вычисленіи функціи $\psi(x)$?

---

[1]) Dedekind. Journal für r. u ang. Math, 54. 1857.

[2]) Liouville. Journ. de math. p. et appliq. (2) 2, 1857.

Начнемъ со случая $n = p^\omega$, гдѣ p простое число. Тогда формула (3) перепишется такъ

$$\psi(1) + \psi(p) + \psi(p^2) + \ldots + \psi(p^{\omega-1}) + \psi(p^\omega) = F(p^\omega). \qquad (4)$$

Примѣняя послѣднюю формулу для числа ω меньшаго на единицу, получимъ

$$\psi(1) + \psi(p) + \psi(p^2) + \ldots + \psi(p^{\omega-1}) = F(p^{\omega-1}), \qquad (5)$$

и мы получаемъ, вычитая (5) изъ (4),

$$\psi(p^\omega) = F(p^\omega) - F(p^{\omega-1})$$

или, обозначая $p^\omega = n$,

$$\psi(n) = F(n) - F\left(\frac{n}{p}\right). \qquad (6)$$

Докажемъ теперь, что если

$$n = p_1^{\omega_1} p_2^{\omega_2} p_3^{\omega_3} \ldots,$$

то изъ равенства (3) будетъ слѣдовать такое

$$\psi(n) = F(n) - \Sigma F\left(\frac{n}{p_1}\right) + \Sigma F\left(\frac{n}{p_1 p_2}\right) - \Sigma F\left(\frac{n}{p_1 p_2 p_3}\right) + \ldots \qquad (7)$$

гдѣ суммы распространены на всевозможныя сочетанія произведеній различныхъ простыхъ множителей $p_1, p_2, p_3, \ldots$ по одному, по два, по три, по четыре и т. д.

Справедливостъ формулы (7) провѣрена для случая (6) одного множителя числа n и можетъ быть для общаго случая доказана по индукціи. Предположимъ эту формулу справедливою для числа m, составленнаго изъ нѣкотораго числа различныхъ простыхъ множителей, покажемъ ея справедливость для числа n, имѣющаго еще одного лишняго простого множителя p

$$n = mp^\omega.$$

Пусть простые множители числа m суть

$$p_1, p_2, p_3, \ldots$$

Обозначимъ всѣхъ дѣлителей числа m черезъ

$$1, d_1, d_2, \ldots m;$$

получаемъ

$$\begin{aligned}
&\psi(1) + \psi(d_1) + \ldots + \psi(m)\\
&\psi(p) + \psi(d_1 p) + \ldots + \psi(mp)\\
&\ldots\ldots\ldots\ldots\\
&\psi(p^\omega) + \psi(d_1 p^\omega) + \ldots + \psi(mp^\omega) = F(n).
\end{aligned}$$

Вычитая изъ обѣихъ частей послѣдняго равенства соотвѣтственныя части равенства для $\omega - 1$, получимъ

$$\psi(p^\omega) + \psi(p^\omega d_1) + \psi(p^\omega d_2) + \ldots + \psi(p^\omega m) = F(n) - F\left(\frac{n}{p}\right). \qquad (8)$$

Введемъ новыя обозначенія

$$\psi(p^\omega x) = \psi_1(x)$$

$$F'(p^\omega x) - F(p^{\omega-1}x) = F_1(x),$$

тогда равенство (8) можетъ быть переписано такъ

$$\sum \psi_1(d_i) = F_1(m).$$

Такъ какъ мы предполагаемъ формулу (7) справедливою для числа m, то можно будетъ написать

$$\psi_1(m) = F_1(m) - \sum F_1\left(\frac{m}{p_1}\right) + \sum F_1\left(\frac{m}{p_1 p_2}\right) - \ldots$$

или окончательно

$$\psi(n) = \left[F(n) - F\left(\frac{n}{p}\right)\right] - \sum\left[F\left(\frac{n}{p_1}\right) - F\left(\frac{n}{pp_1}\right)\right] +$$

$$+ \sum\left[F\left(\frac{n}{p_1 p_2}\right) - F\left(\frac{n}{pp_1 p_2}\right)\right] - \ldots$$

Переписывая эту формулу такъ

$$\psi(n) = F(n) - \sum F\left(\frac{n}{p}\right) + \sum F\left(\frac{n}{pp_1}\right) - \sum F\left(\frac{n}{pp_1 p_2}\right) + \ldots,$$

получаемъ доказательство справедливости формулы (7) для числа n съ большимъ на единицу числомъ различныхъ простыхъ множителей.

Такимъ образомъ теорема Dedekind'a доказана вполнѣ.

§ 32. Формулу (7) предыдущаго параграфа, выражающую законъ обращенія Dedekind'a, можно написать въ болѣе компактномъ видѣ, если ввести въ разсмотрѣніе новую числовую функцію Moebius'a

$$\mu(n),$$

опредѣляемую слѣдующими свойствами:

1) $\mu(1) = 1$,

2) $\mu(n) = 0$, если въ составъ n входятъ простые множители съ показателями большими единицы,

3) $\mu(n) = (-1)^k$, если n есть произведеніе первыхъ степеней k различныхъ простыхъ множителей.

Мы можемъ доказанную формулу Dedekind'a переписать въ такомъ видѣ

$$\psi(n) = \sum \mu(m) F\left(\frac{n}{m}\right), \qquad (1)$$

гдѣ сумма распространена на всѣхъ дѣлителей m числа n.

§ 33. На основаніи сказаннаго легко рѣшить аналогичный вопросъ относительно произведеній.

Пусть задано уравненіе

$$\Pi\psi(\delta) = F(n), \qquad (1)$$

гдѣ произведеніе Π распространено на всѣхъ дѣлителей δ числа n.

Мы приведемъ задачу обращенія равенства, т. е. нахожденія вида функціи $\psi(n)$, къ задачѣ предыдущей, если прологариѳмируемъ уравненіе (1)

$$\sum lg\, \psi(\delta) = lg\, F(n). \qquad (2)$$

Отсюда на основаніи формулы (1) § 32 получимъ

$$lg\, \psi(n) = \sum \mu(m)\, lg\, F\left(\frac{n}{m}\right),$$

или переходя отъ логариѳмовъ къ числамъ, получимъ

$$\psi(n) = \Pi F\left(\frac{n}{m}\right)^{\mu(m)}. \qquad (3)$$

Эта формула (3) могла бы быть получена безъ введенія логариѳмовъ, если бы по аналогіи съ доказательствомъ теоремы Dedekind'a мы вмѣсто дѣйствій сложенія и вычитанія равенствъ примѣнили бы дѣйствія умноженія и дѣленія.

Этимъ я хочу сказать, что формула (3) остается справедливой и при такихъ символахъ, при которыхъ логариѳмированіе недопустимо, лишь бы сохранялись правила алгебры раціональныхъ дѣйствій.

Формула (3) можетъ быть переписана еще такъ

$$\psi(n) = \frac{F(n)\Pi F\left(\frac{n}{p_1 p_2}\right)\dots}{\Pi F\left(\frac{n}{p_1}\right)\Pi F\left(\frac{n}{p_1 p_2 p_3}\right)\dots},$$

гдѣ произведенія Π распространены на сочетанія различныхъ простыхъ множителей p_1, p_2, p_3, ... числа n по одному, два, три и т. д.

§ 34. Покажемъ нѣкоторыя приложенія функціи $\mu(n)$.

Докажемъ слѣдующее равенство

$$\sum \mu(m) = 0, \qquad (1)$$

гдѣ сумма Σ распространяется на всѣхъ дѣлителей m нѣкотораго числа n, причемъ единственное исключеніе представляетъ число $n = 1$, когда получаемъ

$$\mu(1) = 1.$$

Такъ какъ функція $\mu(m)$ равна нулю, если m имѣетъ кратные простые множители, то достаточно разсмотрѣть только такія значенія m, которыя составлены изъ первыхъ степеней различныхъ простыхъ множителей p_1, p_2, ... p_k числа n. Пусть число данныхъ множителей есть k, тогда первую часть равенства можно будетъ переписать такъ

$$\mu(1) + \sum\mu(p_i) + \sum\mu(p_1 p_2) + \sum\mu(p_1 p_2 p_3) + \dots$$

или иначе

$$1 - k + \frac{k(k-1)}{1.2} - \frac{k(k-1)(k-2)}{1.2.3} + \dots,$$

т. е.

$$\sum\mu(m) = (1-1)^k$$

и равняется нулю, что доказываетъ справедливость равенства (1).

§ 35. Разсмотримъ безконечный рядъ уравненій

$$\psi(m.1) + \psi(m.2) + \psi(m.3) + \dots = F(m), \qquad (1)$$

которыя получаются при всевозможныхъ значеніяхъ

$$m = 1, 2, 3, 4, \dots$$

Мы предполагаемъ конечно сходящимся рядъ стоящій въ первой части уравненія (1), а также всѣ ряды, которые у насъ будутъ встрѣчаться, мы будемъ предполагать сходящимися.

Если мы будемъ считать функцію $F(m)$ извѣстною, а функцію $\psi(n)$ искомою, то, заставляя число m пробѣгать натуральный рядъ чиселъ, получимъ безконечное число уравненій линейныхъ относительно безконечнаго числа неизвѣстныхъ

$$\psi(1),\ \psi(2),\ \psi(3),\ \ldots,$$

а именно эти уравненія будутъ

$$\begin{aligned}
\psi(1)+\psi(2)+\psi(3)+\psi(4)+\psi(5)+\psi(6)+\ldots &= F(1)\\
\psi(2)\qquad +\psi(4)\qquad +\psi(6)+\ldots &= F(2)\\
\psi(3)\qquad\qquad +\psi(6)+\ldots &= F(3)\\
\psi(4)+\ldots\ldots\ldots\ldots &= F(4)\\
\psi(5)+\ldots\ldots\ldots &= F(5)\\
\psi(6)+\ldots &= F(6)\\
\ldots\ldots\ldots\ldots &
\end{aligned}$$

Нетрудно рѣшить эти уравненія относительно неизвѣстныхъ. Покажемъ рѣшеніе относительно $\psi(1)$, для этой цѣли умножимъ уравненіе (1), которое можно переписать такъ

$$\sum_n \psi(mn) = F(m),$$

на $\mu(m)$ и просуммируемъ по m

$$\sum_m \sum_n \mu(m)\psi(mn) = \sum_m \mu(m)F(m). \qquad (2)$$

Перепишемъ послѣднее уравненіе (2) такъ

$$\sum_n (\Sigma\mu(d))\psi(n) = \sum_m \mu(m)F(m),$$

гдѣ внутренняя сумма распространяется на всѣхъ дѣлителей d числа n. На основаніи теоремы § 34 замѣчаемъ, что эти суммы обращаются въ нуль, за исключеніемъ первой, соотвѣтствующей $n=1$ и мы получаемъ

$$\psi(1) = \sum_m \mu(m)F(m). \qquad (3)$$

§ 36. Этотъ выводъ формулы (3) § 35, уже давно извѣстный, можно разсматривать какъ замѣчательный примѣръ на теорію, развитую болѣе

или менѣе систематически лишь въ послѣднее время, а именно теорію безконечныхъ опредѣлителей, или, другими словами, теорію системъ уравненій съ безконечнымъ числомъ неизвѣстныхъ. Эта теорія получила въ послѣднее время большое развитіе въ Göttingen'ѣ въ школѣ профессора Hilbert'a, причемъ обратили на себя вниманіе работы его ученика Töplitz'a.

ГЛАВА III.

Теорія сравненій.

§ 1. Если разность двухъ чиселъ a и b дѣлится на число k, т. е. если число

$$\frac{a-b}{k}$$

цѣлое, то будемъ говорить, что числа a и b *сравнимы по модулю* k и будемъ записывать это свойство знакомъ

$$a \equiv b \pmod{k}.$$

Этотъ знакъ носитъ названіе *сравненія*.

Числа a и b мы будемъ предполагать, какъ положительными, такъ и отрицательными; модуль же k будемъ всегда считать положительнымъ.

§ 2. Если число a отъ дѣленія на k дастъ остатокъ r, то мы будемъ имѣть $a = kl + r$, гдѣ l нѣкоторое цѣлое число; слѣдовательно, разность $a - r$ дѣлится на k, и мы получаемъ $a \equiv r \pmod{k}$.

Справедливо также свойство обратное, а именно, что если a и r числа положительныя, число же $r < k$ и сравнимо по модулю k съ a, то r будетъ остатокъ отъ дѣленія a на k; въ самомъ дѣлѣ, сравненіе

$$a \equiv r \pmod{k}$$

даетъ

$$\frac{a-r}{k} = l,$$

гдѣ l цѣлое число, откуда получаемъ

$$a = kl + r.$$

Сравненіе

$$a \equiv 0 \pmod{k}$$

равносильно съ утвержденіемъ, что a дѣлится на k.

§ 3. Для сравненій оказываются справедливыми многія изъ простѣйшихъ свойствъ уравненій. Перечислимъ здѣсь эти свойства.

I. Два числа a и a_1, сравнимыя по модулю k съ третьимъ числомъ b, сравнимы между собой.

Въ самомъ дѣлѣ, сравненія

$$a \equiv b \pmod{k}; \quad a_1 \equiv b \pmod{k}$$

показываютъ, что разности $a - b$ и $a_1 - b$ дѣлятся на k, а слѣдовательно будетъ дѣлиться на k и выраженіе $a - b - (a_1 - b) = a - a_1$ значитъ

$$a \equiv a_1 \pmod{k}.$$

II. Въ сравненіяхъ можно переносить члены изъ одной части въ другую съ перемѣной знака.

Въ самомъ дѣлѣ, покажемъ, что сравненіе

$$a + a_1 \equiv b \pmod{k} \tag{1}$$

влечетъ, какъ слѣдствіе,

$$a \equiv b - a_1 \pmod{k}. \tag{2}$$

Дѣйствительно, сравненіе (1) показываетъ, что дѣлится на k число $a + a_1 - b$, но это число можетъ быть написано такъ

$$a - (b - a_1)$$

и слѣдовательно, дѣлимость его на k показываетъ справедливость сравненія (2).

III. Сравненіе можно складывать и вычитать почленно.

Въ самомъ дѣлѣ, сравненія

$$a \equiv b \pmod{k} \text{ и } a_1 \equiv b_1 \pmod{k}$$

показываютъ дѣлимость на k чиселъ

$$a - b \text{ и } a_1 - b_1,$$

слѣдовательно, должна дѣлиться на k сумма и разность этихъ чиселъ

$$a \pm a_1 - (b \pm b_1)$$

и слѣдовательно, должно имѣть мѣсто сравненіе

$$a \pm a_1 \equiv b \pm b_1 \pmod{k}.$$

IV. Члены сравненія могутъ быть умножаемы на одно и то-же число.

Въ самомъ дѣлѣ, сравненіе

$$a \equiv b \pmod{k},$$

сложенное почленно съ самимъ собою l разъ, даетъ

$$la \equiv lb \pmod{k}.$$

Слѣдовательно, высказанное свойство справедливо при l положительномъ.

Для доказательства справедливости возможности умноженія на отрицательное число вычтемъ послѣднее сравненіе изъ тождественнаго

$$0 \equiv 0 \pmod{k},$$

получаемъ

$$(-l)\,a \equiv (-l)b \pmod{k}.$$

V. Сравненія можно почленно перемножить, т. е. два сравненія

$$a \equiv b \pmod{k} \text{ и } a_1 \equiv b_1 \pmod{k} \tag{3}$$

влекутъ, какъ слѣдствіе, сравненіе

$$a a_1 \equiv b b_1 \pmod{k}. \tag{4}$$

Въ самомъ дѣлѣ, сравненія (3) даютъ

$$a = b + kl$$

и

$$a_1 = b_1 + kl_1.$$

Отсюда

$$aa_1 = bb_1 + k(bl_1 + b_1 l + kll_1).$$

Такъ какъ трехчленъ въ послѣднихъ скобкахъ есть цѣлое число, то произведеніе aa_1 сравнимо съ произведеніемъ bb_1 по модулю k.

VI. Примѣняя послѣднюю теорему объ умноженіи къ нѣсколькимъ одинаковымъ сравненіямъ, получаемъ, что сравненія можно почленно возвышать въ любую цѣлую положительную степень, т. е., что сравненіе

$$a \equiv b \pmod{k}$$

влечетъ, какъ слѣдствіе,

$$a^n \equiv b^n \pmod{k}.$$

VII. Разсмотримъ цѣлую функцію

$$f(x) = p_0 x^n + p_1 x^{n-1} + \ldots + p_n$$

съ цѣлыми коэффиціентами. Тогда сравненіе

$$a \equiv b \pmod{k}$$

будетъ имѣть слѣдствіемъ

$$f(a) \equiv f(b) \pmod{k}. \tag{5}$$

Въ самомъ дѣлѣ, на основаніи свойства VI получаемъ рядъ сравненій

$$a^n \equiv b^n,\ a^{n-1} \equiv b^{n-1},\ \ldots\ a \equiv b,\ 1 \equiv 1 \pmod{k}.$$

Умножая эти сравненія послѣдовательно на коэффиціенты

$$p_0, p_1, \ldots, p_n$$

и складывая, получимъ сравненіе (5), что и требовалось доказать.

VIII. Если число l взаимно простое съ модулемъ k, то сравненіе

$$la \equiv lb \pmod{k} \tag{6}$$

можетъ быть сокращено на число l, т. е. получится

$$a \equiv b \pmod{k}. \tag{7}$$

Въ самомъ дѣлѣ, сравненіе (6) показываетъ, что дѣлится на k число

$$la - lb = l(a - b).$$

Но такъ какъ l число взаимно простое съ k, то должна дѣлиться на k разность $a - b$, т. е. должно удовлетворяться сравненіе (7).

IX. Если одна изъ частей сравненія

$$a \equiv b \pmod{k},$$

напр. b, и модуль k дѣлятся на нѣкоторое число l, то должна дѣлиться на l и другая часть a.

Въ самомъ дѣлѣ

$$a = b + km,$$

откуда слѣдуетъ, что если b и k дѣлится на l, то должно дѣлиться на l и a.

X. Общій множитель членовъ сравненія и модуля можетъ быть сокращенъ, т. е. сравненіе

$$la \equiv lb \pmod{lk} \tag{8}$$

влечетъ, какъ слѣдствіе, сравненіе

$$a \equiv b \pmod{k}. \qquad (9)$$

Въ самомъ дѣлѣ, сравненіе (8) показываетъ, что

$$\frac{la - lb}{lk} = \frac{a - b}{k}$$

есть число цѣлое.

XI. Два числа, сравнимыя по нѣкоторому модулю k, будутъ сравнимы также по всякому дѣлителю этого модуля k.

XII. Два числа, сравнимыя между собой по взаимно простымъ модулямъ

$$k_1, k_2, k_3, \ldots$$

сравнимы также по ихъ произведенію, т. е. сравненія

$$a \equiv b \pmod{k_1}, \quad a \equiv b \pmod{k_2} \ldots$$

влекутъ, какъ слѣдствіе, сравненіе

$$a \equiv b \pmod{k_1 k_2 k_3 \ldots},$$

ибо если разность $a - b$ дѣлится на взаимно простыя числа

$$k_1, k_2, k_3, \ldots,$$

то она, очевидно, дѣлится и на ихъ произведеніе.

§ 4. Если мы перенесемъ всѣ члены сравненія въ одну часть его, то сравненіе приметъ видъ

$$\Omega(u, v, w \ldots) \equiv 0 \pmod{k},$$

гдѣ u, v, w, . . . входящія въ сравненіе буквы.

Одной изъ главныхъ задачъ этой главы будетъ рѣшеніе сравненій съ однимъ неизвѣстнымъ, при чемъ мы будемъ разсматривать сравненія вида

$$f(x) \equiv 0 \pmod{k}, \qquad (1)$$

гдѣ $f(x)$ цѣлая функція отъ одной неизвѣстной x съ цѣлыми коэффиціентами. *Корнемъ* сравненія мы будемъ называть такое число a, которое даетъ тождественное сравненіе

$$f(a) \equiv 0 \pmod{k}. \qquad (2)$$

Не трудно видѣть, что если извѣстенъ одинъ корень a сравненія, то по этому корню можно составить безчисленное множество другихъ корней. Въ самомъ дѣлѣ, на основаніи свойства VII сравненій (см. § 3), мы имѣемъ, что при

$$x \equiv a \pmod{k} \tag{3}$$

будетъ

$$f(x) \equiv f(a) \pmod{k}. \tag{4}$$

Сопоставляя (2) и (4), мы получимъ

$$f(x) \equiv 0 \pmod{k}.$$

Другими словами, окажется, что всякое число x, удовлетворяющее сравненію (3), будетъ корнемъ заданнаго сравненія (1).

Итакъ, корню a сравненія (1) будетъ соотвѣтствовать безчисленное число корней, выражаемыхъ по формулѣ

$$a - kz,$$

гдѣ z произвольное цѣлое число.

§ 5. Во всемъ дальнѣйшемъ мы будемъ называть *классомъ* чиселъ совокупность чиселъ, сравнимыхъ между собой по модулю k.

Если одно изъ чиселъ нѣкотораго класса мы назовемъ a, то очевидно, что всѣ числа этого класса сравнимы съ a по модулю k, и слѣдовательно, общій видъ числа, принадлежащаго къ этому классу, будетъ

$$a - kz,$$

гдѣ z положительное или отрицательное цѣлое число, или нуль.

Въ предыдущемъ §-ѣ мы выдѣли, что если сравненію удовлетворяетъ одно число класса, то ему удовлетворяютъ и всѣ числа этого класса, а потому всѣ числа одного класса, удовлетворяющія сравненію, считаются за одно рѣшеніе этого сравненія. Для характеристики класса чиселъ выбирается обыкновенно одно изъ чиселъ этого класса.

Мы будемъ называть *наименьшимъ положительнымъ вычетомъ* или просто *положительнымъ вычетомъ* числа a по модулю k наименьшее положительное число, принадлежащее къ классу $a - kz$.

Подобнымъ же образомъ *отрицательнымъ вычетомъ* будемъ называть наименьшее по абсолютной величинѣ отрицательное число, заключающееся въ классѣ.

Такъ, напримѣръ, разсмотримъ вычеты числа 5 по модулю 3.

Мы видимъ, что среди чиселъ класса $5 - 3z$ положительнымъ вычетомъ явится число 2, а отрицательнымъ вычетомъ — 1.

Изъ двухъ вычетовъ, положительнаго и отрицательнаго, мы будемъ называть *абсолютно малымъ вычетомъ* тотъ изъ нихъ, абсолютная величина котораго меньше. Въ данномъ примѣрѣ абсолютно малый вычетъ есть -1.

Не трудно дать общую формулу для двухъ вычетовъ нѣкотораго положительнаго числа a по модулю k. Въ самомъ дѣлѣ, положительный вычетъ есть наименьшее положительное число, заключающееся въ формулѣ

$$a - kz = k\left(\frac{a}{k} - z\right).$$

Такъ какъ z есть цѣлое число, то послѣднее число будетъ наименьшимъ положительнымъ въ томъ случаѣ, когда цѣлое число z есть наибольшее изъ не превосходящихъ число $\frac{a}{k}$, т. е. когда

$$z = \left[\frac{a}{k}\right].$$

Слѣдовательно, положительный вычетъ опредѣляется формулой

$$k\left(\frac{a}{k} - \left[\frac{a}{k}\right]\right). \tag{1}$$

Очевидно, что отрицательный вычетъ выразится формулой:

$$k\left(\frac{a}{k} - \left[\frac{a}{k}\right] - 1\right). \tag{2}$$

Сравнимъ абсолютныя величины вычетовъ (1) и (2). Можетъ произойти одно изъ неравенствъ:

$$\frac{a}{k} - \left[\frac{a}{k}\right] \lessgtr 1 + \left[\frac{a}{k}\right] - \frac{a}{k}. \tag{3}$$

При верхнемъ знакѣ абсолютно малымъ будетъ положительный вычетъ; при нижнемъ знакѣ—отрицательный вычетъ. При среднемъ знакѣ равенства оба вычета будутъ имѣть одинаковую абсолютную величину. Въ этомъ послѣднемъ случаѣ мы будемъ говорить, что существуетъ два абсолютно малыхъ вычета: положительный и отрицательный.

Неравенство (3) можно переписать такъ

$$\frac{a}{k} - \left[\frac{a}{k}\right] \lessgtr \frac{1}{2};$$

получается такой способъ нахожденія абсолютно малаго вычета. Разность

$$\frac{a}{k} - \left[\frac{a}{k}\right]$$

представляетъ собою правильную дробь, которая получается отъ выдѣленія цѣлой части дроби $\frac{a}{k}$, и у насъ выходитъ, что, если эта правильная дробь меньше половины, то абсолютно малый вычетъ положительный, если эта дробь больше половины, то абсолютно малый вычетъ отрицательный. Напримѣръ, требуется найти обсолютно малый вычетъ числа 9 по модулю 6. Разсматриваемъ дробь

$$\frac{9}{6} = \frac{3}{2} = 1\frac{1}{2}.$$

Такъ какъ дробная часть послѣдняго смѣшаннаго числа есть половина, то получается два абсолютно малыхъ вычета:

$$+3 \text{ и } -3.$$

§ 6. Не трудно убѣдиться, что *различныхъ классовъ чиселъ по модулю k можетъ быть только k*. Если мы будемъ выбирать за представителя класса положительный вычетъ, то значенія этого положительнаго вычета могутъ быть только такія

$$0, 1, 2, \ldots, k-1. \qquad (1)$$

Покажемъ, что два класса чиселъ, соотвѣтствующіе двумъ различнымъ числамъ α, β изъ ряда (1), должны быть различны между собой, т. е. не могутъ заключать общихъ чиселъ. Въ самомъ дѣлѣ, допустимъ обратное, т. е. предположимъ, что существуетъ число γ, входящее въ оба разсматриваемые класса. Тогда получаемъ

$$\gamma \equiv \alpha \pmod{k},$$

$$\gamma \equiv \beta \pmod{k},$$

откуда

$$\alpha \equiv \beta \pmod{k},$$

и слѣдовательно, разность $\alpha - \beta$ должна дѣлиться на k, что невозможно, ибо оба числа α и β меньше k, а слѣдовательно меньше этого числа и абсолютная величина ихъ разности.

Числа ряда (1) мы будемъ называть *полной системой вычетовъ по модулю k*.

Этимъ вычетамъ соотвѣтствуетъ k различныхъ классовъ чиселъ. Каждое изъ чиселъ, положительныхъ или отрицательныхъ, принадлежитъ къ одному изъ такихъ классовъ.

§ 7. Теорема. *Если число a взаимно простое съ модулемъ k и мы будемъ подставлять въ формулу $ax+b$ вмѣсто x послѣдовательно числа полной системы вычетовъ*

$$0,\ 1,\ 2,\ \ldots,\ k-1, \tag{1}$$

то получимъ систему чиселъ несравнимыхъ между собой.

Въ самомъ дѣлѣ, предположимъ обратное, а именно, что для двухъ чиселъ α, β ряда (1) имѣетъ мѣсто сравненіе

$$a\alpha + b \equiv a\beta + b \pmod{k}.$$

Тогда получаемъ

$$a\alpha \equiv a\beta \pmod{k},$$

и на основаніи свойства VIII сравненій, получаемъ

$$\alpha \equiv \beta \pmod{k},$$

что невозможно.

Итакъ, если въ выраженіи

$$ax+b$$

x пробѣгаетъ полную систему вычетовъ по модулю k, то само выраженіе $ax+b$ пробѣгаетъ также полную систему вычетовъ.

§ 8. *Теорема Euler'a.*

Если число a взаимно простое съ k, то будетъ имѣть мѣсто сравненіе

$$a^{\varphi(k)} \equiv 1 \pmod{k},$$

тотъ φ функція, разсматривавшаяся въ § 23 гл. II.

Пусть числа, взаимно простыя съ k и меньшія этого числа, будутъ

$$a_1,\ a_2,\ a_3,\ \ldots$$

причемъ пусть a обозначаетъ одно изъ нихъ.

Обозначимъ черезъ b_1, b_2, . . . положительные вычеты чиселъ aa_1, aa_2, aa_3, . . . , такъ что имѣемъ рядъ сравненій

$$\left.\begin{aligned} aa_1 &\equiv b_1 \\ aa_2 &\equiv b_2 \\ aa_3 &\equiv b_3 \\ &\ldots \end{aligned}\right\} \pmod{k}.$$

Перемножая эти сравненія, получимъ

$$a^{\varphi(k)} a_1 a_2 a_3 \ldots \equiv b_1 b_2 b_3 \ldots \pmod{k}. \qquad (1)$$

Числа $b_1, b_2, b_3, \ldots$ должны быть взаимно простыя съ k. Въ самомъ дѣлѣ, допустимъ обратное, а именно, что какое нибудь изъ чиселъ b, напр. b_1, имѣетъ нѣкотораго общаго дѣлителя δ съ модулемъ k; тогда по свойству IX сравненій этого же дѣлителя δ должна имѣть первая часть, что невозможно, ибо эта часть представляетъ изъ себя произведеніе чиселъ взаимно простыхъ съ k.

Итакъ, всѣ $b_1, b_2, b_3, \ldots$ суть числа, взаимно простыя съ k.

Не трудно убѣдиться, что среди чиселъ b не можетъ быть одинаковыхъ, ибо всѣ числа

$$aa_1, aa_2, aa_3, \ldots$$

какъ получающіяся отъ подстановки въ выраженіе ax, вмѣсто x, чиселъ, несравнимыхъ по модулю k, должны принадлежать къ различнымъ классамъ (см. § 7) и, слѣдовательно, не могутъ имѣть одинаковыхъ вычетовъ.

Итакъ, числа $b_1, b_2, b_3, \ldots$ суть тѣ же, что и числа $a_1, a_2, a_3, \ldots$, только могутъ отличаться порядкомъ расположенія. Слѣдовательно, имѣетъ, мѣсто равенство

$$a_1 . a_2 . a_3 \ldots = b_1 . b_2 . b_3 \ldots$$

Отсюда на основаніи сравненія (1) получаемъ

$$a^{\varphi(k)} \equiv 1 \pmod{k},$$

что и требовалось доказать.

§ 9. Теорема Euler'a есть обобщеніе теоремы, предложенной раньше Fermat'омъ, когда модуль есть простое число p. При простомъ модулѣ p для всякаго числа a, не дѣлящагося на p, имѣетъ мѣсто сравненіе

$$a^{p-1} \equiv 1 \pmod{p},$$

ибо $\varphi(p) = p - 1$.

§ 10. Въ видѣ легкаго упражненія предлагаемъ читателю доказать слѣдующее предложеніе.

Теорема. Если три числа a, b, c не имѣютъ общаго дѣлителя, то выраженіе

$$ax + b$$

получаетъ $\dfrac{\varphi(ac)}{\varphi(a)}$ разъ значенія взаимно простыя съ c, когда x пробѣгаетъ систему всѣхъ вычетовъ по модулю c.

Сравненія первой степени.

§ 11. Будемъ разсматривать сравненія вида

$$ax - b \equiv 0 \pmod{k}.$$

Придется разсмотрѣть отдѣльно два случая:

1) a взаимно простое съ k,

2) a имѣетъ нѣкотораго общаго дѣлителя δ съ k..

§ 12. Итакъ, предположимъ, что число a взаимно простое съ k.

Для рѣшенія сравненія

$$ax - b \equiv 0 \pmod{k} \qquad (1)$$

достаточно подставить въ выраженіе $ax - b$ всю полную систему вычетовъ.

По сказанному въ параграфѣ 7 получатся числа, вычеты которыхъ образуютъ полную систему. Слѣдовательно, при нѣкоторомъ значеніи x и только при одномъ этомъ $ax - b$ будетъ имѣть вычетъ равный нулю. Слѣдовательно, заданное сравненіе (1) будетъ имѣть одно и только одно рѣшеніе.

§ 13. Посмотримъ, какъ вычислить корень сравненія (1) предыдущаго параграфа. Сравненіе (1) § 12-го равносильно уравненію $ax - b = ky$, гдѣ y цѣлое число.

Итакъ, наша задача привелась къ рѣшенію въ цѣлыхъ числахъ неопредѣленнаго уравненія

$$ax - ky = b. \qquad (1)$$

Изъ элементарнаго курса извѣстно, что уравненіе (1) при a и k взаимно простыхъ имѣетъ рѣшенія, выражаемыя формулами $x = \alpha + kt$ и $y = \beta + at$, гдѣ α и β даютъ одно рѣшеніе уравненія (1), а t произвольное цѣлое число.

Уравненіе

$$x = \alpha + kt$$

можетъ быть представлено въ видѣ сравненія

$$x \equiv \alpha \pmod{k},$$

и мы получаемъ одно рѣшеніе сравненія.

Напримѣръ, требуется рѣшить сравненіе

$$8x - 3 \equiv 0 \pmod{15}.$$

Рѣшаемъ уравненіе

$$8x - 15y = 3;$$

получаемъ

$$x \equiv 6 \pmod{15}.$$

§ 14. Теорема Euler'a даетъ также возможность написать сразу рѣшеніе сравненія первой степени.

Въ самомъ дѣлѣ, пусть задано сравненіе

$$ax - b \equiv 0 \pmod{k}. \qquad (1)$$

По теоремѣ Euler'a имѣемъ

$$a^{\varphi(k)} \equiv 1 \pmod{k}.$$

Умножая на b, получимъ

$$ba^{\varphi(k)} \equiv b \pmod{k},$$

или иначе

$$a\left[ba^{\varphi(k)-1}\right] - b \equiv 0 \pmod{k}.$$

Отсюда получается сразу рѣшеніе сравненія (1) въ видѣ

$$x \equiv ba^{\varphi(k)-1} \pmod{k}.$$

Такъ, напримѣръ, сравненіе

$$8x - 3 \equiv 0 \pmod{15}$$

будетъ имѣть рѣшеніе

$$x \equiv 3.8^{\varphi(15)-1} \pmod{15}.$$

Но

$$3.8^{\varphi(15)-1} = 3.8^{8-1} = 3.8^7 \equiv 6 \pmod{15},$$

что видно изъ формулъ

$$3.8 \equiv 24 \equiv 9 \pmod{15},$$

$$3.8^2 \equiv 9.8 \equiv 12 \pmod{15},$$

$$3.8^3 \equiv 12.8 \equiv 6 \pmod{15},$$

$$3.8^4 \equiv 6.8 \equiv 3 \pmod{15},$$

$$3.8^7 \equiv 3.8^3 \equiv 6 \pmod{15}.$$

§ 15. Обратимся теперь къ случаю, когда въ сравненіи

$$ax - b = 0 \pmod{k} \qquad (1)$$

коэффиціентъ a имѣетъ нѣкоторый общій наибольшій дѣлитель δ съ модулемъ k.

По свойству IX сравненіе будетъ невозможно, если на этого дѣлителя δ не будетъ дѣлиться коэффиціентъ b. Итакъ, предположимъ, что этотъ коэффиціентъ также дѣлится на δ.

Полагая $a = a_1\delta$, $b = b_1\delta$, $k = k_1\delta$, и примѣняя свойство X, приведемъ рѣшеніе сравненія (1) къ рѣшенію новаго сравненія

$$a_1x - b_1 \equiv 0 \pmod{k_1}, \qquad (2)$$

въ которомъ коэффиціентъ a_1 взаимно простой съ модулемъ.

Это сравненіе (2) имѣетъ, какъ мы видѣли, только одно рѣшеніе

$$x \equiv \alpha \pmod{k_1}. \qquad (3)$$

Но очевидно, что числа, принадлежащія къ одному классу по модулю k_1, могутъ принадлежать къ различнымъ классамъ по первоначальному модулю k. При этомъ не трудно убѣдиться, что число такихъ классовъ по модулю k, къ которымъ принадлежатъ числа (3), будетъ равно δ.

Въ самомъ дѣлѣ, если мы напишемъ δ чиселъ

$$\alpha,\ \alpha + k_1,\ \alpha + 2k_1,\ \alpha + 3k_1,\ \ldots,\ \alpha + (\delta - 1)k_1,$$

то эти числа, очевидно, несравнимы по модулю k, ибо разность каждыхъ двухъ изъ этихъ чиселъ по абсолютной величинѣ меньше k.

Такъ какъ всѣ числа (3) будутъ въ то же самое время рѣшеніями заданнаго сравненія (1), то, слѣдовательно, это сравненіе (1) будетъ имѣть δ рѣшеній, опредѣляемыхъ классами

$$\left.\begin{array}{l} x \equiv \alpha \\ x \equiv \alpha + k_1 \\ x \equiv \alpha + 2k_1 \\ \ldots\ldots\ldots\ldots \\ x \equiv \alpha + (\delta - 1)k_1 \end{array}\right| \pmod{k}.$$

Напримѣръ, требуется рѣшить сравненіе

$$15x + 18 \equiv 0 \pmod{21}.$$

Сокращая на 3, получимъ

$$5x + 6 \equiv 0 \pmod{7}.$$

Этому новому сравненію удовлетворяетъ

$$x \equiv 3 \pmod 7 .$$

Составимъ три числа 3, $3+7$, $3+2\,.\,7$, которыя будутъ представителями классовъ, дающихъ рѣшенія

$$x \equiv 3 \pmod{21},$$

$$x \equiv 10 \pmod{21},$$

$$x \equiv 17 \pmod{21}.$$

§ 16. Данъ рядъ сравненій

$$x \equiv \alpha \pmod a ;\ x \equiv \beta \pmod b ;\ x \equiv \gamma \pmod c ;\ \ldots , \qquad (1)$$

гдѣ модули a, b, c, . . . числа взаимно-простыя. Числа же α, β, γ, . . . произвольныя. Требуется найти всѣ числа, удовлетворяющія этимъ сравненіямъ.

Введемъ въ разсмотрѣніе число m, равное произведенію $a\,.\,b\,.\,c\,\ldots$ модулей. Кромѣ того, обозначимъ

$$m = aA = bB = cC = \ldots ,$$

гдѣ

$$A = bc\ \ldots ;\ B = ac\ \ldots ;\ C = ab\ \ldots ;\ \ldots$$

Обозначимъ черезъ a', b', c', . . . числа, удовлетворяющія сравненіямъ

$$Aa' \equiv 1 \pmod a ,$$

$$Bb' \equiv 1 \pmod b ,$$

$$Cc' \equiv 1 \pmod c ,$$

. . . . . .

Каждое изъ этихъ сравненій будетъ имѣть по одному рѣшенію, ибо коэффиціенты A, B, C, . . . взаимно-простые съ соотвѣтственными модулями.

Не трудно убѣдиться, что числа, удовлетворяющія всѣмъ заданнымъ сравненіямъ (1), даются сравненіемъ

$$x \equiv Aa'\alpha + Bb'\beta + Cc'\gamma + \ldots \pmod m . \qquad (2)$$

Въ самомъ дѣлѣ, на основаніи свойства XI сравненіе (2) влечетъ, какъ слѣдствіе

$$x \equiv Aa'\alpha + Bb'\beta + Cc'\gamma + \ldots \pmod a .$$

Но такъ какъ

$$B \equiv C \equiv \ldots \equiv 0 \pmod{a}.$$

а

$$Aa' \equiv 1 \pmod{a},$$

то получаемъ

$$x \equiv \alpha \pmod{a}.$$

Подобнымъ же образомъ провѣрятся всѣ остальныя изъ заданныхъ сравненій.

Съ другой стороны, сравненіе (2) можно получить, какъ слѣдствіе, изъ сравненій (1) и, слѣдовательно, всѣ числа, удовлетворяющія сравненіямъ (1), выражаются въ формѣ (2).

Въ самомъ дѣлѣ, пусть x_1 и x_2 будутъ два числа, удовлетворяющихъ сравненіямъ (1); тогда мы получимъ

$$x_2 - x_1 \equiv 0 \pmod{a}, \; x_2 - x_1 \equiv 0 \pmod{b}, \; \ldots, \; x_2 - x_1 \equiv 0 \pmod{c},$$

откуда на основаніи свойства XII сравненій, получимъ

$$x_2 - x_1 \equiv \pmod{m}.$$

О сравненіяхъ высшихъ степеней.

§ 17. Въ разсматриваемой главѣ мы будемъ заниматься исключительно сравненіями вида

$$ax^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n \equiv 0 \pmod{p}, \qquad (1)$$

при чемъ модуль p будемъ предполагать числомъ простымъ, а коэффиціенты

$$a, \; a_1, \; \ldots, \; a_{n-1}, \; a_n$$

произвольными цѣлыми числами или нулями.

Очевидно, что всѣ члены съ коэффиціентами, дѣлящимися на p, могутъ быть исключены изъ сравненія. Точно такъ же всѣ коэффиціенты могутъ быть замѣнены ихъ положительными вычетами по модулю p.

§ 18. Можно сравненіе (1) предыдущаго §-а привести къ новому виду, въ которомъ коэффиціентъ при старшей степени неизвѣстнаго равенъ единицѣ. Въ самомъ дѣлѣ, умножимъ сравненіе (1) на число a', удовлетворяющее сравненію

$$aa' \equiv 1 \pmod{p}.$$

Это сравненіе всегда имѣетъ рѣшеніе относительно a', ибо коэффиціентъ a взаимно-простой съ p, такъ какъ всякое число, не дѣлящееся на

простое число p, есть взаимно простое съ нимъ. Отсюда, умножая сравненіе (1) предыдущаго §-а на a', приведемъ его къ виду

$$x^n + a' a_1 x^{n-1} + a' a_2 x^{n-2} + \ldots \equiv 0 \pmod{p}.$$

§ 19. Обозначая первую часть сравненія (1) § 17 черезъ $f(x)$, будемъ писать наше сравненіе въ такомъ видѣ

$$f(x) \equiv 0 \pmod{p}. \qquad (1)$$

Пусть α будетъ корнемъ сравненія (1). Будемъ дѣлить $f(x)$ на $x - \alpha$, при чемъ обозначимъ черезъ $f_1(x)$ частное, а черезъ r_1 постоянный остатокъ. Получаемъ, очевидно,

$$r_1 = f(\alpha) \equiv 0 \pmod{p}, \qquad (2)$$

ибо α корень сравненія (1).

Получаемъ

$$f(x) = (x - \alpha) f_1(x) + r_1, \qquad (3)$$

гдѣ r_1 дѣлится на p. Сравненіе (1) принимаетъ видъ

$$(x - \alpha) f_1(x) + r_1 \equiv 0 \pmod{p}$$

или иначе

$$(x - \alpha) f_1(x) \equiv 0 \pmod{p}. \qquad (4)$$

Пусть β будетъ другой корень сравненія (1) (несравнимый съ α по модулю p). Корень β долженъ удовлетворять сравненію (4), т. е. должно быть

$$(\beta - \alpha) f_1(\beta) \equiv 0 \pmod{p}.$$

Но $\beta - \alpha$ не дѣлится на p, слѣдовательно, получаемъ

$$f_1(\beta) \equiv 0 \pmod{p}.$$

Значитъ корень β есть корень сравненія

$$f_1(x) \equiv 0 \pmod{p}. \qquad (5)$$

Дѣлимъ функцію $f_1(x)$ на $x - \beta$; обозначимъ при этомъ частное черезъ $f_2(x)$, а остатокъ черезъ r_2; получимъ $r_2 = f_1(\beta)$, слѣдовательно r_2 дѣлится на p. Мы получаемъ

$$f_1(x) = (x - \beta) f_2(x) + r_2$$

или, подставляя въ равенство (3), получимъ

$$f(x) = (x-\alpha)(x-\beta) f_2(x) + r_1 + r_2(x-\alpha) =$$

$$= (x-\alpha)(x-\beta) f_2(x) + p(lx+m), \qquad (6)$$

гдѣ l и m цѣлыя числа.

Взявъ третій корень γ сравненія (1), замѣтимъ, что этотъ корень будетъ корнемъ сравненія

$$f_2(x) \equiv 0 \pmod p.$$

Получимъ

$$f_2(x) = (x-\gamma) f_3(x) + r_3.$$

Подставляя въ уравненіе (6), получимъ

$$f(x) = (x-\alpha)(x-\beta)(x-\gamma) f_3(x) + p(l_1 x^2 + m_1 x + n_1), \qquad (7)$$

гдѣ

$$l_1,\ m_1,\ n_1,$$

цѣлыя числа.

Продолжая наше разсужденіе далѣе, мы придемъ къ такому выводу:

Если сравненіе (1) будучи степени n, имѣетъ n различныхъ корней $\alpha, \beta, \gamma, \ldots, \lambda$, то имѣетъ мѣсто равенство

$$f(x) = a(x-\alpha)(x-\beta)(x-\gamma)\ldots(x-\lambda) + p\varphi(x), \qquad (8)$$

гдѣ $\varphi(x)$ цѣлая функція степени не выше $n-1$ съ цѣлыми коэффиціентами.

§ 20. Изъ соображеній предыдущаго §-а вытекаетъ, что *сравненіе*

$$f(x) \equiv 0 \pmod p$$

степени n не можетъ имѣть больше n рѣшеній.

Въ самомъ дѣлѣ, предположимъ, что кромѣ n корней $\alpha, \beta, \gamma, \ldots, \lambda$ сравненіе наше имѣетъ еще $n+1$-ый корень μ. Тогда на основаніи формулы (8) предыдущаго §-а заданное сравненіе можетъ быть замѣнено слѣдующимъ, ему равносильнымъ

$$a(x-\alpha)(x-\beta)\ldots(x-\lambda) \equiv 0 \pmod p.$$

Этому послѣднему долженъ удовлетворять корень μ, и мы получаемъ сравненіе

$$a(\mu-\alpha)(\mu-\beta)\ldots(\mu-\lambda) \equiv 0 \pmod p.$$

Это же сравненіе невозможно, ибо a не дѣлится на p и ни одна изъ разностей

$$\mu - \alpha,\ \mu - \beta,\ \mu - \gamma,\ \ldots,\ \mu - \lambda$$

не равна нулю и не дѣлится на p, такъ какъ всѣ корни $\alpha, \beta, \ldots, \lambda, \mu$ предполагаются различными и несравнимыми по модулю p.

§ 21. Теорему предыдущаго §-а можно доказать еще слѣдующимъ образомъ. Если мы предположимъ, что сравненіе

$$f(x) \equiv 0 \pmod{p}$$

степени n имѣетъ больше n рѣшеній, то, обозначая одинъ корень черезъ α и поступая, какъ сказано въ § 19, замѣтимъ, что сравненіе

$$f_1(x) \equiv 0 \pmod{p}$$

должно удовлетворяться всѣми остальными корнями $\beta, \gamma, \ldots$, и слѣдовательно, будучи степени $n-1$-ой, должно имѣть болѣе, чѣмъ $n-1$ корень.

Продолжая далѣе, прійдемъ къ заключенію, что сравненіе первой степени

$$ax - b \equiv 0 \pmod{p}\ .$$

должно имѣть больше одного рѣшенія, что невозможно, ибо по нашему предположенію коэффиціентъ a не дѣлится на p.

§ 22. *Если сравненіе степени n имѣетъ болѣе n корней, то оно должно обращаться въ тождественное сравненіе, у котораго всѣ коэффиціенты дѣлятся на модуль*, и слѣдовательно это сравненіе имѣетъ мѣсто при всякомъ численномъ значеніи x.

Изъ этого соображенія можно вывести формулу (8) § 19. Въ самомъ дѣлѣ, обозначая черезъ $\alpha, \beta, \ldots, \lambda$ n корней сравненія n-ой степени

$$f(x) \equiv 0 \pmod{p},$$

мы замѣтимъ, что эти же корни будутъ корнями такого новаго сравненія

$$f(x) - a(x-\alpha)(x-\beta)\ \ldots\ (x-\lambda) \equiv 0 \pmod{p},$$

гдѣ a коэффиціентъ при старшей степени x въ функціи $f(x)$. Но это сравненіе, очевидно, степени меньшей n, ибо сокращаются члены степени n. Итакъ, это послѣднее сравненіе имѣетъ больше корней, чѣмъ единицъ въ показателѣ степени, слѣдовательно, его первая часть должна имѣть видъ $p\varphi(x)$, гдѣ $\varphi(x)$ цѣлая функція съ цѣлыми коэффиціентами.

§ 23. Положимъ, что сравненіе

$$f(x) \equiv 0 \pmod{p} \tag{1}$$

имѣетъ столько корней, сколько единицъ въ показателѣ степени, и положимъ, что кромѣ того $f(x) = \varphi(x).\psi(x)$, гдѣ φ и ψ цѣлыя функціи съ цѣлыми коэффиціентами. Тогда каждое изъ двухъ сравненій

$$\varphi(x) \equiv 0 \pmod{p}, \quad \psi(x) \equiv 0 \pmod{p} \tag{2}$$

должно имѣть столько корней, сколько единицъ въ показателѣ его степени.

Въ самомъ дѣлѣ, если α есть корень сравненія (1), то $f(\alpha)$ дѣлится на p. Но произведеніе $\varphi(\alpha).\psi(\alpha)$ тогда и только тогда дѣлится на p, когда по крайней мѣрѣ одинъ изъ множителей $\varphi(\alpha)$ или $\psi(\alpha)$ дѣлится на p. Слѣдовательно число α должно быть непремѣнно корнемъ одного изъ сравненій (2).

Допустимъ, что первое изъ сравненій (2), т. е.

$$\varphi(x) \equiv 0 \pmod{p}$$

имѣетъ меньше корней, чѣмъ единицъ въ показателѣ его степени. Тогда всѣ остальные корни сравненія (1) должны быть корнями другого сравненія (2), т. е.

$$\psi(x) \equiv 0 \pmod{p},$$

и вышло бы, что сравненіе это

$$\psi(x) \equiv 0 \pmod{p}$$

имѣетъ больше корней, чѣмъ единицъ въ его степени, что невозможно. Итакъ, *если сравненіе* (1) *имѣетъ максимальное число корней, то такое же число корней имѣютъ оба сравненія* (2).

§ 24. На основаніи теоремы Fermat'a мы замѣчаемъ, что сравненіе

$$x^{p-1} - 1 \equiv 0 \pmod{p}$$

имѣетъ $p-1$ рѣшеній

$$1, 2, 3, \ldots, p-1.$$

Тѣ же рѣшенія будетъ имѣть сравненіе

$$x^{p-1} - 1 - (x-1)(x-2)\ldots(x-p+1) \equiv 0 \pmod{p}.$$

Но это сравненіе степени $p-2$, слѣдовательно, всѣ коэффиценты въ первой части должны дѣлиться на p. Послѣдній коэффиціентъ даетъ сравненіе

$$-1 - 1.2.3\ldots(p-1) \equiv 0 \pmod{p},$$

откуда получается справедливость слѣдующаго сравненія

$$1.2.3\ldots(p-1)\equiv -1 \pmod p.$$

Свойство, выражаемое послѣднимъ сравненіемъ, представляетъ весьма важную теорему, указанную въ первый разъ Wilson'омъ. Теорема Wilson'а замѣчательна тѣмъ, что она характеризуетъ простое число p, т. е., если мы скажемъ, что число

$$1.2.3\ldots(p-1)+1 \tag{1}$$

дѣлится на p, то число p необходимо должно быть простымъ.

Въ самомъ дѣлѣ, допустимъ, что число p не простое, а что оно заключаетъ нѣкотораго дѣлителя q. Такъ какъ число

$$q<p,$$

то оно должно заключаться въ рядѣ чиселъ

$$1, 2, 3, \ldots, p-1.$$

Значитъ, при дѣленіи числа (1) на q должна получаться въ остаткѣ единица, и слѣдовательно, число (1) не можетъ дѣлиться на q и тѣмъ болѣе на p.

§ 25. Дальнѣйшее заключеніе изъ соображеній предыдущаго параграфа состоитъ въ томъ, что если мы обозначимъ

$$(x-1)(x-2)\ldots(x-p+1)=x^{p-1}+q_1x^{p-2}+q_2x^{p-3}+\ldots+q_{p-2}x+q_{p-1},$$

то всѣ коэффиціенты

$$q_1, q_2, \ldots, q_{p-2}, \tag{1}$$

кромѣ послѣдняго дѣлятся на p.

Разсмотримъ теперь

$$S_k=1^k+2^k+3^k+\ldots+(p-1)^k.$$

На основаніи извѣстныхъ изъ алгебры формулъ Newton'а мы замѣчаемъ, что всѣ

$$S_1, S_2, S_3, \ldots, S_{p-2}$$

должны дѣлиться на p, ибо эти выраженія представляются цѣлыми функціями отъ коэффиціентовъ (1) съ цѣлыми коэффиціентами.

Отсюда имѣемъ рядъ сравненій

$$S_1\equiv 0 \pmod p;\ S_2\equiv 0 \pmod p;\ \ldots;\ S_{p-2}\equiv 0 \pmod p.$$

Но такъ какъ $p-1$-я степень всякаго числа сравнима съ единицей, то вытекаетъ, что

$$S_{p-1}\equiv p-1 \pmod p.$$

Слѣдовательно, можно высказать такое предложеніе, что

$$S_k \equiv 0 \pmod p ,$$

если k не дѣлится на $p-1$, и имѣетъ мѣсто сравненіе

$$S_k \equiv p-1 \pmod p$$

при k дѣлящемся на $p-1$.

§ 26. Мы видѣли уже, что сравненіе

$$x^{p-1} - 1 \equiv 0 \pmod p \qquad (1)$$

имѣетъ рѣшеніями числа $1, 2, 3, \ldots p-1$. Если мы умножимъ сравненіе (1) на x, то получимъ сравненіе

$$x^p - x \equiv 0 \pmod p ,$$

которое удовлетворяется всѣми классами

$$0, 1, 2, \ldots p-1 .$$

§ 27. Дѣлимъ функцію $f(x)$ если ея степень больше p, на функцію $x^p - x$; пусть частное отъ этого дѣленія будетъ $Q(x)$, а остатокъ степени меньшей p будетъ $R(x)$, тогда имѣемъ тождество

$$f(x) = (x^p - x)Q\,x) + R(x) .$$

Получаемъ сравненіе

$$f(x) \equiv (x^p - x)Q(x) + R(x) \pmod p ,$$

но $x^p - x \equiv 0 \pmod p$ при всѣхъ значеніяхъ x, слѣдовательно, сравненіе

$$f(x) \equiv 0 \pmod p$$

степени большей p можетъ быть замѣнено всегда сравненіемъ

$$R(x) \equiv 0 \pmod p$$

степени меньшей p.

§ 28. Напримѣръ $f(x) = x^4 + 1$, $p = 3$, тогда мы имѣемъ

$$x^4 + 1 = (x^3 - x)x + x^2 + 1 .$$

Слѣдовательно сравненіе

$$x^4 + 1 \equiv 0 \pmod 3$$

можно замѣнить такимъ

$$x^2 + 1 \equiv 0 \pmod 3 .$$

§ 29. На основаніи сказаннаго въ § 27 можно ограничиться разсмотрѣніемъ сравненій степеней не высшихъ $p-1$.

Теорема. Сравненіе $f(x) \equiv 0 \pmod p$ степени не выше $p-1$ тогда и только тогда имѣетъ максимальное число корней, когда въ остаткѣ отъ дѣленія на $f(x)$ двучлена $x^p - x$ получается полиномъ, всѣ коэффиціенты котораго дѣлятся на p.

Въ самомъ дѣлѣ, положимъ что сравненіе $f(x) \equiv 0 \pmod p$ имѣетъ максимальное число корней. Если степень сравненія есть m, то пусть корни его будутъ

$$a_1, \; a_2, \; \ldots \; a_m. \tag{1}$$

Тогда, дѣля $x^p - x$ на $f(x)$, получимъ частное $Q(x)$ и остатокъ $R(x)$, такъ что будетъ имѣть мѣсто тождество

$$x^p - x = f(x)Q(x) + R(x). \tag{2}$$

Но такъ какъ корни (1) удовлетворяютъ двумъ сравненіямъ

$$x^p - x \equiv 0 \pmod p \quad \text{и} \quad f(x) \equiv 0 \pmod p,$$

то они тоже удовлетворяютъ и сравненію

$$R(x) \equiv 0 \pmod p. \tag{3}$$

На основаніи § 22 мы замѣчаемъ, что всѣ коэффиціенты многочлена $R(x)$ должны дѣлиться на p, ибо сравненіе (3) имѣетъ m корней (1), тогда какъ степень его меньше m.

Обратно, если предположить, что всѣ коэффиціенты $R(x)$ дѣлятся на p, то на основаніи тождества (2) получаемъ

$$x^p - x \equiv f(x)Q(x) \pmod p.$$

Мы замѣчаемъ, что сравненіе

$$f(x)Q(x) \equiv 0 \pmod p$$

имѣетъ p, то есть максимальное число корней. Значитъ и оба сравненія

$$f(x) \equiv 0 \pmod p, \quad Q(x) \equiv 0 \pmod p$$

имѣютъ максимальное число корней, и теорема доказана вполнѣ.

§ 30. Такъ, напримѣръ, сравненіе

$$x^3 - x^2 - 2x \equiv 0 \pmod 5$$

имѣетъ три корня, ибо остатокъ отъ дѣленія $x^5 - x$ на $x^3 - x^2 - 2x$ будетъ $5x^2 + 5x$.

ГЛАВА IV.

Теорія вычетовъ степеней.

§ 1. Возьмемъ нѣкоторое число a, взаимно простое съ модулемъ k. Будемъ разсматривать рядъ степеней числа a

$$1, a, a^2, a^3, \ldots \tag{1}$$

Такъ какъ всѣ числа этого ряда взаимно простыя съ k, то, слѣдовательно, и вычеты всѣхъ степеней числа a должны быть простыми съ k. Но число такихъ вычетовъ конечное и равно $\varphi(k)$, а слѣдовательно, среди чиселъ ряда (1) должны быть числа, сравнимыя по модулю k, и, слѣдовательно, при нѣкоторыхъ цѣлыхъ числахъ n и ν должно имѣть мѣсто сравненіе

$$a^{n+\nu} \equiv a^{\nu} \pmod{k}.$$

Но такъ какъ a простое съ k, то, сокращая сравненіе на a^{ν}, получимъ

$$a^{n} \equiv 1 \pmod{k}. \tag{2}$$

Итакъ, мы видимъ, что существуетъ такое цѣлое число n, при которомъ имѣетъ мѣсто сравненіе (2).

Очевидно, что чиселъ, подобныхъ n, можетъ быть безчисленное множество, ибо, возвышая сравненіе (2) въ произвольную степень l, получимъ

$$a^{nl} \equiv 1 \pmod{k}.$$

Слѣдовательно, всякая степень a, показатель которой кратное n, будетъ имѣть вычетомъ единицу.

Обозначимъ черезъ m наименьшее положительное число, при которомъ имѣетъ мѣсто сравненіе

$$a^{m} \equiv 1 \pmod{k}.$$

Мы будемъ говорить, что *число a принадлежитъ по модулю k къ показателю m.*

Показатель m обладаетъ слѣдующимъ очень важнымъ свойствомъ. *Всѣ числа*

$$1, a, a^2, a^3, \ldots, a^{m-1}$$

не сравнимы между собой по модулю k.

Въ самомъ дѣлѣ, допустивъ обратное, что

$$a^\alpha \equiv a^\beta \pmod{k},$$

гдѣ $m > \alpha > \beta$, получаемъ, что

$$a^{\alpha-\beta} \equiv 1 \pmod{k},$$

и выходило бы, что число a принадлежитъ къ показателю, меньшему m, что невозможно.

Единственныя степени a, дающія вычеты, равные единицѣ, будутъ

$$a^m, a^{2m}, a^{3m}, \ldots$$

На основаніи теоремы Euler'a

$$a^{\varphi(k)} \equiv 1 \pmod{k}$$

мы замѣчаемъ, что показатель $\varphi(k)$ долженъ быть кратнымъ m. Отсюда получается такое предложеніе: *число a, взаимно простое съ k, принадлежитъ всегда къ такому показателю m, который есть дѣлитель числа $\varphi(k)$.*

По примѣру Euler'a [1]) мы будемъ называть *первообразнымъ корнемъ* числа k такое число a, которое принадлежитъ къ наибольшему изъ возможныхъ показателей, т. е. къ показателю $\varphi(k)$. Другими словами, *первообразный корень есть такое число, у котораго наименьшая степень, сравнимая съ единицей, есть $\varphi(k)$.*

§ 2. Не трудно убѣдиться, что *первообразные корни не существуютъ для большинства составныхъ чиселъ.*

Въ самомъ дѣлѣ, возьмемъ число

$$k = p^\alpha q^\beta r^\gamma \ldots,$$

гдѣ p, q, r . . . различныя простыя числа.

---

[1]) Euler, Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia. Novae Comentationes.

Пусть a будетъ первообразный корень числа k; тогда имѣемъ рядъ сравненій

$$a^{\varphi(p^\alpha)} \equiv 1 \pmod{p^\alpha},$$
$$a^{\varphi(q^\beta)} \equiv 1 \pmod{q^\beta},$$
$$\ldots\ldots\ldots$$

Обозначимъ черезъ s наименьшее кратное всѣхъ чиселъ

$$\varphi(p^\alpha) = p^{\alpha-1}(p-1),$$
$$\varphi(q^\beta) = q^{\beta-1}(q-1),$$
$$\varphi(r^\gamma) = r^{\gamma-1}(r-1),$$
$$\ldots\ldots\ldots$$

Тогда мы, очевидно, получимъ рядъ сравненій

$$a^s \equiv 1 \pmod{p^\alpha},\ a^s \equiv 1 \pmod{q^\beta},\ a^s \equiv \pmod{r^\gamma},\ \ldots$$

Такъ какъ модули p^α, q^β, r^γ, ... взаимно простые, то имѣетъ мѣсто сравненіе

$$a^s \equiv 1 \pmod{k}$$

(см. свойство XII сравненій).

Не трудно показать, что во многихъ случаяхъ число

$$s < \varphi(k),$$

и, слѣдовательно, a не можетъ быть первообразнымъ корнемъ.

Такъ, напримѣръ, наименьшее кратное S, чиселъ $\varphi(p^\alpha)$, $\varphi(q^\beta)$, ... будетъ меньше ихъ произведенія, т. е. $\varphi(k)$, если два какія-нибудь изъ этихъ чиселъ будутъ имѣть общаго дѣлителя. Такой случай произойдетъ, если въ составъ числа k входятъ, по крайней мѣрѣ, два нечетныхъ простыхъ числа p и q, ибо тогда $\varphi(p^\alpha)$ и $\varphi(q^\beta)$ числа четныя и имѣютъ общаго множителя 2.

Кромѣ того, не существуетъ первообразныхъ корней, если въ k входитъ одно нечетное простое число и степень простого числа 2, большая единицы, ибо тогда $\varphi(2^\lambda)$ будетъ число четное, такъ какъ

$$\varphi(2^\lambda) = 2^{\lambda-1}.$$

Чтобы докончить разборъ всѣхъ случаевъ, необходимо разсмотрѣть еще предположеніе

$$k = 2^\nu.$$

Въ этомъ случаѣ

$$\varphi(k) = 2^{\nu-1}.$$

Число a, будучи взаимно-простымъ съ k, должно быть нечетнымъ, и слѣдовательно, оно можетъ быть представлено въ такомъ видѣ:

$$a = \pm 1 + 2^2 l,$$

гдѣ l нѣкоторое цѣлое число.

Возвышая въ квадратъ, получимъ

$$a^2 = 1 + 2^3 l_1,$$

гдѣ l_1 новое цѣлое число.

Возвышая далѣе въ квадратъ, получимъ

$$a^{2^2} = 1 + 2^4 l_2.$$

Продолжая далѣе, мы придемъ къ раненству

$$a^{2^{\nu-2}} = 1 + 2^\nu l_{\nu-2}.$$

Но

$$2^{\nu-2} = \frac{\varphi(k)}{2}.$$

Слѣдовательно, мы имѣемъ

$$a^{\frac{1}{2}\varphi(k)} \equiv 1 \pmod{k},$$

и, слѣдовательно, число a не можетъ быть первообразнымъ корнемъ числа k при ν не меньшемъ 2.

Единственное исключеніе будетъ составлять случай

$$\nu = 2.$$

Въ этомъ случаѣ число 4 имѣетъ первообразный корень 3, ибо

$$\varphi(4) = 2$$

и

$$3^2 \equiv 1 \pmod{4}.$$

Резюмируя все сказанное, мы получаемъ слѣдующую теорему:

Число k можетъ имѣть первообразные корни только въ слѣдующихъ случаяхъ:

1) оно есть нечетное простое число или его степень;

2) оно есть удвоенная степень нечетнаго простого числа

и 3) $k = 4$.

§ 3. Приступимъ теперь къ разсмотрѣнію первообразныхъ корней нѣкотораго простого числа p.

На основаніи соображеній § 1 показатель, къ которому принадлежитъ нѣкоторое число a, не дѣлящееся на простое число p, долженъ быть дѣлителемъ числа $p-1$. Разсмотримъ какой нибудь изъ такихъ дѣлителей δ. Тогда число a должно быть корнемъ сравненія

$$x^\delta \equiv 1 \pmod p . \qquad (1)$$

Не трудно убѣдиться, что сравненіе (1) имѣетъ δ корней. Въ самомъ дѣлѣ, сравненіе

$$x^{p-1} - 1 \equiv 0 \pmod p \qquad (2)$$

на основаніи теоремы Fermat'a имѣетъ столько корней, сколько единицъ въ показателѣ степени, но это сравненіе (2) можетъ быть переписано въ такомъ видѣ

$$(x^\delta - 1)\psi(x) \equiv 0 \pmod p ,$$

гдѣ $\psi(x)$ цѣлая функція отъ x съ цѣлыми коэффиціентами.

На основаніи § 7 гл. IV мы замѣчаемъ, что максимальное число корней должно имѣть сравненіе

$$x^\delta - 1 \equiv 0 \pmod p ,$$

что и требовалось показать.

Обратимся теперь къ вопросу, будетъ ли всякій корень сравненія (1) принадлежать къ показателю δ, а не къ какому-либо меньшему.

Допустимъ, что среди корней существуетъ одинъ a, принадлежащій къ показателю δ. Тогда очевидно, что корни сравненія (1) будутъ представляться числами $1, a, a^2, a^3, \ldots, a^{\delta-1}$.

Никакихъ другихъ корней сравненіе (1) имѣть не будетъ. Посмотримъ, къ какому показателю будетъ принадлежать нѣкоторый корень a^r. Обозначимъ черезъ h этого показателя; тогда

$$a^{rh} \equiv 1 \pmod p ,$$

и слѣдовательно, rh должно быть кратнымъ числа δ.

Обозначимъ черезъ k общаго наибольшаго дѣлителя чиселъ r и δ, такъ что $r = kr_1$, $\delta = k\delta_1$, гдѣ r_1 и δ_1 числа взаимно простыя. Тогда число $rh = kr_1 h$ должно дѣлиться на $k\delta_1$, и слѣдовательно, $r_1 h$ должно дѣлиться на δ_1, откуда вытекаетъ, что h должно дѣлиться на δ_1, и мы получаемъ, слѣдовательно, при $h = \delta_1$

$$a^{r\delta_1} = a^{kr_1\delta_1} = a^{r_1\delta} = (a^\delta)^{r_1} \equiv 1 \pmod p ,$$

и, слѣдовательно, оказывается

$$(a^r)^{\delta_1} \equiv 1 \pmod p ,$$

т. е. число a^r принадлежитъ къ показателю δ_1, меньшему δ.

Отсюда мы замѣчаемъ, что степень a^r будетъ принадлежать къ показателю δ только въ томъ случаѣ, когда $k = 1$, т. е. показатель r есть число взаимно простое съ δ.

Такимъ образомъ мы видимъ, что изъ чиселъ ряда $1, a^2, a^3, \ldots, a^{\delta-1}$, дающихъ всѣ рѣшенія сравненія

$$x^\delta \equiv 1 \pmod{p},$$

принадлежатъ показателю δ только тѣ, у которыхъ показатели взаимно простые съ δ. Слѣдовательно, *число чиселъ, принадлежащихъ къ показателю* δ, *должно быть* $\varphi(\delta)$, *если только существуетъ одно изъ такихъ чиселъ*.

Такимъ образомъ, обозначая черезъ $\psi(\delta)$ число чиселъ, принадлежащихъ дѣйствительно къ показателю δ, получаемъ одно изъ двухъ: или

$$\psi(\delta) = \varphi(\delta),$$

или

$$\psi(\delta) = 0.$$

Разсмотримъ числа $1, 2, \ldots, p-1$. Каждое изъ этихъ чиселъ будетъ принадлежать къ нѣкоторому показателю, который будетъ дѣлителемъ числа $p-1$. Поэтому, разсматривая всю сумму

$$\sum \psi(\delta),$$

распространенную на всѣхъ дѣлителей δ числа $p-1$, мы замѣчаемъ, что эта сумма равна $p-1$, ибо при счетѣ числа чиселъ, принадлежащихъ каждому показателю, каждое изъ чиселъ ряда $1, 2, \ldots, p-1$ встрѣтится одинъ разъ, и мы имѣемъ равенство

$$\sum \psi(\delta) = p - 1.$$

Но мы видѣли уже (см. § 26 гл. II) справедливость равенства

$$\sum \varphi(\delta) = p - 1.$$

Отсюда получаемъ

$$\sum \psi(\delta) = \sum \varphi(\delta).$$

Каждый изъ членовъ лѣвой части или равняется соотвѣтствующему члену правой, или же равенъ нулю. Но второе предположеніе невозможно, ибо, при равенствѣ нулю котораго либо члена лѣвой части, въ правой части остается лишній положительный членъ, и равенство перестаетъ быть возможнымъ.

Отсюда получаемъ окончательное равенство

$$\psi(\delta) = \varphi(\delta),$$

справедливое для всѣхъ дѣлителей числа $p-1$.

§ 4. Соображенія предыдущаго параграфа указываютъ не только на существованіе первообразныхъ корней для всякаго простого числа p, но, кромѣ того, приводятъ къ заключенію, что такихъ первообразныхъ корней будетъ $\varphi(p-1)$.

§ 5. Возьмемъ какой нибудь первообразный корень g простого числа p. Тогда степени

$$g,\ g^2,\ g^3,\ \ldots,\ g^{p-1} \equiv 1 \pmod p \qquad (1)$$

будутъ несравнимы между собой по модулю p, а потому всякое произвольно взятое число a, не сравнимое съ нулемъ по модулю p, будетъ сравнимо по модулю p съ однимъ изъ чиселъ нашего ряда (1), такъ что для всякаго числа будетъ существовать показатель α, удовлетворяющій сравненію

$$a \equiv g^\alpha \pmod p.$$

Мы будемъ называть показатель α *индексомъ* числа a и обозначать

$$\alpha = Ind\, a.$$

Изученіе индексовъ чиселъ приводитъ къ теоріи, имѣющей большую аналогію съ теоріей логарифмовъ.

Первообразный корень g называется *основаніемъ* индексовъ.

§ 6. Для всякаго простого числа p можно составить таблицу индексовъ, относящихся къ которому нибудь изъ первообразныхъ корней. Такъ, напримѣръ, для простого числа 19 при основаніи 10 получается слѣдующая таблица:

Число	0	1	2	3	4	5	6	7	8	9
		0	17	5	16	2	4	12	15	10
1	1	6	3	13	11	7	14	8	9	

Въ 1839 году было издано сочиненіе: *Canon Arithmeticus* Jacobi, заключающее таблицы индексовъ для всѣхъ простыхъ чиселъ до 1000 [1]). (Извлеченіе изъ этихъ таблицъ помѣщено въ концѣ книги).

[1]) Таблицы Jacobi продолжены по моему предложенію студентами Кіевскаго Университета для простыхъ модулей до 2000. При вычисленіяхъ пользовались счетными машинами. Эти таблицы до сихъ поръ не опубликованы, онѣ находятся въ библіотекѣ Кіевскаго Университета.

§ 7. Докажемъ теорему, что *индексъ произведенія чиселъ*

$$A, B, C, \ldots$$

сравнимъ съ суммой индексовъ множителей по модулю $p-1$.

Въ самомъ дѣлѣ, имѣемъ рядъ сравненій

$$g^{Ind\,A} \equiv A \pmod p, \quad g^{Ind\,B} \equiv B \pmod p, \quad g^{Ind\,C} \equiv C \pmod p, \quad \ldots$$

Перемножая эти сравненія, получимъ

$$g^{Ind\,A + Ind\,B + Ind\,C + \cdots} \equiv ABC \ldots \pmod p.$$

Но, съ другой стороны

$$g^{Ind\,(ABC\ldots)} \equiv ABC \ldots \pmod p.$$

Раздѣляя, получимъ

$$g^{Ind\,A + Ind\,B + Ind\,C + \ldots - Ind\,(ABC\ldots)} \equiv 1 \pmod p.$$

Но g есть первообразный корень; слѣдовательно, показатель

$$Ind\,A + Ind\,B + Ind\,C + \ldots - Ind\,(ABC\ldots)$$

дѣлится на $p-1$, и мы получаемъ сравненіе, выражающее справедливость теоремы

$$Ind\,(ABC\ldots) \equiv Ind\,A + Ind\,B + Ind\,C + \ldots \pmod{p-1}.$$

Какъ слѣдствіе изъ этой теоремы, получается, что

$$Ind\,(A^n) \equiv n\,Ind\,A \pmod{p-1},$$

§ 8. Какой бы изъ первообразныхъ корней числа p ни былъ взятъ за основаніе индексовъ, *индексъ единицы равенъ нулю*. Подобнымъ же образомъ *индексъ числа* -1 *одинъ и тотъ же для всякаго* g *и равенъ* $\frac{p-1}{2}$ *(за исключеніемъ* $p=2$).

Въ самомъ дѣлѣ, сравненіе $g^{p-1} - 1 \equiv 0 \pmod p$ можетъ быть переписано такъ

$$(g^{\frac{p-1}{2}} - 1)(g^{\frac{p-1}{2}} + 1) \equiv 0 \pmod p,$$

и мы видимъ, слѣдовательно, что дѣлится на p одинъ изъ множителей

$$g^{\frac{p-1}{2}} - 1, \quad g^{\frac{p-1}{2}} + 1.$$

Но сравненіе

$$g^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$$

невозможно, ибо въ противномъ случаѣ число g не было бы первообразнымъ корнемъ, такъ какъ степень числа g съ показателемъ, меньшимъ $p-1$, была бы сравнима съ единицей.

Итакъ, имѣетъ мѣсто сравненіе

$$g^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p},$$

и слѣдовательно,

$$g^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

откуда

$$Ind\ (-1) = \frac{p-1}{2},$$

причемъ это равенство не зависитъ отъ выбора основанія g.

§ 9. Подобно теоріи логариѳмовъ, теоріи индексовъ упрощаетъ значительно выкладки въ разныхъ вопросахъ теоріи чиселъ.

Въ видѣ примѣра возьмемъ задачу рѣшенія сравненія первой степени.

Положимъ, требуется рѣшить сравненіе

$$8x + 13 \equiv 0 \pmod{19}.$$

Переписываемъ это такъ

$$8x \equiv -13 \pmod{19},$$

или иначе

$$8x \equiv 6 \pmod{19},$$

откуда

$$Ind\ x + Ind\ 8 \equiv Ind\ 6 \pmod{18}$$

и

$$Ind\ x \equiv Ind\ 6 - Ind\ 8 \pmod{18}.$$

Изъ таблицы индексовъ получаемъ

$$Ind\ x \equiv 4 - 15 \pmod{18},$$

$$Ind\ x \equiv -11 \pmod{18},$$

$$Ind\ x \equiv 7 \pmod{18}.$$

Отсюда

$$x \equiv 15 \pmod{19}.$$

§ 10. Приложимъ теорію индексовъ къ рѣшенію двучленныхъ сравненій вида

$$x^n \equiv q \pmod{p}, \tag{1}$$

гдѣ p простое число.

Обозначимъ черезъ ξ индексъ искомаго числа x; получаемъ

$$n\xi \equiv Ind\, q \pmod{p-1} \tag{2}$$

Если n число взаимно простое съ $p-1$, то сравненіе (2), первой степени относительно ξ, дастъ одно рѣшеніе, и слѣдовательно, также заданное двучленное сравненіе (1) имѣетъ одно рѣшеніе.

Обозначимъ теперь черезъ δ общаго наибольшаго дѣлителя чиселъ n и $p-1$; тогда необходимымъ условіемъ для возможности сравненія (2), а слѣдовательно, и сравненія (1), будетъ (см. § 3 главы III)

$$Ind\, q \equiv 0 \pmod{\delta}. \tag{3}$$

Если условіе (3) выполнено, тогда на основаніи соображеній § 15 гл. III сравненіе (2) имѣетъ δ рѣшеній, а слѣдовательно, δ рѣшеній будетъ имѣть и заданное сравненіе (1).

Условіе (3) должно, очевидно, имѣть мѣсто независимо отъ выбора основанія g таблицы индексовъ, поэтому представимъ его въ другой формѣ. Сравненіе (3) даетъ

$$Ind\, q = \delta\varepsilon,$$

гдѣ ε цѣлое число. Итакъ, имѣемъ

$$q \equiv g^{\delta\varepsilon} \pmod{p}.$$

Возвысимъ это сравненіе въ степень $\frac{p-1}{\delta}$, тогда получимъ

$$q^{\frac{p-1}{\delta}} \equiv g^{(p-1)\varepsilon} \equiv 1 \pmod{p}.$$

Итакъ, условіе, необходимое и достаточное для существованія δ рѣшеній сравненія (1), состоитъ въ справедливости сравненія

$$q^{\frac{p-1}{\delta}} \equiv 1 \pmod{p}. \tag{4}$$

Если сравненіе (4) не удовлетворяется, то двучленное сравненіе (1) не имѣетъ рѣшенія.

§ 11. При $q = 1$ сравненіе (4) предыдущаго §-а всегда удовлетворяется, слѣдовательно, сравненіе

$$x^n \equiv 1 \pmod{p} \qquad (1)$$

имѣетъ всегда δ рѣшеній.

Если n есть дѣлитель числа $p-1$, т. е. $\delta = n$, то сравненіе (1) имѣетъ n рѣшеній. Это мы видѣли уже изъ другихъ соображеній.

§ 12. Примѣнимъ нашу теорію къ рѣшенію сравненія

$$x^{12} \equiv 13 \pmod{17}. \qquad (1)$$

Составляемъ таблицу индексовъ для модуля 17 при основаніи 10:

N	0	1	2	3	4	5	6	7	8	9
		0	10	11	4	7	5	9	14	6
1	1	13	15	12	3	2	8			

Имѣемъ

$$12\ Ind\ x \equiv 12 \pmod{16} \qquad (2)$$

или, сокращая на 4

$$3\ Ind\ x \equiv 3 \pmod{4}$$

или

$$Ind\ x \equiv 1 \pmod{4}.$$

Отсюда получаемъ слѣдующихъ четыре рѣшенія сравненія (2):

$$Ind\ x \equiv 1 \pmod{16},$$
$$Ind\ x \equiv 5 \pmod{16},$$
$$Ind\ x \equiv 9 \pmod{16},$$
$$Ind\ x \equiv 13 \pmod{16}.$$

Отсюда по таблицѣ индексовъ получаемъ слѣдующія четыре рѣшенія заданнаго сравненія (1)

$$x \equiv 10 \pmod{17},$$
$$x \equiv 6 \pmod{17},$$
$$x \equiv 7 \pmod{17},$$
$$x \equiv 11 \pmod{17}.$$

Способъ Коркина рѣшенія двучленныхъ сравненій.

§ 13. Въ связи съ теоріей первообразныхъ корней и индексовъ находится метода рѣшенія двучленныхъ сравненій, предложенная Коркинымъ въ его посмертномъ мемуарѣ, напечатанномъ въ Московскомъ Математическомъ сборникѣ [1]) подъ заглавіемъ „*О распредѣленіи цѣлыхъ чиселъ по простому модулю и о двучленныхъ сравненіяхъ, съ таблицей первообразныхъ корней и характеровъ, къ нимъ относящихся, для простыхъ чиселъ, меньшихъ 4000*“.

Метода Коркина основана на введеніи нѣкоторыхъ чиселъ, которыя онъ называетъ *характерами*.

При помощи таблицы этихъ характеровъ получается способъ находить рѣшенія двучленныхъ сравненій, степень которыхъ есть дѣлитель $p-1$, гдѣ p есть простой модуль, по которому разсматривается сравненіе.

Таблица Коркина, составленная для простыхъ чиселъ меньшихъ 4000 была продолжена пр. К. Поссе до 10000 [2]). Въ виду того, что наибольшая таблица индексовъ до сихъ поръ публикованная Canon Arithmeticus Jacobi идетъ лишь до 1000 и что едва ли можно ожидать въ скоромъ времени составленія и изданія таблицъ индексовъ до 10000, таблица Коркина и Поссе будетъ очень полезною для рѣшенія двучленныхъ сравненій.

Мы приводимъ въ концѣ книги извлеченіе изъ этой таблицы, идущее до 2000.

§ 14. Будемъ разсматривать лишь такія сравненія

$$x^\delta \equiv a \pmod p \tag{1}$$

гдѣ δ дѣлитель числа $p-1$. Мы видѣли уже, что условіемъ необходимымъ и достаточнымъ для существованія рѣшеній сравненія (1) будетъ справедливость сравненія

$$a^{\frac{p-1}{\delta}} \equiv 1 \pmod p \tag{2}$$

Если сравненіе (2) не удовлетворяется, то сравненіе (1) не имѣетъ рѣшеній относительно x, и число a называется *невычетомъ степени δ простого числа p*. Если же сравненіе (2) имѣетъ мѣсто, то сравненіе (1) имѣетъ δ корней и число a носитъ названіе *вычета степени δ простого числа p*. При $\delta = 2$ вычетъ и невычетъ называются *квадратичными*.

---

[1]) Томъ двадцать седьмой. Выпускъ первый. Стр. 28—137. 1909.

[2]) Математическій сборникъ. Москва, а также Acta mathematica t. 35.

§ 15. Очевидно, что можно ограничиться разсмотрѣніемъ случая $b = q$, гдѣ q простое число, входящее въ составъ $p - 1$.

Сравненіе

$$x^q \equiv a \pmod p \tag{1}$$

будетъ имѣть q корней, если

$$a^{\frac{p-1}{q}} \equiv 1 \pmod p.$$

Въ теоріи двучленныхъ сравненій по простому модулю существуетъ полная аналогія съ алгебраической теоріей двучленныхъ уравненій, а именно, въ алгебрѣ, двучленное уравненіе $x^q = a$ имѣетъ q корней, изъ которыхъ достаточно знать одинъ, который можно обозначить черезъ $\sqrt[q]{a}$, остальные корни будутъ имѣть видъ

$$t_1 \sqrt[q]{a},\ t_2 \sqrt[q]{a},\ \ldots\ t_{q-1} \sqrt[q]{a},$$

гдѣ $t_1, t_2, \ldots t_{q-1}$ будутъ мнимыми корнями уравненія $t^q = 1$, причемъ можно положить $t_2 = t_1^2$, $t_3 = t_1^3$, $\ldots\ t_{q-1} = t_1^{q-1}$.

Подобное свойство существуетъ у сравненій (1), а именно если извѣстно одно рѣшеніе сравненія (1) α, то $q - 1$ другихъ получается въ видѣ

$$\alpha u_1,\ \alpha u_2,\ \ldots\ \alpha u_{q-1},$$

гдѣ $u_1, u_2, \ldots u_{q-1}$ суть рѣшенія, отличныя отъ единицы, сравненія

$$x^q \equiv 1 \pmod p. \tag{2}$$

Такъ же какъ и при уравненіяхъ, имѣютъ мѣсто сравненія

$$u_2 \equiv u_1^2,\ u_3 \equiv u_1^3,\ \ldots\ u_{q-1} \equiv u_1^{q-1},$$

ибо, если сравненіе (2) имѣетъ корень u_1, то и всякая степень этого корня есть корень сравненія.

Коркинъ предлагаетъ называть корни

$$u_0 \equiv 1,\ u_1,\ u_2,\ \ldots\ u_{q-1}$$

сравненія (2) *главными характерами*.

Очевидно, что число

$$a^{\frac{p-1}{q}}$$

будучи корнемъ сравненія (2), будетъ сравнимо съ однимъ изъ главныхъ характеровъ

$$a^{\frac{p-1}{q}} \equiv u_r \pmod p. \tag{3}$$

Число u_i есть, по Коркину, характеръ числа a въ томъ смыслѣ, что если $u_i = 1$, то a есть вычетъ степени q; при всѣхъ другихъ значеніяхъ характера число a есть невычетъ. Каждому характеру u_i соотвѣтствуетъ $\frac{p-1}{q}$ корней сравненія (3).

Такъ, напримѣръ, при $p = 43$, $q = 7$ получаемъ

Главный характеръ	Числа a соотвѣтствующія главному характеру
$u_0 = 1$	1, 6, 7, 36, 37, 42
$u_1 = 11$	4, 15, 19, 24, 28, 39
$u_2 \equiv u_1^2 \equiv 35$	10, 16, 17, 26, 27, 33
$u_3 \equiv u_1^3 \equiv 41$	3, 18, 21, 22, 25, 40
$u_4 \equiv u_1^4 \equiv 21$	2, 12, 14, 29, 31, 41
$u_5 \equiv u_1^5 \equiv 16$	5, 8, 13, 30, 35, 38
$u_6 \equiv u_1^6 \equiv 4$	9, 11, 20, 23, 32, 34

§ 16. Пусть простое число q входитъ въ $p-1$ съ показателемъ α, такъ что

$$p = q^\alpha N + 1,$$

гдѣ

$$N = qN_1 + \rho;\ 0 < \rho < q.$$

Будемъ разсматривать выраженіе

$$a^{\frac{p-1}{q^\beta}}.$$

Это выраженіе будетъ корнемъ двучленнаго уравненія

$$x^{q^\beta} - 1 \equiv 0 \pmod p,$$

Если мы обозначимъ черезъ g первообразный корень числа p, то за главные характеры можно будетъ принять вычеты чиселъ

$$u_0 \equiv g^{\frac{p-1}{q}0},\ u_1 \equiv g^{\frac{p-1}{q}1},\ u_2 \equiv g^{\frac{p-1}{q}2},\ \ldots\ u_{q-1} \equiv g^{\frac{p-1}{q}(q-1)}.$$

Если $\alpha = 1$, то главные характеры достаточны для рѣшенія двучленныхъ сравненій. Если же $\alpha > 1$, то кромѣ главныхъ характеровъ Коркинъ вводитъ въ разсмотрѣніе еще другіе характеры, которые онъ называетъ

дополнительными

$$u_i' \equiv g^{\frac{p-1}{q^2}i}, \quad u_i'' \equiv g^{\frac{p-1}{q^3}i}, \quad \ldots \quad u_i^{(\alpha-1)} \equiv g^{\frac{p-1}{q^\alpha}i}. \qquad (1)$$

гдѣ i пробѣгаетъ полную систему вычетовъ по модулю q. Характеры u_i' Коркинъ называетъ *характерами второго порядка*, характеры u_i'' — *характерами третьяго порядка* и т. д.

Различныхъ порядковъ характеровъ будетъ α. Въ своей таблицѣ для каждаго простого множителя числа $p-1$ Коркинъ дастъ по одному основному характеру каждаго порядка, изъ котораго другіе получаются возвышеніемъ въ степень.

Табличные характеры суть числа (1) при $i=1$, при чемъ нижніе значки пропускаются

$$u \equiv g^{\frac{p-1}{q}}, \quad u' \equiv g^{\frac{p-1}{q^2}}, \quad u'' \equiv g^{\frac{p-1}{q^3}}, \quad \ldots \quad u^{(\alpha-1)} \equiv g^{\frac{p-1}{q^\alpha}}.$$

§ 17. Нетрудно усмотрѣть слѣдующія свойства характеровъ

$$[u_i^{(\beta)}]^q \equiv u_i^{(\beta-1)} \qquad (1)$$

$$u_i^{(\beta)} u_{q-i}^{(\beta)} \equiv u_1^{(\beta-1)} \qquad (2)$$

$$u_0^{(\beta)} \equiv 1. \qquad (3)$$

§ 18 Изобразимъ q-адически (см. гл. II § 16) индексъ ω второй части a сравненія

$$x^q \equiv a \pmod p. \qquad (1)$$

Пусть будетъ

$$\omega = \lambda_0 + \lambda_1 q + \lambda_2 q^2 + \ldots$$

Если a есть вычетъ степени q, то на основаніи § 10 должна равняться нулю первая цифра λ_0, т. е.

$$\omega = \lambda_1 q + \lambda_2 q^2 + \ldots$$

Итакъ

$$a \equiv g^{\lambda_1 q + \lambda_2 q^2 + \ldots}$$

тогда

$$a^N \equiv g^{\frac{p-1}{q^\alpha}(\lambda_1 q + \lambda_2 q^2 + \lambda_3 q^3 + \ldots)} \equiv u_{\lambda_1}^{(\alpha-2)} u_{\lambda_2}^{(\alpha-3)} u_{\lambda_3}^{(\alpha-4)} \ldots \qquad (2)$$

Рядъ множителей обрывается на томъ мѣстѣ, гдѣ верхній значекъ характера становится нулемъ, т. е. характеръ дѣлается главнымъ. Остальные множители равны единицѣ.

Ищемъ одно изъ рѣшеній сравненія

$$\Omega^q \equiv a^N \pmod p \tag{3}$$

получаемъ

$$\Omega \equiv g^{\frac{p-1}{q^\alpha}(\lambda_1 + \lambda_2 q + \lambda_3 q^3 + \dots)} \equiv u_{\lambda_1}^{(\alpha-1)} u_{\lambda_2}^{(\alpha-2)} u_{\lambda_3}^{(\alpha-3)} \dots$$

Число Ω получается изъ (2) увеличеніемъ на единицу верхнихъ значковъ характеровъ.

Принимая обозначенія § 16 $N = qN_1 + \rho$, замѣчаемъ, что можно подобрать два цѣлыхъ числа τ и σ такъ, чтобы было

$$q\tau - \rho\sigma = 1 .$$

Перепишемъ сравненіе (1) такъ

$$x^q \equiv a^{q\tau - \rho\sigma} . \tag{4}$$

Возвысивъ далѣе обѣ части сравненія (3) въ степень σ, получимъ

$$\Omega^{q\sigma} \equiv a^{N\sigma} \equiv a^{N_1 q\sigma + \rho\sigma} . \tag{5}$$

Перемножая сравненія (4) и (5), получимъ

$$(x\Omega^\sigma)^q \equiv a^{q(N_1\sigma + \tau)} ,$$

откуда приходимъ къ сравненію первой степени

$$x\Omega^\sigma \equiv a^{N_1\sigma + \tau} . \tag{6}$$

Такимъ образомъ, одинъ изъ корней x двучленнаго сравненія (1) найденъ, остальные получатся черезъ умноженіе на главные характеры. Все дѣло сводится къ нахожденію q-адическихъ цифръ $\lambda_1, \lambda_2, \lambda_3, \dots$ индекса числа a.

§ 19. Коркинъ даетъ хорошій способъ нахожденія цифръ λ_i при помощи его таблицы.

Если задано сравненіе (1), то несомнѣнно, что надо начать дѣло съ провѣрки сравненія $a^{\frac{p-1}{q}} \equiv 1$, или иначе $a^{q^{\alpha-1}N} \equiv 1$; если это сравненіе не удовлетворяется, то и заданное невозможно.

Коркинъ предлагаетъ эту провѣрку производить при помощи послѣдовательнаго вычисленія вычетовъ по модулю p чиселъ

$$a^N , \; a^{qN} , \; a^{q^2 N} .$$

Быть можетъ единица появится раньше чѣмъ при $a^{q^{\beta-1}N}$.

Пусть будетъ

$$a^{q^{\beta}N} \equiv 1,$$

тогда

$$a^{q^{\beta-1}N} \equiv \xi_1$$

будетъ однимъ изъ главныхъ характеровъ; такъ какъ число ξ_1 у насъ уже вычислено, то остается только посмотрѣть, съ какою степенію табличнаго главнаго характера это число сравнимо.

Пусть окажется, что

$$\xi_1 \equiv u^{\lambda_1} \equiv u_{\lambda_1},$$

тогда число

$$a^{q^{\beta-2}N} \equiv \xi_2$$

будетъ корнемъ сравненія

$$\xi_2^{\,q} \equiv \xi_1$$

или сравненія

$$\xi_2^{\,q} \equiv u_{\lambda_1}.$$

Примѣняя свойство (1) § 17, получимъ

$$\xi_2 \equiv u'_{\lambda_1}\mu, \qquad (1)$$

гдѣ μ одинъ изъ главныхъ характеровъ. Такъ какъ ξ_2 и u'_{λ_1} извѣстны, ибо ξ_2 уже вычислено, а u'_{λ_1} находится по таблицѣ какъ степень табличнаго характера u', то легко найдемъ, съ какимъ изъ главныхъ характеровъ сравнимо число μ, т. е. получаемъ

$$\mu \equiv u_{\lambda_2},$$

такъ что

$$\xi_2 \equiv u'_{\lambda_1}u_{\lambda_2}.$$

Далѣе число

$$a^{q^{\beta-3}N} \equiv \xi_3$$

будетъ корнемъ сравненія

$$\xi_3^{\,q} \equiv u'_{\lambda_1}u_{\lambda_2},$$

такъ что

$$\xi_3 \equiv u''_{\lambda_1}u'_{\lambda_2}\mu', \qquad (2)$$

гдѣ μ' опять одинъ изъ главныхъ характеровъ, мы его найдемъ зная ξ_3

u''_{λ_1}, u'_{λ_2}, такъ что получится

$$\xi_3 \equiv u''_{\lambda_1} u'_{\lambda_2} u_{\lambda_3}.$$

Продолжая далѣе разсужденіе, мы придемъ, наконецъ, къ числу

$$a^{N},$$

причемъ получимъ его представленіе черезъ характеры, а значитъ и цифры λ_1, λ_2, ...

§ 20. Главные характеры μ, μ', ... опредѣляются сравненіями первой степени (1), (2), ... Для болѣе удобнаго на практикѣ рѣшенія этихъ сравненій можно воспользоваться свойствами (2) и (3) (см. § 17) характеровъ.

Такъ, напримѣръ, для рѣшенія сравненія

$$\xi_3 \equiv u''_{\lambda_1} u'_{\lambda_2} \mu'$$

относительно μ', умножаемъ обѣ части на $u''_{q-\lambda_1}$; получимъ

$$\xi_3 u''_{q-\lambda_1} \equiv u_1' u'_{\lambda_2} \mu' \equiv u'_{1+\lambda_2} \mu'.$$

Умножая далѣе на $u'_{q-1-\lambda_2}$, получимъ

$$\xi_3 u''_{q-\lambda_1} u'_{q-1-\lambda_2} \equiv u_1 \mu'$$

и наконецъ

$$\xi_3 u''_{q-\lambda_1} u'_{q-1-\lambda_2} u_{q-1} \equiv \mu'.$$

§ 21. Что касается рѣшенія квадратныхъ сравненій, т. е. случая $q = 2$, то главный характеръ

$$g^{\frac{p-1}{2}}$$

равенъ всегда -1. Очевидно, что нѣтъ надобности его приводить въ таблицѣ. Коркинъ понижаетъ на единицу верхніе значки и вводитъ для случая $q = 2$ обозначенія

$$f \equiv g^{\frac{p-1}{2^2}}, \quad f' \equiv g^{\frac{p-1}{2^3}}, \quad \ldots \quad f^{(\alpha-2)} \equiv g^{\frac{p-1}{2^\alpha}}.$$

Для случая $q = 3$, Коркинъ обозначаетъ характеры буквами

$$z, z', z'', \ldots$$

Для простыхъ множителей большихъ 3 вводятся по порядку ихъ величины обозначенія

$$u, u', \ldots; v, v', \ldots; w, w', \ldots; \ldots \text{ и т. д.}$$

§ 23. Поясним приведенную теорію примѣрами.

I примѣръ. Требуется рѣшить сравненіе

$$x^5 \equiv 121 \pmod{751}.$$

Здѣсь $p-1 = 2.3.5^3$, $\alpha = 3$, $N = 6 = 1\ 5 + 1$, $N_1 = 1$, $\rho = 1$.

Составляемъ вычетъ $a^N = 121^6$ по модулю 751. Вычисленіе производимъ такъ

$$121^2 \equiv 372;\ 121^3 \equiv 372.121 \equiv 703,\ 121^6 \equiv 703^2 \equiv 51,$$

такъ что

$$a^{N_0} \equiv 51.$$

Далѣе $a^{qN} \equiv 51^5 \equiv 80$, $a^{q^2N} \equiv 80^5 \equiv 1$.

Итакъ, сравненіе возможно и имѣетъ 5 корней.

Вычисляя вычетъ степеней даннаго въ таблицѣ характера $u = 460$, мы находимъ

$$80 \equiv 460^4 \equiv u_4.$$

Извлекая изъ обѣихъ частей корень 5-ой степени получимъ

$$51 \equiv u_4'\mu$$

или $u_1'51 \equiv u_1\mu$, или еще такъ $u_1'u_4 51 \equiv \mu$, откуда взявъ изъ таблицы $u_1' = u' = 171$ получимъ

$$\mu \equiv 80.171.51 \equiv 1,$$

такъ что

$$a^N \equiv 51 \equiv u_4'.$$

Далѣе находимъ

$$\Omega \equiv u_4'' \equiv (u'')^4 \equiv 100^4 \equiv 595.$$

Рѣшая неопредѣленное уравненіе

$$5\tau - \sigma = 1,$$

получимъ

$$\tau = 1,\ \sigma = 4.$$

Отсюда одинъ изъ корней x заданнаго сравненія найдется по сравненію (6) § 18

$$x595^4 \equiv 121^{1\cdot 4+1} \pmod{751},$$

$$43x \equiv 168 \pmod{751}.$$

Рѣшая неопредѣленное уравненіе

$$43x - 751y \equiv 168,$$

получимъ

$$x \equiv 458 \pmod{751}.$$

Остальныя рѣшенія заданнаго сравненія получатся черезъ умноженіе на степени табличнаго главнаго характера $u = 460$

$$458.460 \equiv 400;\ 400.460 \equiv 5;\ 4.460 \equiv 47;\ 47.460 \equiv 592.$$

II примѣръ. Рѣшить сравненіе

$$x^2 \equiv 569 \pmod{769}.$$

Здѣсь $p - 1 = 2^8.3$, $N = 3$, $N_1 = 1$, $\sigma = 1$, $\tau = 2$.

Дѣло сводится къ сравненію

$$x\Omega \equiv 569^2 \pmod{769}.$$

Необходимо найти Ω. Для этой цѣли представимъ $a^N \equiv 569^3 \equiv 676$ черезъ характеры.

Вычисляемъ вычеты чиселъ

$$\begin{gathered} a^N \equiv 676,\ a^{2N} \equiv 190,\ a^{2^2N} \equiv 726,\ a^{2^3N} \equiv 311, \\ a^{2^4N} \equiv 596,\ a^{2^5N} \equiv 707,\ a^{2^6N} \equiv 768 \equiv -1,\ a^{2^7N} \equiv 1. \end{gathered} \tag{1}$$

Слѣдовательно сравненіе возможно.

Такъ какъ главные характеры при $q = 2$ суть $+1$ и -1, то числа μ суть ± 1.

Итакъ

$$a^{2^5N} \equiv \pm f \equiv \pm 62, \text{ ибо } f^2 \equiv -1.$$

Сравнивая съ числами (1) получимъ знакъ —

$$a^{2^5N} \equiv -f.$$

Извлекая корень квадратный, получимъ

$$a^{2^4N} \equiv \mp ff' \equiv \pm (62.729) \equiv \pm 569.$$

Сравнивая съ (1), замѣчаемъ, что надо сохранить знакъ $+$, такъ что

$$a^{2^4N} \equiv ff'.$$

Извлекая корень квадратный, получимъ

$$a^{2^3N} \equiv \pm f'f'' \equiv \pm (27.729) \equiv \pm 458.$$

Сравнивая съ (1), ставимъ знакъ —

$$a^{2^2N} \equiv -f'f''.$$

Извлекая корень квадратный, имѣемъ

$$a^{2^2N} \equiv \pm ff''f''' \equiv \pm (62 \cdot 27 \cdot 300) \equiv \pm 43.$$

Сравнивая съ (1), получаемъ знакъ —

$$a^{2^2N} \equiv -ff''f'''.$$

Извлекая корень квадратный, получимъ

$$a^{2N} \equiv \pm ff'f'''f^{\text{IV}} \equiv \pm (62 \cdot 729 \cdot 300 \cdot 231) \equiv \pm 579,$$

надо будетъ поставить знакъ —

$$a^{2N} \equiv -ff'f'''f^{\text{IV}}$$

и, наконецъ,

$$a^{N} \equiv \pm ff'f''f^{\text{IV}}f^{\text{V}} \equiv \pm 93,$$

что даетъ знакъ —

$$a^{N} \equiv -ff'f''f^{\text{IV}}f^{\text{V}}.$$

Отсюда за Ω можно принять число

$$\Omega \equiv ff'f''f'''f^{\text{V}}f^{\text{VI}} \equiv 743.$$

Придется рѣшать сравненіе

$$743x \equiv 12 \pmod{769}$$

или, что одно и тоже, неопредѣленное уравненіе

$$743x - 769y = 12.$$

Получаемъ окончательно

$$x \equiv 177 \pmod{769}.$$

Другое рѣшеніе заданнаго квадратнаго сравненія получится черезъ умноженіе на -1.

$$x \equiv -177 \equiv 592 \pmod{769}.$$

§ 24. Способъ Коркина нуждается въ добавленіи, относящемся къ рѣшенію сравненія

$$x^n \equiv a \pmod{p} \qquad (1)$$

въ случаѣ n взаимно простого съ $p-1$.

Мы знаемъ, что въ этомъ случаѣ сравненіе (1) имѣетъ только одно рѣшеніе при всякомъ a.

Дѣлимъ число $p-1$ на n и обозначимъ черезъ ρ остатокъ этого дѣленія

$$p-1 = nM + \rho .$$

ρ будетъ числомъ взаимно простымъ съ n.

Подбираемъ два числа τ и σ такъ, чтобы было

$$n\tau - \rho\sigma = 1 .$$

Получаются два сравненія

$$x^n \equiv a^{n\tau - \rho\sigma},$$

$$1 \equiv a^{nM+\rho}.$$

Перемножая первое изъ нихъ съ σ-ою степенію второго, получимъ

$$x^n \equiv a^{n(M\sigma+\tau)}$$

или окончательно искомое рѣшеніе сравненія (1)

$$x \equiv a^{M\sigma+\tau}.$$

Примѣръ. Требуется рѣшить сравненіе

$$x^7 \equiv 100 \pmod{607} .$$

Здѣсь

$$p-1 = 606 = 7 \cdot 86 + 4 , \; 7 \cdot 3 - 5 \cdot 4 = 1 ,$$

$$n = 7 , \; M = 86 , \; \rho = 4 , \; \sigma = 3 , \; \tau = 5 , \; x \equiv 100^{3 \cdot 5 + 3} \equiv 335 .$$

§ 25. Я привожу въ концѣ книги извлеченіе изъ таблицы Коркина до 2000. Если употреблять счетныя машины, то рѣшеніе квадратныхъ и двучленныхъ сравненій по способу Коркина есть дѣло нѣсколькихъ минутъ. Я долженъ обратить вниманіе на то обстоятельство, что Коркинъ употребляетъ абсолютно малые вычеты, считая, что черезъ это достигается упрощеніе выкладокъ. При употребленіи счетныхъ машинъ такое уменьшеніе чиселъ никакой роли не играетъ и является предпочтительнѣе разсматривать только положительные вычеты.

Вообще могу самымъ настоятельнымъ образомъ рекомендовать при занятіяхъ теоріей чиселъ употреблять счетныя машины. Особенно можно

рекомендовать русскую машину „Ариѳмометръ В. Т. Однера“, какъ самую простую. Опытъ показываетъ, что при бережномъ и умѣломъ съ нею обращеніи машина сохраняется въ цѣлости очень долгое время. Вычисленіе безошибочно и совершенно не утомляетъ вычислителя.

§ 26. Въ заключеніе сообщу одну теорему элементарнаго характера, приведенную въ статьѣ пр. К. Поссе [1]).

Если число a принадлежитъ къ показателю m, а число b къ показателю n по простому модулю p, и въ разложеніяхъ m и n на простые множители нѣтъ общихъ простыхъ множителей съ одинаковыми показателями степеней, то произведеніе ab принадлежитъ къ показателю N, гдѣ N наименьшее кратное чиселъ m и n.

Пусть индексъ числа a будетъ α, а индексъ числа b будетъ β.

Имѣемъ

$$\alpha m = (p-1)\mu, \tag{1}$$

$$\beta n = (p-1)\nu, \tag{2}$$

гдѣ μ взаимно простое съ m, а ν съ n.

Пусть δ будетъ общій наибольшій дѣлитель чиселъ m и n, тогда, полагая

$$m_1 = \frac{m}{\delta}, \quad n_1 = \frac{n}{\delta},$$

будемъ имѣть

$$N = mn_1 = nm_1,$$

причемъ m_1 и n_1 числа взаимно простыя.

Умножая равенство (1) на n_1, а (2) на m_1 и складывая, получимъ

$$(\alpha+\beta)N = (p-1)(\mu n_1 + \nu m_1).$$

Произведеніе ab будетъ принадлежать къ показателю N, если $\mu n_1 + \nu m_1$ будетъ числомъ взаимно простымъ съ N. При условіи теоремы это будетъ имѣть мѣсто, ибо всякій простой дѣлитель числа N будетъ обязательно заключаться или въ m_1 или въ n_1. Свойство произведенія ab принадлежать къ показателю N можетъ падать если будутъ существовать простые множители, входящіе въ одинаковыхъ степеняхъ въ m и n. Простой примѣръ этого обстоятельства даетъ случай когда число 2 входитъ въ m и n въ одинаковыхъ степеняхъ. Въ этомъ случаѣ всѣ четыре числа μ, ν, m_1, n_1,

---

[1]) *К. Поссе.* Замѣтка о рѣшеніи двучленныхъ сравненій съ простымъ модулемъ по способу Коркина. Сообщеніе Харьковскаго Мат. Общ. 1909.

нечетныя, но число $\mu n_1 + \nu m_1$ четное, слѣдовательно, не взаимно простое съ $N = m_1 n_1 \delta$.

§ 27. Покажемъ, что таблица Коркина равносильна полной таблицѣ индексовъ, ибо можно найти индексъ всякаго числа a.

Если a не вычетъ степени q, то можно выразить a^{qN} черезъ характеры совершенно такъ, какъ Коркинъ выражаетъ a^N. Придется только начать со сравненія $a^{q^\alpha N} \equiv 1$, а не съ $a^{q^{\alpha-1} N} \equiv 1$. Роль Ω будетъ играть a^N. Когда a былъ вычетъ, то при вычисленіи Ω достаточно было увеличить на единицу всѣ верхніе значки характеровъ; теперь же придется кромѣ этого увеличенія умножить все произведеніе на прилично выбранный характеръ.

Итакъ мы получаемъ во всѣхъ случаяхъ

$$a^N \equiv u_{\lambda_0}^{(\alpha-1)} u_{\lambda_1}^{(\alpha-2)} u_{\lambda_2}^{(\alpha-3)} \ldots$$

Пусть индексъ числа a будетъ ω, тогда

$$g^{N\omega} \equiv g^{N(\lambda_0 + \lambda_1 q + \lambda_2 q^2 + \ldots)}$$

Откуда

$$\omega \equiv \lambda_0 + \lambda_1 q + \lambda_2 q^2 + \ldots \pmod{q^\alpha}.$$

Продѣлавъ то же самое по всѣмъ остальнымъ простымъ числамъ r^β, $t^\gamma \ldots$, входящимъ въ составъ $p - 1$, получаемъ

$$\omega \equiv \mu_0 + \mu_1 r + \mu_2 r^2 + \ldots \pmod{r^\beta}$$

$$\omega \equiv \nu_1 + \nu_1 t + \nu_2 t^2 + \ldots \pmod{t^\gamma}$$

. . . . . .

Рѣшая послѣднія совмѣстныя сравненія (см. гл. III § 16), находимъ искомый индексъ. Поясним сказанное примѣрами.

I примѣръ. Требуется найти индексъ числа 37 по модулю 257.

Итакъ $p = 257$, $p - 1 = 2^8$.

Составляемъ вычеты степеней a.

$$a \equiv 37,\ a^2 \equiv 84,\ a^{2^2} \equiv 117,\ a^{2^3} \equiv 68,\ a^{2^4} \equiv 255,\ a^{2^5} \equiv 4,\ a^{2^6} \equiv 16,$$

$$a^{2^7} \equiv 256 \equiv -1.$$

Получаемъ послѣдовательно

$$a^{2^6} \equiv f,\ a^{2^5} \equiv -f',\ a^{2^4} \equiv -ff'',\ a^{2^3} \equiv ff'f''',\ a^{2^2} \equiv -f'f''f^{iv},$$

$$a^2 \equiv -ff''f'''f^v,\ a \equiv ff'f'''f^{iv}f^{vi}.$$

Написавъ

$$a = f_1^{VI} f_0^{V} f_1^{IV} f_1''' f_0'' f_1' f_1$$

получимъ искомый индексъ

$$\omega = 1 + 0 \cdot 2 + 1 \cdot 2^2 + 1 \cdot 2^3 + 0 \cdot 2^4 + 1 \cdot 2^5 + 1 \cdot 2^6 = 109 .$$

Если бы въ выраженіи a передъ характеромъ стоялъ знакъ —, то необходимо было бы въ ω прибавить еще одинъ членъ $1 \cdot 2^7$ соотвѣтствующій главному характеру -1.

II примѣръ. Требуется найти индексъ числа 442 при модулѣ 571.

Имѣемъ $p = 571$, $p - 1 = 2 \cdot 3 \cdot 5 \cdot 19$.

1) $\frac{p-1}{2} = 285$

$$442^2 \equiv 82 , \quad 442^4 \equiv 443 , \quad 442^8 \equiv 396 , \quad 442^{16} \equiv 362 , \quad 442^{32} \equiv 285 ,$$

$$442^{64} \equiv 143 , \quad 442^{128} \equiv 464 , \quad 442^{256} \equiv 29 , \quad 442^{272} \equiv 220 , \quad 442^{280} \equiv 328 ,$$

$$442^{284} \equiv 270 , \quad 442^{285} \equiv 1 .$$

Слѣдовательно

$$\omega \equiv 0 \pmod 2$$

2) $\frac{p-1}{3} = 190$

$$442^{160} \equiv 339 , \quad 442^{176} \equiv 524 , \quad 442^{184} \equiv 231 , \quad 442^{188} \equiv 124 , \quad 442^{190} \equiv 461 .$$

Сравниваемъ съ характерами $z \equiv 109$, $z^2 \equiv 461$.

Слѣдовательно

$$\omega \equiv 2 \pmod 3 .$$

3) $\frac{p-1}{5} = 114$

$$442^{96} \equiv 214 , \quad 442^{112} \equiv 383 , \quad 442^{114} \equiv 1 ,$$

слѣдовательно,

$$\omega \equiv 0 \pmod 5 .$$

4) $\frac{p-1}{19} = 30$

$$442^{24} \equiv 31 , \quad 442^{28} \equiv 29 , \quad 442^{30} \equiv 94 .$$

Сравниваемъ со степенями характера

$$v \equiv 271 , \quad v^2 \equiv 353 , \quad v^3 \equiv 306 , \quad v^4 \equiv 131 , \quad v^5 \equiv 99 , \quad v^6 \equiv 563 , \quad v^7 \equiv 116 ,$$

$$v^8 \equiv 31 .$$

Идти далѣе не надо, ибо мы имѣемъ

$$442^{24} \equiv v^8 .$$

или

$$g^{24\omega} \equiv g^{30.8}$$

откуда

$$24\omega \equiv 240 \pmod{2.3.5.19};$$

$$\omega \equiv 10 \pmod{19}.$$

Для нахожденія искомаго индекса ω рѣшаемъ совмѣстно сравненія (см. гл. III § 16).

$\omega \equiv 0 \pmod 2$	$\alpha = 0$	$A = 285,\ a' = 1$
$\omega \equiv 2 \pmod 3$	$\beta = 2$	$B = 190,\ b' = 1$
$\omega \equiv 0 \pmod 5$	$\gamma = 0$	$C = 114,\ c' = 4$
$\omega \equiv 10 \pmod{19}$	$\delta = 10$	$D = 30,\ d' = 7$

откуда

$$\omega \equiv 0.285.1 + 2.190.1 + 0.114.4 + 10.30.7 \pmod{p-1}$$

и наконецъ

$$\omega = 200.$$

ГЛАВА V.

О квадратичныхъ вычетахъ.

§ 1. Будемъ разсматривать сравненіе второй степени

$$ax^2 + bx + c \equiv 0 \pmod{k}. \qquad (1)$$

Не трудно убѣдиться, что это сравненіе сводится къ сравненію первой степени въ слѣдующихъ двухъ случаяхъ

1) $k = 2$,

и

2) $a \equiv 0 \pmod{k}$.

Въ самомъ дѣлѣ, въ первомъ случаѣ сравненіе (1) можно переписать такъ

$$ax(x-1) + (a+b)x + c \equiv 0 \pmod{2}.$$

Но $x(x-1)$ всегда дѣлится на 2, и слѣдовательно, при всякихъ значеніяхъ x имѣемъ

$$ax(x-1) \equiv 0 \pmod{2},$$

откуда получаемъ сравненіе первой степени

$$(a+b)x + c \equiv 0 \pmod{2}.$$

Во второмъ случаѣ при всякомъ x имѣетъ мѣсто

$$ax^2 \equiv 0 \pmod{k},$$

слѣдовательно, получаемъ

$$bx + c \equiv 0 \pmod{k}.$$

§ 2. Предположимъ теперь, что k не равно 2 и a не дѣлится на k. Тогда, умножая сравненіе (1) § 1 на $4a$, получимъ

$$(2ax + b)^2 - b^2 + 4ac \equiv 0 \pmod{k}.$$

Обозначая $2ax + b = y$, приходимъ къ рѣшенію сравненія

$$y^2 \equiv b^2 - 4ac \pmod{k}.$$

§ 3. Займемся сначала изученіемъ сравненій вида

$$x^2 \equiv q \pmod{p}, \tag{1}$$

гдѣ p нечетное простое число, а q не дѣлится на p.

Общій наибольшій дѣлитель чиселъ 2 и $p-1$ есть, очевидно, 2; слѣдовательно, сравненіе (1) будетъ имѣть два рѣшенія (см. § 11 гл. IV), если будетъ имѣть мѣсто условіе

$$q^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \tag{2}$$

и не будетъ имѣть ни одного рѣшенія, если сравненіе (2) не удовлетворяется.

Покажемъ, что этотъ второй случай (отсутствіе рѣшеній) характеризуется сравненіемъ вида, подобнаго сравненію (2). Въ самомъ дѣлѣ, по теоремѣ Fermat'a

$$q^{p-1} \equiv 1 \pmod{p},$$

слѣдовательно, разность

$$q^{p-1} - 1 = (q^{\frac{p-1}{2}} - 1)(q^{\frac{p-1}{2}} + 1)$$

должна дѣлиться на простое число p.

Но если сравненіе (2) не имѣетъ мѣста, то множитель

$$q^{\frac{p-1}{2}} - 1$$

не дѣлится на p; тогда долженъ дѣлиться на p второй множитель

$$q^{\frac{p-1}{2}} + 1,$$

и слѣдовательно, должно имѣть мѣсто сравненіе

$$q^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \tag{3}$$

Будемъ на основаніи сказаннаго въ предыдущей главѣ число q называть *квадратичнымъ вычетомъ* числа p, если оно удовлетворяетъ сравненію (2), и *квадратичнымъ невычетомъ*, если оно удовлетворяетъ сравненію (3). Названіе квадратичный вычетъ указываетъ что число q является по модулю p вычетомъ нѣкотораго квадрата x^2.

Это понятіе о квадратичныхъ вычетахъ распространяется на какія угодно составныя числа, причемъ число q называется квадратичнымъ вычетомъ составного числа k, если сравненіе

$$x^2 \equiv q \pmod{k}$$

имѣетъ рѣшеніе, и квадратичнымъ невычетомъ въ случаѣ невозможности послѣдняго сравненія.

§ 4. Въ теоріи квадратичныхъ вычетовъ имѣются въ виду главнымъ образомъ слѣдующія двѣ задачи.

I. По данному числу k указать всѣ его квадратичные вычеты q и для каждаго изъ этихъ вычетовъ рѣшить сравненіе

$$x^2 \equiv q \pmod{k}.$$

II. По данному числу q найти всѣ числа k, для которыхъ q есть квадратичный вычетъ.

§ 5. Мы начнемъ съ первой задачи и будемъ сначала предполагать модуль числомъ простымъ. Поставимъ себѣ задачей опредѣлить изъ ряда чиселъ

$$1, 2, 3, \ldots, p-1 \qquad (1)$$

число квадратичныхъ вычетовъ простого числа p.

Квадратичные вычеты суть не что иное, какъ рѣшенія относительно q слѣдующаго двучленнаго сравненія.

$$q^{\frac{p-1}{2}} \equiv 1 \pmod{p}. \qquad (2)$$

Такъ какъ во второй части этого сравненія находится единица, то по соображеніямъ § 11 гл. IV сравненіе (2) имѣетъ ровно $\frac{p-1}{2}$ рѣшеній.

Обозначимъ эти рѣшенія

$$q_1, q_2, \ldots, q_{\frac{p-1}{2}}. \qquad (3)$$

Числа (3) и будутъ квадратичными вычетами числа p. Остальныя же числа ряда (1), число которыхъ равно также $\frac{p-1}{2}$, будутъ невычетами.

Числа ряда (3) можно получить слѣдующимъ образомъ. Возьмемъ первую половину чиселъ ряда (1)

$$1, 2, 3, \ldots, \frac{p-1}{2} \qquad (4)$$

и возвысимъ ихъ въ квадратъ

$$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2. \qquad (5)$$

Можно утверждать, что положительные вычеты квадратовъ (5) по модулю p дадутъ полную систему квадратичныхъ вычетовъ (3).

Въ самомъ дѣлѣ, очевидно, что всякій положительный вычетъ квадрата есть въ то же время квадратичный вычетъ. Остается, слѣдовательно, доказать, что всѣ положительные вычеты чиселъ (5) различны между собою; другими словами, доказать, что числа (5) несравнимы по модулю p.

Предположимъ обратно, что въ рядѣ (5) существуетъ два числа r^2 и s^2, сравнимыя по модулю p; тогда разность

$$r^2 - s^2 = (r+s)(r-s)$$

должна дѣлиться на простое число p. Но это невозможно, ибо оба множителя $r+s$ и $r-s$ по абсолютной величинѣ меньше p, такъ какъ числа r и s не превосходятъ $\frac{p-1}{2}$. Слѣдовательно, ни одинъ изъ множителей $r+s$, $r-s$ не можетъ дѣлиться на p.

Не трудно убѣдиться, что квадраты чиселъ другой половины ряда (1), т. е чиселъ

$$\frac{p+1}{2}, \frac{p+3}{2}, \ldots, p-1$$

дадутъ тѣ же самые квадратичные вычеты (3), ибо

$$(p-r)^2 = p^2 - 2pr + r^2 \equiv r^2 \pmod{p}.$$

Такъ напримѣръ, составимъ рядъ квадратичныхъ вычетовъ для $p=13$. Число этихъ вычетовъ

$$\frac{p-1}{2} = 6.$$

Возвышаемъ въ квадратъ числа 1, 2, 3, 4, 5, 6. Получаемъ рядъ сравненій

$$1^2 \equiv 1 \pmod{13}; \quad 2^2 \equiv 4 \pmod{13}; \quad 3^2 \equiv 9 \pmod{13};$$

$$4^2 \equiv 3 \pmod{13}; \quad 5^2 \equiv 12 \pmod{13}; \quad 6^2 \equiv 10 \pmod{13}.$$

Отсюда получаются слѣдующіе квадратичные вычеты

$$1, 3, 4, 9, 10, 12.$$

§ 6. *Произведеніе двухъ вычетовъ* [1]) q_1, q_2 *есть также вычетъ,* ибо существуетъ два числа x_1, x_2, удовлетворяющія сравненіямъ

$$x_1^2 \equiv q_1 \pmod p, \quad x_2^2 \equiv q_2 \pmod p.$$

Слѣдовательно, существуетъ число $x_1 x_2$, удовлетворяющее сравненію

$$(x_1 x_2)^2 \equiv q_1 q_2 \pmod p.$$

§ 7. Покажемъ теперь, что *произведеніе вычета* q *на невычетъ* t *даетъ невычетъ.*

Мы видѣли уже, что отъ умноженія на число q, не дѣлящееся на p, системы чиселъ

$$1, 2, \ldots, p-1 \tag{1}$$

получаются числа, несравнимыя между собою по модулю p и, слѣдовательно, въ своихъ положительныхъ вычетахъ, воспроизводящія ту же систему чиселъ. Числа ряда (1) распадаются на двѣ части: квадратичные вычеты и невычеты. На основаніи предыдущаго §-а мы видимъ, что при умноженіи квадратичныхъ вычетовъ на вычетъ q должна воспроизводиться та же часть ряда (1), образованная квадратичными вычетами. Слѣдовательно, невычеты должны получаться отъ умноженія вычета q на невычеты.

§ 8. Соображенія, аналогичныя приведеннымъ въ предыдущемъ §-ѣ, показываютъ, что *произведеніе невычета на невычетъ даетъ вычетъ,* ибо, если мы умножимъ на невычетъ всѣ числа, то при умноженіи вычетовъ получаются, какъ мы видѣли, невычеты; слѣдовательно, умноженіе невычетовъ дастъ, обратно, вычеты.

§ 9. *Произведенія ряда чиселъ* $a, b, c, \ldots$ *даетъ вычетъ или невычетъ, суди по тому, будетъ ли среди множителей четное число невычетовъ или нечетное.*

Въ этомъ можно убѣдиться еще такимъ образомъ. Равенство

$$(abc \ldots)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} c^{\frac{p-1}{2}} \ldots$$

показываетъ, что первая его часть будетъ сравнима съ $+1$ или -1,

[1]) Въ дальнѣйшемъ „квадратичный вычетъ“ = „вычетъ“.

смотря по тому, будетъ ли число множителей, сравнимыхъ съ -1, четное или нечетное.

§ 10. Legendre ввелъ въ разсмотрѣніе символъ

$$\left(\frac{q}{p}\right),$$

опредѣляемый равенствомъ

$$\left(\frac{q}{p}\right) = 1,$$

если q квадратичный вычетъ числа p, и равенствомъ

$$\left(\frac{q}{p}\right) = -1,$$

если q невычетъ.

Такимъ образомъ, всегда имѣетъ мѣсто сравненіе

$$q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod{p}.$$

Изъ опредѣленія символа Legendre'a слѣдуетъ такое его свойство

$$\left(\frac{qrs\ldots}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{r}{p}\right)\left(\frac{s}{p}\right)\ldots$$

§ 11. Обратимся теперь къ разсмотрѣнію вычетовъ чиселъ составныхъ.

Начнемъ со случая, когда модуль квадратнаго сравненія есть степень простого нечетнаго числа. Поставимъ себѣ задачей найти число рѣшеній

$$x^2 \equiv q \pmod{p^m}. \qquad (1)$$

гдѣ m нѣкоторое цѣлое число, а q квадратичный вычетъ числа p^m, который будемъ предполагать числомъ, взаимно простымъ съ модулемъ, т. е. не дѣлящимся на p.

Введемъ въ разсмотрѣніе сравненіе

$$x^2 \equiv q \pmod{p}. \qquad (2)$$

Если невозможно сравненіе (2), то, очевидно, не будетъ удовлетворяться и сравненіе (1), ибо если разность $x^2 - q$ не дѣлится на p, то она не будетъ дѣлиться и на p^m. Покажемъ, что всякому рѣшенію a сравненія (2) можно сопоставить рѣшеніе сравненія (1).

Введемъ въ разсмотрѣніе двѣ цѣлыя функціи

$$\varphi(x) \text{ и } \psi(x),$$

опредѣляемыя тождествомъ

$$(a+\sqrt{x})^m = \varphi(x) + \psi(x)\sqrt{x}, \tag{3}$$

гдѣ

$$\varphi(x) = a^m + \frac{m(m-1)}{1.2}a^{m-2}x + \ldots,$$

а

$$\psi(x) = ma^{m-1} + \frac{m(m-1)(m-2)}{1.2.3}a^{m-3}x + \ldots$$

Функціи $\varphi(x)$ и $\psi(x)$ имѣютъ цѣлые коэффиціенты, значитъ, подстановка въ нихъ вмѣсто x всякаго цѣлаго числа даетъ число цѣлое.

Изъ тождества (3) получимъ другое тождество, измѣняя знакъ у корня

$$(a-\sqrt{x})^m = \varphi(x) - \psi(x)\sqrt{x}, \tag{4}$$

откуда получимъ

$$\varphi(x) = \frac{(a+\sqrt{x})^m + (a-\sqrt{x})^m}{2},$$

а

$$\psi(x) = \frac{(a+\sqrt{x})^m - (a-\sqrt{x})^m}{2\sqrt{x}}.$$

Сравненіе

$$a^2 \equiv q \pmod{p}$$

даетъ два такихъ

$$\varphi(q) \equiv \varphi(a^2) \pmod{p}$$

и

$$\psi(q) \equiv \psi(a^2) \pmod{p}.$$

Но

$$\varphi(a^2) = 2^{m-1}a^m,$$

а

$$\psi(a^2) = 2^{m-1}a^{m-1}.$$

Сравненіе

$$\varphi(q) \equiv 2^{m-1}a^m \pmod{p}$$

показываетъ, что $\varphi(q)$ не должно дѣлиться на p, ибо a не можетъ дѣлиться на p, такъ какъ въ обратномъ случаѣ дѣлилось бы на p число q, что противорѣчитъ предположенію.

Подобнымъ же образомъ покажемъ, что $\psi(q)$ не дѣлится на p.

Перемножая тождества (3) и (4), получимъ

$$(a^2-x)^m = [\varphi(x)]^2 - x[\psi(x)]^2. \tag{5}$$

Подставляя въ равенство (5) $x = q$, получимъ

$$(a^2-q)^m = [\varphi(q)]^2 - q[\psi(q)]^2.$$

Но $a^2 - q$ дѣлится на p, слѣдовательно, вторая часть послѣдняго равенства должна дѣлится на p^m, и мы получаемъ сравненіе:

$$[\varphi(q)]^2 \equiv q[\psi(q)]^2 \pmod{p^m}. \qquad (6)$$

Рѣшаемъ сравненіе первой степени

$$\psi(q)x \equiv \varphi(q) \pmod{p^m}, \qquad (7)$$

имѣющее одинъ корень, ибо $\psi(q)$ число взаимно-простое съ p^m.

Не трудно убѣдится, что получаемое такимъ образомъ число x есть корень заданнаго сравненія (1).

Въ самомъ дѣлѣ, возвышаемъ сравненіе (7) въ квадратъ

$$[\psi(q)]^2x^2 \equiv [\varphi(q)]^2 \pmod{p^m}.$$

На основаніи сравненія (6), получимъ:

$$[\psi(q)]^2x^2 \equiv q[\psi(q)]^2 \pmod{p^m},$$

откуда, сокращая на $[\psi(q)]^2$, получимъ заданное сравненіе.

Мѣняя знакъ у x, получимъ второе рѣшеніе $-x$ сравненія (1).

Покажемъ теперь, что заданное сравненіе (1) не имѣетъ больше рѣшеній. Обозначимъ черезъ y произвольное рѣшеніе разсматриваемаго сравненія. Тогда имѣютъ мѣсто два сравненія

$$x^2 \equiv q \pmod{p^m}, \quad y^2 \equiv q \pmod{p^m}.$$

Отсюда получимъ

$$y^2 - x^2 \equiv 0 \pmod{p^m}$$

или

$$(y + x)(y - x) \equiv \pmod{p^m}.$$

Не трудно убѣдиться, что не возможно совмѣстное существованіе обоихъ сравненій

$$y + x \equiv 0 \pmod{p}$$

и

$$y - x \equiv 0 \pmod{p},$$

ибо въ противномъ случаѣ имѣло бы мѣсто сравненіе

$$2x \equiv 0 \pmod{p},$$

что давало бы

$$x \equiv 0 \pmod{p}$$

и

$$q \equiv 0 \pmod{p}.$$

Итакъ, степень p^m должна входить множителемъ въ одинъ изъ двучленовъ $y+x$ или $y-x$, и слѣдовательно, мы приходимъ къ одному изъ двухъ сравненій $y \equiv x \pmod{p^m}$ или $y \equiv -x \pmod{p^m}$, показывающимъ, что сравненіе (1) не имѣетъ другихъ рѣшеній, кромѣ x и $-x$.

§ 12. Обратимся теперь къ случаю, когда модуль есть степень числа 2, и разсмотримъ сравненіе

$$x^2 \equiv q \pmod{2^m}.$$

Число q мы должны предполагать числомъ нечетнымъ.

Начнемъ со случая

$$m = 1;$$

тогда, очевидно, придется разсматривать сравненіе

$$x^2 \equiv 1 \pmod 2.$$

Сравненіе будетъ имѣть только одинъ корень, образованный классомъ чиселъ нечетныхъ.

Если

$$m = 2,$$

то сравненіе

$$x^2 \equiv q \pmod 4$$

возможно только въ случаѣ

$$q \equiv 1 \pmod 4,$$

ибо квадратъ всякаго нечетнаго числа $2n+1$ выражается по формулѣ

$$4n^2 + 4n + 1$$

и, слѣдовательно, сравнимъ съ единицей по модулю 4.

Сравненіе

$$x^2 \equiv 1 \pmod 4$$

имѣетъ, очевидно, только два рѣшенія

$$x \equiv 1 \pmod 4, \quad x \equiv -1 \pmod 4$$

При $m \equiv 3$

$$x^2 \equiv q \pmod 8. \qquad (1)$$

Всякое нечетное число можетъ быть представлено въ видѣ $4n \pm 1$. Квадратъ такого числа выразится по формулѣ $16n^2 \pm 8n + 1$, и слѣдовательно, число q должно удовлетворять сравненію $q \equiv 1 \pmod 8$.

Если это условіе удовлетворяется, то сравненіе (1) имѣетъ четыре корня

$$x \equiv 1, \quad x \equiv 3, \quad x \equiv 5, \quad x \equiv 7 \pmod 8.$$

§ 13. Обращаемся теперь къ общему случаю

$$x^2 \equiv q \pmod{2^m}, \tag{1}$$

гдѣ

$$m > 3.$$

Очевидно, что сравненіе (1) возможно только въ случаѣ возможности сравненія

$$x^2 \equiv q \pmod 8. \tag{2}$$

откуда получается необходимое условіе возможности сравненія (1)

$$q \equiv 1 \pmod 8.$$

Покажемъ теперь, что это условіе достаточное, и что при его выполненіи сравненіе (1) имѣетъ рѣшеніе. Для этой цѣли покажемъ, что всякому рѣшенію сравненія (2) можно сопоставить нѣкоторое рѣшеніе сравненія (1), такъ что сравненіе (1) должно имѣть, по крайней мѣрѣ, четыре рѣшенія.

Не трудно показать, что всякому рѣшенію α сравненія

$$x^2 \equiv q \pmod{2^\mu}$$

можно сопоставить рѣшеніе сравненія

$$x^2 \equiv q \pmod{2^{\mu+1}} \tag{3}$$

Мы имѣемъ

$$\alpha^2 - q = 2^\mu h \tag{4}$$

гдѣ h нѣкоторое цѣлое число.

Будемъ искать рѣшеніе сравненія (3) въ такой формѣ

$$x = \alpha + 2^{\mu-1} y \tag{5}$$

Возвышая въ квадратъ, получаемъ

$$x^2 = \alpha^2 + 2^\mu \alpha y + 2^{2\mu-2} y^2.$$

Складывая съ равенствомъ (4), будемъ имѣть

$$x^2 - q = 2^\mu h + 2^\mu \alpha y + 2^{2\mu-2} y^2.$$

x, опредѣляемый по формулѣ (5), будетъ рѣшеніемъ сравненія (3), если y подберемъ на основаніи сравненія

$$2^\mu h + 2^\mu \alpha y + 2^{2\mu-2} y^2 \equiv 0 \pmod{2^{\mu+1}}$$

Но если

$$\mu \geqslant 3,$$

то

$$2\mu - 2 \geqslant \mu + 1;$$

слѣдовательно, послѣднее сравненіе можно переписать такъ

$$2^\mu(h + \alpha y) \equiv 0 \pmod{2^{\mu+1}}.$$

Сокращая это сравненіе на 2^p, получимъ

$$h + \alpha y \equiv 0 \pmod 2 ; \qquad (6)$$

это же сравненіе можно рѣшить, ибо α число нечетное.

Итакъ, подставляя въ формулу (5), вмѣсто y, корень сравненія (6), получимъ для x значеніе, удовлетворяющее сравненію (3).

Итакъ, можно считать доказаннымъ, что по четыремъ рѣшеніямъ сравненія (2) можно найти четыре соотвѣтственныхъ рѣшенія сравненія (1).

Покажемъ теперь, что, кромѣ полученныхъ такимъ образомъ рѣшеній, не будетъ существовать другихъ рѣшеній сравненія (1).

Въ самомъ дѣлѣ, обозначимъ черезъ z произвольное рѣшеніе сравненія (1), а черезъ x одно какое нибудь опредѣленное изъ рѣшеній. Тогда должно имѣть мѣсто сравненіе

$$z^2 - x^2 \equiv 0 \pmod{2^m}. \qquad (7)$$

Оба числа z и x нечетныя, слѣдовательно, оказываются четными числа $z + x$ и $z - x$.

Сокращая сравненіе (7) на 4 получимъ

$$\frac{z+x}{2} \cdot \frac{z-x}{2} \equiv 0 \pmod{2^{m-2}}.$$

Такъ какъ разность двухъ чиселъ

$$\frac{z+x}{2}, \quad \frac{z-x}{2}$$

есть нечетное число x, то изъ этихъ чиселъ одно должно быть нечетнымъ, и слѣдовательно, какъ необходимое слѣдствіе послѣдняго сравненія, должно получаться одно изъ двухъ слѣдующихъ

$$\frac{z+x}{2} \equiv 0 \pmod{2^{m-2}} \quad \text{или} \quad \frac{z-x}{2} \equiv 0 \pmod{2^{m-2}}$$

или, что одно и тоже

$$z + x \equiv 0 \pmod{2^{m-1}} \quad \text{или} \quad z - x \equiv 0 \pmod{2^{m-1}}.$$

Итакъ, всѣ рѣшенія z сравненія (1) должны заключаться въ двухъ классахъ:

$$x, \; x + 2^{m-1}, \; x + 2 \cdot 2^{m-1}, \; x + 3 \cdot 2^{m-1}, \ldots$$

и

$$-x, \; -x + 2^{m-1}, \; -x + 2 \cdot 2^{m-1}, \; -x + 3 \cdot 2^{m-1}, \ldots$$

Эти всѣ числа распадаются по модулю 2^m на четыре класса, откуда получается только четыре рѣшенія:

$$z \equiv x \pmod{2^m}, \quad z \equiv x + 2^{m-1} \pmod{2^m},$$

$$z \equiv -x \pmod{2^m}, \quad z \equiv -x + 2^{m-1} \pmod{2^m}.$$

§ 14. Резюмируя сказанное въ предыдущемъ §-ѣ, можемъ высказать такую теорему.

Теорема. *Сравненіе* $x^2 \equiv q \pmod{2^m}$ *1) всегда возможно при* $m = 1$ *и имѣетъ одинъ корень, 2) при* $m = 2$ *оно возможно въ случаѣ* $q \equiv 1 \pmod 4$ *и имѣетъ 2 корня, 3) при* $m \geqslant 3$ *сравненіе возможно, если* $q \equiv 1 \pmod 8$, *и имѣетъ всегда четыре корня.*

§ 15. Обращаемся теперь къ рѣшенію сравненія

$$x^2 \equiv q \pmod k, \tag{1}$$

гдѣ k произвольное составное число.

Пусть $k = abc\ldots$, гдѣ множители a, b, c, ... суть степени простыхъ чиселъ, входящихъ въ k, и слѣдовательно, числа взаимно простыя.

Не трудно видѣть, что сравненіе (1) возможно только при возможности всѣхъ сравненій

$$x^2 \equiv q \pmod a, \quad x^2 \equiv q \pmod b, \quad x^2 \equiv q \pmod c, \ldots \tag{2}$$

Отсюда должно имѣть мѣсто

$$\left(\frac{q}{p}\right) = 1$$

для всякаго нечетнаго простого числа p, входящаго въ k.

Если среди простыхъ множителей заключается 2, то должны удовлетворяться условія теоремы § 14.

Разсмотримъ сначала только степени нечетныхъ простыхъ чиселъ. Тогда каждое изъ сравненій (2) имѣетъ два корня.

Пусть α будетъ корень перваго сравненія (2), β корень второго, γ третьяго и т. д. Тогда x, удовлетворяющій сравненію (1), опредѣлится изъ системы сравненій

$$x \equiv \alpha \pmod a, \quad x \equiv \beta \pmod b, \quad x \equiv \gamma \pmod c, \ldots$$

Всякое число $x = \rho$, удовлетворяющее послѣднимъ сравненіямъ, удовлетворяетъ сравненіямъ (2), а слѣдовательно, и сравненію (1).

Въ § 16 главы III мы видѣли, какъ найти такое число ρ.

Если черезъ μ мы обозначимъ число сравненій (2), то, комбинируя по одному каждое изъ двухъ рѣшеній каждаго сравненія (2), получимъ 2^μ различныхъ чиселъ ρ, удовлетворяющихъ заданному сравненію (1).

Обращаемся теперь къ случаю, когда кромѣ μ степеней нечетныхъ простыхъ чиселъ входитъ въ модуль k еще степень числа 2. Если эта степень первая, то число рѣшеній сравненія (1) остается по прежнему 2^μ, ибо сравненіе

$$x^2 \equiv q \pmod 2$$

имѣетъ только одинъ корень.

Если въ число k входитъ множителемъ число 4, то сравненіе

$$x^2 \equiv q \pmod 4$$

имѣетъ два корня, и слѣдовательно, общее число рѣшеній сравненія (1) будетъ $2^{\mu+1}$.

Наконецъ, при существованіи въ k множителя 2^m, гдѣ $m \geqslant 3$, получается $2^{\mu+2}$ рѣшеній сравненія (1).

§ 16. Обращаемся теперь къ разсмотрѣнію обратной задачи.

Найти по заданному числу q всѣ числа k, относительно которыхъ q будетъ квадратичнымъ *вычетомъ*.

Сравненіе

$$x^2 \equiv q \pmod k$$

показываетъ, что искомое число k есть не что иное, какъ дѣлитель выраженія

$$x^2 - q, \tag{1}$$

и слѣдовательно, для рѣшенія задачи надо найти всѣхъ дѣлителей чиселъ $x^2 - q$, получаемыхъ при всевозможныхъ значеніяхъ x.

Не трудно убѣдиться, что эти дѣлители совпадаютъ съ дѣлителями слѣдующей квадратичной формы

$$\xi^2 - q\eta^2, \tag{2}$$

гдѣ ξ и η взаимно простыя числа.

Что всякій дѣлитель выраженія (1) есть также дѣлитель выраженія 2), слѣдуетъ изъ того, что выраженіе (1) получается изъ (2) при

$$\xi = x, \quad \eta = 1.$$

Справедливо также обратное заключеніе. Пусть k будетъ дѣлитель формы (2). Число η должно быть взаимно простымъ съ k, ибо, если бы эти два числа имѣли множителя δ, то этотъ множитель долженъ былъ бы входить въ число ξ, а слѣдовательно, ξ и η не могли бы быть взаимно простыми.

Найдемъ корень x сравненія

$$\eta x \equiv \xi \pmod{k}, \tag{3}$$

которое имѣетъ одно только рѣшеніе.

Сопоставляя сравненіе (3) со сравненіемъ $\xi^2 \equiv q\eta^2 \pmod{k}$, выражающимъ, что k есть дѣлитель формы (2), получимъ $\eta^2 x^2 \equiv q\eta^2 \pmod{k}$. Сокращая на η^2, получимъ $x^2 \equiv q \pmod{k}$, что и требовалось доказать, т. е. что k дѣлитъ выраженіе

$$x^2 - q.$$

§ 17. Итакъ, обратимся къ задачѣ: найти всѣ модули k, при которыхъ возможно сравненіе

$$x^2 \equiv q \pmod{k}. \tag{1}$$

Возможность сравненія (1), какъ мы видѣли, зависитъ отъ характера простыхъ множителей числа k. Случай множителя 2, какъ трактующійся на основаніи элементарныхъ соображеній, мы оставимъ въ сторонѣ.

Остается, слѣдовательно, перейти къ разсмотрѣнію нечетныхъ простыхъ множителей числа k. Мы приходимъ такимъ образомъ къ задачѣ: *найти всѣ простыя числа p, относительно которыхъ данное число q есть квадратичный вычетъ;* эта же послѣдняя задача приводится къ разсмотрѣнію простыхъ множителей числа q (это число можетъ быть задано, какъ положительнымъ, такъ и отрицательнымъ).

Итакъ, мы приходимъ къ рѣшенію такой задачи: *найти всѣ простыя числа p, при которыхъ имѣютъ мѣсто сравненія*

$$x^2 \equiv -1 \pmod{p}, \quad x^2 \equiv 2 \pmod{p}, \quad x^2 \equiv q \pmod{p},$$

гдѣ q нечетное простое число.

§ 18. Займемся сначала сравненіемъ

$$x^2 \equiv -1 \pmod{p}. \tag{1}$$

Должно имѣть мѣсто сравненіе

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Отсюда получаемъ

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Итакъ, для возможности сравненія (1) необходимо, чтобы число

$$\frac{p-1}{2}$$

было четное, т. е.

$$\frac{p-1}{2} = 2n,$$

откуда $p = 4n + 1$.

Получаемъ теорему, что *— 1 есть квадратичный вычетъ для всѣхъ простыхъ чиселъ вида $4n + 1$ и квадратичный невычетъ для всѣхъ простыхъ чиселъ вида $4n + 3$.*

На основаніи соображеній §§ 16 и 17 замѣчаемъ, что *всѣ простыя формы $x^2 + y^2$ должны быть вида $4n + 1$.*

Euler доказалъ слѣдующую замѣчательную теорему: *всякое простое число вида $4n + 1$ можетъ быть представлено только однимъ способомъ въ видѣ суммы $x^2 + y^2$ двухъ квадратовъ*, при чемъ существуетъ предложеніе обратное: *если число вида $4n + 1$ только однимъ способомъ раскладывается на сумму двухъ квадратовъ, то оно простое.*

§ 19. Обратимся къ доказательству одного весьма важнаго закона, называемаго *закономъ взаимности двухъ простыхъ чиселъ* и выражаемаго формулой

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}},$$

гдѣ p и q нечетныя простыя числа.

Въ первый разъ этотъ законъ въ полномъ объемѣ, хотя въ иной формѣ, былъ высказанъ Euler'омъ въ мемуарѣ: Observationes circa divisiones quadratorum per numeros primos. Commentationes Arithmeticae. Tom. I, p. 477.

Euler не привелъ однако доказательства. Legendre въ сочиненіи Recherches d'analyse indeterminée. Hist. de l'Acad. de paris. 1785 p. 465 независимо отъ Euler'а пришелъ къ нахожденію закона и ему удалось дать строгое доказательство, хотя и не всего закона въ полномъ его объемѣ.

Первый доказалъ законъ взаимности Gauss. Ему удалось дать семь различныхъ между собой вполнѣ строгихъ доказательствъ.

Послѣ Gauss'а можно насчитать около пятидесяти доказательствъ, данныхъ другими учеными.

Приступимъ къ разсмотрѣнію сравненія

$$x^2 \equiv q \pmod{p},$$

гдѣ p нечетное простое число, а q другое простое число.

Разсмотримъ рядъ чиселъ

$$q,\ 2q,\ \ldots,\ \frac{p-1}{2}q.$$

Пусть положительные вычеты этихъ чиселъ по модулю p будутъ

$$r_1, r_2, \ldots, r_{\frac{p-1}{2}}.$$

Обозначимъ черезъ

$$a_1, a_2, \ldots, a_\rho \tag{1}$$

тѣ изъ числа этихъ вычетовъ, которые больше $\frac{p}{2}$, а черезъ

$$b_1, b_2, \ldots, b_\sigma \tag{2}$$

вычеты, меньшіе $\frac{p}{2}$.

Всѣ числа a_i и b_k различны между собой. Числа

$$p - a_1, p - a_2, \ldots, p - a_\rho \tag{3}$$

будутъ меньше $\frac{p}{2}$. Покажемъ, что эти новыя числа отличны отъ чиселъ (2). Въ самомъ дѣлѣ, допустивъ обратное, а именно, что

$$p - a = b, \tag{4}$$

получимъ

$$a + b = p,$$

и, слѣдовательно,

$$a + b \equiv 0 \pmod{p}.$$

Но такъ какъ a и b суть вычеты двухъ чиселъ

$$sq \text{ и } tq,$$

то должно имѣть мѣсто

$$sq + tq \equiv 0 \pmod{p}$$

или

$$s + t \equiv 0 \pmod{p},$$

что невозможно, ибо оба положительныхъ числа s, t не превосходятъ $\frac{p-1}{2}$.

Итакъ, равенство (4) невозможно; слѣдовательно, числа (3) и (2) даютъ въ общей сложности $\frac{p-1}{2}$ различныхъ чиселъ, меньшихъ $\frac{p}{2}$, т. е., другими словами, эти двѣ системы чиселъ обнимаютъ систему

$$1, 2, 3, \ldots, \frac{p-1}{2}.$$

Перемножая числа (2) и (3), получаемъ равенство

$$(p - a_1)(p - a_2) \ldots (p - a_\rho) b_1 b_2 \ldots b_\sigma = 1 \cdot 2 \cdot 3 \ldots \frac{p-1}{2}.$$

Отсюда, выкидывая члены, сравнимые съ нулемъ по модулю p, получимъ сравненіе

$$(-1)^{\rho} a_1 a_2 \ldots a_{\rho} b_1 b_2 \ldots b_{\sigma} \equiv 1 \cdot 2 \cdot 3 \ldots \frac{p-1}{2} \pmod{p}. \qquad (5)$$

Перемножая сравненія

$$q \equiv r_1 \pmod{p},$$
$$2q \equiv r_2 \pmod{p},$$
$$\ldots\ldots\ldots$$
$$\ldots\ldots\ldots$$
$$\frac{p-1}{2}\, q \equiv r_{\frac{p-1}{2}} \pmod{p},$$

получимъ

$$q^{\frac{p-1}{2}} \cdot 1 \cdot 2 \cdot 3 \ldots \frac{p-1}{2} \equiv r_1 r_2 \ldots r_{\frac{p-1}{2}} \pmod{p},$$

или иначе

$$q^{\frac{p-1}{2}} \cdot 1 \cdot 2 \cdot 3 \ldots \frac{p-1}{2} \equiv a_1 a_2 \ldots a_{\rho} b_1 b_2 \ldots b_{\sigma} \pmod{p} \qquad (6)$$

Сопоставляя сравненія (5) и (6), получимъ

$$q^{\frac{p-1}{2}} \equiv (-1)^{\rho} \pmod{p},$$

откуда

$$\left(\frac{q}{p}\right) \equiv (-1)^{\rho}. \qquad (7)$$

Получается теорема: *если среди вычетовъ:*

$$r_1, r_2, \ldots, r_{\frac{p-1}{2}}$$

существуетъ ρ *большихъ* $\frac{p}{2}$, *то* q *будетъ квадратичнымъ вычетомъ числа* p, *если* ρ *будетъ четное, и невычетомъ, если* ρ *число нечетное.*

§ 20. Равенство (7) предыдущаго §-а позволяетъ трактовать вполнѣ задачу, поставленную въ § 17, относительно сравненія

$$x^2 \equiv 2 \pmod{p},$$

Рѣшеніе задачи формулируется въ видѣ слѣдующей теоремы, указанной Fermat'омъ и доказанной въ первый разъ Lagrange'емъ.

Теорема. *Число 2 есть квадратичный вычетъ простыхъ чиселъ вида* $8n+1$ и $8n+7$ *и невычетъ для простыхъ чиселъ вида* $8n+3$ и $8n+5$.

Въ самомъ дѣлѣ, при $q = 2$ числа

$$q, 2q, \ldots, \frac{p-1}{2}\, q$$

обращаются въ слѣдующія

$$2,\ 4,\ \ldots,\ p-1. \qquad (1)$$

Такъ какъ эти числа меньше p, то они совпадаютъ со своими вычетами по модулю p.

Для нахожденія числа ρ необходимо указать всѣ числа ряда (1), большія $\frac{p}{2}$. Итакъ, ρ нужно будетъ опредѣлить изъ неравенства

$$2\left\{\frac{p-1}{2}-\rho\right\}<\frac{p}{2}<2\left\{\frac{p-1}{2}-\rho+1\right\}.$$

Получаемъ неравенство

$$\frac{p-2}{4}<\rho<\frac{p+2}{4}.$$

Значитъ

$$\rho=\left[\frac{p+2}{4}\right] \text{ (см. Гл. II § 13).}$$

Разсмотримъ теперь предположенія

$$p=8n+1,\ 8n+3,\ 8n+5,\ 8n+7.$$

Получимъ

$$\rho=\left[\frac{8n+3}{4}\right],\ \left[\frac{8n+5}{4}\right],\ \left[\frac{8n+7}{4}\right],\ \left[\frac{8n+9}{4}\right],$$

т. е.

$$\rho=2n,\ 2n+1,\ 2n+1,\ 2n+2.$$

Итакъ, мы видимъ, что четныя значенія для ρ получаются въ двухъ случаяхъ

$$8n+1 \text{ и } 8n+7,$$

что подтверждаетъ справедливость высказанной теоремы.

§ 21. Обращаемся теперь къ случаю, когда q есть нечетное простое число.

Сохраняя обозначенія § 19, получаемъ рядъ равенствъ

$$\left.\begin{aligned} q&=p\left[\frac{q}{p}\right]+r_1\\ 2q&=p\left[\frac{2q}{p}\right]+r_2\\ &\cdots\cdots\cdots\\ &\cdots\cdots\cdots\\ p'q&=p\left[\frac{p'q}{p}\right]+r_{p'}\end{aligned}\right\}, \qquad (1)$$

гдѣ

$$p' = \frac{p-1}{2}.$$

Введемъ обозначенія

$$\Sigma a_i = A,$$

$$\Sigma b_i = B$$

и

$$P = \left[\frac{q}{p}\right] + \left[\frac{2q}{p}\right] + \ldots + \left[\frac{p'q}{p}\right].$$

Тогда получимъ, складывая равенства (1),

$$q\frac{p^2-1}{8} = pP + A + B. \tag{2}$$

Такъ какъ числа

$$p - a_1,\ p - a_2,\ \ldots,\ p - a_\rho,\ b_1,\ \ldots,\ b_\sigma$$

суть не что иное, какъ всѣ числа ряда

$$1,\ 2,\ \ldots,\ \frac{p-1}{2},$$

то, складывая, получимъ

$$p\rho - A + B = \frac{p^2-1}{8}. \tag{3}$$

Вычитая равенство (3) изъ (2), получимъ

$$(q-1)\frac{p^2-1}{8} = p(P-\rho) + 2A.$$

Такъ какъ имѣетъ мѣсто сравненіе

$$p \equiv -1 \pmod 2,$$

то получимъ слѣдующее сравненіе

$$\rho \equiv P + \frac{p^2-1}{8}(q-1) \pmod 2. \tag{4}$$

Разсмотримъ сначала случай

$$q = 2.$$

Въ этомъ случаѣ всѣ числа

$$q,\ 2q,\ \ldots,\ p'q$$

не превосходятъ $2p'$, слѣдовательно, они меньше p, откуда равняются нулю всѣ знаки E въ выраженіи P, такъ что получимъ

$$P = 0,$$

и мы получаемъ сравненіе

$$\rho \equiv \frac{p^2-1}{8} \pmod 2.$$

Отсюда получаемъ

$$\left(\frac{2}{p}\right) = (-1)^\rho = (-1)^{\frac{p^2-1}{8}}. \tag{5}$$

Равенство (5) еще разъ подтверждаетъ справедливость теоремы Fermat'a, доказанной нами въ § 20.

Если q число простое нечетное, то $q-1$ дѣлится на 2 и сравненіе (4) даетъ

$$\rho \equiv P \pmod 2;$$

слѣдовательно, получаемъ

$$\left(\frac{q}{p}\right) = (-1)^{\left[\frac{q}{p}\right]+\left[\frac{2q}{p}\right]+\cdots+\left[\frac{pq}{p}\right]}. \tag{6}$$

Обозначимъ для сокращенія

$$Q = \left[\frac{p}{q}\right]+\left[\frac{2p}{p}\right]+\cdots+\left[\frac{q'p}{q}\right], \text{ гдѣ } q' = \frac{q-1}{2}.$$

На основаніи соображеній Гл. II § 21

$$P + Q = \frac{p-1}{2}\frac{q-1}{2}. \tag{7}$$

Такъ какъ оба числа p и q простыя нечетныя, то будемъ имѣть два равенства

$$\left(\frac{q}{p}\right) = (-1)^P, \quad \left(\frac{p}{q}\right) = (-1)^Q.$$

Отсюда получаемъ

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{P+Q},$$

что на основаніи равенства (7) даетъ формулу

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

выражающую законъ взаимности двухъ нечетныхъ простыхъ чиселъ.

§ 22. Для удобства вычисленія символа Legendre'a, а также и для приложенія къ другимъ вопросамъ, Jacobi сдѣлалъ [1]) весьма важное обобщеніе символа Legendre'a.

[1]) Jacobi, Journ. f. Math 30 p. 172.

Пусть разсматривается нѣкоторое нечетное число P, разлагающееся на простыхъ множителей

$$p, p_1, p_2 \cdots$$

такъ что

$$P = pp_1p_2 \cdots$$

Опредѣлимъ новый символъ

$$\left(\frac{M}{P}\right)$$

при помощи равенства

$$\left(\frac{M}{P}\right) = \left(\frac{M}{p}\right)\left(\frac{M}{p_1}\right)\left(\frac{M}{p_2}\right)\cdots$$

при чемъ число M мы предполагаемъ взаимно простымъ съ числомъ P.

Если M квадратичный вычетъ числа P, то онъ долженъ быть согласно § 15 квадратичнымъ вычетомъ относительно всѣхъ простыхъ чиселъ

$$p, p_1, p_2, \cdots$$

такъ что имѣемъ равенства

$$\left(\frac{M}{p}\right) = 1. \quad \left(\frac{M}{p_1}\right) = 1, \quad \left(\frac{M}{p_2}\right) = 1, \ldots$$

Слѣдовательно, окончательно получимъ

$$\left(\frac{M}{P}\right) = 1. \tag{1}$$

Обратное предложеніе однако несправедливо, а именно, если имѣетъ мѣсто равенство (1), то изъ этого не слѣдуетъ, что M есть квадратичный вычетъ числа P, потому что символъ Jacobi будетъ равенъ $+1$ также въ томъ случаѣ, если среди входящихъ въ его составъ символовъ Legendre'a будетъ четное число, равныхъ (-1), между тѣмъ какъ достаточно для существованія такихъ равныхъ (-1) символовъ, чтобы число M было невычетомъ относительно нѣкоторыхъ простыхъ множителей числа P. Но тогда число M должно быть невычетомъ и относительно всего произведенія P.

Если имѣетъ мѣсто равенство

$$\left(\frac{M}{P}\right) = -1,$$

то число M, очевидно, невычетъ числа P.

Символъ Jacobi замѣчателенъ тѣмъ, что для него удовлетворяются всѣ выведенныя нами свойства символа Legendre'a.

§ 23. Докажемъ справедливость равенства

$$\left(\frac{M}{P}\right)\left(\frac{M}{Q}\right)=\left(\frac{M}{PQ}\right),$$

гдѣ P и Q взаимно простыя числа.

Раскладывая на простые множители, получимъ

$$P=pp_1p_2\ldots$$

$$Q=qq_1q_2\ldots$$

Получаемъ

$$\left(\frac{M}{PQ}\right)=\left(\frac{M}{p}\right)\left(\frac{M}{p_1}\right)\ldots\left(\frac{M}{q}\right)\left(\frac{M}{q_1}\right)\ldots=\left(\frac{M}{P}\right)\left(\frac{M}{Q}\right),$$

что и требовалось доказать.

§ 24. Не трудно убѣдиться въ справедливости слѣдующаго равенства

$$\left(\frac{L}{P}\right)\left(\frac{M}{P}\right)\left(\frac{N}{P}\right)\ldots=\left(\frac{LMN\ldots}{P}\right). \qquad (1)$$

Въ самомъ дѣлѣ, полагая $P=pp_1p_2\ldots$, получимъ

$$\left(\frac{L}{P}\right)=\left(\frac{L}{p}\right)\left(\frac{L}{p_1}\right)\left(\frac{L}{p_2}\right)\ldots$$

$$\left(\frac{M}{P}\right)=\left(\frac{M}{p}\right)\left(\frac{M}{p_1}\right)\left(\frac{M}{p_2}\right)\ldots \qquad (2)$$

$$\left(\frac{N}{P}\right)=\left(\frac{N}{p}\right)\left(\frac{N}{p_1}\right)\left(\frac{N}{p_2}\right)\ldots$$

. . . . . .

. . . . . .

Но въ § 10 мы имѣли уже, что

$$\left(\frac{L}{p}\right)\left(\frac{M}{p}\right)\left(\frac{N}{p}\right)\ldots=\left(\frac{LMN\ldots}{p}\right).$$

Слѣдовательно, перемножая равенства (2), получимъ

$$\left(\frac{L}{P}\right)\left(\frac{M}{P}\right)\left(\frac{N}{P}\right)\ldots=\left(\frac{LMN\ldots}{p}\right)\left(\frac{LMN\ldots}{p_1}\right)\left(\frac{LMN\ldots}{p_2}\right)\ldots,$$

откуда на основаніи опредѣленія символа Jacobi получается равенство (1).

Слѣдствіемъ выведенной теоремы будетъ упрощеніе выкладокъ съ символомъ Jacobi, состоящее въ томъ, что въ числителѣ такого символа можно пропускать множители, равные полному квадрату, ибо, если

$$M = L,$$

то имѣетъ мѣсто равенство:

$$\left(\frac{L^2 N \ldots}{P}\right) = \left(\frac{N \ldots}{P}\right),$$

такъ какъ множитель $\left(\frac{L}{P}\right)^2$ даетъ $(+1)$.

§ 25. Если

$$M \equiv M_1 \pmod{P}, \tag{1}$$

то

$$\left(\frac{M}{P}\right) = \left(\frac{M_1}{P}\right). \tag{2}$$

Въ самомъ дѣлѣ, сравненіе (1) влечетъ за собою, какъ слѣдствіе, рядъ такихъ

$$M \equiv M_1 \pmod{p}, \quad M \equiv M_1 \pmod{p_1}, \quad M \equiv M_1 \pmod{p_2} \ldots$$

откуда получаемъ

$$\left(\frac{M}{p}\right) = \left(\frac{M_1}{p}\right), \quad \left(\frac{M}{p_1}\right) = \left(\frac{M_1}{p_1}\right), \quad \left(\frac{M}{p_2}\right) = \left(\frac{M_1}{p_2}\right), \ldots$$

Перемножая эти равенства, получимъ равенство (2).

Итакъ, мы видимъ, что *въ символѣ Jacobi можно числителя его замѣнять остаткомъ, происходящимъ отъ дѣленія его на знаменателя.*

§ 26. *Имѣетъ мѣсто при всякомъ нечетномъ числѣ P равенство:*

$$\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}. \tag{1}$$

Въ самомъ дѣлѣ, принимая во вниманіе разложеніе на простые множители

$$P = pp_1p_2 \ldots,$$

получимъ

$$P = [1 + (p-1)][1 + (p_1 - 1)][1 + (p_2 - 1)] + \ldots =$$

$$= 1 + \Sigma(p-1) + 4k,$$

гдѣ k цѣлое число, а знакъ Σ распространяется на всѣхъ простыхъ множителей.

Итакъ,

$$\frac{P-1}{2} = \Sigma\frac{p-1}{2} + 2k,$$

т. е.

$$(-1)^{\Sigma\frac{p-1}{2}} = (-1)^{\frac{P-1}{2}}. \qquad (2)$$

Но, перемножая равенства

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{-1}{p_1}\right) = (-1)^{\frac{p_1-1}{2}}, \quad \left(\frac{-1}{p_2}\right) = (-1)^{\frac{p_2-1}{2}}, \ldots$$

и принимая во вниманіе равенство (2), получимъ равенство (1).

§ 27. Не трудно доказать также справедливость равенства

$$\left(\frac{2}{P}\right) = (-1)^{\frac{p^2-1}{8}}. \qquad (1)$$

Въ самомъ дѣлѣ, если p нечетное число, то $p^2 - 1$ дѣлится на 4, и слѣдовательно

$$P^2 = [1 + (p^2 - 1)][1 + (p_1{}^2 - 1)][1 + (p_2{}^2 - 1)] \ldots$$

даетъ

$$P^2 - 1 \equiv \sum(p^2 - 1) \pmod{16}.$$

Сокращая это сравненіе на 8, получимъ

$$\frac{P^2-1}{8} \equiv \sum\frac{p^2-1}{8} \pmod 2,$$

такъ что

$$(-1)^{\frac{P^2-1}{8}} = (-1)^{\Sigma\frac{p^2-1}{8}},$$

откуда слѣдуетъ справедливость равенства (1).

§ 28. Символъ Jacobi удовлетворяетъ равенству

$$\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}, \qquad (1)$$

которое, въ случаѣ P и Q нечетныхъ простыхъ, выражаетъ законъ взаимности.

На основаніи вышеприведенныхъ свойствъ символа Jacobi мы имѣемъ равенство

$$\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right) = H\left(\frac{q}{p}\right)\left(\frac{p}{q}\right),$$

гдѣ произведеніе Π распространяется на всѣ сочетанія каждаго нечетнаго простого дѣлителя числа Q съ каждымъ такимъ же дѣлителемъ p числа P. (P и Q мы предполагаемъ нечетными).

На основаніи закона взаимности можно написать

$$\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right) = \Pi(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = (-1)^{\sum\frac{p-1}{2}\frac{q-1}{2}}.$$

Очевидно, что

$$\sum\frac{p-1}{2}\frac{q-1}{2} = \sum\frac{p-1}{2}\sum\frac{q-1}{2}.$$

Но мы увидѣли, что

$$\sum\frac{p-1}{2} \equiv \frac{P-1}{2} \pmod 2,$$

а

$$\sum\frac{q-1}{2} \equiv \frac{Q-1}{2} \pmod 2,$$

слѣдовательно, имѣетъ мѣсто равенство (1).

§ 29. Для нѣкоторыхъ вопросовъ приложенія важно установить значеніе символа Jacobi въ случаѣ отрицательнаго знаменателя, при чемъ мы вводимъ такое опредѣленіе

$$\left(\frac{Q}{-P}\right) = \left(\frac{Q}{P}\right),$$

но при этомъ надо имѣть въ виду слѣдующее обстоятельство, а именно, что свойства символа Jacobi, выраженныя въ §§ 26 и 28, не всегда примѣняются, всѣ же остальныя свойства имѣютъ мѣсто и для новаго обобщенія символа Jacobi.

Свойство § 26 не имѣетъ мѣста при P отрицательномъ. Что касается до свойства § 28, выражающаго обобщенный законъ взаимности, *то оно сохраняется, если только одно изъ чиселъ P и Q отрицательное.*

Въ самомъ дѣлѣ, мы имѣемъ

$$\left(\frac{Q}{-P_1}\right)\left(\frac{-P_1}{Q}\right) = \left(\frac{Q}{P_1}\right)\left(\frac{P_1}{Q}\right)\left(\frac{-1}{Q}\right) =$$

$$= (-1)^{\frac{P_1-1}{2}\cdot\frac{Q-1}{2}}(-1)^{\frac{Q-1}{2}} = (-1)^{\left[\frac{P_1-1}{2}+1\right]\frac{Q-1}{2}}.$$

Прибавимъ къ множителю $\frac{P_1-1}{2}+1$ четное число $-1-P_1$, получимъ

$$\left(\frac{Q}{-P_1}\right)\left(\frac{-P_1}{Q}\right)=(-1)^{\frac{-P_1-1}{2}\cdot\frac{Q-1}{2}}.$$

Или обозначая $-P_1=P$, получаемъ

$$\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}},$$

что и требовалось показать.

§ 30. Приведенныя въ послѣднихъ параграфахъ свойства символа Jacobi даютъ удобный способъ вычисленія какъ символа Jacobi, такъ и символа Legendre'a.

Положимъ, что требуется вычислить численное значеніе символа

$$\left(\frac{783456}{9073421}\right).$$

Примѣняя опредѣленіе символа Jacobi, получимъ

$$\left(\frac{783456}{9073421}\right)=\left(\frac{2}{9073421}\right)^5\cdot\left(\frac{24483}{9073421}\right),$$

но по формулѣ § 27

$$\left(\frac{2}{9073421}\right)=-1,$$

слѣдовательно, заданный символъ будетъ равенъ

$$-\left(\frac{24483}{9073421}\right).$$

По закону взаимности получаемъ

$$-\left(\frac{24483}{9073421}\right)=-\left(\frac{9073421}{24483}\right),$$

но въ числителѣ символа можно написать остатокъ отъ дѣленія числителя на знаменателя, поэтому

$$-\left(\frac{9073421}{24483}\right)=-\left(\frac{14711}{24483}\right).$$

Разсуждая аналогично и дальше, имѣемъ

$$-\left(\frac{14711}{24483}\right)=\left(\frac{24483}{14711}\right)=\left(\frac{9772}{14711}\right)=\left(\frac{2}{14711}\right)^2\cdot\left(\frac{2443}{14711}\right)=\left(\frac{2443}{14711}\right)=$$

$$=-\left(\frac{14711}{2443}\right)=-\left(\frac{53}{2443}\right)=-\left(\frac{2443}{53}\right)=-\left(\frac{5}{53}\right)=-\left(\frac{53}{5}\right)=-\left(\frac{-2}{5}\right)=$$

$$=-\left(\frac{-1}{5}\right)\cdot\left(\frac{2}{5}\right);$$

но

$$\left(\frac{-1}{5}\right)=+1,\ \text{а}\ \left(\frac{2}{5}\right)=-1,$$

слѣдовательно, заданный символъ есть $+1$.

§ 31. Укажемъ очень простое правило Eisenstein'а[1]) для вычисленія символа Jacobi.

Если p и p_1 два взаимно простыхъ нечетныхъ числа, то составимъ систему уравненій

$$\begin{aligned}
p &= kp_1 + \varepsilon p_2\\
p_1 &= k_1p_2 + \varepsilon_1 p_3\\
p_2 &= k_2p_3 + \varepsilon_2 p_4\\
&\cdots\cdots\cdots\\
p_n &= k_np_{n+1} + \varepsilon_n,
\end{aligned}$$

гдѣ числа p, p_1, p_2, $\ldots$ p_n, p_{n+1} всѣ *положительныя нечетныя и убывающія*, т. е.

$$p > p_1 > p_2 > \ldots > p_n > p_{n+1},$$

а

$$\varepsilon=\pm 1,\ \varepsilon_1=\pm 1,\ \varepsilon_2=\pm 1,\ \ldots$$

Очевидно, что всѣ числа k, k_1, k_2, $\ldots$ должны быть четными.

Напишемъ около каждаго равенства

$$p_\mu = k_\mu p_{\mu+1} + \varepsilon_\mu p_{\mu+2}$$

нѣкоторое число, которое мы назовемъ *обочнымъ*.

---

[1]) Eisenstein, Einfacher Algorithmus zur Bestimmung des Werthes von $\left(\frac{a}{b}\right)$. Journ. f. Math. B. 27, 1844.

Пусть это обочное число есть *единица*, если имѣютъ мѣсто сравненія

$$p_{\nu+1} \equiv -1 \pmod 4\,, \quad \varepsilon_\nu p_{\nu+2} \equiv -1 \pmod 4$$

и *нуль* во всѣхъ остальныхъ случаяхъ.

Теорема Eisenstein'а состоитъ въ томъ, что *символъ* $\left(\frac{p}{p_1}\right)$ *равенъ* $(-1)^{\Sigma}$, *гдѣ* Σ *есть сумма обочныхъ чиселъ.*

Справедливость этой теоремы слѣдуетъ изъ такихъ формулъ

$$\left(\frac{p}{p_1}\right) = \left(\frac{\varepsilon p_2}{p_1}\right) = (-1)^{\frac{1}{2}(p_1-1)\frac{1}{2}(\varepsilon p_2-1)} \left(\frac{p_1}{p_2}\right) \quad ^{1)}$$

$$\left(\frac{p_1}{p_2}\right) = \left(\frac{\varepsilon_1 p_3}{p_2}\right) = (-1)^{\frac{1}{2}(p_2-1)\frac{1}{2}(\varepsilon_1 p_3-1)} \left(\frac{p_2}{p_3}\right)$$

. . . .

$$\left(\frac{p_n}{p_{n+1}}\right) = \left(\frac{\varepsilon_n}{p_{n+1}}\right) = (-1)^{\frac{1}{2}(p_{n+1}-1)\frac{1}{2}(\varepsilon_n-1)},$$

откуда черезъ умноженіе получимъ

$$\left(\frac{p}{p_1}\right) = (-1)^{\frac{1}{2}(p_1-1)\frac{1}{2}(\varepsilon p_2-1) + \frac{1}{2}(p_2-1)(\varepsilon_1 p_3-1) + \dots + \frac{1}{2}(p_{n+1}-1)\frac{1}{2}(\varepsilon_n-1)} =$$

$$= (-1)^{\Sigma},$$

что и требовалось доказать.

Примѣръ. Требуется найти значеніе $\left(\frac{4535}{2477}\right)$

$$\begin{array}{r|r|l}
2477 & 4535 & 2 \\
 & 4954 & \\
 & -419 & 2477 \mid 6 \\
 & & 2514 \\
 & & -37 \mid 419 \mid 12 \\
 & & \quad 444 \\
 & & \quad -25 \mid 37 \mid 2 \\
 & & \qquad 50 \\
 & & \qquad -13 \mid 25 \mid 2 \\
 & & \qquad\quad 26 \\
 & & \qquad\quad -1
\end{array}$$

Обочное число	
0	$4535 = 2 \cdot 2477 - 419$
1	$2477 = 6 \cdot 419 - 37$
0	$419 = 12 \cdot 37 - 25$
0	$37 = 2 \cdot 25 - 13$
0	$25 = 2 \cdot 13 - 1$

---

1) $\left(\frac{p_1}{\varepsilon p_2}\right) = \left(\frac{p_1}{p_2}\right)$ на основаніи § 29.

Отсюда окончательно

$$\left(\frac{4535}{2477}\right) = (-1)^{\varepsilon+1+0+0+0} = -1 .$$

§ 32. Обращаемся теперь къ окончанію рѣшенія задачи, поставленной въ § 17, а именно, къ нахожденію всѣхъ нечетныхъ простыхъ чиселъ, для которыхъ заданное число D есть квадратичный вычетъ.

Поставимъ задачу болѣе общимъ образомъ, а именно: найдемъ всѣ нечетныя положительныя числа n, взаимно простыя съ D и удовлетворяющія уравненію

$$\left(\frac{D}{n}\right) = +1 . \tag{1}$$

Въ § 16 мы видѣли, что задача приводится къ разсмотрѣнію дѣлителей квадратичной формы

$$x^2 - Dy^2 .$$

Что касается числа D, то мы его можемъ предполагать не дѣлящимся ни на какой квадратъ цѣлаго числа; слѣдовательно, относительно числа D можно дѣлать слѣдующія предположенія

1) или $D = \pm P$,

2) или $D = \pm 2P$,

гдѣ P есть произведеніе первыхъ степеней нѣкоторыхъ нечетныхъ простыхъ чиселъ.

§ 33. I.

$$D = \pm P \equiv 1 \pmod 4 .$$

Возьмемъ положительное число n, взаимно простое съ числомъ $2D$. Тогда, на основаніи обобщеннаго закона взаимности, получимъ

$$\left(\frac{D}{n}\right) = \left(\frac{n}{P}\right).$$

Итакъ, для нахожденія всѣхъ чиселъ n, удовлетворяющихъ уравненію (1) § 31, достаточно разсмотрѣть всѣ числа, несравнимыя между собою по модулю P, при чемъ придется разсматривать только $\varphi(P)$ чиселъ, меньшихъ P и взаимно простыхъ съ P.

Покажемъ, что изъ этихъ чиселъ существуетъ

$$\frac{1}{2}\varphi(P)$$

чиселъ таковыхъ, что удовлетворяютъ равенству

$$\left(\frac{n}{P}\right) = +1,$$

а другія

$$\frac{1}{2}\varphi(P)$$

этихъ чиселъ удовлетворяютъ уравненію

$$\left(\frac{n}{P}\right) = -1.$$

Будемъ числа первой категоріи называть числами a, а числа второй категоріи обозначать черезъ b. Если число P есть простое число, то справедливость этого предложенія мы уже видѣли въ § 5 главы V, ибо въ этомъ случаѣ числа a суть не что иное, какъ квадратичные вычеты числа P, а числа b квадратичные невычеты.

Обращаясь теперь къ общему случаю нечетнаго составного числа P, покажемъ прежде всего, что существуетъ по крайней мѣрѣ одно число b, удовлетворяющее равенству

$$\left(\frac{b}{P}\right) = -1.$$

Въ самомъ дѣлѣ, такъ какъ число D мы не предполагаемъ равнымъ единицѣ, то существуетъ по крайней мѣрѣ одинъ простой множитель p, заключающійся въ числѣ P; получаемъ

$$P = p \cdot P_1,$$

гдѣ p и P_1 числа взаимно простыя.

На основаніи соображеній § 16 главы III можемъ подобрать число b такъ, чтобы оно удовлетворяло двумъ сравненіямъ

$$b \equiv \beta \pmod{p} \text{ и } b \equiv 1 \pmod{P_1}, \tag{1}$$

гдѣ β одинъ изъ невычетовъ числа p.

Отсюда мы видимъ, что

$$\left(\frac{b}{P}\right) = \left(\frac{b}{p}\right)\left(\frac{b}{P_1}\right) = \left(\frac{\beta}{p}\right)\left(\frac{1}{P_1}\right) = -1.$$

Итакъ, найдя по крайней мѣрѣ одно изъ чиселъ b, покажемъ, что половина всѣхъ чиселъ, взаимно простыхъ съ P, принадлежитъ къ числамъ a, а половина къ числамъ b.

Обозначимъ черезъ m всякое число, меньшее P и взаимно простео съ P и разсмотримъ сумму:

$$S = \sum \left(\frac{m}{P}\right),$$

гдѣ сумма распространяется на всѣ числа m.

Такъ какъ найденное нами число b взаимно простое съ P [на основаніи формулъ (1)], то, слѣдовательно, всѣ числа bm имѣютъ своими вычетами по модулю P всю систему чиселъ m (см. § 7 главы III).

Итакъ, имѣемъ

$$S = \sum \left(\frac{bm}{P}\right) = \sum \left(\frac{b}{P}\right)\left(\frac{m}{P}\right) = \left(\frac{b}{P}\right)\sum \left(\frac{m}{P}\right) = -S,$$

откуда

$$S = 0.$$

Значитъ, въ суммѣ $\sum \left(\frac{m}{P}\right)$ такое же число членовъ, равныхъ $+1$, какъ и членовъ, равныхъ -1.

Мы можемъ ограничиться разсмотрѣніемъ нечетныхъ значеній m, если всякое четное число m замѣнимъ нечетнымъ числомъ $m + P$; при этомъ мы должны расширить число классовъ чиселъ и разсматривать числа уже по модулю $2P$, такъ что окончательно мы получаемъ $\frac{1}{2}\varphi(P)$ классовъ чиселъ, удовлетворяющихъ или условіямъ

$$\left(\frac{D}{n}\right) = +1\,;\ n \equiv a \pmod{2P}$$

или условіямъ

$$\left(\frac{D}{n}\right) = -1\,.\ n \equiv b \pmod{2P},$$

гдѣ a и b нечетныя числа.

Поясникъ сказанное примѣромъ

$$P = 33\,;\ \varphi(P) = 20\,.$$

Всѣ числа, меньшія P и взаимно-простыя съ P, будутъ

$$\pm 1\,;\ \pm 2\,;\ \pm 4\,;\ \pm 5\,;\ \pm 7\,;\ \pm 8\,;\ \pm 10\,;\ \pm 13\,;\ \pm 14\,;\ \pm 16\,.$$

Провѣрка даетъ

$$a = \pm 1\,;\ \pm 2\,;\ \pm\ 4\,;\ \pm\ 8\,;\ \pm 16\,,$$

а

$$b = \pm 5\,;\ \pm 7\,;\ \pm 10\,;\ \pm 13\,;\ \pm 14\,;$$

слѣдовательно,

$$\left(\frac{33}{n}\right) = +1,$$

когда

$$n \equiv 1;\ 17;\ 25;\ 29;\ 31;\ 35;\ 37;\ 41;\ 49;\ 65 \pmod{66}$$

и

$$\left(\frac{33}{n}\right) = -1,$$

когда

$$n \equiv 5;\ 7;\ 13;\ 19;\ 23;\ 43;\ 47;\ 53;\ 59;\ 61 \pmod{66}.$$

§ 34. II.

$$D = \pm P \equiv 3 \pmod 4.$$

Обозначая снова черезъ n положительное число, взаимно простое съ числомъ $2D$, получимъ, примѣняя обобщенный законъ взаимности:

$$\left(\frac{D}{n}\right) = (-1)^{\frac{D-1}{2}\cdot\frac{n-1}{2}}\left(\frac{n}{P}\right) = (-1)^{\frac{n-1}{2}}\cdot\left(\frac{n}{P}\right);$$

и будетъ слѣдующее рѣшеніе нашей задачи

$$\left(\frac{D}{n}\right) = +1,$$

когда

$$n \equiv 1 \pmod 4 \text{ и } n \equiv a \pmod P$$

или когда

$$n \equiv 3 \pmod 4 \text{ и } n \equiv b \pmod P,$$

и

$$\left(\frac{D}{n}\right) = -1,$$

когда

$$n \equiv 1 \pmod 4 \text{ и } n \equiv b \pmod P$$

или когда

$$n \equiv 3 \pmod 4 \text{ и } n \equiv a \pmod P.$$

Итакъ, мы видимъ, что задача приводится къ прежней задачѣ нахожденія чиселъ a и b, удовлетворяющихъ условіямъ

$$\left(\frac{a}{P}\right) = +1 \text{ и } \left(\frac{b}{P}\right) = -1.$$

Такъ какъ въ этомъ случаѣ число n должно удовлетворять двумъ сравненіямъ по модулю 4 и по модулю P, то получаются классы чиселъ по модулю $4P$.

Примѣръ.

$$D = +15.$$

Тогда

$$\left(\frac{D}{n}\right) = +1,$$

если

$$n \equiv 1 \pmod 4$$

и

$$n \equiv +1;\ +2;\ +4;\ -7 \pmod{15}$$

или если

$$n \equiv 3 \pmod 4$$

и

$$n \equiv -1;\ -2;\ -4;\ +7 \pmod{15},$$

и

$$\left(\frac{D}{n}\right) = -1,$$

если

$$n \equiv 1 \pmod 4$$

и

$$n \equiv -1;\ -2;\ -4;\ +7 \pmod{15}$$

или если

$$n \equiv 3 \pmod 4$$

и

$$n \equiv +1;\ +2;\ +4;\ -7 \pmod{15}.$$

Отсюда слѣдуетъ окончательно

$$\left(\frac{15}{n}\right) = +1,$$

когда

$$n \equiv 1;\ 7;\ 11;\ 17;\ 43;\ 49;\ 53;\ 59 \pmod{60}$$

и

$$\left(\frac{15}{n}\right) = -1,$$

когда

$$n \equiv 13;\ 19;\ 23;\ 29;\ 31;\ 37;\ 41;\ 47 \pmod{60}.$$

§ 35. III.

$$D = \pm 2P \equiv 2 \pmod 8.$$

Въ этомъ случаѣ, если n означаетъ положительное число, взаимно простое съ D, имѣемъ

$$\left(\frac{D}{n}\right) = (-1)^{\frac{1}{8}(n^2-1)} \cdot \left(\frac{n}{P}\right)$$

и, слѣдовательно,

$$\left(\frac{D}{n}\right) = +1,$$

если

$$n \equiv \pm 1 \pmod 8 \quad \text{и} \quad n \equiv a \pmod P$$

или если

$$n \equiv \pm 3 \pmod 8 \quad \text{и} \quad n \equiv b \pmod P,$$

и

$$\left(\frac{D}{n}\right) = -1,$$

если

$$n \equiv \pm 1 \pmod 8 \quad \text{и} \quad n \equiv b \pmod P$$

или если

$$n \equiv \pm 3 \pmod 8 \quad \text{и} \quad n \equiv a \pmod P.$$

Каждой парѣ сравненій соотвѣтствуетъ классъ чиселъ n по модулю $8P$.

§ 36. IV.

$$D = \pm 2P \equiv 6 \pmod 8.$$

Въ этомъ случаѣ

$$\left(\frac{D}{n}\right) = (-1)^{\frac{1}{2}(n-1) + \frac{1}{8}(n^2-1)} \cdot \left(\frac{n}{P}\right);$$

слѣдовательно,

$$\left(\frac{D}{n}\right) = +1,$$

если

$$n \equiv 1;\ 3 \pmod 8 \quad \text{и} \quad n \equiv a \pmod P$$

или если

$$n \equiv 5;\ 7 \pmod 8 \quad \text{и} \quad n \equiv b \pmod P$$

и

$$\left(\frac{D}{n}\right) = -1,$$

если

$$n \equiv 1;\ 3 \pmod 8 \quad \text{и} \quad n \equiv b \pmod P$$

или если

$$n \equiv 5;\ 7 \pmod 8 \quad \text{и} \quad n \equiv a \pmod P.$$

И въ этомъ случаѣ получаются классы чиселъ n по модулю $8P$.

ГЛАВА VI.

Связь съ теоріей группъ.

§ 1. Euler'ова теорія вычетовъ степеней по простому модулю, изложенная нами въ предыдущей главѣ можетъ быть разсматриваема какъ частный случай болѣе общей теоріи, носящей названіе *теоріи группъ*.

Эта теорія, настолько же старая по ея внутреннему содержанію, какъ сама математическая мысль, получила лишь въ послѣднее время окончательную формулировку.

Въ основѣ теоріи лежитъ понятіе о такъ называемой *группѣ* однородныхъ предметовъ, понятіе, давшее возможность сблизить самыя разнородныя части математики.

§ 2. Формулируемъ понятіе о группѣ въ его современномъ самомъ общемъ видѣ. Разсматривается совокупность $\mathfrak{M}$ нѣкоторыхъ однородныхъ предметовъ. Эти предметы могутъ быть самой разнообразной природы: числа, формулы, аналитическія операціи, геометрическія фигуры, механическія движенія и т. д. Число предметовъ совокупности $\mathfrak{M}$ можетъ быть какъ конечное такъ и безконечное.

§ 3. Установимъ понятіе объ операціи *сопоставленія* или *композиціи* предметовъ совокупности $\mathfrak{M}$. Предположимъ, что указаны правила, по которымъ всякимъ двумъ предметамъ A и B совокупности $\mathfrak{M}$ сопоставляемъ нѣкоторый опредѣленный предметъ C той же совокупности. Такое сопоставленіе будемъ обозначать символическимъ равенствомъ

$$A * B = C$$

гдѣ знакъ $*$ есть знакъ композиціи, которую будемъ иногда называть *символическимъ умноженіемъ*. Композицію будемъ предполагать, вообще говоря дѣйствіемъ не перестановочнымъ, то есть будемъ считать два результата композиціи

$$A * B \text{ и } B * A,$$

вообще говоря, различными.

§ 4. *Опредѣленіе группы. Группой называется всякая совокупность G предметовъ $\mathfrak{M}$, обладающая слѣдующими четырьмя свойствами:*

I. *Композиція всякихъ двухъ предметовъ совокупности G даетъ предметъ той же совокупности.*

II. *Композиція предметовъ совокупности G обладаетъ сочетательнымъ (ассоціативнымъ) закономъ*

$$A*(B*C)=(A*B)*C.$$

III. *Существуютъ въ совокупности G предметы I такого вида, что для всякаго предмета A изъ совокупности G имѣетъ мѣсто равенство*

$$A*I=A.$$

Предметъ I носитъ названіе **правой единицы** *группы.*

IV. *Для нѣкоторой опредѣленной изъ единицъ I и для всякаго предмета A совокупности G существуетъ въ совокупности G другой предметъ X, удовлетворяющій равенству*

$$A*X=I;$$

элементъ X носитъ названіе **праваго обратнаго относительно A**.

§ 5. Предметы, входящіе въ составъ группы, носятъ названіе ея *элементовъ.*

Если число элементовъ группы конечное, то группа называется *конечною*, въ обратномъ случаѣ *безконечною.* Число элементовъ конечной группы называется ея *порядкомъ.*

Можно доказать, что данные въ предыдущемъ параграфѣ четыре постулата: I, II, III, и IV, опредѣляющіе группу, независимы между собой.

§ 6. Не имѣя въ виду излагать полную теорію группъ, мы остановимся только на самыхъ важныхъ свойствахъ группъ.

Покажемъ прежде всего, что существуетъ только одна единственная единица въ группѣ.

Допустимъ существованіе двухъ единицъ I и I_1, причемъ единица I есть та, которая требуется въ постулатѣ IV.

На основаніи постулата IV можемъ единицѣ I_1 сопоставить элементъ X такой, чтобы было

$$I_1*X=I. \tag{1}$$

Умножая въ смыслѣ композиціи это равенство слѣва на I_1, получимъ

$$I_1*(I_1*X)=I_1*I,$$

откуда

$$(I_1*I_1)*X=I_1*I, \tag{2}$$

но I и I_1 единицы, слѣдовательно

$$I_1 * I_1 = I_1, \quad I_1 * I = I_1,$$

и равенство (2) дастъ

$$I_1 * X = I_1,$$

откуда, сравнивая съ (1), получимъ

$$I = I_1.$$

§ 7. Покажемъ, что единственная правая единица I есть въ то же самое время и лѣвая. Положимъ что

$$I * A = B. \tag{1}$$

Докажемъ, что $B = A$.

Возьмемъ для A правый обратный элементъ Y и умножимъ на него справа равенство (1)

$$I * A * Y = B * Y,$$

гдѣ

$$A * Y = I, \tag{2}$$

получаемъ

$$I * I = B * Y.$$

Сравнивая съ (2) получимъ

$$A * Y = B * Y.$$

Умножая послѣднее равенство справа на элементъ обратный Y получимъ

$$A = B$$

что и требовалось доказать.

§ 8. Покажемъ наконецъ, что правый обратный элементъ есть въ то же самое время и лѣвый обратный, то есть что равенство

$$A * X = I \tag{1}$$

влечетъ за собой какъ слѣдствіе

$$X * A = I. \tag{2}$$

Въ самомъ дѣлѣ, умножая равенство (1) слѣва на X, получимъ

$$X * A * X = X,$$

и наконецъ, умножая справа на элементъ обратный X, получимъ равенство (2).

§ 9. Резюмируя сказанное, мы замѣчаемъ, что въ группѣ существуетъ всегда единственная единица, ее мы будемъ обозначать черезъ 1.

При символическомъ умноженіи въ смыслѣ композиціи элементовъ группы элементы равные единицѣ можно пропускать

$$1 * A * 1 * B * C = A * B * C .$$

Кромѣ того для всякаго элемента A существуетъ въ группѣ элементъ обратный, которой мы будемъ обозначать знакомъ A^{-1}, причемъ можно будетъ писать

$$A * A^{-1} = 1 ; \; A^{-1} * A = 1 .$$

Нетрудно убѣдиться, что обратный элементъ единственный.

Обратный элементъ для обратнаго есть первоначальный, т. е.

$$(A^{-1})^{-1} = A .$$

Нетрудно видѣть, что для группы рѣшаются всегда уравненія первой степени

$$A * X = B, \; Y * A = B,$$

гдѣ A и B заданные элементы, а X элементъ искомый. Мы получаемъ

$$X = A^{-1} * B, \; Y = B * A^{-1}.$$

§ 10. Если для всякихъ двухъ элементовъ группы имѣетъ мѣсто *переставочный (коммутативный)* законъ композиціи т. е.

$$A * B = B * A$$

то группа носитъ названіе *абелевой* или *коммутативной*.

11. Разсмотримъ классы чиселъ (см. гл. III § 5) по нѣкоторому модулю k. Установимъ операцію композиціи классовъ, которую будемъ обозначать какъ обыкновенное умноженіе въ алгебрѣ, то есть вмѣсто знака $A * B$ будетъ писать $A . B$.

Всякій классъ A по модулю k состоитъ изъ чиселъ вида $a + kx$, гдѣ x цѣлое число, причемъ a есть какое нибудь произвольно выбранное число класса A.

Возьмемъ изъ класса A нѣкоторое число a, а изъ класса B число b, тогда подъ классомъ C, составленнымъ изъ классовъ A и B при помощи композиціи $C = A . B$ будемъ разумѣть классъ, образованный изъ чиселъ

$$x \equiv ab \pmod{k} .$$

Такъ напр., при $k = 10$, получается отъ композиціи классовъ

$$A = (3 + 10x) \text{ и } B = (4 + 10x)$$

классъ

$$C = (2 + 10x)$$

ибо

$$2 \equiv 3 \cdot 4 \pmod{10}.$$

§ 12. Посмотримъ, образуютъ ли группу различные классы по модулю k.

Первый постулатъ I имѣетъ мѣсто, ибо отъ композиціи двухъ классовъ получается всегда также классъ.

Второй постулатъ II также имѣетъ мѣсто, такъ какъ композиціи классовъ соотвѣтствуетъ умноженіе по модулю, которое, какъ обыкновенное умноженіе цѣлыхъ чиселъ, обладаетъ свойствомъ сочетательнымъ

$$(ab)c = a(bc).$$

Третій постулатъ III о существованіи единицы также подтверждается, ибо такую единицу представляетъ классъ чиселъ x, удовлетворяющихъ сравненію

$$x \equiv 1 \pmod{k}.$$

Обращаемся теперь къ четвертому постулату о существованіи для всякаго элемента обратнаго, то есть, о рѣшеніи символическаго уравненія

$$AX = 1.$$

Искомый классъ X обратный классу A найдется черезъ рѣшеніе сравненія

$$xa \equiv 1 \pmod{k},$$

гдѣ a одно изъ чиселъ класса A.

Очевидно, что послѣднее сравненіе невозможно, если коэффиціентъ a не есть число взаимно простое съ k.

Итакъ, классы по модулю k не образуютъ группу, ибо для классовъ A не взаимно простыхъ съ k не существуетъ обратнаго элемента, и слѣдовательно, постулатъ IV не имѣетъ мѣста.

§ 13. Мы получимъ группу, если разсмотримъ только классы взаимно простые съ модулемъ k. Такимъ образомъ получается очень важная въ анализѣ группа *приведенныхъ вычетовъ по модулю k*. Очевидно, что порядокъ такой группы равенъ $\varphi(k)$.

Если k число простое, то $\varphi(k) = k - 1$ и приведенные вычеты будутъ

$$1, 2, 3, \ldots k-1.$$

Итакъ, въ этомъ случаѣ группу приведенныхъ вычетовъ образуютъ всѣ классы кромѣ одного, соотвѣтствующаго нулю.

§ 14. Теорема Euler'a $a^{\varphi(k)} \equiv 1 \pmod{k}$ и ея частный случай при k простомъ, теорема Fermat'a $a^{k-1} \equiv 1 \pmod{k}$, суть въ свою очередь частные случаи болѣе общей теоремы, относящейся къ произвольнымъ конечнымъ группамъ.

Если мы обозначимъ для сокращенія

$$A * A = A^2,\ A * A * A = A^3,\ A * A * A * A = A^4, \text{ и т. д.,}$$

то можно будетъ высказать такую теорему.

Теорема. Если h есть порядокъ группы G то для всякаго ея элемента A имѣетъ мѣсто равенство

$$A^h = 1 .$$

§ 15. Для доказательства этой теоремы введемъ въ разсмотрѣніе одно новое весьма важное понятіе, а именно, понятіе о *подгруппѣ*.

Если изъ элементовъ группы G можно составить новую группу G_1, то эта группа G_1 называется *подгруппой* или *дѣлителемъ* группы G.

§ 16. *Теорема Lagrange'a.* Порядокъ подгруппы конечной группы есть дѣлитель порядка самой группы.

Пусть задана группа G порядка n и разсматривается нѣкоторая ея подгруппа H порядка m.

Пусть элементы группы H будутъ

$$1,\ A_1,\ A_2,\ A_3,\ \ldots\ A_{m-1}. \qquad (1)$$

Если элементы (1) исчерпываютъ группу G то $H = G$ и $m = n$. Теорема справедлива.

Если элементы (1) не исчерпываютъ группу G, то въ этой послѣдней можно найти такой элементъ B_1, который не входитъ въ подгруппу H. Будемъ композицію элементовъ обозначать какъ обыкновенное умноженіе и составимъ рядъ элементовъ

$$B_1,\ A_1 . B_1,\ A_2 . B,\ A_3 . B_1,\ \ldots\ A_{m-1} . B_1, \qquad (2)$$

не трудно убѣдиться, что элементы ряда (2) различны между собой и отличны отъ элементовъ ряда (1). Въ самомъ дѣлѣ, если предположимъ, что

$$A_i . B_1 = A_k . B_1 ,$$

то по умноженію обѣихъ частей справа на B_1^{-1} получимъ

$$A_i = A_k ,$$

что невозможно, ибо въ рядѣ (1) элементы не повторяются.

Невозможно, чтобы одинъ элементъ ряда (2) равнялся элементу ряда (1), т. е. другими словами, невозможно равенство

$$A_i . B_1 = A_k ,$$

ибо тогда по умноженіи слѣва на A_i^{-1}, мы получимъ

$$B_1 = A_i^{-1} . A_k ;$$

выходило бы, что B_1 принадлежитъ къ подгруппѣ H, ибо къ этой подгруппѣ принадлежатъ оба элемента

$$A_i^{-1} \text{ и } A_k .$$

Если ряды (1) и (2) исчерпываютъ группу G, то будетъ, очевидно, $2m = n$ и теорема справедлива. Если ряды (1) и (2) группы G не исчерпываютъ, то въ этой группѣ G можно найти новый элементъ B_2, не входящій ни въ одинъ изъ рядовъ (1) и (2), тогда въ группѣ G будетъ заключаться весь рядъ

$$B_2 , \; A_1 . B_2 , \; A_2 . B_2 , \; \ldots \; A_{m-1} . B_2 . \qquad (3)$$

Рядъ (3) заключаетъ только различные элементы, отличные отъ элементовъ рядовъ (1) и (2).

Послѣ послѣдовательнаго составленія нѣкотораго числа k рядовъ (1), (2), (3) и т. д. конечная группа будетъ исчерпана, и мы получаемъ

$$mk = n ,$$

откуда мы видимъ, что цѣлое число m есть, дѣйствительно, дѣлитель числа n.

Ряды (2), (3), и т. д. носятъ названіе *сопряженныхъ системъ* по отношенію къ подгруппѣ H.

§ 17. Возьмемъ произвольный элементъ A группы G и составимъ рядъ степеней

$$A , \; A^2 , \; A^3 , \; A^4 , \; \ldots \qquad (1)$$

продолженный неопредѣленно.

Нетрудно убѣдиться, что если группа G конечная, то рядъ (1) дастъ нѣкоторую ея подгруппу.

Такъ какъ всѣ элементы безконечнаго ряда (1) суть въ то же самое время элементы конечной группы G, то всѣ элементы ряда (1) не могутъ быть различны, а, слѣдовательно, въ ряду (1) должны встрѣчаться одинаковые элементы, напримѣръ

$$A^{k+l} = A^l .$$

Умножая это равенство справа (или слѣва) на $(A^{-1})^l$, получимъ

$$A^k = 1 . \qquad (2)$$

Итакъ, существуетъ нѣкоторое цѣлое число k, удовлетворяющее равенству (2). Пусть q будетъ наименьшій показатель, при которомъ имѣетъ мѣсто равенство

$$A^q = 1 . \qquad (3)$$

Очевидно, что тогда всякій показатель k, удовлетворяющій уравненію (2), долженъ быть числомъ кратнымъ наименьшаго q. Въ самомъ дѣлѣ, будемъ дѣлить k на q, обозначая черезъ s частное и черезъ r остатокъ, такъ что

$$k = qs + r, \text{ гдѣ } r < q .$$

Уравненіе

$$A^k = 1$$

даетъ

$$A^k = A^{qs+r} = A^{qs} . A^r = 1^s . A^r = A^r = 1 ,$$

и мы получимъ уравненіе противорѣчащее тому, что q есть наименьшій показатель, дающій единицу.

Итакъ, должно быть $r = 0$, и мы получаемъ

$$k = qs ,$$

что и требовалось доказать.

§ 18. Пусть q будетъ наименьшій показатель, при которомъ имѣетъ мѣсто равенство

$$A^q = 1 ,$$

тогда говорятъ, что элементъ A *принадлежитъ къ показателю q*.

Не трудно убѣдиться, что q долженъ быть дѣлителемъ порядка n группы. Это слѣдуетъ изъ теоремы Lagrange'a, ибо элементы

$$1 , A^1 , A^2 , A^3 , \ldots A^{q-1} \qquad (1)$$

всѣ различны и образуютъ группу.

То, что всѣ элементы (1) различны, слѣдуетъ изъ того, что равенство

$$A^i = A^j , \text{ гдѣ } j < i < q ,$$

влечетъ какъ слѣдствіе такое невозможное

$$A^{i-j} = 1 ,$$

ибо $i - j < q$.

Элементы (1) образуютъ группу, ибо кромѣ первыхъ трехъ постулатовъ выполняется еще и постулатъ IV, такъ какъ всякому элементу A^i соотвѣтствуетъ обратный A^{q-i}.

§ 19. Изъ соображеній предыдущаго §-а слѣдуетъ теорема § 14, которую мы и хотѣли доказать.

Въ самомъ дѣлѣ, показатель q, къ которому принадложитъ элементъ A, есть дѣлитель порядка n группы; значитъ $n = qs$.

Возвышая символически, въ смыслѣ композиціи, въ степень s равенство

$$A^q = 1,$$

получимъ

$$A^n = 1,$$

что и требовалось доказать.

§ 20. Очевидно, что для теоріи группъ не важно установленіе механизма символическаго умноженія, т. е. при помощи какого алгориѳма или, вообще говоря, по какимъ правиламъ будетъ это умноженіе производиться, а важно лишь указаніе структуры группы, т. е. указаніе того, какой именно элементъ C группы получается отъ символическаго умноженія двухъ данныхъ элементовъ A и B. Структура группы есть нѣчто не зависящее отъ природы элементовъ ея. Можно указать двѣ группы совершенно разной природы, имѣющія одно и то же число элементовъ и одинаковую структуру.

Въ самомъ дѣлѣ, положимъ, что можно составить двѣ группы: одну изъ элементовъ

$$A_1, A_2, \ldots A_n.$$

другую изъ элементовъ

$$B_1, B_2, \ldots B_n,$$

которыя обладаютъ свойствомъ, что всякому равенству

$$A_i A_k = A_l$$

будетъ соотвѣтствовать равенство

$$B_i B_k = B_l.$$

Такія двѣ группы, имѣющія одинаковую структуру, называются *изоморфными* и могутъ считаться за одну и ту же группу съ точки зрѣнія теоріи группъ.

§ 21. Поставимъ теперь слѣдующую важную задачу.

Нельзя ли заданной абелевой группѣ предметовъ какой угодно природы

$$A_1, A_2, \ldots A_n \qquad (1)$$

сопоставить изоморфную группу

$$\alpha_1, \alpha_2, \ldots \alpha_n, \qquad (2)$$

элементы которой α_i суть числа, такимъ образомъ, чтобы символическому умноженію элементовъ группы (1)

$$A_i . A_k$$

соотвѣтствовало обыкновенное умноженіе

$$\alpha_i \alpha_k$$

соотвѣтствующихъ чиселъ (2)?

Эта задача имѣетъ утвердительное рѣшеніе, а именно группа чиселъ (2) можетъ быть всегда составлена, причемъ составлена не однимъ, а нѣсколькими способами.

Числа α_i носятъ названіе *характеровъ*[1]) соотвѣтственныхъ элементовъ A_i. Мы будемъ характеръ обозначать знакомъ

$$\alpha_i = \chi(A_i).$$

Нетрудно видѣть, что характеромъ групповой единицы должно быть непремѣнно число 1, потому что групповая единица при символическомъ умноженіи на другой элементъ не мѣняетъ этого послѣдняго, а, значитъ, его характеръ долженъ быть такимъ числомъ, которое при умноженіи не мѣняетъ множителя; такое число только одно, единица 1. Итакъ, символическому равенству $A_i = 1$ должно соотвѣтствовать обыкновенное $\alpha_i = 1$, или, иначе,

$$1 = \chi(1).$$

Пусть m_i будетъ показатель, къ которому принадлежитъ элементъ A_i, тогда, очевидно, символическому равенству

$$A_i^{m_i} = 1$$

должно соотвѣтствовать числовое

$$\alpha_i^{m_i} = 1. \qquad (1)$$

Итакъ, характеры абелевой группы оказываются корнями изъ единицы.

Отсюда дѣлается понятной та замѣчательная связь, которая существуетъ между абелевыми группами съ одной стороны и теоріей двучленныхъ уравненій (1) съ другой. Такъ какъ многіе называютъ теорію двучленныхъ уравненій теоріей дѣленія круга, начала которой установлены Gauss'омъ, то получается связь между абелевыми группами и теоріей дѣленія круга.

§ 22. Frobenius и Schur[2]) обобщили понятіе о характерахъ абелевыхъ группъ на случай группъ какихъ угодно.

---

[1]) Это названіе введено Gauss'омъ и Dirichlet.

[2]) Sitzungsberichte der Berliner Academie 1896. 1905.

ГЛАВА VII.

Теорія полей.

§ 1. Теорія *ансамблей или множествъ* (Mengenlehre), изучающая совокупности предметовъ съ самой широкой точки зрѣнія, является въ настоящее время самой общей математической дисциплиной и въ нѣкоторыхъ ея частяхъ настолько выходитъ въ область общей философской мысли, что почти теряетъ математическое свое содержаніе.

Мы переходимъ отъ понятія ансамбля, какъ совокупности предметовъ самаго общаго вида, къ понятію о *группѣ*, если мы устанавливаемъ законъ спариванія этихъ предметовъ или, какъ мы сказали въ предыдущей главѣ, законъ ихъ композиціи.

Понятіе о группѣ дѣлается уже, но зато оно пріобрѣтаетъ больше математическаго содержанія.

Дальнѣйшее суженіе понятія ансамбля мы получимъ, если подчинимъ его предметы двумъ различнымъ законамъ композиціи, тогда мы приходимъ къ понятію о *полѣ* (область раціональности, Zahlkörper).

§ 2. Самымъ важнымъ примѣромъ поля является такъ называемое *раціональное поле*.

Къ нему мы приходимъ изъ слѣдующихъ соображеній. Если мы разсмотримъ совокупность чиселъ раціональныхъ, то мы замѣчаемъ, что эта совокупность обладаетъ групповымъ характеромъ относительно двухъ дѣйствій: сложенія и умноженія.

Въ самомъ дѣлѣ, всѣ раціональныя числа образуютъ абелеву группу относительно *сложенія*, ибо существуютъ свойства

$$a + b = b + a$$

$$(a + b) + c = a + (b + c).$$

Существуетъ одна единица этой группы, а именно число 0 (нуль). Всякому элементу a группы соотвѣтствуетъ ему обратный $-a$, ибо

$$a+(-a)=0.$$

На основаніи сказаннаго въ § 9 предыдущей главы, въ группѣ всегда возможно рѣшеніе уравненія первой степени

$$a+x=b,$$

то есть всегда выполняется дѣйствіе вычитанія, какъ операція обратная сложенію.

§ 3. На основаніи сказаннаго мы можемъ назвать совокупность раціональныхъ чиселъ *аддитивной группой*. Единицей этой группы является число нуль. Если мы это число *отнимемъ*, то получаемъ совокупность чиселъ представляющихъ абелеву группу относительно *дѣйствія умноженія*, ибо существуютъ свойства

$$ab=ba$$

$$(ab)c=a(bc).$$

Единицей этой группы является число 1; всякому элементу a соотвѣтствуетъ обратный $\frac{1}{a}$, ибо

$$a\frac{1}{a}=1.$$

Въ этой группѣ, которую назовемъ *мультипликативною*, всегда возможно рѣшеніе уравненія первой степени

$$ax=b$$

т. е. всегда возможно дѣйствіе *дѣленія*.

§ 4. Число 0, умноженное на любое число разсматриваемой совокупности даетъ 0 т. е.

$$0.a=0.$$

§ 5. Дѣйствія сложенія и умноженія удовлетворяютъ *распредѣлительному* (дистрибутивному) закону

$$(a+b)c=ac+bc.$$

§ 6. Совокупность чиселъ, обладающихъ указаными въ §§ 2, 3, 4, 5 формальными законами дѣйствій сложенія и умноженія, мы будемъ называть *числовымъ полемъ*.

Элементарная алгебра даетъ три примѣра подобныхъ полей: 1, полераціональныхъ чиселъ, 2, поле чиселъ вещественныхъ (какъ раціональныхъ, такъ и ирраціональныхъ), 3, поле чиселъ комплексныхъ.

Общее опредѣленіе поля.

Полемъ мы будемъ называть совокупность такихъ предметовъ $a, b, c, \ldots$, названныхъ его *элементами*, которые можно подчинить двумъ различнымъ пріемамъ композиціи, изъ которыхъ одинъ назовемъ *сложеніемъ* $(a+b)$, а другой *умноженіемъ* (ab), при чемъ имѣютъ мѣсто слѣдующіе постулаты.

I. Всѣ элементы поля образуютъ группу относительно сложенія, единицу которой обозначимъ черезъ 0.

II. Всѣ элементы поля за исключеніемъ 0 образуютъ группу относительно умноженія.

III. Имѣетъ мѣсто распредѣлительный законъ

$$(a+b)c = ac + bc.$$

IV. Для всякаго элемента a имѣетъ мѣсто

$$0 \cdot a = 0.$$

V. Обѣ группы аддитивная и мультипликативная суть абелевы т. е.

$$a + b = b + a, \quad ab = ba.$$

§ 7. Сдѣлаемъ нѣсколько весьма важныхъ замѣчаній по поводу только что даннаго опредѣленія поля.

Вслѣдствіе группового характера поля дѣйствіе вычитанія въ немъ всегда возможно. Что касается до дѣйствія дѣленія, то оно возможно для всѣхъ элементовъ за исключеніемъ случая дѣленія на единицу аддитивной группы. Эта единица обладаетъ въ полѣ всѣми свойствами числа 0 элементарной алгебры.

Произведеніе нѣсколькихъ множителей въ полѣ можетъ тогда и только тогда равняться аддитивной единицѣ, если одинъ изъ множителей равенъ этой единицѣ.

§ 8. Разсматривая внимательно указанные въ § 6 пять постулатовъ, мы можемъ замѣтить, что въ постулатѣ V достаточно требовать *только, чтобы мультипликативная группа была перестановочною*. тогда можно

доказать, что при существованіи четырехъ первыхъ постулатовъ и аддитивная группа будетъ перестановочна.

Въ самомъ дѣлѣ, возьмемъ единицу мультипликативной группы [1] и два произвольныхъ элемента a и b. Будемъ имѣть на основаніи первыхъ постулатовъ

$$a+b+a+b=(a+b)+(a+b)=[1](a+b)+[1](a+b)=$$

$$=\{[1]+[1]\}(a+b)=(a+b)\{[1]+[1]\}=a\{[1]+[1]\}+b\{[1]+[1]\}=$$

$$=\{[1]+[1]\}a+\{[1]+[1]\}b=a+a+b+b$$

итакъ,

$$a+b+a+b=a+a+b+b,$$

Прибавляя къ обѣимъ частямъ слѣва $-a$ и справа $-b$, получимъ

$$b+a=a+b,$$

т. е. получаемъ коммутативность аддитивной группы.

§ 9. Разсматривая три поля, извѣстныхъ изъ элементарной алгебры, мы замѣчаемъ, что первое поле *раціональныхъ чиселъ* заключается какъ часть въ двухъ остальныхъ: полѣ *вещественныхъ чиселъ* и полѣ *комплексныхъ чиселъ*.

Если элементы поля Ω входятъ въ составъ другого поля Ω_1, то поле Ω носитъ названіе *дѣлителя* поля Ω_1. Такъ, напримѣръ, поле вещественныхъ чиселъ есть дѣлитель поля комплексныхъ чиселъ.

Не трудно показать, что поле раціональныхъ чиселъ есть дѣлитель всякаго поля. Въ самомъ дѣлѣ, возьмемъ какой нибудь элементъ ω поля Ω, тогда поле Ω должно заключать элементъ $\frac{\omega}{\omega}$, т. е. число единицу; изъ единицы же можно получить всѣ цѣлыя числа при помощи сложенія, вычитанія и умноженія, изъ цѣлыхъ же чиселъ происходятъ дробныя черезъ дѣленіе.

Болѣе строгая формулировка только что указаннаго свойства получится, если мы введемъ весьма важное понятіе о такъ называемомъ *изоморфизмѣ* полей.

Такъ какъ элементами поля могутъ быть предметы какой угодно природы, не обязательно числа, то мы считаемъ за одно поле два такъ называемыхъ изоморфныхъ поля т. е. такихъ, что всякому раціональному

соотношенію

$$f(a, b, c, \ldots) = 0$$

элементовъ $a, b, c, \ldots$ одного поля соотвѣтствуетъ тождественное соотношеніе

$$f(a', b', c', \ldots) = 0$$

соотвѣтственныхъ элементовъ $a', b', c', \ldots$ другого.

Такой изоморфизмъ двухъ полей устанавливаетъ однозначное соотвѣтствіе каждому элементу a перваго поля нѣкотораго опредѣленнаго элемента a' другого.

Если поле таково, что его элементы не числа, а предметы другой природы, то мультипликативная единица [1] поля можетъ не быть числомъ 1, тогда получаемъ теорему, что всякое поле Ω имѣетъ дѣлителемъ нѣкоторое другое поле R, изоморфное съ полемъ раціональныхъ чиселъ; это поле R назовемъ *ариѳметическою частью* поля Ω.

§ 10. Пусть задано числовое поле Ω и нѣкоторое число α, не входящее въ составъ поля Ω. Разсмотримъ теперь поле, образованное числами поля Ω, а также всевозможными новыми, получаемыми отъ комбинированія числа α съ числами поля Ω при помощи основныхъ дѣйствій.

Очевидно, что всякое число новаго поля будетъ вида

$$\frac{\varphi(\alpha)}{\psi(\alpha)}$$

гдѣ $\varphi(\alpha)$ и $\psi(\alpha)$ суть цѣлыя функціи отъ α съ коэффиціентами, принадлежащими полю Ω.

Будемъ обозначать новое поле такъ

$$\Omega(\alpha)$$

и говорить, что оно происходитъ отъ *присоединенія* къ полю Ω числа α.

Если къ полю $\Omega(\alpha)$ присоединимъ новое число β, то получимъ поле

$$\Omega(\alpha\ \beta),$$

которое происходитъ изъ поля Ω черезъ присоединеніе двухъ чиселъ α и β.

Подобнымъ же образомъ можно присоединить любое число чиселъ.

§ 11. Разсмотримъ цѣлую раціональную функцію

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n,$$

съ коэффиціентами

$$a_0,\ a_1,\ \ldots\ a_{n-1},\ a_n$$

принадлежащими къ нѣкоторому полю Ω.

Будемъ называть такую функцію *принадлежащею полю* Ω, или просто *функціей поля* Ω.

Если функція $f(x)$ разлагается на два множителя

$$\varphi(x) \text{ и } \psi(x),$$

такъ что

$$f(x) = \varphi(x)\psi(x),$$

причемъ цѣлыя функціи $\varphi(x)$ и $\psi(x)$ принадлежатъ тому же полю Ω, то будемъ говорить, что функція $f(x)$ *приводимая въ полѣ* Ω, т. е. нахожденіе ея корней приводится къ нахожденію корней функцій $\varphi(x)$ и $\psi(x)$ меньшихъ степеней.

Если разложеніе функціи $f(x)$ на множители, принадлежащіе тому же полю, невозможно, то говорятъ, что функція *неприводима* въ полѣ Ω.

Одна и та же функція можетъ быть неприводимою въ одномъ полѣ и приводимою въ другомъ. Такъ напримѣръ, функція

$$x^4 + 1$$

неприводима въ полѣ раціональныхъ чиселъ и приводима въ такомъ полѣ, которое получается отъ присоединенія къ раціональнымъ числамъ числа

$$\sqrt{2},$$

ибо

$$x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1).$$

Въ полѣ всѣхъ чиселъ какъ вещественныхъ такъ и комплексныхъ всякая функція выше первой степени приводима и раскладывается на линейные множители, что составляетъ основную теорему алгебры.

§ 12. Необходимо обратить вниманіе, что формула Taylor'a для цѣлыхъ функцій остается справедливою и для цѣлыхъ функцій нѣкотораго поля, ибо эта формула

$$f(x+h) = f(x) + hf'(x) + \frac{h^2}{1\,.\,2}f''(x) + \ldots + \frac{h^n}{1\,.\,2\,.\,3\ldots n}f^{(n)}(x)$$

происходитъ отъ разложенія $f(x+h)$ по степенямъ h; для цѣлыхъ же функцій такое разложеніе совершается при помощи раціональныхъ дѣйствій.

Разъ формула Taylor'a сохраняется въ полѣ, то отсюда вытекаютъ для поля всѣ тѣ же слѣдствія относительно кратныхъ корней, которыя излагаются въ алгебрѣ.

§ 13. Теорема. *Неприводимая въ полѣ* Ω *функція* $f(x)$ *не имѣетъ общаго дѣлителя съ другою* $F(x)$ *того же поля, если* $F(x)$ *не дѣлится на* $f(x)$.

Эта теорема, имѣющая большое значеніе, почти очевидна. Въ самомъ дѣлѣ, будемъ искать общаго наибольшаго дѣлителя полиномовъ

$$F(x) \text{ и } f(x)$$

послѣдовательнымъ дѣленіемъ. Очевидно, что коэффиціенты этого общаго дѣлителя происходятъ при помощи раціональныхъ операцій изъ коэффиціентовъ функцій $F(x)$ и $f(x)$, слѣдовательно, общій дѣлитель долженъ принадлежать тому же полю Ω. Но заданная функція $f(x)$ не имѣетъ въ полѣ Ω другихъ дѣлителей кромѣ самое себя и постояннаго числа. Отсюда, общій наибольшій дѣлитель долженъ быть равнымъ самой функціи $f(x)$ или быть постояннымъ.

Слѣдствіе I. Неприводимая функція не можетъ имѣть кратныхъ корней.

Въ самомъ дѣлѣ, если бы существовалъ кратный корень, то производная $f'(x)$, имѣя общаго дѣлителя съ неприводимой функціей $f(x)$, должна была бы дѣлиться на $f(x)$, что невозможно, ибо степень производной ниже степени самой функціи.

Слѣдствіе II. Если функція $F(x)$ *обращается въ нуль при одномъ изъ корней неприводимой функціи* $f(x)$, *то она уничтожается и при всѣхъ остальныхъ корняхъ функціи* $f(x)$.

Слѣдствіе III. Если степень цѣлой функціи $F(x)$ *ниже степени неприводимой функціи* $f(x)$ *и если* $F(x)$ *обращается въ нуль при одномъ корнѣ функціи* $f(x)$, *то функція* $F(x)$ *должна тождественно обращаться въ нуль, т. е. всѣ ея коэффиціенты должны равняться нулю.*

Слѣдствіе IV. Приводимая функція разлагается однимъ только способомъ на неприводимыхъ множителей. При этомъ двѣ цѣлыхъ функціи, отличающіяся постояннымъ множителемъ, не считаются различными.

§ 14. Присоединенія новыхъ величинъ раздѣляются на двѣ категоріи: присоединенія *алгебраическія* и присоединенія *трансцендентныя*.

Присоединеніе называется трансцендентнымъ, если между различными степенями присоединяемой буквы x не устанавливается никакихъ соотношеній. Поле, получаемое отъ присоединенія къ полю Ω трансцендентной величины X, является совокупностью всѣхъ раціональныхъ функцій отъ X съ коэффиціентами изъ поля Ω.

Гораздо болѣе простой видъ имѣетъ поле, когда между различными степенями присоединяемой буквы α имѣетъ мѣсто линейное соотношеніе, т. е., другими словами, когда присоединяемая величина α есть корень ал-

гебраическаго уравненія

$$F(x) = 0\,, \qquad (1)$$

гдѣ $F(x)$ неприводимая въ основномъ полѣ Ω функція.

Мы будемъ называть также и уравненіе (1) *неприводимымъ* въ полѣ Ω. Черезъ присоединеніе къ полю Ω корня α уравненія (1) получается поле $\Omega(\alpha)$, которое называется *алгебраическимъ полемъ*.

§ 15. Пусть уравненіе $F(x) = 0$ имѣетъ видъ

$$x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n = 0\,,$$

гдѣ a_1, a_2, $\ldots$ a_{n-1}, a_n суть числа поля Ω.

Степень n послѣдняго уравненія носитъ названіе *степени* алгебраическаго поля $\Omega(\alpha)$.

Самый общій видъ числа Θ поля $\Omega(\alpha)$ есть

$$\Theta = \frac{\varphi(\alpha)}{\psi(\alpha)}\,,$$

гдѣ φ и ψ цѣлыя функціи съ коэффиціентами изъ поля Ω.

Изъ общаго курса алгебры извѣстно, что всякая раціональная функція отъ корня неприводимаго уравненія n-ой степени можетъ быть представлена при помощи раціональныхъ выкладокъ въ видѣ цѣлой функціи степени не выше $n - 1$, т. е.

$$\Theta = c_o + c_1\alpha + c_2\alpha^2 + \ldots + c_{n-1}\alpha^{n-1} \qquad (1)$$

гдѣ коэффиціенты

$$c_o\,,\ c_1\,,\ c_2\,,\ \ldots\ c_{n-1}$$

принадлежатъ также къ полю Ω.

Такое представленіе (1) элемента Θ возможно однимъ способомъ, ибо, если бы существовало другое представленіе

$$\Theta = c_o' + c_1'\alpha + c_2'\alpha^2 + \ldots + c'_{n-1}\alpha^{n-1}, \qquad (2)$$

то корень α неприводимаго уравненія степени n поля Ω удовлетворялъ бы уравненію

$$c - c_o' + (c_1 - c_1')\alpha + (c_2 - c_2')\alpha^2 + \ldots + (c_{n-1} - c'_{n-1})\alpha^{n-1} = 0$$

того же поля, откуда на основаніи слѣдствія III § 13 получаемъ

$$c_o' = c_o\,,\ c_1' = c_1\,,\ \ldots\ c'_{n-1} = c_{n-1}\,.$$

Итакъ, поле $\Omega(\alpha)$ есть совокупность чиселъ Θ, опредѣляемыхъ формулой (1), гдѣ коэффиціенты

$$c_0, c_1, c_2, \ldots c_{n-1}$$

суть всевозможные элементы поля Ω.

§ 16. Мы будемъ разсматривать алгебраическія поля болѣе общаго вида

$$\Omega(\alpha, \beta, \gamma, \ldots),$$

получаемыя отъ присоединенія къ полю Ω корней

$$\alpha, \beta, \gamma,$$

одного или нѣсколькихъ уравненій поля Ω.

Докажемъ теперь весьма важное предложеніе, состоящее въ томъ, что одновременное присоединеніе нѣсколькихъ корней одного или нѣсколькихъ уравненій равносильно присоединенію *одного* корня *одного* уравненія. Такимъ путемъ мы приходимъ къ заключенію, что самый общій видъ алгебраическаго поля даетъ поле происходящее отъ присоединенія къ основному одного только алгебраическаго числа.

§ 17. Докажемъ предварительно лемму.

Лемма. Пусть

$$\Phi_1(x, y, z, \ldots), \Phi_2(x, y, z, \ldots), \Phi_3(x, y, z, \ldots), \ldots$$

суть цѣлыя раціональныя функціи перемѣнныхъ $x, y, z, \ldots$ съ произвольными коэффиціентами. Если ни у одной изъ этихъ функцій всѣ коэффиціенты не обращаются сразу въ нуль, то можно на безчисленное число способовъ дать перемѣннымъ такія раціональныя значенія, что ни одна изъ функцій не обратится въ нуль.

Предложеніе очевидно для случая, когда функціи зависятъ отъ одной независимой перемѣнной. Очевидно, что въ этомъ случаѣ функціи будутъ обращаться въ нуль только при своихъ корняхъ, число же такихъ корней конечное, а потому, если независимому перемѣнному дадимъ значеніе, отличное отъ этихъ корней, то ни одна изъ функцій

$$\Phi_1, \Phi_2, \Phi_3, \ldots$$

не обратится въ нуль.

Что касается большаго числа независимыхъ перемѣнныхъ, то нетрудно убѣдиться въ справедливости леммы въ случаѣ m перемѣнныхъ, если лемма доказана для $m-1$ перемѣнныхъ.

Каждую изъ функцій можно представить въ видѣ полинома отъ одной изъ перемѣнныхъ, напр. x, съ коэффиціентами, которые будутъ цѣлыми функціями отъ $m-1$ остальныхъ перемѣнныхъ

$$y, z, \ldots$$

По предположенію справедливости леммы въ случаѣ $m-1$ перемѣнныхъ можно будетъ буквамъ

$$y, z, \ldots$$

на безчисленное число способовъ придать такія раціональныя значенія, что не уничтожатся сразу коэффиціенты каждой изъ этихъ функцій, а тогда остальной перемѣнной можно дать такое значеніе, что всѣ функціи будутъ отличны отъ нуля.

§ 18. Разсмотримъ поле

$$\Omega(\alpha, \beta, \gamma, \ldots).$$

Возьмемъ линейную функцію

$$\xi = x\alpha + y\beta + z\gamma + \ldots,$$

гдѣ α — корень нѣкотораго уравненія

$$A(x) = 0 \tag{1}$$

изъ поля Ω, β — корень уравненія

$$B(x) = 0, \tag{2}$$

γ — корень уравненія

$$C(x) = 0 \quad \text{и т. д.} \tag{3}$$

Обозначая черезъ $\alpha_1, \beta_1, \gamma_1 \ldots$ другую комбинацію корней соотвѣтственныхъ уравненій, положимъ

$$\xi_1 = x\alpha_1 + y\beta_1 + z\gamma_1 + \ldots$$

Составимъ подобнымъ образомъ новыя выраженія $\xi_2, \xi_3, \ldots$ Число такихъ выраженій будетъ равно произведенію степеней функціи $A(x)$, $B(x)$, $C(x)$, $\ldots$ Замѣтимъ кстати, что нѣтъ надобности предполагать всѣ уравненія (1), (2), (3), $\ldots$ различными.

Разности

$$\xi - \xi_1, \ \xi - \xi_2, \ \xi - \xi_3, \ \ldots$$

суть линейныя функціи отъ $x, y, z, \ldots$, причемъ ни одна изъ нихъ не

равна тождественно нулю, ибо мы, очевидно, предполагаемъ уравненія (1), (2), (3), ... неприводимыми и, слѣдовательно, не имѣющими кратныхъ корней.

По леммѣ § 15 можно дать $x, y, z, \ldots$ такія раціональныя численныя значенія, что всевозможныя разности, составленныя изъ функцій ξ, ξ_1, ξ_2, ... будутъ отличны отъ нуля, а, слѣдовательно, и всѣ значенія ξ, ξ_1, ξ_2, . . будутъ различны между собой.

Обратимъ теперь вниманіе, что всякая функція симметричная относительно корней каждаго изъ уравненій (1), (2), (3), ... по извѣстной теоремѣ алгебры будетъ выражаться раціонально черезъ коэффиціенты этихъ уравненій. Слѣдовательно, такая величина есть число поля Ω.

Къ подобнымъ функціямъ принадлежатъ, очевидно, коэффиціенты полинома

$$F(t) = (t - \xi)(t - \xi_1)(t - \xi_2) \ldots$$

Уравненіе $F(t) = 0$ есть, слѣдовательно, уравненіе поля Ω. не имѣющее кратныхъ корней. Одинъ изъ корней этого уравненія есть ξ.

Пусть Θ будетъ какой нибудь элементъ поля

$$\Omega(\alpha, \beta, \gamma, \ldots)$$

и, слѣдовательно, цѣлая функція отъ корней

$$\alpha, \beta, \gamma, \ldots$$

Обозначимъ черезъ

$$\Theta_1, \Theta_2, \ldots$$

величины, которыя происходятъ изъ величины Θ черезъ замѣну корней

$$\alpha, \beta, \gamma, \ldots$$

новыми комбинаціями корней

$$\alpha_1, \beta_1, \gamma_1, \ldots$$

$$\alpha_2, \beta_2, \gamma_2, \ldots$$

$$\ldots\ldots\ldots$$

Разсмотримъ функцію

$$F(t)\left[\frac{\Theta}{t-\xi} + \frac{\Theta_1}{t-\xi_1} + \frac{\Theta_2}{t-\xi_2} + \ldots\right].$$

Очевидно, что эта функція есть цѣлая относительно t. Коэффиціенты ея суть симметрическія функціи корней уравненій (1), (2), (3), ... а потому эта цѣлая функція, которую мы обозначимъ черезъ $\psi(t)$, принадлежитъ къ полю Ω.

Отсюда мы получаемъ

$$\frac{\psi(t)}{F(t)} = \frac{\Theta}{t-\xi} + \frac{\Theta_1}{t-\xi_1} + \frac{\Theta_2}{t-\xi_2} + \ldots$$

По теоремѣ Lagrange'a мы знаемъ, что

$$\Theta = \frac{\psi(\xi)}{F'(\xi)}.$$

Итакъ, Θ выражается раціональною функціею отъ ξ съ коэффиціентами, принадлежащими къ полю Ω. Слѣдовательно, всякая величина поля $\Omega(\alpha, \beta, \gamma, \ldots)$ принадлежитъ полю $\Omega(\xi)$. Съ другой стороны очевидно, что всякая величина поля $\Omega(\xi)$ есть въ тоже время элементъ поля $\Omega(\alpha, \beta, \gamma, \ldots)$, ибо ξ выражается раціонально черезъ $\alpha, \beta, \gamma, \ldots$

Итакъ, мы заключаемъ о полной тождественности двухъ полей, что можно выразить равенствомъ

$$\Omega(\xi) = \Omega(\alpha, \beta, \gamma, \ldots).$$

§ 19. Kronecker'у мы обязаны геніальными соображеніями, относящимися къ трансцедентнымъ присоединеніямъ и находящимися въ извѣстной аналогіи съ теоремой, доказаной въ предыдущемъ параграфѣ. Въ знаменитомъ мемуарѣ „Grundzüge einer arithmetischen Theorie der algebraischen Grössen“ Kronecker вводитъ въ разсмотрѣніе раціональныя функціи отъ любого числа перемѣнныхъ независимыхъ съ коэффиціентами, принадлежащими къ данному полю. У Kronecker'а получается теорія, которая также не зависитъ отъ числа присоединенныхъ перемѣнныхъ. Коренное различіе состоитъ въ томъ, что Kronecker пользуется трансцендентнымъ присоединеніемъ для изученія свойствъ основного поля, которое онъ предполагаетъ алгебраическимъ. Weber во второмъ томѣ своей алгебры даетъ хорошее изложеніе теоріи Kronecker'а, причемъ называетъ эту теорію „*теоріей функціоналовъ*“.

§ 20. Поставимъ вопросъ, когда два алгебраическихъ поля изоморфны. Мы будемъ предполагать у обоихъ полей основнымъ полемъ *раціональное поле* Ω.

Пусть одно поле будетъ $\Omega(\alpha)$; если это поле изоморфно другому Ω_1, то элементу α перваго поля долженъ соотвѣтствовать элементъ α_1 другого. Разсмотримъ неприводимое уравненіе

$$a_0\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha + a_n = 0; \qquad (1)$$

очевидно, что на основаніи принципа изоморфности этому уравненію въ другомъ полѣ должно соотвѣтствовать такое

$$a_0\alpha_1^n + a_1\alpha_1^{n-1} + \ldots + a_{n-1}\alpha_1 + a_n = 0,$$

ибо раціональнымъ числамъ одного поля должны соотвѣтствовать тѣ же самыя числа въ другомъ.

Итакъ, мы получаемъ

$$\Omega_1 = \Omega(\alpha_1),$$

т. е. алгебраическому полю $\Omega(\alpha)$ соотвѣтствуетъ какъ изоморфное поле $\Omega(\alpha_1)$, гдѣ α_1 другой корень того же самаго уравненія (1).

§ 19. Присоединяя послѣдовательно корни

$$\alpha,\ \alpha_1,\ \alpha_2,\ \ldots$$

одного и того же неприводимаго уравненія, получимъ рядъ полей

$$\Omega(\alpha),\ \Omega(\alpha_1),\ \Omega(\alpha_2),\ \ldots$$

изоморфныхъ между собой, которыя называются *сопряженными* съ полемъ

$$\Omega(\alpha).$$

Если всѣ сопряженныя поля тождественны между собой, то поле $\Omega(\alpha)$ носитъ названіе *нормальнаго* поля.

§ 20. Итакъ, мы видѣли рядъ примѣровъ на безконечныя поля. Основными являются три главныхъ поля элементарной алгебры. Затѣмъ имѣютъ важное значеніе поля, получаемыя отъ присоединенія новыхъ элементовъ. Исчерпываются ли этими примѣрами всѣ мыслимыя поля? Отвѣтъ на этотъ вопросъ оказывается отрицательнымъ. Въ послѣднее время данъ примѣръ новаго вида поля. Такое поле образуютъ символы новой природы, введенные въ науку K. Hensel'емъ подъ названіемъ *p-адическихъ чиселъ*. Я считаю необходимымъ сказать нѣсколько словъ объ этихъ числахъ.

§ 21. Возьмемъ нѣкоторое простое число p и будемъ разсматривать системныя (десятичныя) дроби при системѣ счисленія, имѣющей основаніемъ число p. Такъ, напримѣръ, системная дробь

$$b_4 b_3 b_2 b_1 b_0,\ a_1 a_2 a_3 a_4 \ldots, \tag{1}$$

гдѣ цифры b_4, b_3, b_2, b_1, b_0, a_1, $\ldots$ суть цѣлыя числа меньшія p или нули, обозначаетъ какъ извѣстно сумму

$$b_4 p^4 + b_3 p^3 + b_2 p^2 + b_1 p + b_0 + \frac{a_1}{p} + \frac{a_2}{p^2} + \frac{a_3}{p^3} + \ldots$$

Hensel предлагаетъ употреблять подъ названіемъ p-адическихъ чиселъ, тѣ же самые символы (1), но только производить надъ этими числами дѣйствія сложенія, вычитанія, умноженія и дѣленія по другимъ правиламъ.

Измѣненіе правилъ простѣйшихъ дѣйствій, указанное Hensel'емъ, состоитъ въ томъ, что разряды, которымъ соотвѣтствуютъ цифры въ обычной ариѳметикѣ возрастаютъ справа налѣво, Hensel же предполагаетъ разряды возрастающими слѣва направо, т. е. какъ будто бы символъ (1) обозначалъ сумму

$$\frac{b_4}{p^4}+\frac{b_3}{p^3}+\frac{b_2}{p^2}+\frac{b_1}{p}+b_0+a_1p+a_2p^2+a_3p^3+\ldots \qquad (2)$$

Такимъ образомъ въ правилѣ сложенія, если при сложеніи соотвѣтствующихъ цифръ накопляется единица высшаго разряда, то ее надо прибавлять къ ближайшей цифрѣ *направо*, а не къ лѣвой цифрѣ какъ въ ариѳметикѣ. Подобнымъ же образомъ при вычитаніи, если необходимо занять единицу высшаго разряда, то ее надо занимать изъ ближайшей направо стоящей цифры.

Могутъ возразить, что при безконечномъ числѣ цифръ p-адическаго числа сумма (2) представляетъ рядъ расходящійся и потому не допустима къ употребленію. Но дѣло въ томъ, что мы можемъ вовсе не отождествлять p-адическаго числа съ суммой (2), а лишь пользоваться видомъ этой суммы для установленія дѣйствій надъ p-адическими числами.

Вообще говоря p-адическія числа суть символы, съ которыми *не совмѣщается никакого понятія о величинѣ*, и для которыхъ понятія больше и меньше отпадаютъ.

Не останавливаясь подробно на теоріи чиселъ p-адическихъ, пояснимъ дѣйствія съ этими числами на примѣрахъ.

Пусть будетъ $p=5$.

Сложеніе.

$$\begin{array}{r} 1111111 \\ 2,341021 \\ 3,003443 \\ 4,432411 \\ \hline 4,3324311 \end{array}$$

Начинаемъ всѣ дѣйствія съ крайнихъ лѣвыхъ цифръ.

Складываемъ первыя цифры

$$2+3+4=5\,.\,1+4\,.$$

Пишемъ первую цифру 4 суммы и единицу высшаго рязряда прибавляемъ къ суммѣ слѣдующихъ направо цифръ.

Вычитаніе.

$$\begin{array}{r} \ldots\ldots\ldots \\ -\ 2,431021000000\ldots \\ 3,244322400000\ldots \\ \hline 4,141143044444\ldots \end{array}$$

Умноженіе.

$$\begin{array}{r} 2,341 \\ 3,122 \\ \hline \end{array}$$

$$\begin{array}{lr} 2,341 \times 3 = & \ldots . \; 6,(9)(12)(3) \\ 2,341 \times 0,1 = & \ldots \quad (2)(3)(4)(1) \\ 2,341 \times 0,02 = & \ldots \quad (4)(6)(8)(2) \\ 2,341 \times 0,002 = & \ldots \quad (4)(6)(8)(2) \end{array}$$

$$1,2\ 1\ 1\ 4\ 3\ 4$$

Дѣленіе. Для установленія дѣленія надо будетъ при нахожденіи каждой послѣдовательной цифры частнаго рѣшать сравненіе вида

$$ax \equiv b \pmod{p}$$

$$\begin{array}{l|l} 2,143 & 3,1 \\ 2,11 & 4,014333\ldots \\ \hline 033 & \\ 31 & \\ \hline 200 & \\ 211 & \\ \hline 434444\ldots & \\ 44 & \\ \hline 43444\ldots & \\ \ldots\ldots & \end{array}$$

Первая цифра частнаго получается изъ сравненія

$$3x \equiv 2 \pmod{5},$$

т. е.

$$x = 4.$$

Нетрудно усмотрѣть, что раціональнымъ числамъ будутъ соотвѣтствовать періодическія p-адическія числа. При этомъ всѣ раціональныя числа какъ положительныя такъ и отрицательныя попадутъ среди p-адическихъ чиселъ.

Число $i = \sqrt{-1}$ находится среди p-адическихъ при $p = 5$, ибо -1 есть квадратичный вычетъ числа 5. Получается $i = 2,121\ldots$, $-i = 3,323\ldots$ такъ что можно написать такое p-адическое тождество

$$x^2 + 1 = (x - 2,121\ldots)(x - 3,323\ldots).$$

Выраженіе $x^2 - 2$ неразложимо p-адически при $p = 5$, ибо 2 есть невычетъ числа 5.

Существуетъ простое правило узнать по виду періодическаго p-адическаго числа, какому обыкновенному числу оно соотвѣтствуетъ: положительному или отрицательному.

Если послѣдняя (направо) цифра періода больше послѣдней (направо) цифры, стоящей передъ періодомъ, то p-адическое число соотвѣтствуетъ отрицательному числу, напримѣръ

$$-2 = 3,444\ldots \text{ (ибо } 4 > 3).$$

Если же послѣдняя цифра періода меньше послѣдней цифры передъ первымъ періодомъ, то число соотвѣтствуетъ положительному числу напримѣръ

$$\frac{2,143}{3,1} = \frac{2 + 1 . 5 + 4 . 5^2 + 3 . 5^3}{3 + 1 . 5} = 4,\ 014333 \ldots \text{(ибо } 3 < 4).$$

§ 22. Нетрудно убѣдиться, что p-адическія числа образуютъ поле.

Если мы будемъ разсматривать g-адическія числа, то есть, такія числа, гдѣ основаніемъ счисленія является составное число g, то такія числа не образуютъ уже поля, потому что при такихъ числахъ произведеніе двухъ отличныхъ отъ нуля чиселъ можетъ давать нуль

Напримѣръ при $g = 10$

$$\begin{array}{r} 5,213023 \ldots \\ 2,110100 \\ \hline (10),426046 \ldots \\ 521302 \ldots \\ 52130 \ldots \\ 521 \ldots \\ \hline 0,000000 \ldots \end{array}$$

ГЛАВА VIII.

Теорія конечнаго поля.

§ 1. Обращаемся теперь къ разсмотрѣнію очень важнаго вопроса, важнаго какъ въ принципіальномъ отношеніи такъ и по его приложеніямъ. Вопросъ этотъ слѣдующій: *не существуетъ ли совокупность конечнаго числа нѣкоторыхъ предметовъ, удовлетворяющая всѣмъ постулатамъ приведеннаго въ главѣ VII общаго опредѣленія поля.*

Отвѣтъ получается положительный. Такія совокупности существуютъ и каждая изъ нихъ называется *конечнымъ полемъ.*

Оказывается, что построеніе конечнаго поля существенно зависитъ отъ двухъ чиселъ: произвольно выбраннаго *простого* числа p и также произвольно выбраннаго *натуральнаго* числа n.

Каждой парѣ чиселъ p и n соотвѣтствуетъ *одно, опредѣленное,* конечное поле.

§ 2. Обозначимъ черезъ $\overline{0}$ и $\overline{1}$ тѣ элементы искомаго поля, которые являются единицами аддитивной и мультипликативной группъ.

Элементы конечнаго поля не могутъ быть числами въ томъ смыслѣ слова, какъ это понятіе установлено въ элементарной алгебрѣ. Ибо комбинируя единицу $\overline{1}$ аддитивно самое съ собой можемъ получить безчисленное число элементовъ

$$\overline{1}+\overline{1},\ \overline{1}+\overline{1}+\overline{1},\ \overline{1}+\overline{1}+\overline{1}+\overline{1},\ldots$$

поля, что противорѣчитъ его конечности.

Итакъ, элементы конечнаго поля не могутъ быть числами, а должны быть предметами другой природы, и дѣйствія въ полѣ должны быть опредѣлены нѣсколько иначе.

§ 3. Прежде всего подчеркнемъ коренную разницу между конечнымъ и безконечнымъ полемъ.

Разсужденія предыдущей главы показываютъ намъ, что существуютъ различныя не изоморфныя безконечныя поля. Конечное же поле существуетъ только одно въ смыслѣ ариѳметической характеристики.

§ 4. Два изоморфныхъ поля мы будемъ считать за одно, ибо въ приложеніяхъ алгебры полей къ рѣшенію различныхъ вопросовъ для насъ является важнымъ не точное установленіе природы элементовъ поля, а лишь установленіе законовъ дѣйствій надъ элементами, другими словами законовъ вычисленія, дающихъ возможность всегда найти какой элементъ поля въ результатѣ указанныхъ дѣйствій получается.

§ 5. Будемъ обозначать элементы искомаго конечнаго поля, получающіеся отъ сложенія мультипликативной единицы съ самое собой знаками послѣдовательныхъ натуральныхъ чиселъ съ черточками наверху

$$\bar{1}+\bar{1}=\bar{2},\ \bar{2}+\bar{1}=\bar{3},\ \bar{3}+\bar{1}=\bar{4},\ \ldots \qquad (1)$$

Такъ какъ поле конечное, то въ ряду элементовъ

$$\bar{2},\ \bar{3},\ \bar{4},\ \bar{5},\ \ldots$$

должны быть одинаковые, напримѣръ,

$$\bar{p}+\bar{q}=\bar{q}.$$

Отсюда

$$\bar{p}=\bar{0}. \qquad (2)$$

Мы видимъ, что одинъ изъ элементовъ ряда (1) долженъ быть равенъ *нулю*, т. е. аддитивной единицѣ.

Пусть элементъ $\bar{p}$ будетъ тотъ изъ равныхъ нулю элементовъ ряда (1), который соотвѣтствуетъ наименьшему числу p. Легко показать, что это число p должно быть простымъ. Въ самомъ дѣлѣ, допустимъ, что p распадается на два меньшихъ множителя

$$p=ab,$$

тогда равенство (2) можно переписать такъ

$$\bar{ab}=0$$

или иначе

$$\bar{a}.\bar{b}=0.$$

На основаніи свойства поля должно получаться одно изъ двухъ

$$a=0,\ \ \bar{b}=0.$$

Что противорѣчитъ тому, что p есть наименьшее число, дающее нуль.

§ 6. Если p наименьшее число, при которомъ $\bar{p} = 0$, то элементы

$$\bar{0},\ \bar{1},\ \bar{2},\ \ldots\ \overline{p-1}$$

различны между собой, дальнѣйшіе же p элементовъ

$$\bar{p},\ \overline{p+1},\ \overline{p+2},\ \ldots\ \overline{2p-1} \qquad (2)$$

образуютъ тотъ же рядъ, что и элементы (1), и т. д. Однимъ словомъ, равенству

$$\bar{a} = \bar{b}$$

въ конечномъ полѣ соотвѣтствуетъ сравненіе

$$a \equiv b \pmod{p}.$$

Конечное поле можетъ состоять только изъ элементовъ ряда (1), и мы приходимъ къ простѣйшему виду конечнаго поля, къ такъ называемому *числовому полю.*

Числовое поле изоморфно съ полемъ, образованнымъ классами чиселъ по простому полю p.

Итакъ, элементами подобнаго поля оказываются не сами числа, а *классы чиселъ по модулю.*

§ 7. Посмотримъ, какъ должны производиться раціональныя дѣйствія въ числовомъ полѣ.

Что касается дѣйствій сложенія, вычитанія и умноженія, то эти дѣйствія производятся надъ соотвѣтственными вычетами классовъ по правиламъ обыкновенной ариѳметики цѣлыхъ чиселъ, и въ результатѣ придется взять вычетъ по разсматриваемому модулю.

Напримѣръ, разсмотримъ поле классовъ по модулю 7, состоящее изъ семи элементовъ

$$\bar{0},\ \bar{1},\ \bar{2},\ \bar{3},\ \bar{4},\ \bar{5},\ \bar{6}.$$

Если требуется вычислить въ полѣ выраженіе

$$(\bar{5} + \bar{6})(\bar{2} - \bar{4})$$

то надо классы замѣнить соотвѣтствующими вычетами

$$(5 + 6)(2 - 4) = -22$$

и полученный результатъ замѣнить его положительнымъ вычетомъ 6 по модулю 7.

Получаемъ

$$(\overline{5}+\overline{6})(\overline{2}-\overline{4})=\overline{6}.$$

§ 8. Обращаемся теперь къ разъясненію правила дѣленія въ числовомъ полѣ. Пусть требуется вычислить дробь

$$\frac{\overline{a}}{\overline{b}}$$

въ разсматриваемомъ $(\mathrm{mod}\,p)$ полѣ.

Имѣемъ

$$\overline{x}=\frac{\overline{a}}{\overline{b}}, \tag{2}$$

гдѣ $\overline{x}$ нѣкоторый элементъ поля.

Переписывая (2) такъ

$$\overline{xb}=\overline{a}$$

приходимъ къ рѣшенію сравненія

$$xb\equiv a\,(\mathrm{mod}\,p).$$

Напримѣръ, при $p=7$

$$\frac{\overline{2}}{\overline{3}}=\overline{3},$$

ибо $3\,.\,3\equiv 2\,(\mathrm{mod}\,7)$.

§ 9. Рѣшеніе уравненій въ числовомъ полѣ оказывается равносильнымъ съ рѣшеніемъ сравненій по простому модулю

$$f(x)\equiv 0\,(\mathrm{mod}\,p),$$

отсюда мы видимъ, почему сравненія по простому модулю играютъ особенно важную роль.

§ 10. Мы будемъ называть цѣлую функцію

$$f(x)=a_0x^n+a_1x^{n-1}+a_2x^{n-2}+\ldots+a_n$$

функціей принадлежащей къ числовому полю, если ея коэффиціенты суть вычеты по модулю p.

Можно установить понятіе о *неприводимости* функціи $f(x)$ по *модулю* p, если не существуетъ *тождественнаго* сравненія

$$f(x)\equiv\varphi(x)\psi(x)\,(\mathrm{mod}\,p),$$

гдѣ функціи $\varphi(x)$ и $\psi(x)$ суть функціи съ цѣлыми коэффиціентами степеней ниже степени функціи $f(x)$.

§ 11. *Теорема Schönemann'a. При простомъ модулѣ p существуетъ тождественное сравненіе*

$$[f(x)]^p \equiv f(x^p) \pmod p$$

гдѣ $f(x) = a_0x^n + a_1x^{n-1} + \ldots a_n$ съ цѣлыми коэффиціентами.

Прежде всего очевидно, что при всякихъ значеніяхъ $a, b, \ldots g$ существуетъ сравненіе

$$(a + b + \ldots + g)^p \equiv a^p + b^p + \ldots + g^p \pmod p,$$

ибо на основаніи соображеній § 17. гл. II мы замѣчаемъ, что всѣ полиноміальные коэффиціенты дѣлятся на p.

Отсюда

$$[f(x)]^p \equiv a_0{}^p(x^p)^n + a_1{}^p(x^p)^{n-1} + a_2{}^p(x^p)^{n-2} + \ldots \equiv$$

$$\equiv a_0(x^p)^n + a_1(x^p)^{n-1} + a_2(x^p)^{n-2} + \ldots \equiv f(x^p),$$

и теорема доказана.

§ 12. Обращаемся теперь къ разсмотрѣнію конечныхъ полей болѣе общаго вида.

Повторяя наши разсужденія, мы замѣчаемъ, что въ каждомъ конечномъ полѣ должно заключаться числовое поле, соотвѣтствующее нѣкоторому простому числу p. Будемъ для обозначенія элементовъ этого поля употреблять знаки натуральныхъ чиселъ безъ черточки на верху.

Итакъ, въ составъ разсматриваемаго конечнаго поля должны входить элементы, обозначенные знаками

$$0, 1, 2, 3, \ldots p-1. \tag{1}$$

Положимъ, что кромѣ этихъ элементовъ еще существуетъ элементъ x поля, тогда должны въ полѣ существовать еще элементы

$$x + x = 1.x + 1.x = (1 + 1)x = 2x, \; 2x + x = 3x, \; 4x, \ldots$$

т. е., другими словами, элементы

$$x, 2x, 3x, \ldots (p-1)x. \tag{2}$$

Складывая элементы ряда (1) съ элементами (2), получимъ элементы вида

$$\alpha_1 + \alpha_2 x, \tag{3}$$

гдѣ коэффиціенты α_1 и α_2 пробѣгаютъ полную систему вычетовъ по модулю p. Получаемъ p^2 элементовъ поля. Нетрудно видѣть, что всѣ они различны между собой, ибо равенство

$$\alpha_1 + \alpha_2 x = \alpha_1' + \alpha_2' x$$

черезъ рѣшеніе относительно x давало бы элементъ числового поля (1), а мы предположили, что элементъ x отличенъ отъ элементовъ (1).

Можетъ случиться, что поле исчерпывается элементами вида (3), тогда число элементовъ конечнаго поля будетъ равно p^2.

Если поле не исчерпывается элементами (3), то долженъ существовать нѣкоторый элементъ y, не представляющійся въ формулѣ (3), тогда поле можетъ имѣть видъ

$$\alpha_1 + \alpha_2 x + \alpha_3 y$$

гдѣ всѣ коэффиціенты α_1, α_2, α_3 пробѣгаютъ полную систему вычетовъ по простому модулю p.

Продолжая далѣе разсужденіе исчерпаемъ все поле.

Итакъ, конечное поле образуется элементами вида

$$\alpha_1 + \alpha_2 x + \alpha_3 y + \ldots \alpha_{n-1} t + \alpha_n u,$$

гдѣ коэффиціенты пробѣгаютъ вычеты по простому модулю p, и мы приходимъ къ теоремѣ.

Число элементовъ конечнаго поля равно всегда p^n, гдѣ p простое число, а n число натуральное.

Число p мы будемъ называть *основаніемъ* поля, а число n его *порядкомъ*.

Поле перваго порядка есть числовое.

§ 13. Замѣчательный примѣръ общаго поля порядка n указанъ былъ въ первый разъ Galois. Разсмотримъ его.

Пусть задана нѣкоторая цѣлая функція $f(x)$ степени n съ цѣлыми коэффиціентами, неприводимая по простому модулю p.

Galois образуетъ поле, составленное изъ p^n символовъ вида

$$\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_{n-1} x^{n-1}, \qquad (1)$$

гдѣ всѣ коэффиціенты α_i пробѣгаютъ полную систему вычетовъ по модулю p, причемъ дѣйствія надъ этими символами опредѣляются такъ.

Дѣйствіе сложенія двухъ символовъ

$$\begin{aligned} A &= \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_{n-1} x^{n-1} \\ B &= \beta_0 + \beta_1 x + \beta_2 x^2 + \ldots + \beta_{n-1} x^{n-1} \end{aligned} \qquad (2)$$

опредѣляется такъ: складываемъ ихъ алгебраически

$$(\alpha_0+\beta_0)+(\alpha_1+\beta_1)x+(\alpha_2+\beta_2)x^2+\ldots+(\alpha_{n-1}+\beta_{n-1})x^{n-1},$$

замѣняемъ далѣе всѣ коэффиціенты

$$\alpha_0+\beta_0,\ \alpha_1+\beta_1,\ \alpha_2+\beta_2,\ \ldots\ \alpha_{n-1}+\beta_{n-1}$$

ихъ вычетами по модулю p

$$\gamma_0,\ \gamma_1,\ \gamma_2\ \cdots\ \gamma_{n-1}.$$

Символъ

$$C=\gamma_0+\gamma_1x+\gamma_2x^2+\ldots+\gamma_{n-1}x^{n-1}$$

мы будемъ считать за сумму символовъ A и B и писать

$$A+B=C.$$

Для умноженія установимъ подобное же правило, а именно, перемножимъ A и B алгебраически какъ многочлены перемѣнной независимой x, найдемъ далѣе остатокъ D отъ дѣленія произведенія AB на основную функцію $f(x)$. Если при умноженіи и дѣленіи многочленовъ производить съ коэффиціентами этихъ многочленовъ дѣйствія не по правиламъ обыкновенной алгебры, а по правиламъ дѣйствій въ числовомъ полѣ, то коэффиціенты остатка D будутъ принадлежать *числовому* полю. Такъ какъ этотъ остатокъ будетъ степени не выше $n-1$, то будетъ имѣть видъ (1) и мы его будемъ считать за произведеніе символовъ A и B и писать

$$A.B=D.$$

Нѣтъ надобности подробно останавливаться на томъ, что при такихъ опредѣленіяхъ сложенія и умноженія символы (1) образуютъ дѣйствительно конечное поле. Необходимо обратить вниманіе читателя лишь на то обстоятельство, что *неприводимость* функціи $f(x)$, на которую мы постоянно дѣлимъ, есть дѣйствительно требованіе обязательное, иначе не будетъ существовать поля.

Въ самомъ дѣлѣ, пусть $f(x)$ будетъ функціей приводимой въ числовомъ полѣ, т. е.

$$f(x)=\varphi(x)\psi(x);$$

функціи $\varphi(x)$ и $\psi(x)$ будутъ элементами нашей совокупности (1) отличными отъ нуля, ибо нуль получается *только, когда* всѣ коэффиціенты $\alpha_0,\ \alpha_1,\ \alpha_2,\ \ldots\ \alpha_{n-1}$ *равны нулю.*

Такъ какъ при разсматриваніи функцій отъ x съ коэффиціентами числового поля мы должны постоянно откидывать кратности функціи $f(x)$,

то очевидно, что *сама функція* $f(x)$ равносильна $f(x) - f(x)$ т. е. *равносильна нулю*. Мы получаемъ

$$0 = \varphi(x)\psi(x),$$

что противорѣчитъ основному свойству поля.

§ 14. Полученное нами поле мы будемъ называть *полемъ Galois*.

Резумируя сказанное въ § 13, можно дать двѣ различныхъ формулировки поля Galois.

I. *Выкладки поля Galois можно разсматривать какъ дѣйствія надъ функціональными сравненіями по такъ называемому двойному модулю.*

Разсматривается совокупность всѣхъ цѣлыхъ функцій отъ x съ цѣлыми коэффиціентами.

Очевидно, что эти функціи образуютъ совокупность предметовъ, воспроизводящихся черезъ примѣненіе трехъ дѣйствій: сложенія, вычитанія и умноженія, *но не дѣленія*.

Мы беремъ произвольное простое число p и нѣкоторую функцію $f(x)$ изъ нашей совокупности *неприводимую* по модулю p, тогда условимся, что сравненіе

$$\varphi(x) \equiv \psi(x) \,[\mathrm{mod}\, p,\ f(x)]$$

по двойному модулю (по числу p и функціи $f(x)$) выражаетъ тотъ фактъ, что разность

$$\varphi(x) - \psi(x)$$

можетъ быть представлена въ видѣ

$$\varphi(x) - \psi(x) = p\omega(x) + f(x)\omega_1(x), \qquad (1)$$

гдѣ $\omega(x)$ и $\omega_1(x)$ цѣлыя функціи съ цѣлыми коэффиціентами.

Если мы будемъ функцію $f(x)$ предполагать *примарною*, т. е. такою, что старшій коэффиціентъ ея равенъ единицѣ, то провѣрка равенства (1) можетъ быть произведена, очевидно, такъ: дѣлимъ $\varphi(x) - \psi(x)$ алгебраически на $f(x)$; остатокъ долженъ быть такою функціей отъ x, у которой всѣ коэффиціенты дѣлятся на p.

Нетрудно видѣть, что поле Galois есть не что иное какъ поле классовъ (вычетовъ) по двойному модулю.

II. Можно трактовать элементы поля Galois какъ нѣкоторые *мнимые символы* въ теоріи чиселъ.

§ 15. Остановимся болѣе подробно на выясненіи второго толкованія.

Припомнимъ, какъ вводятся мнимыя числа въ элементарной алгебрѣ. Берется уравненіе

$$x^2 + 1 = 0$$

не имѣющее рѣшеній въ числахъ вещественныхъ, т. е. въ тѣхъ числахъ, которыя до введенія чиселъ мнимыхъ являются единственными существующими. Затѣмъ расширяется понятіе о числѣ въ томъ смыслѣ, что къ вещественнымъ числамъ присоединяется нѣкоторый новый символъ i, который считается за число новой природы, такъ называемое *мнимое* число.

Природа числа i не разъясняется въ абсолютномъ смыслѣ слова, что и не нужно для математики.

Для математики необходимо и достаточно знать, какъ производить надъ этимъ новымъ знакомъ дѣйствія сложенія, вычитанія, умноженія и дѣленія.

Знакъ i считается корнемъ уравненія (1) лишь въ томъ смыслѣ, что i^2 считается равнымъ отрицательному числу -1. Отсюда, какъ извѣстно, получаются всѣ выкладки надъ числомъ i.

Въ результатѣ выкладокъ всегда остается только первая степень i т. е. числа вида

$$\alpha_0 + \alpha_1 i \tag{2}$$

Можно было бы обобщить понятіе о комплексномъ числѣ (2) на уравненія болѣе высокой степени.

Возьмемъ уравненіе съ коэффиціентами изъ нѣкотораго поля R

$$f(x) = 0 \tag{3}$$

нѣкоторой степени n, которое будемъ предполагать неприводимымъ въ полѣ R, и всѣ корни котораго мнимые. Обозначимъ черезъ i какой нибудь изъ корней уравненія (3), тогда, какъ мы знаемъ, всѣ раціональныя функціи отъ i будутъ имѣть видъ

$$\alpha_0 + \alpha_1 i + \alpha_2 i^2 + \ldots + \alpha_{n-1} i^{n-1} \tag{4}$$

и, слѣдовательно, является вопросъ, не надо ли вводить комплексныя числа вида (4).

Въ элементарной алгебрѣ однако нѣтъ надобности въ такомъ обобщеніи, ибо извѣстно, что комлексныя числа вида (2) достаточны для полнаго рѣшенія алгебраическихъ уравненій.

Указанное нами обобщеніе (4) комплексныхъ чиселъ играетъ большую роль лишь въ высшихъ частяхъ алгебры, въ которыхъ она переходитъ, собственно говоря, въ теорію чиселъ. Это обобщеніе приводитъ, какъ мы видѣли, къ весьма важному понятію алгебраическаго поля.

§ 16. Обращаемся теперь къ сравненіямъ высшихъ степеней по простому модулю.

Если задано сравненіе

$$f(x) \equiv 0 \pmod{p}, \tag{1}$$

гдѣ $f(x)$ примарная съ цѣлыми коэффиціентами, неприводимая по модулю p цѣлая функція степени n. то сравненіе (1), очевидно, не имѣетъ рѣшеній, ибо, если бы существовало рѣшеніе α этого сравненія, то было бы

$$f(x) \equiv (x - \alpha) f_1(x) \equiv 0 \pmod{p}$$

и функція $f(x)$ была бы приводимою.

Итакъ, можно сказать, что рѣшенія сравненія (1) суть нѣкоторыя *мнимости* съ точки зрѣнія теоріи чиселъ. Обозначимъ черезъ i мнимый корень сравненія (1) и разсмотримъ комплексные символы

$$\alpha_o + \alpha_1 i + \alpha_2 i^2 + \ldots \alpha_{n-1} i^{n-1} \qquad (2)$$

съ цѣлыми коэффиціентами. Эти символы (2) и суть не что иное, какъ извѣстныя *мнимости Galois.*

Дѣйствія надъ этими символами можно по аналогіи съ алгеброй установить двояко, а именно.

I. Или можно сказать, что во всякомъ сравненіи

$$F(i) \equiv 0 \pmod{p}.$$

надо высшія степени мнимости i, начиная съ n-ой степени, исключить при помощи сравненія

$$f(i) \equiv 0 \pmod{p}.$$

II. Или можно не вводить никакихъ мнимостей съ точки зрѣнія теоріи чиселъ, а просто разсматривать корень i уравненія

$$f(x) = 0$$

и разсматривать поле, получаемое отъ присоединенія къ полю раціональныхъ чиселъ числа i. Элементы такого поля будутъ, очевидно, имѣть видъ (2) съ раціональными коэффиціентами α_i.

Часть этого поля, которую образуютъ числа вида (2) съ цѣлыми коэффиціентами α_i представляетъ изъ себя такую систему чиселъ, которыя воспроизводятся отъ трехъ дѣйствій: сложенія, вычитанія и умноженія, *но не дѣленія.*

Такую систему чиселъ Dedekind называетъ *порядкомъ* (терминъ взятъ изъ Gauss'овой теоріи квадратичныхъ формъ), а Hilbert называетъ Zahlring.

Итакъ, разсмотримъ порядокъ, образованный числами (2) при цѣлыхъ коэффиціентахъ.

Условимся считать числа порядка сравнимыми по простому модулю p *тогда и только тогда*, когда соотвѣтственные коэффиціенты сравнимы

по модулю p, т. е. будемъ считать сравненіе

$$\alpha_o + \alpha_1 i + \alpha_2 i^2 + \ldots + \alpha_{n-1} i^{n-1} \equiv \alpha_o' + \alpha_1' i + \alpha_2 i^2 + \ldots + \alpha_{n-1}' i^{n-1} \pmod{p}$$

равносильнымъ съ рядомъ такихъ

$$\alpha_o \equiv \alpha_o' \pmod{p}, \quad \alpha_1 \equiv \alpha_1' \pmod{p}, \quad \ldots \quad \alpha_{n-1} \equiv \alpha_{n-1}' \pmod{p}.$$

Итакъ, общій результатъ нашихъ замѣчаній можетъ быть высказанъ такъ.

Поле Galois есть не что иное какъ совокупность вычетовъ по модулю p символовъ вида (2) съ цѣлыми коэффиціентами, причемъ безразлично, какъ трактовать эти символы, какъ мнимости Galois, или какъ элементы порядка.

Въ заключеніе я желаю подчеркнуть фактъ возможности при помощи разсмотрѣнія сравненій по двойному модулю $[p, f(x)]$ избѣжать яваго введенія мнимости i, представляющей корень сравненія $f(x) \equiv 0 \pmod{p}$, не имѣющаго рѣшеній, ибо сравненіе $F(i) \equiv 0 \pmod{p}$ равносильно дѣлимости по модулю p функціи $F(x)$ на функцію $f(x)$.

§ 17. Теперь мы приходимъ къ разсужденіямъ, имѣющимъ первостепенную важность для теоріи чиселъ, причемъ будемъ доказывать теорему.

Теорема. Для всякаго простого основанія p и всякаго порядка n существуетъ одно и только одно конечное поле, изоморфное съ полемъ Galois.

Для доказательства этой теоремы надо доказать слѣдующія положенія.

1) Для всякихъ чиселъ p и n существуетъ поле Galois.

2) Это поле Galois *единственное*, т. е. не зависитъ отъ выбора неприводимой по модулю p функціи степени n. Поля при разныхъ функціяхъ изоморфны.

3) Конечное поле изоморфно съ полемъ Galois.

§ 18. Для доказательства существованія поля Galois необходимо доказать, что для всякаго простого числа p существуютъ неприводимыя по модулю p функціи всякой степени n.

Станемъ на точку зрѣнія сравненій по двойному модулю.

Пусть будетъ

$$X = \alpha_o + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_{n-1} x^{n-1}.$$

Такъ какъ классы функцій X по двойному модулю $[\mathrm{mod}\, p, f(x)]$ образуютъ поле Galois, то воспользуемся тѣмъ обстоятельствомъ, что всѣ

отличные отъ нуля элементы X поля образуютъ мультипликативную группу порядка $p^n - 1$. Значитъ на основаніи § 14 гл. VI должно существовать въ полѣ Galois уравненіе

$$X^{p^n-1} - 1 = 0, \tag{1}$$

имѣющее мѣсто для всякаго отличнаго отъ нуля элемента X поля.

Уравненіе (1) представляетъ не что иное какъ сравненіе

$$X^{p^n-1} - 1 \equiv 0 \,[\mathrm{mod}\, p,\ f(x)]. \tag{2}$$

Такъ какъ это сравненіе удовлетворяется всякою функціею X, то оно должно удовлетворяться также при $X = x$, т. е. когда

$$\alpha_0 = 0,\ \alpha_1 = 1,\ \alpha_2 = 0,\ \ldots\ \alpha_{n-1} = 0$$

и мы получаемъ

$$x^{p^n-1} - 1 \equiv 0 \,[\mathrm{mod}\, p,\ f(x)],$$

умножая на x получимъ

$$x^{p^n} - x \equiv 0 \,[\mathrm{mod}\, p,\ f(x)] \tag{3}$$

т. е.

$$x^{p^n} - x \equiv f(x)\varphi(x) \,(\mathrm{mod}\, p).$$

Получаемъ теорему:

Теорема. Всякая неприводимая по модулю p функція степени n, если она существуетъ, есть дѣлитель по этому модулю выраженія

$$x^{p^n} - x.$$

§ 19. Такъ какъ въ полѣ Galois сравненіе (3) § 18 равносильно уравненію $x^{p^n} = x$, то возвышая обѣ его части въ степень p^n, получимъ

$$(x^{p^n})^{p^n} = x^{p^n p^n} = x^{p^{2n}} = x^{p^n} = x,$$

или

$$x^{p^{2n}} = x,$$

возвышая еще разъ, получимъ $x^{p^{3n}} = x$, продолжая далѣе, получимъ уравненіе

$$x^{p^{mn}} = x,$$

которое равносильно сравненію

$$x^{p^{mn}} - x \equiv 0 \,[\mathrm{mod}\, p,\ f(x)],$$

и мы приходимъ къ теоремѣ:

Теорема. Всякая неприводимая по модулю p функція $f(x)$, показатель степени которой d есть дѣлитель числа n, дѣлитъ по модулю p выраженіе

$$x^{p^n} - x.$$

§ 20. *Теорема. Выраженіе* $x^{p^m} - x$ *не можетъ дѣлиться по модулю* p *на неприводимую функцію степени выше* n.

Пусть будетъ $F(x)$ неприводимая по модулю p функція степени m, гдѣ $m > n$.

Будемъ разсматривать сравненія по двойному модулю $[p, F(x)]$, т. е. другими словами, конечное поле Galois порядка m, соотвѣтствующее функціи $F(x)$.

Возьмемъ произвольный элементъ этого поля

$$\chi(x);$$

этотъ элементъ есть функція $m-1$ степени отъ x съ цѣлыми коэффиціентами по модулю p.

На основаніи теоремы Schönemann'a имѣемъ

$$[\chi(x)]^p \equiv \chi(x^p) \pmod p$$

тѣмъ болѣе будетъ имѣть мѣсто сравненіе по двойному модулю

$$[\chi(x)]^p \equiv \chi(x^p) [\text{mod } p,\ F(x)].$$

Примѣняя разсужденіе n разъ, получимъ

$$[\chi(x)]^{p^n} \equiv \chi(x^{p^n}) [(\text{mod } p,\ F(x)]. \tag{1}$$

Мы имѣемъ въ виду доказать, что выраженіе $x^{p^n} - x$ не можетъ дѣлиться на $F(x)$ по модулю p. Допустимъ обратное, а именно

$$x^{p^n} - x \equiv 0 \ [\text{mod } p,\ F(x)]$$

или

$$x^{p^n} \equiv x \ [\text{mod } p,\ F(x)].$$

Откуда

$$\chi(x^{p^n}) \equiv \chi(x) \ [\text{mod } p,\ F(x)]. \tag{2}$$

Сопоставляя сравненія (1) и (2), получимъ

$$[\chi(x)]^{p^n} \equiv \chi(x) \ [\text{mod } p,\ F(x)]$$

или иначе всякій элементъ $\chi(x)$ поля порядка m удовлетворяетъ уравненію

$$X^{p^n} - X = 0 \tag{3}$$

въ этомъ полѣ. Мы пришли къ противорѣчію, ибо всѣхъ элементовъ поля p^m и они должны быть корнями уравненія (3) степени p^n, что невозможно ибо $p^m > p^n$. Необходимо обратить вниманіе читателя на то обстоятельство, что уравненіе въ полѣ не можетъ имѣть больше корней, чѣмъ

единицъ въ показателѣ его степени. Доказательство то же, что и въ обыкновенной алгебрѣ.

§ 21. *Теорема. Если неприводимая по модулю p функція $f(x)$ дѣлитъ по тому же модулю выраженіе $x^{p^n}-x$, то степень m функціи $f(x)$ должна быть дѣлителемъ числа n.*

Будемъ дѣлить число n на m и обозначимъ черезъ q частное, а черезъ μ остатокъ, тогда мы получаемъ $n=mq+\mu$, гдѣ $\mu<m$.

Имѣемъ два сравненія

$$x^{p^n}-x\equiv 0\,[\mathrm{mod}\,p,\ f(x)]\,. \tag{1}$$

$$x^{p^m}-x\equiv 0\,[\mathrm{mod}\,p,\ f(x)]\,. \tag{2}$$

Сравненіе (1) требуется по условію теоремы, сравненіе же (2) доказано въ § 19.

Возвышая сравненіе (2) q разъ въ степень p^m, получимъ

$$x^{p^{mq}}\equiv x\,[\mathrm{mod}\,p,\ f(x)]\,. \tag{3}$$

Сравненіе (1) можно будетъ переписать такъ

$$(x^{p^{mq}})^{p^\mu}\equiv x\,[\mathrm{mod}\,p,\ f(x)]\,,$$

откуда на основаніи (3) мы имѣемъ

$$x^{p^\mu}-x\equiv 0\,[\mathrm{mod}\,p,\ f(x)]\,,$$

но $\mu<m$, и мы получаемъ противорѣчіе съ § 20, если μ не равно нулю. Итакъ $\mu=0$, что и требовалось доказать.

§ 22. Послѣднее весьма важное замѣчаніе состоитъ въ томъ, что всякая неприводимая функція можетъ входить въ выраженіе $x^{p^n}-x$ только въ первой степени. Для этой цѣли достаточно показать, что функція $x^{p^n}-x$ и ея производная $p^n x^{p^n-1}-1$ не могутъ имѣть общихъ дѣлителей въ числовомъ полѣ модуля p. Это очевидно, ибо производная по модулю p равна постоянному числу -1.

§ 23. Резюмируя сказанное, мы замѣчаемъ что функція $x^{p^m}-x$ раскладывается по модулю p на рядъ неодинаковыхъ неприводимыхъ множителей, степени которыхъ суть дѣлители d числа n, и которые мы можемъ предполагать примарными.

Соберемъ всѣхъ множителей, имѣющихъ степень, равную нѣкоторому опредѣленному дѣлителю d, и обозначимъ черезъ $\Omega_d(x)$ ихъ произведеніе.

Можемъ написать равенство въ числовомъ полѣ $(\mathrm{mod}\, p)$

$$x^{p^n} - x = \Pi \Omega_d(x), \tag{1}$$

гдѣ произведеніе Π распространяется на всѣхъ дѣлителей числа n. Если не существуетъ множителей нѣкоторой степени d, то $\Omega_d(x) = 1$.

Обозначая черезъ $\omega(d)$ число неприводимыхъ функцій степени d, получимъ черезъ сравненіе степеней въ обѣихъ частяхъ уравненія (1)

$$p^n = \Sigma d\omega(d). \tag{2}$$

Примѣняя принципъ обращенія, указанный въ § 31 гл. II, получимъ

$$n\omega(n) = p^n - \Sigma p^{\frac{n}{q}} + \Sigma p^{\frac{n}{q_1 q_2}} - \Sigma p^{\frac{n}{q_1 q_2 q_3}} + \ldots \pm p^{\frac{n}{q_1 q_2 q_3 \cdots}}$$

Очевидно, что $\omega(n)$ не можетъ равняться нулю, ибо равенство $\omega(n) = 0$ послѣ сокращенія на послѣдній членъ $p^{\frac{n}{q_1 q_2 q_3 \cdots}}$ давало бы

$$pP \pm 1 = 0,$$

гдѣ P цѣлое число.

Итакъ $\omega(n)$ не равняется нулю, и мы приходимъ къ заключенію, что существуетъ $\omega(n)$ функцій всякой степени n, неприводимыхъ по модулю p.

Тѣмъ же пріемомъ обращенія можемъ дѣйствительно найти функціи $\Omega_n(x)$. Примѣняя формулу (3) § 33 гл. II (Стр. 38), получимъ

$$\Omega_n(x) = \frac{(x^{p^n} - x)\Pi(x^{p^{\frac{n}{q_1 q_2}}} - x)\ldots}{\Pi(x^{p^{\frac{n}{q}}} - x)\,\Pi(x^{p^{\frac{n}{q_1 q_2 q_3}}} - x)\ldots} \tag{3}$$

Покажемъ, что послѣднее дробное выраженіе приводится по модулю p къ цѣлому полиному.

Разсмотримъ какой нибудь настоящій дѣлитель d цѣлаго числа n. Покажемъ, что всякая функція $f(x)$ неприводимая по модулю p степени d входитъ одинаковое число разъ множителемъ какъ въ числитель такъ и въ знаменатель.

Пусть простыя числа $q_1, q_2, q_3, \ldots q_l$ суть тѣ, которыя входятъ въ число n въ степеняхъ большихъ чѣмъ въ d, тогда d дѣлитъ число

$$\frac{n}{q_1 q_2 q_3 \ldots q_l}.$$

Но не дѣлитъ $\frac{n}{q_s}$, гдѣ $s = l+1, l+2, \ldots$

Обозначимъ

$$\Pi_k = \Pi(x^{p^{q_1 q_2 \cdots q_k}} - x),$$

тогда при $k > l$ полиномъ $f(x)$ не входитъ множителемъ въ Π_k.

Если же $k \leqq l$, то $f(x)$ входитъ множителемъ въ выраженіе Π_k столько разъ, сколько можно составить сочетаній изъ l величинъ $q_1 q_2 \cdots q_l$ по k, т. е. C_l^k.

Итакъ, $f(x)$ входитъ въ числитель выраженія (3) $1 + C_l^2 + C_l^4 + C_l^6 + \ldots$ разъ, а въ знаменатель $C_l' + C_l^3 + C_l^5 + \ldots$ разъ. Эти же оба числа равны между собой, ибо ихъ разность есть $(1-1)^l = 0$.

§ 24. Итакъ, мы доказали существованіе неприводимой по модулю p функціи всякой степени n, тѣмъ самымъ доказано существованіе поля Galois для всякихъ чиселъ p и n.

Покажемъ теперь, что существуетъ только одно поле Galois съ основаніемъ p и порядкомъ n, для этой цѣли надо показать, что всѣ поля Galois, образованныя различными $\omega(n)$ неприводимыми функціями степени n, изоморфны.

Возьмемъ двѣ такія функціи

$$f(x) \text{ и } f'(x).$$

Обозначимъ два поля Galois, образованныя этими функціями, черезъ

$$G[p^n] \text{ и } G'[p^n].$$

Прежде всего замѣтимъ, что оба поля заключаютъ одно и тоже числовое поле

$$G[p].$$

Въ этомъ послѣднемъ функція $x^{p^n} - x$ дѣлится на обѣ функціи $f(x)$ и $f'(x)$. То есть

$$x^{p^n} - x = f(x) f'(x) \varphi(x).$$

Теорема о сравненіяхъ съ максимальнымъ числомъ корней, приведенная въ § 23 гл. III, переносится на любое конечное поле. Уравненіе $x^{p^n} - x = 0$ имѣетъ максимальное число корней, а именно ему удовлетворяютъ всѣ p^n элементовъ обоихъ полей $G[p^n]$, $G'[p^n]$, значитъ оба уравненія

$$f(x) = 0, \quad f'(x) = 0,$$

имѣютъ максимальное число корней въ обоихъ поляхъ. Возьмемъ уравненіе $f(x) = 0$ и пусть y будетъ одинъ изъ его корней въ полѣ $G'[p^n]$. Составимъ поле $G[p^n]$ при помощи функціи $f(x)$, *употребляя символъ* y. Элементами этого поля являются символы

$$a_0 + a_1 y + a_2 y^2 + \ldots + a_{n-1} y^{n-1} \qquad (1)$$

гдѣ α_i элементы числового поля $G[p]$. Дѣйствія надъ символами (1) подчиняются, очевидно, законамъ поля $G[p^n]$. Съ другой стороны символы (1) принадлежатъ полю $G'[p^n]$, ибо y, остававшійся все время символомъ, природа котораго не играла роли, есть элементъ поля $G'[p^n]$. Для того чтобы убѣдиться, что символы (1) заполняютъ *другое* поле $G'[p^n)$ достаточно показать, что въ этомъ новомъ полѣ символы (1) *всѣ различны между собой.*

Въ этомъ легко убѣдиться изъ того соображенія, что предположеніе равенства двухъ символовъ (1) противорѣчитъ неприводимости функціи $f(x)$ въ числовомъ полѣ $G[p]$.

Итакъ, изоморфизмъ двухъ полей $G[p^n]$, $G'[p^n]$ доказанъ.

§ 25. Обращаемся теперь къ окончательному доказательству теоремы, что всякое конечное поле порядка n съ основаніемъ p изоморфно съ полемъ $G[p^n]$.

Покажемъ, что на всякое конечное поле n-аго порядка распространяется теорія *первообразныхъ корней и индексовъ*, изложенная нами въ IV главѣ.

Разсмотримъ мультипликативную группу поля [1]). Эта группа имѣетъ порядокъ $p^n - 1$.

Будемъ говорить, что въ нашемъ конечномъ полѣ элементъ x *принадлежитъ къ показателю* δ, если δ есть наименьшее число, при которомъ имѣетъ мѣсто уравненіе $x^\delta = 1$.

На основаніи теоремы Lagrange'a δ долженъ быть дѣлителемъ числа $p^n - 1$ (см. § 16 гл. VI).

Повторяя буквально разсужденія § 3 главы IV, мы докажемъ, что существуютъ элементы, принадлежащіе къ показателю, равному всякому дѣлителю δ числа $p^n - 1$, и что число такихъ чиселъ есть $\varphi(\delta)$.

Итакъ, мы видимъ, что будетъ существовать

$$\varphi(p^n - 1)$$

элементовъ конечнаго поля, принадлежащихъ къ показателю $p^n - 1$. Каждый изъ такихъ элементовъ w называется первообразнымъ элементомъ поля. Все поле будетъ образовано степенями этого элемента и элементомъ 0.

$$0,\ 1,\ w,\ w^2,\ w^3,\ \ldots,\ w^{p^n-3},\ w^{p^n-2}.$$

Очевидно, что всякому отличному отъ нуля элементу a поля будетъ соотвѣтствовать *индексъ* α по уравненію

$$a = w^\alpha.$$

[1]) Все поле безъ элемента 0.

Индексы общаго конечнаго поля сравнимы по модулю $p^n - 1$ и обладаютъ свойствами аналогичными съ индексами числового поля $n = 1$.

§ 26. Для доказательства изоморфизма конечнаго поля произвольнаго вида съ полемъ Galois достаточно показать, что первообразный элементъ w есть корень уравненія

$$f(x) = 0$$

степени равной порядку n поля и неприводимаго въ числовомъ полѣ.

На основаніи уравненія $x^{p^n-1} - 1 = f(x)\varphi(x) = 0$ степень функціи $f(x)$ должна быть дѣлителемъ числа n (см. § 21). Покажемъ, что предположеніе, что степень m этой функціи меньше n, приводитъ къ противорѣчію.

Очевидно, что выраженія

$$0,\ 1,\ x,\ x^2,\ x^3,\ \ldots\ x^{p^n-3},\ x^{p^n-2} \tag{1}$$

сравнимы по двойному модулю $[\mathrm{mod}\, p,\ f(x)]$ съ выраженіями вида

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_{m-1} x^{m-1}, \tag{2}$$

гдѣ коэффиціенты пробѣгаютъ числовое поле $G[p]$. Различныхъ выраженій (2) будетъ p^m и значитъ при $m < n$ не могутъ быть различными въ разсматриваемомъ полѣ всѣ элементы ряда (1). Итакъ $m = n$ и мы приходимъ къ выводу, что конечное поле общаго вида изоморфно съ полемъ вычетовъ по двойному модулю т. е. съ полемъ $G[p^n]$.

§ 27. Для болѣе подробнаго знакомства съ законами, дѣйствующими въ конечномъ полѣ, можно рекомендовать.

Serret. Algèbre. Tome II (1910).

Сохоцкій. Теорія чиселъ (1889).

Dickson. Linear Groups (1901).

ГЛАВА IX.

Нѣкоторыя приложенія конечнаго поля.

§ 1. Въ срединѣ 19-го столѣтія было сдѣлано въ математикѣ открытіе первостепенной важности. Kummer предложилъ ввести въ теорію чиселъ новые символы, которые онъ назвалъ *идеальными числами*. Введеніе этихъ чиселъ составило эпоху и несомнѣнно еще долгое время будетъ главнымъ предметомъ изслѣдованій спеціалистовъ теоріи чиселъ.

Въ дальнѣйшемъ изложеніи я дамъ краткое понятіе объ идеальномъ числѣ. Болѣе подробное изложеніе будетъ дано въ печатномъ моемъ сочиненіи подъ заглавіемъ „Теорія идеаловъ“.

Важность введенія въ науку идеальныхъ чиселъ лежитъ прежде всего, конечно, въ тѣхъ серіозныхъ приложеніяхъ, которыя и вызвали ихъ появленіе въ свѣтъ. Но помимо приложеній теорія идеальныхъ чиселъ имѣетъ большое принципіальное значеніе, которое обнаруживается между прочимъ въ связи этой теоріи съ конечнымъ полемъ.

Теорія идеальныхъ чиселъ заставляетъ смотрѣть на наши обыкновенныя простыя числа, 2, 3, 5, 7, ... какъ на составныя и считать ихъ произведеніями настоящихъ простыхъ элементовъ, которыми являются такъ называемыя *простыя идеальныя числа*.

Чтобы подчеркнуть связь идеальныхъ чиселъ съ конечнымъ полемъ, достаточно привести теорему.

Конечное поле самаго общаго вида изоморфно съ совокупностью классовъ по простому идеальному модулю.

Мы не будемъ останавливаться на приведенной теоремѣ, считая этотъ предметъ выходящимъ изъ рамокъ элементарнаго курса, а отошлемъ читателя къ нашему сочиненію: „Теорія идеаловъ“. Здѣсь же мы остановимся на болѣе элементарныхъ приложеніяхъ конечныхъ полей.

§ 2. Galois началъ разсматривать конечное поле подъ вліяніемъ изученія теоріи алгебраическаго рѣшенія уравненій, которая, какъ извѣстно, и была главнымъ предметомъ его изслѣдованій.

Покажемъ, почему въ этой теоріи Galois долженъ былъ придти къ разсмотрѣнію конечнаго поля.

Благодаря Abel'у выяснилось, что при алгебраическомъ рѣшеніи уравненій все дѣло сводится къ уравненіямъ степени p^n, т. е. степень которыхъ есть степень простого числа. Благодаря Galois мы знаемъ условія необходимыя и достаточныя для рѣшенія уравненія въ радикалахъ въ случаѣ $n = 1$ и знаемъ общій видъ радикальнаго выраженія, рѣшающаго задачу въ этомъ случаѣ.

Что касается общаго случая, то до сихъ поръ, т. е. въ продолженіе почти 100 лѣтъ, разсмотрѣніе общаго случая не приводитъ къ сколько нибудь общимъ заключеніямъ.

Оставшіяся въ посмертныхъ бумагахъ Galois, нѣкоторыя общія замѣчанія оказались частью не вѣрными, частью мало полезными.

Единственно, что осталось послѣ Galois несомнѣннымъ и чего не избѣгъ никто изъ немногочисленныхъ неустрашимыхъ изслѣдователей этого вопроса, это приложеніе разсмотрѣнія конечнаго поля $G[p^n]$.

Обыкновенно, если разсматривается примитивное уравненіе степени p^n, то его корни обозначаются элементами конечнаго поля. Приходится разсматривать какъ извѣстно *подстановки* этихъ корней, то есть различныя перетасовки взаимнаго расположенія этихъ корней. Все дѣло сводится къ разсмотрѣнію группъ подстановокъ элементовъ конечнаго поля. Остановимся нѣсколько подробнѣе на указанномъ вопросѣ.

§ 3. Начнемъ съ весьма простого примѣра: разсмотримъ въ полѣ $G[p^n]$ соотношеніе

$$y = ax + b,$$

гдѣ a и b два заданныхъ элемента поля, при чемъ a не нуль, тогда не трудно убѣдиться, что если x пробѣгаетъ всѣ элементы поля

$$x_1, x_2, x_3, \ldots x_{p^n}, \tag{1}$$

то y пробѣгаетъ также поле, то есть значенія

$$y_k = ax_k + b$$

или, другими словами, значенія

$$y_1, y_2, y_3, \ldots y_{p^n} \tag{2}$$

отличаются отъ значеній (1) только ихъ порядкомъ.

Итакъ, можно сказать, что линейная функція

$$ax + b$$

производитъ подстановку элементовъ поля, причемъ перемѣщеніе (1) этихъ элементовъ переходитъ въ другое ихъ перемѣщеніе (2).

Для доказательства, что въ рядѣ (2) нѣтъ одинаковыхъ элементовъ, замѣчаемъ, что равенство

$$y_k = y_l$$

или

$$ax_k + b = ax_l + b$$

влекло бы за собой

$$x_k = x_l,$$

что невозможно, ибо по нашему предположенію рядъ (1) заключаетъ по одному всѣ элементы поля и въ немъ нѣтъ нѣсколькихъ одинаковыхъ.

Свойство линейной функціи $ax + b$ пробѣгать всѣ элементы поля есть обобщеніе свойства, изложеннаго въ § 7 главы III и относящагося къ сравненіямъ.

Итакъ, линейная функція $ax + b$ производитъ подстановку элементовъ поля, которую выразимъ знакомъ

$$[x,\ ax + b], \tag{3}$$

показывающимъ, что всякій x переходитъ въ $ax + b$, или знакомъ

$$\begin{pmatrix} x_1 & x_2 & \dots & x_{p^n} \\ ax_1 + b & ax_2 + b & \dots & x_{p^n} + b \end{pmatrix}.$$

Подстановка вида (3) носитъ названіе *линейной*.

Посмотримъ, сколько можетъ существовать такихъ линейныхъ подстановокъ. Такъ какъ число b совершенно произвольно, то оно можетъ принимать столько значеній, сколько элементовъ въ полѣ, т. е. p^n. Число же значеній a на единицу меньше, ибо a не должно равняться нулю. Значитъ общее число всевозможныхъ линейныхъ подстановокъ равняется

$$p^n(p^n - 1). \tag{4}$$

Линейныя подстановки (3), очевидно, образуютъ группу, ибо, если послѣ подстановки

$$z = a_1 y + b_1$$

произведемъ подстановку

$$y = a_2 x + b_2,$$

то получимъ опять линейную подстановку

$$z = a_1(a_2 x + b_2) + b_1$$

или

$$z = a_1 a_2 x + a_1 b_2 + b_1 .$$

Эта группа называется *общей линейной группой конечнаго поля* и имѣетъ порядокъ (4).

§ 4. Поясним линейную группу на примѣрѣ поля $G[2^2]$, то есть въ случаѣ $p = 2$, $n = 2$.

Неприводимая по модулю 2 функція 2-ой степени будетъ $i^2 + i + 1$, ибо сравненіе

$$i^2 + i + 1 = 0 \pmod 2$$

не имѣетъ рѣшеній.

Поле должно состоять изъ четырехъ элементовъ

$$0, \quad 1$$

$$i, \quad i + 1.$$

Обозначимъ эти элементы буквами

$$\alpha = 0, \ \beta = 1, \ \gamma = i, \ \delta = i + 1 .$$

Линейная группа имѣетъ въ данномъ случаѣ порядокъ

$$2^2(2^2 - 1) = 12 .$$

Разсмотримъ одну изъ подстановокъ этой группы, напримѣръ

$$[x, \ \delta x + \beta] .$$

Элементъ α долженъ переходить въ $\delta\alpha + \beta$, но $\alpha = 0$, слѣдовательно, α переходитъ въ β.

Элементъ β долженъ переходить въ $\delta\beta + \beta$ или въ $(i + 1) . 1 + 1 = i + 2 = i$, итакъ β переходитъ въ γ.

Элементъ γ переходитъ въ $\delta\gamma + \beta$, или $(i+1)i + 1$, или $i^2 + i + 1 = 0$, т. е. элементъ γ переходитъ въ α.

Наконецъ, элементъ δ переходитъ въ $\delta^2 + \beta$, или $(i + 1)^2 + 1 = i^2 + 2i + 2 = i^2 = -i - 1 = i + 1$, значитъ δ остается безъ измѣненія.

Мы имѣемъ, слѣдовательно, подстановку

$$\begin{pmatrix} \alpha, & \beta, & \gamma, & \delta \\ \beta, & \gamma, & \alpha, & \delta \end{pmatrix}.$$

§ 5. Интересно указать условія, необходимыя и достаточныя для того, чтобы цѣлая функція $f(x)$ въ полѣ самаго общаго вида давала подстановку этого поля.

Этотъ вопросъ былъ разобранъ Hermite'омъ [1]) и Dickson'омъ [2]).

Я приведу здѣсь простыя и важныя замѣчанія моего многоуважаемаго ученика О. Ю. Шмидта [3]), студента университета св. Владиміра, занимающагося съ успѣхомъ уравненіями, степень которыхъ есть степень простого числа.

Будемъ разсматривать функцію $f(x)$ степени $p^n - 1$, ибо высшія степени можно уничтожить на основаніи уравненія $x^{p^n} - x = 0$.

Если функція $f(x)$ даетъ, дѣйствительно, подстановку S, то и функція

$$f_2(x) = f(f(x))$$

даетъ подстановку, которая будетъ не чѣмъ инымъ какъ квадратомъ S^2 первой подстановки.

Вообще говоря, мы вводимъ рядъ функцій

$$f(x),\ f_2(x),\ f_3(x),\ \ldots\ f_k(x),$$

которыя послѣдовательно получаются при помощи рекурентнаго процесса

$$f_k(x) = f_{k-1}(f(x)).$$

Такъ какъ подстановка S входитъ въ составъ группы всѣхъ подстановокъ, перемѣщающихъ p^n элементовъ, то она какъ элементъ конечной группы должна принадлежать къ нѣкоторому показателю, т. е.

$$S^m = 1$$

или иначе

$$f_m(x) = x.$$

Написавъ послѣднее уравненіе въ такомъ видѣ

$$f_{m-1}(f(x)) = x,$$

мы замѣчаемъ, что должна существовать функція

$$\Phi(x)$$

степени $p^n - 1$, обладающая свойствомъ, что равенство

$$\Phi(f(x) = x \qquad (1)$$

есть тождество.

---

[1]) *Hermite.* Comptes Rendus. Vol. 57 (1863) pp. 750—757.

[2]) *L. Dickson.* Linear groups. Leipzig. 1901. p. 59.

[3]) *О. Шмидтъ.* Объ уравненіяхъ, рѣшаемыхъ въ радикалахъ, степень которыхъ есть степень простого числа. Кіевъ 1913.

Существованіе для всякой функціи $f(x)$, дающей подстановку, соотвѣтственной $\Phi(x)$ есть не что иное, какъ требованіе существованія для всякаго элемента группы ему обратнаго.

Будемъ искать функцію $\Phi(x)$ при помощи способа неопредѣленныхъ коэффиціентовъ, а именно пусть

$$\Phi(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_{p^n-1} x^{p^n-1}.$$

Получимъ равенство

$$\alpha_0 + \alpha_1 f(x) + \alpha_2 [f(x)]^2 + \ldots = x,$$

которое должно быть тождествомъ, если мы на основаніи $x^{p^n} - x = 0$, уничтожимъ всѣ степени x большія $p^n - 1$.

Получаемъ p^n уравненій первой степени относительно неизвѣстныхъ коэффиціентовъ α_i. Опредѣлитель Δ этой системы уравненій не долженъ равняться нулю, чтобы было возможно однозначное нахожденіе функціи $\Phi(x)$.

Опредѣлитель Δ есть цѣлая функція отъ коэффиціентовъ функціи $f(x)$. Покажемъ, что условіемъ необходимымъ и достаточнымъ для того, чтобы функція $f(x)$ давала подстановку, является *неравенство нулю* опредѣлителя Δ.

Необходимость условія мы уже видѣли, покажемъ его достаточность.

Допустимъ, что при Δ отличномъ отъ нуля функція $f(x)$ не пробѣгаетъ вполнѣ поля, если x его пробѣгаетъ. Другими словами, допустимъ, что могутъ при разныхъ значеніяхъ x получаться одинаковыя значенія функціи. Напр.

$$f(x_1) = f(x_2) \tag{2}$$

Такъ какъ Δ не равно нулю, то можно найти функцію $\Phi(x)$. Уравненіе (2) даетъ

$$\Phi(f(x_1)) = \Phi(f(x_2))$$

или окончательно

$$x_1 = x_2,$$

что противорѣчитъ допущенію.

§ 6. Разсмотримъ еще одинъ примѣръ изъ теоріи группъ, а именно, такъ называемую *дробную линейную группу.*

Разсмотримъ соотношеніе

$$y = \frac{ax + b}{cx + d},$$

которое мы будемъ называть дробнымъ линейнымъ преобразованіемъ перемѣнной x въ y.

Здѣсь a, b, c, d суть нѣкоторые элементы поля $G[p^n]$. Заставимъ перемѣнную x пробѣгать поле и посмотримъ, когда перемѣнная y будетъ также пробѣгать все поле. Для этой цѣли всякое равенство

$$\frac{ax_1+b}{cx+d}=\frac{ax_2+b}{cx_2+d} \tag{1}$$

должно влечь за собой какъ необходимое слѣдствіе равенство

$$x_1=x_2,$$

но равенство (1) можетъ быть переписано такъ

$$(ad-bc)(x_1-x_2)=0.$$

Значитъ необходимымъ и достаточнымъ условіемъ, чтобы дробная функція выражала подстановку состоитъ въ неравенствѣ нулю опредѣлителя $ab-cd$.

Дробныя линейныя подстановки образуютъ, очевидно, группу.

При разсмотрѣніи дробной линейной группы надо кромѣ элементовъ поля ввести еще одинъ элементъ, аналогичный безконечности въ элементарной алгебрѣ и который мы будемъ обозначать знакомъ ∞. Этотъ элементъ мы будемъ употреблять условно, предполагая, что онъ удовлетворяетъ слѣдующимъ постулативнымъ свойствамъ:

1. $\infty=\frac{a}{0}$, гдѣ a любой изъ неравныхъ нулю элементовъ поля.

2. $\infty+\lambda=\lambda+\infty=\infty$, $\lambda\infty=\infty\lambda=\infty$, $\frac{\infty}{\lambda}=\infty$ при всякомъ отличномъ отъ нуля λ

3. $\frac{a\infty+b}{c\infty+d}=\frac{a}{c}$.

Итакъ, дробная линейная группа есть группа перемѣщающая p^n+1 предметовъ, а именно: элементы поля и ∞.

§ 7. Является конечно не случайнымъ совпаденіе близости съ конечнымъ полемъ двухъ съ перваго взгляда совершенно разнородныхъ теорій: а именно, теоріи алгебраическаго рѣшенія уравненій и теоріи сравненій высшихъ степеней по простому идеальному модулю. Несомнѣнно, эти двѣ теоріи имѣютъ большое сродство, изученіе котораго можно усиленно рекомендовать молодымъ ученымъ. Кое что въ этомъ направленіи уже сдѣлано. Я имѣю въ виду прекрасные результаты Hilbert'a, опубликованные во второй главѣ (Zweiter Theil) сочиненія Die Theorie der algebraischen Zahlkörper. Bericht, erstattet der deutschen Mathematiker Vereinigung.

§ 8. Обращаемся теперь къ другимъ соображеніямъ, имѣющимъ большую важность для теоріи чиселъ. Такъ какъ формальная алгебра раціональныхъ дѣйствій сохраняется во всѣхъ ея подробностяхъ для конечнаго поля, сравненія же по простому модулю представляютъ простѣйшій случай конечнаго поля, то ясно, что масса свойствъ уравненій переносится тѣмъ самымъ на сравненія. Вотъ источникъ той аналогіи между уравненіями и сравненіями, которая подчеркивалась старыми авторами, какъ напримѣръ, Cauchy и Poisson'омъ.

Теперь же для насъ очевидно, что аналогія идетъ гораздо глубже и распространяется на сравненія по идеальному модулю.

§ 9. Чтобы показать примѣръ указанной аналогіи, мы разсмотримъ вопросы о первообразныхъ корняхъ простого числа p.

Мы поступимъ такъ: рѣшимъ одинъ вопросъ обыкновенной алгебры при помощи раціональныхъ дѣйствій; тогда эти дѣйствія сохраняются для конечнаго поля и, парафразируя на это послѣднее результатъ, получимъ теорему относящуюся къ полю.

Возьмемъ вопросъ о нахожденіи уравненія обыкновенной алгебры, которому удовлетворяютъ только первообразные корни изъ единицы степени n. Обозначая это уравненіе

$$X_n = 0, \tag{1}$$

не трудно убѣдиться, что функція X_n будетъ цѣлою степени $\varphi(n)$ (по числу первообразныхъ корней) съ цѣлыми коэффиціентами.

Въ виду того, что первообразные корни изъ единицы степени n суть такіе, которые удовлетворяютъ уравненію

$$x^n - 1 = 0$$

и не удовлетворяютъ никакому другому вида

$$x^d - 1 = 0,$$

гдѣ d есть настоящій дѣлитель числа n, мы должны выписать всѣ уравненія

$$x^{d_1} - 1 = 0,\ x^{d_2} - 1 = 0,\ x^{d_3} - 1 = 0,\ \ldots,$$

гдѣ d_1, d_2, d_3, ... суть всѣ настоящіе дѣлители числа n.

Вычисленіе функціи X_n совершится такъ. Находимъ при помощи послѣдовательнаго дѣленія общаго наибольшаго дѣлителя функціи $x^n - 1$ и функціи $x^{d_1} - 1$.

Пусть этототъ дѣлитель будетъ $\omega(x)$, такъ что

$$x^n - 1 = \omega(x) f(x).$$

Удаляемъ этого дѣлителя $\omega(x)$ и разсмотримъ функцію $f(x)$. Ищемъ далѣе общаго наибольшаго дѣлителя $f(x)$ и $x^{d_2} - 1$, пусть этотъ дѣлитель будетъ $\omega_1(x)$, такъ что $f(x) = \omega_1(x) f_1(x)$. Переходимъ къ разсмотрѣнію функціи $f_1(x)$ и продолжаемъ подобнымъ образомъ удаленіе общихъ дѣлителей съ функціями $x^{d_3} - 1$, $x^{d_4} - 1$, ... пока не придемъ окончательно къ функціи X_n. Такъ какъ всѣ послѣдовательныя дѣленія совершаются при помощи раціональныхъ дѣйствій, то окончательная функція X_n должна быть съ раціональными коэффиціентами. Считая въ ней старшій коэффиціентъ равнымъ единицѣ и принимая во вниманіе теорему Gauss'a [1]), замѣчаемъ, что всѣ коэффиціенты функціи X_n должны быть числами цѣлыми.

Приведенный способъ вычисленія X_n не удобенъ на практикѣ вслѣдствіе большихъ выкладокъ и служитъ не столько настоящимъ способомъ вычисленія, сколько спосссбомъ доказательства существованія функціи X_n и раціональности ея коэффиціентовъ.

Функція X_n оказывается неприводимою въ раціональномъ полѣ. На доказательствѣ этого факта я не буду останавливаться, ссылаясь на мой университетскій курсъ алгебраическаго анализа. Въ этомъ курсѣ даются также болѣе совершенныя правила для вычисленія функціи X_n.

Очевидно, что уравненіе $X_n = 0$ будетъ въ конечномъ полѣ представлять изъ себя уравненіе, которому удовлетворяютъ элементы поля принадлежащіе къ показателю n и только эти элементы. Конечно, чтобы уравненіе $X_n = 0$ имѣло въ полѣ корни, необходимо, чтобы n было дѣлителемъ порядка мультипликативной группы поля.

Переходя въ частности къ числовому полю, мы можемъ сказать, что сравненіе

$$X_{p-1} \equiv 0 \pmod{p}$$

имѣетъ корнями всѣ первообразные корни простого числа p.

Такъ, напримѣръ, для $p = 73$ мы получаемъ $\varphi(72) = 24$ и кромѣ того

$$x^{72} - 1 = (x^{36} - 1)(x^{12} + 1)(x^{24} - x^{12} + 1)$$

значитъ

$$X_{72} = x^{24} - x^{12} + 1.$$

§ 10. *Теорема. Функція* $\mu(n)$ *введенная въ § 32 главы II, есть сумма первообразныхъ корней изъ единицы степени* n.

---

[1]) Д. Граве. Курсъ алгебраическаго анализа. (Литогр.). 1910.

Для доказательства предположимъ число n разложеннымъ на простые множители

$$n = p_1^{\omega_1} p_2^{\omega_2} p_3^{\omega_3} \ldots$$

Лемма. Пусть r будетъ первообразный корень степени a изъ единицы, а s первообразный корень степени b изъ единицы. Если числа a и b взаимно простыя, то произведеніе этихъ корней будетъ первообразнымъ корнемъ степени ab изъ единицы.

Пусть t будетъ наименьшій показатель, при которомъ имѣетъ мѣсто равенство

$$(rs)^t = 1 .$$

Возвышая обѣ части этого уравненія въ степень a, получимъ

$$s^{at} = 1 .$$

Очевидно, что at должно быть кратностью показателя b, къ которому принадлежитъ s, т. е. должно быть

$$at = by$$

a и b числа взаимно простыя, слѣдовательно t дѣлится на b. Совершенно подобнымъ образомъ докажемъ, что t дѣлится также на a, слѣдовательно,

$$t = abz .$$

Очевидно, что наименьшее значеніе t получится при $z = 1$ и лемма доказана.

На основаніи доказанной леммы мы можемъ сказать, что сумма первообразныхъ корней степени n изъ единицы представится въ видѣ

$$\Sigma r_1 . \Sigma r_2 . \Sigma r_3 \ldots \qquad (1)$$

произведенія суммъ первообразныхъ корней степени $p_1^{\omega_1}$, $p_2^{\omega_2}$, $p_3^{\omega_3}\ldots$

Но

$$X_{p^\omega} = \frac{x^{p^\omega} - 1}{x^{p^{\omega-1}} - 1} = x^{p^{\omega-1}(p-1)} + x^{p^{\omega-1}(p-2)} + \ldots + x^{p^{\omega-1}} + 1$$

и

$$X_p = x^{p-1} + x^{p-2} + \ldots + 1 .$$

Поэтому сумма Σr первообразныхъ корней, какъ коэффиціентъ второго по порядку члена функціи X_{p^ω} съ обратнымъ знакомъ, будетъ, или равна *нулю*, если $\omega > 1$, или равна -1, если $\omega = 1$.

Итакъ, произведеніе (1) равно нулю, если по крайней мѣрѣ одинъ изъ показателей ω_1, ω_2, ω_3, ... больше единицы, и это произведеніе равно

$(-1)^k$, гдѣ k число различныхъ простыхъ чиселъ, входящихъ въ составъ n, если только всѣ эти числа входятъ въ первой степени. Итакъ, тождественность произведенія (1) съ функціей $\mu(n)$ установлена.

§ 11. Перенося все сказанное на поле Galois, получимъ знаменитую теорему Gauss'a, относящуюся къ суммѣ первообразныхъ корней γ простого числа p, а именно

$$\Sigma\gamma \equiv \mu(p-1) \pmod{p}.$$

§ 12. Безъ труда мы находимъ другую теорему Gauss'a, относящуюся къ произведенію первообразныхъ корней γ, ибо

$$X_n = \frac{(x^n-1)\Pi(x^{\overline{p_1p_2}}-1)\ldots}{\Pi(x^{\overline{p_1}}-1)\Pi(x^{\overline{p_1p_2p_3}}-1)\ldots}$$

и значитъ

$$X_n(0) = 1.$$

§ 13. Сдѣлаемъ еще одно весьма важное замѣчаніе, относящееся къ приложенію конечнаго поля, а именно, что въ этомъ полѣ сохраняется вся теорія опредѣлителей и связанная съ нею теорія рѣшенія системъ линейныхъ уравненій.

При рѣшеніи уравненій первой степени въ полѣ, условіемъ необходимымъ и достаточнымъ для существованія одной опредѣленной системы рѣшеній является, очевидно, также неравенство нулю опредѣлителя.

Весьма важно подчеркнуть еще разъ теорему, относящуюся къ однороднымъ уравненіямъ

$$\begin{aligned} &a_1^{(1)}x_1 + a_2^{(1)}x_2 + \ldots + a_n^{(1)}x_n = 0 \\ &a_1^{(2)}x_2 + a_2^{(2)}x_2 + \ldots + a_n^{(2)}x_n = 0 \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &a_1^{(n)}x_1 + a_2^{(n)}x_n + \ldots + a_n^{(n)}x_n = 0 \end{aligned} \tag{1}$$

Если такія уравненія удовлетворяются системой элементовъ поля

$$x_1, x_2, \ldots x_n,$$

которые не равны всѣ нулю, то долженъ въ полѣ равняться нулю опредѣлитель

$$\Delta = \begin{vmatrix} a_1^{(1)} \ldots a_n^{(1)} \\ \ldots\ldots \\ a_1^{(n)} \ldots a_n^{(n)} \end{vmatrix}.$$

Если же опредѣлитель Δ не равенъ нулю, то всѣ числа $x_1, x_2, \ldots x_n$ должны быть равны нулю.

Если поле конечное числовое, то равенство нулю замѣняется дѣлимостью на p и уравненія сравненіями, а потому теорему можно формулировать такъ.

Если сравненія

$$\left.\begin{aligned} a_1^{(1)}x_1 + a_2^{(1)}x_2 + \ldots + a_n^{(1)}x_n &\equiv 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ a_1^{(n)}x_1 + a_2^{(n)}x_2 + \ldots + a_n^{(n)}x_n &\equiv 0 \end{aligned}\right\} \pmod p \qquad (2)$$

удовлетворяются элементами числового поля $x_1, x_2, \ldots x_n$, *которые не дѣлятся всѣ на* p, *то долженъ дѣлиться на* p *опредѣлитель* Δ.

§ 14. Имѣетъ значеніе разсмотрѣть сравненія (2) § 13 въ полѣ, распространенномъ трансцедентнымъ путемъ изъ конечнаго числового, то есть разсматривать цѣлыя функціи съ произвольнымъ числомъ перемѣнныхъ независимыхъ, коэффиціенты которыхъ принадлежать числовому полю.

Если буквы въ сравненіяхъ (2) § 13 обозначаютъ такія функціи и мы будемъ всякое сравненіе

$$a \equiv 0 \pmod p$$

понимать въ смыслѣ дѣлимости на p всѣхъ коэффиціентовъ функціи a, то будетъ имѣть мѣсто одно изъ двухъ:

или

$$x_1 \equiv 0,\ x_2 \equiv 0,\ \ldots\ x_n \equiv 0 \pmod p,$$

или

$$\Delta \equiv 0 \pmod p.$$

§ 15. Обращаемъ, наконецъ, вниманіе на теорію алгебраическаго рѣшенія уравненій въ полѣ. Дѣло въ томъ, что въ конечномъ полѣ существуетъ относительно рѣшенія уравненій въ радикалахъ теорема аналогичная теоремѣ Abel'a, а именно, что уравненія 2-ой, 3-ей и 4-ой степени имѣютъ общія рѣшенія въ радикалахъ, причемъ видъ этихъ рѣшеній совершенно тотъ же, что и въ обыкновенной алгебрѣ, слѣдовательно, не зависитъ отъ свойствъ поля.—Уравненія же степени выше 4-й не имѣетъ рѣшеній, видъ которыхъ не зависѣлъ бы отъ свойствъ поля.

Въ разъясненіе къ сказанному надо добавить, что подъ радикаломъ $\sqrt[n]{A}$ въ полѣ, гдѣ A элементъ поля, разумѣется корень уравненія $y^n = A$.

Такъ какъ въ общей формулѣ рѣшенія квадратнаго уравненія, а также въ формулѣ Cardan'a для уравненій третьей степени, коэффиціенты уравненія дѣлятся на степени чиселъ 2 и 3, то, очевидно, что получаются исключенія въ поляхъ съ основаніемъ 2 или 3.

Какъ на примѣръ примѣненія разсмотрѣнія формулъ Cardan'a въ ариѳметическомъ полѣ, можно указать на замѣчательныя изслѣдованія *Г. Ѳ. Вороного,* помѣщенныя въ его сочиненіи *„О цѣлыхъ алгебраическихъ числахъ, зависящихъ отъ корня уравненія третьей степени.*

§ 16. Здѣсь я долженъ обратить вниманіе читателя на мемуаръ моего многоуважаемаго ученика А. М. Островскаго, студента марбургскаго университета, подъ заглавіемъ „Къ алгебрѣ конечныхъ полей“ (Протоколы физико-математическаго общества. Кіевъ 1913), въ которомъ авторъ даетъ много новыхъ результатовъ, относящихся къ приложеніямъ конечнаго поля. Особеннаго вниманія заслуживаютъ приложенія къ рѣшенію уравненій поля въ радикалахъ. Здѣсь автору удалось сдѣлать существенный шагъ впередъ. Galois обратилъ вниманіе на исключительные случаи, о которыхъ я упомянулъ въ § 15. Такъ, напримѣръ, Galois заявляетъ [1]), что сравненіе $x^2 + x + 1 \equiv 0 \pmod 2$ не рѣшается въ радикалахъ, ибо выраженіе $\frac{-1+\sqrt{-3}}{2}$ имѣетъ по модулю 2 неопредѣленный видъ $\frac{0}{0}$. Островскій показываетъ возможность раскрытія подобныхъ неопредѣленностей поля. Для этой цѣли онъ примѣняетъ p-адическія числа Hensel'a. Получается полная аналогія съ дифференціальнымъ исчисленіемъ. Какъ въ дифференціальномъ исчисленіи раскрытіе неопредѣленностей основано на примѣненіи понятія о непрерывности, такъ и здѣсь пришлось пользоваться continuum'омъ p-адическихъ чиселъ.

Согласно предположеніямъ, которыя я высказывалъ въ 1911 году на семинарѣ въ Кіевскомъ Университетѣ, гдѣ принималъ участіе и Островскій, выясняется значеніе теоремы Pellet [2]), изъ которой можно вывести Hilbert'овскіе результаты теоріи относительныхъ полей (Relativkörper).

Островскій надѣется получить теорію относительныхъ полей черезъ примѣненіе конечнаго поля въ связи съ p-адическими числами.

Въ заключеніе укажу на новую и важную теорему Островскаго:

Если $F(x)$ неприводимая по подулю p функція и коэффиціентъ при старшей степени x въ $F(x)$ равенъ 1, то уравненіе $F(x) = 0(p)$ въ области p-адическихъ чиселъ есть абелево циклическое.

---

[1]) *Galois*. Oeuvres complètes. p. 17.

[2]) *Dickson*: Linear Groups. p. 133.

ГЛАВА X.

Элементарная теорія непрерывныхъ дробей.

§ 1. Современная теорія чиселъ развилась главнымъ образомъ подъ вліяніемъ задачъ такъ называемаго *анализа Діофанта*. Подъ этимъ именемъ разумѣется теорія рѣшеній въ цѣлыхъ числахъ неопредѣленныхъ уравненій, т. е. такихъ, гдѣ число неизвѣстныхъ превышаетъ число уравненій. Особенно важную роль въ наукѣ играли неопредѣленныя уравненія 2-й степени. Благодаря изслѣдованіямъ Euler'a и особенно Lagrange'a была создана замѣчательная *теорія періодическихъ непрерывныхъ дробей*, которая вылилась потомъ въ теорію бинарныхъ квадратичныхъ формъ, изложенную Gauss'омъ въ его знаменитомъ сочиненіи по теоріи чиселъ, подъ заглавіемъ „Disquisitiones Arithmeticae".

Мы займемся теперь элементами теоріи непрерывныхъ дробей.

§ 2. Будемъ разсматривать алгоритмъ Эвклида для нахожденія общаго наибольшаго дѣлителя 2-хъ чиселъ p и q.

Обозначимъ число q черезъ p_1 и предположимъ, что это число меньше числа p. Дѣлимъ p на p_1 и обозначимъ чрезъ α_0 частное, а черезъ p_2 остатокъ; тогда имѣемъ

$$p = \alpha_0 p_1 + p_2 . \tag{1}$$

Дѣлимъ далѣе p_1 на p_2 и обозначимъ черезъ α_1 частное, а черезъ p_3 остатокъ; получаемъ

$$p_1 = \alpha_1 p_2 + p_3 . \tag{2}$$

Продолжая послѣдовательное дѣленіе далѣе, получаемъ

$$p_2 = \alpha_2 p_3 + p_4 \tag{3}$$

. . . . . .

$$p_{\nu-1} = \alpha_{\nu-1} p_\nu + p_{\nu+1} . \tag{ν}$$

Послѣдовательные остатки

$$p_2, p_3, \ldots, p_{\nu+1} \qquad (*)$$

убываютъ, а такъ какъ они суть цѣлыя числа и такъ какъ цѣлыхъ чиселъ, меньшихъ числа p_2, конечное число, то послѣдовательное дѣленіе наше должно прерваться послѣ конечнаго числа дѣйствій.

Можетъ произойти одно изъ двухъ:

1) Послѣдній остатокъ $p_{\nu+1}$ отличенъ отъ единицы и дѣлитъ на цѣло предыдущій остатокъ p_ν. Тогда этотъ остатокъ есть, очевидно, общій наибольшій дѣлитель заданныхъ чиселъ p и q, ибо очевидно, что на этотъ послѣдній остатокъ должны дѣлиться всѣ предыдущіе остатки ряда (*), а также и числа p и p_1; съ другой стороны, всякій дѣлитель чиселъ p и p_1, а также всякихъ 2-хъ рядомъ стоящихъ остатковъ, долженъ дѣлить всѣ слѣдующіе остатки, а, слѣдовательно, и остатокъ $p_{\nu+1}$.

2) Если заданныя числа p и p_1 взаимно простыя, то общій наибольшій дѣлитель ихъ долженъ равняться единицѣ, а, слѣдовательно, послѣдній остатокъ долженъ быть равенъ единицѣ, или получаемъ слѣдующій рядъ равенствъ

$$\left.\begin{aligned} p &= \alpha_0 p_1 + p_2 \\ p_1 &= \alpha_1 p_2 + p_3 \\ &\cdots\cdots\cdots \\ p_{\nu-1} &= \alpha_{\nu-1} p_\nu + 1 \end{aligned}\right| \quad \ldots\ldots\ldots\ldots \quad (**).$$

§ 3. Равенства (**) предыдущаго §-а можно переписать такъ

$$\frac{p}{q} = \alpha_0 + \frac{p_2}{p_1} = \alpha_0 + \cfrac{1}{\cfrac{p_1}{p_2}}$$

$$\frac{p_1}{p_2} = \alpha_1 + \cfrac{1}{\cfrac{p_2}{p_3}}$$

$$\cdots\cdots\cdots$$

$$\frac{p_{\nu-1}}{p_\nu} = \alpha_{\nu-1} + \frac{1}{p_\nu}.$$

Изъ этихъ равенствъ мы получаемъ слѣдующее разложеніе въ непрерывную дробь раціональнаго числа $\frac{p}{q}$

$$\frac{p}{q} = \alpha_0 + \cfrac{1}{\alpha_1 + \cfrac{1}{\alpha_2 + \cdots\cdots + \cfrac{1}{\alpha_{\nu-1} + \cfrac{1}{p_\nu}}}}. \qquad (1)$$

Цѣлыя числа

$$\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{\nu-1}, p,$$

носятъ названіе *неполныхъ частныхъ* непрерывной дроби.

Непрерывную дробь (1) мы будемъ для сокращенія обозначать знакомъ

$$\frac{p}{q} = (\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{\nu-1}, p_\nu).$$

По способу разложенія мы видимъ, что p_ν есть цѣлое число большее единицы, ибо равенъ 1 только слѣдующій остатокъ $p_{\nu+1}$. Поэтому существуетъ небольшая двойственность въ символѣ непрерывныхъ дробей, состоящая въ томъ, что во всякой непрерывной дроби (1) число звеньевъ можно увеличить на единицу, ибо вмѣсто послѣдняго неполнаго частнаго p_ν можно написать

$$(p_\nu - 1) + \frac{1}{1}.$$

Значитъ, ту же самую непрерывную дробь можно будетъ переписать такъ

$$\frac{p}{q} = (\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{\nu-1}, (p_\nu - 1), 1).$$

Такъ какъ

$$p_\nu > 1,$$

то $p_\nu - 1$ будетъ цѣлое число, отличное отъ нуля.

Мы видимъ, слѣдовательно, что *при разложеніи раціональнаго числа въ непрерывную дробь можно имѣть по желанію четное или нечетное число звеньевъ.*

§ 4. Будемъ теперь раскладывать въ непрерывную дробь нѣкоторое вещественное положительное ирраціональное число x. Обозначимъ черезъ α_0 цѣлую часть числа x. Тогда можно будетъ написать

$$x = \alpha_0 + \frac{1}{x_1}, \tag{1}$$

гдѣ

$$x_1 > 1.$$

Обозначимъ черезъ α_1 цѣлую часть числа x_1; тогда получимъ

$$x_1 = \alpha_1 + \frac{1}{x_2}, \tag{2}$$

$$x_2 > 1.$$

Продолжая вычисленіе цѣлыхъ частей

$$\alpha_2, \alpha_3, \ldots, \alpha_{n-1}$$

чиселъ

$$x_2, x_3, \ldots, x_{n-1},$$

получимъ рядъ равенствъ

$$x_2 = \alpha_2 + \frac{1}{x_3}, \ldots x_{n-1} = \alpha_{n-1} + \frac{1}{x_n}.$$

Получаемъ слѣдующее разложеніе ирраціональнаго числа x въ непрерывную дробь

$$x = \alpha_0 + \frac{1}{\alpha_1 + \frac{1}{\alpha_2 + \ddots + \frac{1}{\alpha_{n-1} + \frac{1}{x_n}}}},$$

что можно записать символомъ

$$x = (\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{n-1}, x_n), \qquad (3)$$

гдѣ x_n нѣкоторое ирраціональное число, большее единицы.

Число x_n мы будемъ называть *полнымъ частнымъ*.

Поэтому формула (3) не представляетъ настоящаго разложенія ирраціональнаго числа въ непрерывную дробь, и надо продолжить дальнѣйшее выдѣленіе цѣлыхъ частей чиселъ x_n, такъ что *при разложеніи ирраціональнаго числа въ непрерывную дробь получаемъ безконечную дробь*.

§ 5. Будемъ разсматривать выраженіе

$$x = (\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{n-1}, x_n),$$

гдѣ

$$\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{n-1}$$

числа цѣлыя, а

$$x_n$$

число ирраціональное.

Докажемъ, что число x можно представить въ такомъ видѣ

$$x = \frac{P_n x_n + P_{n-1}}{Q_n x_n + Q_{n-1}}, \qquad (1)$$

гдѣ

$$P_n, P_{n-1}, Q_n, Q_{n-1}$$

суть цѣлыя положительныя числа.

Въ самомъ дѣлѣ, для значеній

$$n = 1; 2$$

теорема провѣряется непосредственно.

Въ самомъ дѣлѣ

$$x = \alpha_0 + \frac{1}{x_1} = \frac{\alpha_0 x_1 + 1}{1 . x_1 + 0}.$$

такъ что

$$P_0 = 1, \qquad Q_0 = 0,$$

$$P_1 = \alpha_0, \qquad Q_1 = 1.$$

Подобнымъ же образомъ

$$x = \alpha_0 + \frac{1}{\alpha_1 + \frac{1}{x_2}} = \alpha_0 + \frac{x_2}{\alpha_1 x_2 + 1} = \frac{(\alpha_1 \alpha_0 + 1) x_2 + \alpha_0}{\alpha_1 x_2 + 1},$$

откуда получаемъ

$$P_2 = \alpha_1 \alpha_0 + 1 \text{ и } Q_2 = \alpha_1.$$

Для доказательства общей теоремы покажемъ, что если теорема справедлива для нѣкотораго цѣлаго значенія n, то она будетъ справедлива и для значенія n, на единицу бо́льшаго.

Въ самомъ дѣлѣ

$$(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}, x_n) =$$

$$= \left(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}, \alpha_n + \frac{1}{x_{n+1}}\right).$$

Значитъ, подставляя въ равенство (1) вмѣсто x_n выраженіе

$$\alpha_n + \frac{1}{x_{n+1}},$$

получимъ

$$x = \frac{P_n \left(\alpha_n + \frac{1}{x_{n+1}}\right) + P_{n-1}}{Q_n \left(\alpha_n + \frac{1}{x_{n+1}}\right) + Q_{n-1}} = \frac{(P_n \alpha_n + P_{n-1}) x_{n+1} + P_n}{(Q_n \alpha_n + Q_{n-1}) x_{n+1} + Q_n}. \qquad (2)$$

Обозначимъ для сокращенія

$$P_{n+1} = P_n \alpha_n + P_{n-1}$$

$$Q_{n+1} = Q_n \alpha_n + Q_{n-1}. \qquad (3)$$

Формулы (3) показываютъ, что если

$$P_n, \; P_{n-1}, \; Q_n, \; Q_{n-1}$$

числа цѣлыя положительныя, то таковы же будутъ и числа P_{n+1} и Q_{n+1}.

Значитъ, высказанная теорема о возможности представленія числа x подъ видомъ (1) доказана, ибо такой же видъ имѣетъ это число при n на единицу бо́льшемъ.

Итакъ, общая формула (1) справедлива при всякомъ числѣ n, при чемъ всѣ числа

$$P_0, P_1, P_2, \ldots \tag{4}$$

$$Q_0, Q_1, Q_2, \ldots \tag{5}$$

суть цѣлыя положительныя, и числа P_n и Q_n возрастаютъ безпредѣльно, если разложеніе числа x въ непрерывную дробь безконечное.

Числа P_n начинаютъ возрастать со значенія, равнаго единицѣ, при чемъ, если $\alpha_0 = 1$, то два первыхъ числа одинаковы $P_0 = P_1 = 1$, и возрастаніе начинается съ числа P_2. Q_n начинаетъ возрастать со значенія 0 при $n = 0$ $Q_0 = 0$; слѣдующія два могутъ быть равны между собою при $\alpha_1 = 1$, такъ что $Q_1 = Q_2 = 1$, и возрастаніе начинается съ числа Q_3.

Относительно чиселъ Q_n можно высказать такое общее предложеніе, эти числа удовлетворяютъ неравенствамъ $0 \leqq Q_{n-1} \leqq Q_n$; при чемъ лѣвое равенство имѣетъ мѣсто при $n = 1$, правое же равенство можетъ имѣть мѣсто при $n = 2$. При $n > 2$ получаемъ, конечно

$$0 < Q_{n-1} < Q_n. \tag{6}$$

§ 6. Не трудно убѣдиться въ существованіи равенства

$$\frac{P_n}{Q_n} = (\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{n-1}). \tag{1}$$

Въ самомъ дѣлѣ, съ одной стороны мы имѣемъ, подставляя вмѣсто x_n безконечность

$$(\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{n-1}, \infty) =$$

$$= \alpha_0 + \frac{1}{\alpha_1 + \frac{1}{\alpha_1 + \ddots + \frac{1}{\alpha_{n-1} + \frac{1}{\infty}}}} =$$

$$= \alpha_0 + \frac{1}{\alpha_1 + \frac{1}{\alpha_2 + \ddots + \frac{1}{\alpha_{n-1}}}} = (\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{n-1});$$

съ другой стороны

$$(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}, x_n) = \frac{P_n + \frac{P_{n-1}}{x_n}}{Q_n + \frac{Q_{n-1}}{x_n}}.$$

Подставляя въ это равенство вмѣсто x_n безконечность, получимъ равенство (1), которое требовалось доказать.

Итакъ дробь $\frac{P_n}{Q_n}$ есть не что иное, какъ величина конечной дроби, которую мы получаемъ изъ разсматриваемой безконечной, обрывая дробь на послѣднемъ неполномъ частномъ α_{n-1}.

Дроби $\frac{P_n}{Q_n}$ называются *подходящими* дробями разсматриваемой безконечной непрерывной дроби.

§ 7. Умножая первое изъ равенствъ (3) § 5 на Q_n, а второе на P_n и вычитая, получимъ

$$P_{n+1}Q_n - Q_{n+1}P_n = -(P_nQ_{n-1} - Q_nP_{n-1}). \qquad (1)$$

Примѣняя формулу (1) къ значеніямъ числа n, равнымъ

$$1, 2, 3, \ldots, n-1,$$

получимъ

$$P_2Q_1 - Q_2P_1 = -(\alpha_0 . 0 - 1 . 1) = (-1)^2$$
$$P_3Q_2 - Q_3P_2 = -(P_2Q_1 - Q_2P_1)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$P_nQ_{n-1} - Q_nP_{n-1} = -(P_{n-1}Q_{n-2} - Q_{n-1}P_{n-2}).$$

Перемножая послѣднія равенства и сокращая, получимъ

$$P_nQ_{n-1} - Q_nP_{n-1} = (-1)^n. \qquad (2)$$

Формула (2) приводитъ къ цѣлому ряду весьма важныхъ выводовъ относительно подходящихъ дробей.

§ 8. *Всѣ подходящія дроби суть дроби несократимыя,* ибо на основаніи формулы (2) предыдущаго §-а общій наибольшій дѣлитель чиселъ P_n и Q_n долженъ былъ бы дѣлить стоящую во второй части единицу, что невозможно, если этотъ общій дѣлитель отличенъ отъ единицы.

§ 9. Переписавъ равенство (2) § 7 въ такомъ видѣ

$$\frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)^n}{Q_nQ_{n-1}}, \qquad (1)$$

замѣчаемъ, что, если n число четное, то 2-я часть положительная, слѣдовательно, *всякая подходящая дробь четнаго порядка больше предыдущей подходящей дроби.*

§ 10. Не трудно убѣдиться, что *всякая дробь четнаго порядка больше всякой дроби нечетнаго порядка.*

Для этой цѣли докажемъ теорему

Теорема. *Подходящія дроби нечетнаго порядка возрастаютъ, оставаясь меньше разлагаемаго въ непрерывную дробь ирраціональнаго числа x, подходящія же дроби четнаго порядка убываютъ съ возрастаніемъ значка n, оставаясь больше числа x.*

Въ самомъ дѣлѣ, примѣняя формулу (1) предыдущаго §-а къ значеніямъ n и $n-1$, получимъ

$$\frac{P_n}{Q_n}-\frac{P_{n-2}}{Q_{n-2}}=\left(\frac{P_n}{Q_n}-\frac{P_{n-1}}{Q_{n-1}}\right)+\left(\frac{P_{n-1}}{Q_{n-1}}-\frac{P_{n-2}}{Q_{n-2}}\right)=$$

$$-\frac{(-1)^n}{Q_nQ_{n-1}}+\frac{(-1)^{n-1}}{Q_{n-1}Q_{n-2}}=\frac{(-1)^n}{Q_{n-1}}\left(\frac{1}{Q_n}-\frac{1}{Q_{n-2}}\right).$$

Такъ какъ $Q_n>Q_{n-2}$, то знакъ разности $\frac{P_n}{Q_n}-\frac{P_{n-2}}{Q_{n-2}}$ совпадаетъ со знакомъ числа $(-1)^{n+1}$.

Итакъ, подходящія дроби четнаго порядка

$$\frac{P_2}{Q_2},\ \frac{P_4}{Q_4},\ \frac{P_6}{Q_5},\ \ldots$$

убываютъ съ возрастаніемъ значка дроби, а подходящія дроби нечетнаго порядка

$$\frac{P_1}{Q_1},\ \frac{P_3}{Q_3},\ \frac{P_5}{Q_5},\ \ldots$$

возрастаютъ.

Сравнимъ теперь величину подходящей дроби съ величиною числа, разлагаемаго въ непрерывную дробь, т. е. разсмотримъ разность

$$\frac{P_n}{Q_n}-x=\frac{P_n}{Q_n}-\frac{P_nx_n+P_{n-1}}{Q_nx_n+Q_{n-1}}=\frac{(-1)^n}{Q_n(Q_nx_n+Q_{n-1})}. \qquad (1)$$

Такъ какъ числа x_n, Q_{n-1} и Q_n положительныя, то знакъ разности

$$\frac{P_n}{Q_n}-x$$

совпадаетъ со знакомъ числа $(-1)^n$, такъ что всѣ подходящія дроби чет-

наго порядка больше числа x, а всѣ подходящія нечетнаго порядка меньше числа x.

Не трудно убѣдиться, что если x ирраціональное число, т. с. если непрерывная дробь безконечная, то x есть предѣлъ къ которому стремится $\frac{P_n}{Q_n}$ при возрастаніи n до безконечности.

Въ самомъ дѣлѣ,

$$x_n > a_n,$$

слѣдовательно,

$$Q_n x_n + Q_{n-1} > Q_n a_n + Q_{n-1},$$

т. е.

$$Q_n x_n + Q_{n-1} > Q_{n+1},$$

а, слѣдовательно, подавно

$$Q_n x_n + Q_{n-1} > Q_n,$$

такъ что получаемъ по формулѣ (1)

$$\left| \frac{P_n}{Q_n} - x \right| < \frac{1}{Q_n^2}. \qquad (2)$$

Неравенство (2) показываетъ, что число x есть дѣйствительно предѣлъ дроби $\frac{P_n}{Q_n}$, т. к. Q_n при возрастаніи n возрастаетъ безпредѣльно.

§ 11. Архимедово число $\frac{22}{7}$ и число Адріана Меція $\frac{355}{113}$, оказывается, суть не что иное, какъ двѣ подходящія дроби при разложеніи числа π въ непрерывную дробь, которая имѣетъ видъ

$$\pi = 3 + \frac{1}{7} + \frac{1}{15} + \frac{1}{1} + \frac{1}{1} + \frac{1}{292} + \ldots\ldots$$

Lagrange показалъ, что изъ дробей, знаменатели которыхъ не превосходятъ числа 7, число $\frac{22}{7}$ выражаетъ число π наиболѣе близко; подобнымъ же образомъ нельзя найти раціональной дроби, которая имѣла бы знаменатель, не превосходящій числа 113, и выражала бы число π ближе, чѣмъ дробь $\frac{355}{113}$.

Lagrange резюмировалъ это замѣчаніе въ слѣдующей весьма важной теоремѣ:

Теорема. *Не существуетъ никакой рціональной дроби* $\frac{M}{N}$, *которая заключалась бы между двумя рядомъ стоящими подходящими* $\frac{P_n}{Q_n}$ и $\frac{P_{n-1}}{Q_{n-1}}$, *при чемъ знаменатель* N *не превосходилъ бы числа* Q_n.

Въ самомъ дѣлѣ, предположимъ, что дробь $\frac{M}{N}$ заключается между указанными подходящими; тогда имѣютъ одинъ и тотъ же знакъ двѣ разности

$$\frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}} \text{ и } \frac{M}{N} - \frac{P_{n-1}}{Q_{n-1}}.$$

Вторую разность мы не предполагаемъ равной нулю, потому что мы не желаемъ дѣлать предположенія, что промежуточная дробь $\frac{M}{N}$ совпадаетъ съ которой-нибудь изъ подходящихъ.

Такъ какъ абсолютная величина 1-й разности больше абсолютной величины 2-й, то мы можемъ написать неравенство

$$(-1)^n\left(\frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}}\right) > (-1)^n\left(\frac{M}{N} - \frac{P_{n-1}}{Q_{n-1}}\right)$$

или иначе

$$\frac{1}{Q_n Q_{n-1}} > (-1)^n\left(\frac{M}{N} - \frac{P_{n-1}}{Q_{n-1}}\right).$$

Умножая обѣ части неравенства на NQ_{n-1}, получимъ

$$\frac{N}{Q_n} > (-1)^n(MQ_{n-1} - P_{n-1}N).$$

Во второй части этого неравенства находится положительное цѣлое число, отличное отъ нуля, значитъ, знаменатель N промежуточной дроби долженъ быть больше, чѣмъ Q_n, что и требовалось доказать.

§ 12. Непрерывныя дроби даютъ возможность очень просто рѣшать неопредѣленныя уравненія первой степени.

Будемъ разсматривать уравненіе

$$\alpha y - \beta x = 1, \qquad (1)$$

гдѣ α и β цѣлыя числа.

Требуется рѣшить въ цѣлыхъ числахъ это неопредѣленное уравненіе.

Очевидно, что для возможности задачи необходимо, чтобы числа α и β были взаимно простыя.

Пусть найдено одно рѣшеніе x_0, y_0 этого неопредѣленнаго уравненія, такъ что получается тождество

$$\alpha y_0 - \beta x_0 = 1.$$

Вычитая это тождество изъ уравненія (1), получимъ

$$\alpha(y - y_0) = \beta(x - x_0).$$

Числа α и β взаимно простыя, слѣдовательно, разность $y - y_0$ должна дѣлиться на β, а разность $x - x_0$ должна дѣлиться на α, и мы получаемъ

$$x - x_0 = \alpha t, \quad y - y_0 = \beta s,$$

гдѣ t и s — числа цѣлыя, причемъ $s = t$.

Отсюда мы видимъ, что общее рѣшеніе заданнаго неопредѣленнаго уравненія въ цѣлыхъ числахъ выражается такъ

$$\left.\begin{aligned} x &= x_0 + \alpha t \\ y &= y_0 + \beta t \end{aligned}\right\} \qquad (2)$$

съ произвольнымъ цѣлымъ числомъ t.

Задача сводится, слѣдовательно, къ нахожденію одного рѣшенія x_0, y_0.

Для нахожденія этого рѣшенія разложимъ $\frac{\beta}{\alpha}$ въ непрерывную дробь. Пусть эта дробь будетъ:

$$\frac{\beta}{\alpha} = (a_0 . a_1, a_2, \ldots, a_{n-1}).$$

Эта дробь конечная и, слѣдовательно,

$$\frac{P_n}{Q_n} = \frac{\beta}{\alpha},$$

т. е.

$$P_n = \beta \text{ и } Q_n = \alpha.$$

Возьмемъ формулу:

$$P_{n-1}Q_n - Q_{n-1}P_n = (-1)^{n-1}.$$

Мы видѣли уже въ § 3, что число n можно сдѣлать по желанію какъ четнымъ, такъ и нечетнымъ, слѣдовательно, можемъ достигнуть того, что будетъ

$$Q_nP_{n-1} - P_nQ_{n-1} = 1$$

или

$$\alpha P_{n-1} - \beta Q_{n-1} = 1,$$

т. е.

$$x_0 = Q_{n-1}, \quad y_0 = P_{n-1}.$$

Примѣръ.

Для примѣра рѣшимъ въ цѣлыхъ числахъ неопредѣленное уравненіе

$$14y - 25x = 1.$$

Разлагая $\frac{25}{14}$ въ непрерывную дробь, находимъ

$$\frac{25}{14} = (1, 1, 3, 1, 2).$$

Слѣдовательно, $P_5 = 25$ и $Q_5 = 14$.

Составивъ подходящую дробь $\frac{P_4}{Q_4}$, находимъ $P_4 = 9$ и $Q_4 = 5$, а такъ какъ $P_4Q_5 - P_5Q_4 = (-1)^4 = 1$, то искомымъ рѣшеніемъ будетъ $x_0 = 5$ и $y_0 = 9$ или окончательно

$$x = 5 + 14t,$$

$$y = 9 + 25t.$$

§ 13. Обращаясь къ уравненію самаго общаго вида

$$\alpha y - \beta x = \gamma, \qquad (1)$$

мы замѣчаемъ, что общій наибольшій дѣлитель α и β долженъ быть дѣлителемъ числа γ. Раздѣливъ на этого дѣлителя, мы замѣчаемъ, что сводимъ задачу къ рѣшенію такого уравненія, гдѣ числа α и β взаимно простыя.

Для рѣшенія уравненія (1) рѣшимъ сначала уравненіе

$$\alpha y - \beta x = 1,$$

и останется только умножить частное рѣшеніе x_0 и y_0, получаемое изъ послѣдняго уравненія, на число γ, общее же рѣшеніе получится по тѣмъ же формуламъ (2) §-а 12.

Примѣръ.

Для примѣра рѣшимъ въ цѣлыхъ числахъ неопредѣленное уравненіе

$$14y - 25x = 13.$$

Изъ § 12 мы знаемъ, что для уравненія $14y - 25x = 1$ одно рѣшеніе будетъ $x_0 = 5$ и $y_0 = 9$, слѣдовательно, общее рѣшеніе заданнаго уравненія будетъ $x = 65 + 14t$, $y = 117 + 25t$.

§ 14. Существуетъ только одно рѣшеніе неопредѣленнаго уравненія

$$\alpha y - \beta x = 1,$$

въ которомъ y заключается въ границахъ отъ 0 до β, при чемъ обѣ эти границы мы одновременно не включаемъ, такъ что мы докажемъ суще-

ствованіе такого числа или при условіи

$$0 \leqq y < \beta,$$

или при условіи

$$0 < y \leqq \beta.$$

Въ сказанномъ можно просто убѣдиться изъ разсмотрѣнія формулы

$$y = y_0 + \beta t.$$

Разность двухъ рѣшеній выражается по формулѣ

$$y - y_0 = \beta t,$$

при чемъ наименьшее значеніе этой разности есть β, и всегда существуетъ для всякаго рѣшенія y_0 другое y, разность которыхъ есть точно β.

Отсюда мы замѣчаемъ, что въ границахъ отъ 0 до β не можетъ быть двухъ значеній y, ибо тогда разность этихъ значеній, будучи меньше числа β, должна была бы дѣлиться на β, что невозможно.

Точно такъ же невозможно предположить, что ни одно значеніе y-ка не попадаетъ въ промежутокъ отъ 0 до β, ибо въ подобномъ случаѣ существовали бы такія два рядомъ стоящія значенія y-ка, разность которыхъ была бы больше, чѣмъ β.

§ 15. На основаніи соображеній § 10 мы замѣчаемъ, что, если $\frac{P}{Q}$ есть подходящая дробь изъ разложенія числа x въ непрерывную, то будетъ

$$x - \frac{P}{Q} = \pm \frac{\theta}{Q^2}, \tag{1}$$

гдѣ $0 < \theta < 1$.

Поставимъ теперь себѣ обратный вопросъ.

Допустимъ, что существуетъ соотношеніе (1), спрашивается при какихъ условіяхъ $\frac{P}{Q}$ будетъ, дѣйствительно, одною изъ подходящихъ.

Беремъ формулу (1) § 10

$$x - \frac{P_n}{Q_n} = \frac{(-1)^{n+1}}{Q_n (Q_n x_n + Q_{n-1})} \tag{2}$$

Допустимъ, что $\frac{P}{Q} = \frac{P_n}{Q_n}$. На основаніи § 3 мы можемъ число n всегда по произволу сдѣлать четнымъ, или нечетнымъ, тогда можно будетъ подобрать n такъ, чтобы знакъ $(-1)^{n+1}$ совпадалъ со знакомъ (1). Сопостав-

ляя (1) и (2), получимъ

$$\frac{1}{Q_n(Q_n x_n + Q_{n-1})} = \frac{\theta}{Q_n^2}, \quad \theta = \frac{Q_n}{Q_n x_n + Q_{n-1}},$$

но $x_n > 1$, слѣдовательно,

$$\theta < \frac{Q_n}{Q_n + Q_{n-1}}. \tag{3}$$

Условіе (3) будетъ также и достаточнымъ.

Такъ какъ имѣетъ мѣсто всегда неравенство

$$\frac{Q_n}{Q_n + Q_{n-1}} > \frac{1}{2},$$

то мы получаемъ теорему:

Если имѣетъ мѣсто неравенство

$$\left| x - \frac{P}{Q} \right| < \frac{1}{2Q^2},$$

то $\frac{P}{Q}$ *будетъ подходящею дробью изъ разложенія* x *въ непрерывную.*

О разложеніи ирраціональныхъ чиселъ въ непрерывныя дроби.

§ 16. Приступая къ болѣе подробному изученію разложенія ирраціональныхъ чиселъ въ непрерывныя дроби, мы введемъ весьма важное понятіе о такъ называемой *эквивалентности чиселъ*.

Это понятіе введено было впервые Lagrange'омъ для ирраціональныхъ чиселъ простѣйшаго вида, а именно для ирраціональныхъ корней квадратнаго уравненія съ цѣлыми коэффиціентами.

§ 17. Мы будемъ называть эквивалентными такія два числа x и y, между которыми существуетъ зависимость

$$y = \frac{\alpha x + \beta}{\gamma x + \delta}, \tag{1}$$

гдѣ α, β, γ и δ суть цѣлыя числа, удовлетворяющія равенству

$$\alpha\delta - \beta\gamma = \varepsilon,$$

гдѣ

$$\varepsilon = \pm 1.$$

Свойство эквивалентности есть свойство обратимое, т. е. обратно, x выражается черезъ y при помощи формулы, подобной (1)

$$x = \frac{\delta y - \beta}{-\gamma y + \alpha}, \tag{2}$$

при чемъ имѣетъ мѣсто равенство

$$\delta\alpha - (-\gamma)(-\beta) = \alpha\delta - \beta\gamma = \varepsilon .$$

§ 18. Не трудно показать, что *два числа, эквивалентныя третьему, эквивалентны между собой.*

Въ самомъ дѣлѣ, возьмемъ равенство (1) изъ предыдущаго параграфа и еще другое

$$x = \frac{\alpha' z + \beta'}{\gamma' z + \delta'},$$

гдѣ

$$\alpha'\delta' - \beta'\gamma' = \varepsilon' \quad (\varepsilon' = \pm 1).$$

Тогда числа z и y эквивалентны числу x. Покажемъ, что эти два числа будутъ эквивалентны между собой.

Подставляя вмѣсто x выраженіе черезъ z въ формулу (1) предыдущаго параграфа, мы получимъ

$$y = \frac{\alpha'' z + \beta''}{\gamma'' z + \delta''},$$

гдѣ

$$\left.\begin{aligned} \alpha'' &= \alpha\alpha' + \beta\gamma' \\ \beta'' &= \alpha\beta' + \beta\delta' \\ \gamma'' &= \gamma\alpha' + \delta\gamma' \\ \delta'' &= \gamma\beta' + \delta\delta' \end{aligned}\right\} \tag{1}$$

На основаніи теоремы объ умноженіи опредѣлителей, выходитъ

$$\alpha''\delta'' - \beta''\gamma'' = \begin{vmatrix} \alpha\alpha' + \beta\gamma', & \alpha\beta' + \beta\delta' \\ \gamma\alpha' + \delta\gamma', & \gamma\beta' + \delta\delta' \end{vmatrix} = (\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma') = \varepsilon\varepsilon'. \tag{2}$$

Итакъ, мы видимъ по формуламъ (1), что коэффиціенты α'', β'', γ'', δ'' суть числа цѣлыя и, кромѣ того, на основаніи формулы (2) опредѣлитель

$$\alpha''\delta'' - \beta''\gamma'' = \pm 1 ;$$

значитъ, дѣйствительно, числа y и z эквивалентны.

Формулу (1) предыдущаго параграфа мы будемъ толковать такъ: будемъ говорить, что для полученія y надъ числомъ x произведена *эквивалентная подстановка.*

Эту подстановку будемъ обозначать символомъ

$$S = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}.$$

Выраженіе

$$\alpha\delta - \beta\gamma$$

мы будемъ называть *опредѣлителемъ подстановки,* само же разенство (1) предыдущаго параграфа мы будемъ писать такъ

$$y = S(x) = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}(x). \tag{3}$$

Разсмотрнмъ другую подстановку

$$x = S'(z) = \begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix}(z). \tag{4}$$

Если мы подставимъ въ формулу (3) вмѣсто x его выраженіе изъ формулы (4), то мы получимъ

$$y = S''(z) = \begin{pmatrix} \alpha'', & \beta'' \\ \gamma'', & \delta'' \end{pmatrix}(z). \tag{5}$$

Мы будемъ называть подстановку S'' *произведеніемъ* двухъ подстановокъ: подстановки S и подстановки S' — и писать

$$SS' = S'',$$

при чемъ на первое мѣсто ставить знакъ той подстановки S, въ уравненіе которой (3) подставлена величина изъ другой подстановки.

Получаемъ, очевидно, теорему:

Опредѣлитель произведенія 2-хъ подстановокъ равенъ произведенію опредѣлителей множителей.

Итакъ, *сколько бы эквивалентныхъ подстановокъ мы не перемножали, мы получаемъ въ результатѣ всегда эквивалентную подстановку.*

§ 19. Послѣднія соображенія приводятъ насъ къ заключенію, что подстановки образуютъ группу.

Относительно произведенія подстановокъ $SS'S''S'''\ldots$ необходимо замѣтить, что оно обладаетъ сочетательнымъ закономъ $(SS')S'' = S(S'S'')$, перестановительнаго же закона $SS' = S'S$ вообще говоря не существуетъ.

§ 20. Не трудно убѣдиться, что въ какомъ бы порядкѣ мы не перемножили двѣ подстановки

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} \varepsilon\delta, & -\varepsilon\beta \\ -\varepsilon\gamma, & \varepsilon\alpha \end{pmatrix},$$

гдѣ $\varepsilon = \alpha\delta - \beta\gamma$, мы получимъ подстановку

$$\begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}, \qquad (1)$$

которая даетъ тождественное преобразованіе $x = x$.

Тождественную подстановку (1) обыкновенно обозначаютъ знакомъ 1, ибо въ произведеніи подстановокъ такую подстановку можно не писать.

Обыкновенно обозначаютъ

$$S^{-1} = \begin{pmatrix} \varepsilon\delta, & -\varepsilon\beta \\ -\varepsilon\gamma, & \varepsilon\alpha \end{pmatrix},$$

если

$$S = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}.$$

Мы получаемъ $SS^{-1} = S^{-1}S = 1$. Подстановка S^{-1} называется *подстановкой обратной* относительно подстановки S.

§ 21. *Всѣ раціональныя числа эквивалентны между собой.*

Возьмемъ два раціональныхъ числа

$$\frac{p}{q} \quad \text{и} \quad \frac{p'}{q'}.$$

Мы предполагаемъ обѣ дроби несократимыми. Очевидно, что по соображеніямъ § 12 можно найти 4 цѣлыхъ числа ξ, η, ξ', η', которыя будутъ удовлетворять двумъ уравненіямъ $p\eta - q\xi = \varepsilon$ и $p'\eta' - q'\xi' = \varepsilon'$, гдѣ ε и ε' суть ± 1.

Разсмотримъ двѣ подстановки

$$S = \begin{pmatrix} p, & \xi \\ q, & \eta \end{pmatrix} \quad \text{и} \quad S_1 = \begin{pmatrix} p', & \xi' \\ q', & \eta' \end{pmatrix}.$$

Составимъ подстановку

$$SS_1^{-1} = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}. \qquad (1)$$

Числа α, β, γ и δ выйдутъ нѣкоторыя цѣлыя числа, для которыхъ

$$\alpha\delta - \beta\gamma = \pm 1.$$

Умножимъ равенство (1) справа на подстановку S_1, получимъ

$$SS_1^{-1}S_1 = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} S_1,$$

т. е.

$$S = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} S_1$$

или

$$\begin{pmatrix} p, & \xi \\ q, & \eta \end{pmatrix} = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \begin{pmatrix} p', & \xi' \\ q', & \eta' \end{pmatrix},$$

откуда получаемъ

$$p = \alpha p' + \beta q'$$

$$q = \gamma p' + \delta q'.$$

Отсюда получаемъ

$$\frac{p}{q} = \frac{\alpha \dfrac{p'}{q'} + \beta}{\gamma \dfrac{p'}{q'} + \delta}.$$

Итакъ, два произвольно взятыхъ раціональныхъ числа $\frac{p}{q}$ и $\frac{p'}{q'}$ эквивалентны между собою.

§ 22. Обращаясь къ числамъ ирраціональнымъ, мы прежде всего должны сдѣлать слѣдующее замѣчаніе, что *для всякаго числа x будутъ эквивалентны числа*

$$-x \quad и \quad \frac{1}{x}.$$

Въ самомъ дѣлѣ,

$$-x = \begin{pmatrix} -1, & 0 \\ 0, & 1 \end{pmatrix} (x);$$

точно такъ же

$$\frac{1}{x} = \begin{pmatrix} 0, & 1 \\ 1, & 0 \end{pmatrix} (x).$$

§ 23 Перейдемъ теперь къ разложенію въ непревывныя дроби чиселъ ирраціональныхъ и докажемъ слѣдующую важную теорему, что *разложенія въ непрерывную дробь двухъ чиселъ эквивалентныхъ будутъ таковы, что, начиная съ нѣкотораго мѣста, въ обоихъ разложеніяхъ идутъ тѣ же самыя неполныя частныя*, такъ что два эквивалентныхъ числа раскладываются всегда въ такія двѣ непрерывныя дроби

$$x = (a_0, a_1, a_2, a_3, \ldots, a_{n-1}, a_n, a_{n+1}, \ldots) \qquad (1)$$

$$y = (b_0, b_1, b_2, b_3, \ldots, b_{m-1}, a_n, a_{n+1}, \ldots), \qquad (2)$$

такъ что различіе 2-хъ эквивалентныхъ чиселъ можетъ состоять только въ конечномъ числѣ первыхъ неполныхъ частныхъ.

Прямая теорема, а именно, что двѣ непрерывныя дроби, у которыхъ, начиная съ нѣкотораго мѣста, общія неполныя частныя совпадаютъ, даютъ числа эквивалентныя, доказывается просто, а именно, обозначая для сокращенія

$$x_n = (a_n, a_{n+1}, a_{n+2}, \ldots),$$

мы имѣемъ

$$x = (a_0, a_1, \ldots, a_{n-1}, x_n)$$

$$y = (b_0, b_1, \ldots, b_{m-1}, x_n).$$

На основаніи соображеній § 5 имѣемъ

$$x = \frac{P_n x_n + P_{n-1}}{Q_n x_n + Q_{n-1}},$$

$$y = \frac{T_m x_n + T_{m-1}}{S_m x_n + S_{m-1}}.$$

Но мы замѣчаемъ, что

$$P_n Q_{n-1} - Q_n P_{n-1} = (-1)^n,$$

$$T_m S_{m-1} - T_{m-1} S_m = (-1)^m,$$

слѣдовательно, число x эквивалентно съ полнымъ частнымъ x_n, и съ тѣмъ же числомъ x_n эквивалентно число y; значитъ, оба числа x и y эквивалентны между собой.

Попутно замѣтимъ еще, что *всякая непрерывная дробь эквивалентна съ каждымъ изъ ряда ея послѣдовательныхъ полныхъ частныхъ.*

§ 24. Нѣсколько труднѣе доказать предложеніе обратное, а именно, покажемъ, что разложенія 2-хъ произвольныхъ ирраціональныхъ эквивалентныхъ чиселъ въ непрерывныя дроби согласуются начиная съ нѣкотораго мѣста.

Возьмемъ 2 эквивалентныхъ числа x и y, связанныхъ равенствомъ

$$y = \frac{\alpha x + \beta}{\gamma x + \delta}, \tag{1}$$

гдѣ

$$\alpha\delta - \beta\gamma = \varepsilon.$$

Разложимъ число x въ непрерывную дробь

$$x = (a_0, a_1, a_2, \ldots, a_{n-1}, x_n),$$

гдѣ для сокращенія обозначено

$$x_n = (a_n, a_{n+1}, \ldots).$$

Въ этомъ разложеніи отрицательнымъ можетъ быть только одно 1-е число a_0, а всѣ остальныя положительны.

Итакъ,

$$x = \frac{P_n x_n + P_{n-1}}{Q_n x_n + Q_{n-1}}, \qquad (2)$$

гдѣ

$$P_n Q_{n-1} - Q_n P_{n-1} = (-1)^n.$$

Итакъ, мы получаемъ, что

$$y = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \begin{pmatrix} P_n, & P_{n-1} \\ Q_n, & Q_{n-1} \end{pmatrix} (x_n) = \frac{T_n x_n + T_{n-1}}{S_n x_n + S_{n-1}}, \qquad (*)$$

гдѣ

$$T_n = \alpha P_n + \beta Q_n, \; T_{n-1} = \alpha P_{n-1} + \beta Q_{n-1},$$

$$S_n = \gamma P_n + \delta Q_n, \; S_{n-1} = \gamma P_{n-1} + \delta Q_{n-1}.$$

Получаемъ, очевидно,

$$T_n S_{n-1} - S_n T_{n-1} = (-1)^n \varepsilon.$$

Разсмотримъ выраженіе S_n; его можно переписать на основаніи предыдущихъ формулъ такимъ образомъ

$$S_n = Q_n \left(\gamma \frac{P_n}{Q_n} + \delta \right).$$

При увеличеніи значка n дробь $\frac{P_n}{Q_n}$ имѣетъ своимъ предѣломъ ирраціональное число x, слѣдовательно,

$$\gamma \frac{P_n}{Q_n} + \delta$$

будетъ имѣть предѣломъ число

$$\gamma x + \delta, \qquad (4)$$

это же послѣднее число не можетъ равняться нулю, потому что x число ирраціональное.

Число (4) можно предполагать положительнымъ, потому что въ обратномъ случаѣ можно перемѣнить знаки у всѣхъ коэффиціентовъ: α, β, γ и δ.

Итакъ, мы видимъ, что число S_n при достаточно большомъ значеніи индекса n, будетъ имѣть знакъ плюсъ (+).

Кромѣ того, имѣя формулы

$$P_{n+1} = P_n a_n + P_{n-1}, \; Q_{n+1} = Q_n a_n + Q_{n-1}$$

и, умножая первую изъ нихъ на γ, вторую на δ и складывая, получимъ

$$S_{n+1} = S_n a_n + S_{n-1}.$$

Такъ какъ всѣ числа a_n — цѣлыя положительныя, то, начиная съ нѣкотораго n, всѣ S_n положительныя и возрастаютъ, и мы при достаточно большомъ n имѣемъ

$$S_n > S_{n-1} > 0. \tag{5}$$

Разложимъ раціональную дробь $\frac{T_n}{S_n}$ въ непрерывную; получимъ

$$\frac{T_n}{S_n} = (b_0, b_1, b_2, \ldots, b_{m-1}),$$

гдѣ всѣ b, кромѣ перваго, положительны (b_0 можетъ быть и отрицательнымъ).

Обозначимъ предпослѣднюю подходящую дробь черезъ $\frac{T'}{S'}$ и покажемъ, что

$$\frac{T'}{S'} = \frac{T_{n-1}}{S_{n-1}}.$$

Въ самомъ дѣлѣ, мы имѣемъ

$$T_n S' - T' S_n = (-1)^m. \tag{6}$$

Выборомъ числа m можно достигнуть того, что будетъ

$$(-1)^m = (-1)^n \epsilon.$$

Мы видимъ, слѣдовательно, что уравненіе (6) удовлетворяется слѣдующимъ рѣшеніемъ $S' = S_{n-1}$, $T' = T_{n-1}$.

Остается убѣдиться, что это рѣшеніе есть единственное.

На основаніи теоремы § 5 мы замѣчаемъ, что при достаточно большомъ числѣ n, т. е. при достаточно большомъ числѣ m, будемъ имѣть $S_n > S' > 0$, а тогда по теоремѣ § 14 мы замѣчаемъ, что для S' остается только единственное рѣшеніе $S' = S_{n-1}$ [смотри неравенство (5)].

Итакъ, составимъ слѣдующее ирраціональное число

$$(b_0, b_1, b_2, \ldots, b_{m-1}, x_n);$$

получимъ

$$(b_0, b_1, b_2, \ldots, b_{m-1}, x_n) = \frac{T_n x_n + T_{n-1}}{S_n x_n + S_{n-1}}; \tag{7}$$

но на основаніи формулы (*) мы замѣчаемъ, что послѣднее ирраціональное число есть не что иное, какъ y, т. е.

$$y = (b_0,\ b_1,\ b_2,\ \ldots,\ b_{m-1},\ x_n) =$$

$$= (b_0,\ b_1,\ b_2,\ \ldots,\ b_{m-1},\ a_n,\ a_{n+1},\ \ldots).$$

Итакъ, доказано, что два эквивалентныхъ ирраціональныхъ числа имѣютъ, начиная съ нѣкотораго мѣста, общее разложеніе въ непрерывную дробь.

ГЛАВА XI.

Основы теоріи бинарныхъ квадратичныхъ формъ.

§ 1. Начало ариѳметической теоріи бинарныхъ квадратичныхъ формъ, т. е. теоріи трехчленовъ вида

$$ax^2 + bxy + cy^2$$

было положено изученіемъ вопросовъ о представленіи цѣлыхъ чиселъ квадратичными формами. Характерной въ этомъ отношеніи является теорема Fermat'a, доказанная Euler'омъ [1]), о томъ, что *всякое простое число p вида $4n + 1$ представляется только однимъ способомъ въ видѣ суммы двухъ квадратовъ.*

Напримѣръ

$$5 = 1^2 + 2^2,\ 13 = 2^2 + 3^2,\ 17 = 4^2 + 1^2,\ 29 = 2^2 + 5^2,\ \ldots$$

Тутъ дѣло идетъ о представленіи простого числа p квадратичной формой $x^2 + y^2$, то есть, о рѣшеніи въ цѣлыхъ числахъ неопредѣленнаго уравненія

$$p = x^2 + y^2,$$

гдѣ p число простое, а x и y обыкновенныя цѣлыя числа.

§ 2. Euler и Lagrange дали рядъ теоремъ, аналогичныхъ приведенной.

Теорема. Всякое простое число слѣдующихъ двухъ формъ $8n + 1$ и $8n + 3$ раскладывается однимъ и только однимъ способомъ на сумму квадрата и удвоеннаго квадрата.

Напримѣръ, $41 = 3^2 + 2 \cdot 4^2$.

---

[1]) *Euler.* Demonstratio theorematis Fermatiani, omnem numerum primum formae $4n + 1$ esse summam duorum quadratorum. Comm. Arith. T. 1, p. 35.

Теорема. Всякое простое число вида $3n+1$ раскладывается только однимъ способомъ на сумму квадрата и тройного квадрата.

Напримѣръ, $31 = 2^2 + 3 \cdot 3^2$.

Не останавливаясь на подобныхъ теоремахъ, постараемся вкратцѣ резюмировать направленіе теоріи квадратичныхъ формъ въ XVIII столѣтіи. Тутъ приходится говорить главнымъ образомъ о дѣятельности Euler'a и Lagrange'a, которымъ и обязана наука основными понятіями въ разсматриваемой области.

Euler имѣлъ цѣлью приложеніе теоріи представленія чиселъ квадратичными формами главнымъ образомъ къ двумъ задачамъ капитальной важности: къ разложенію большихъ чиселъ на множители и къ рѣшенію неопредѣленныхъ уравненій въ цѣлыхъ числахъ.

Изслѣдованія Euler'a при всей ихъ важности касались немногихъ простѣйшихъ формъ. Они были обобщены Lagrange'омъ и приведены къ виду изящныхъ и важныхъ теорій, краткому изложенію которыхъ и будетъ посвящена настоящая глава.

§ 3. Прежде всего надо указать, что первое самое общее рѣшеніе въ цѣлыхъ числахъ, а также и въ числахъ раціональныхъ, неопредѣленнаго уравненія второй степени съ двумя неизвѣстными

$$\alpha x^2 + \beta xy + \gamma y^2 + \delta x + \varepsilon y + \zeta = 0$$

принадлежитъ Lagrange'у и изложено имъ въ 1769 году въ мемуарѣ „Sur la solution des problèmes indéterminés du second degré".

До Lagrange'a разсматривались уравненія частнаго вида, какъ, напримѣръ, извѣстное уравненіе

$$t^2 - Du^2 = 1,$$

предложенное Fermat'омъ и рѣшенное, по словамъ Euler'a, въ первый разъ Pell'емъ.

Euler занимался также общей задачей второй степени, и имъ были написаны три мемуара „De Solutione problematorum Diophantcorum per numeros integros 1732 — 33", „De resolutione formularum quadraticarum indeterminatarum per numeros integros 1762 — 63", „Resolutio aequationis $Ax^2 + 2Bxy + Cy^2 + 2Dx + 2Ey + F = 0$ per numeros tam rationales quam integros. 1773".

Не смотря на то, что эти три мемуара заслуживаютъ внимательнаго изученія, какъ все написанное этимъ великимъ человѣкомъ, однако они не заключаютъ полнаго рѣшенія вопроса. Третій мемуаръ Euler'a появился послѣ мемуара Lagrange'a, такъ что приходится предположить, что Euler не былъ знакомъ съ мемуаромъ послѣдняго.

§ 4. Вторая большая теорія Lagrange'a, относящаяся къ квадратичной области, состоитъ въ теоріи дѣлителей квадратичныхъ формъ. Эта теорія, развитая Legendre'омъ, состоитъ въ нахожденіи дѣлителей данной формы $x^2 + Ay^2$, причемъ эти дѣлители представляются формами вида $mz + \alpha$, гдѣ z произвольное цѣлое число или формулами вида $au^2 + 2buv + cv^2$, гдѣ u, v суть произвольныя взаимно простыя числа.

Для знакомства съ этой теоріей можно рекомендовать „Теорію сравненій“ Чебышева.

§ 5. Необходимо признать, что коронным бриліантомъ въ вѣнцѣ славы Lagrange'a является замѣченная имъ и подробно разобранная связь уравненія Pell'a съ періодическими непрерывными дробями.

§ 6. На рубежѣ XVIII и XIX столѣтій появилась въ 1801 году знаменитая книга Gauss'a „Disquisitiones arithmeticae“, въ которой дано новое изложеніе теоріи квадратичныхъ формъ. Это сочиненіе изобилуетъ замѣчательными по глубинѣ идеями и дало поводъ къ широкимъ обобщеніямъ, наложившимъ отпечатокъ на всю науку XIX столѣтія.

Эквивалентность формъ.

§ 7. Начнемъ со введеннаго Lagrange'омъ понятія объ *эквивалентности* квадратичныхъ формъ.

Будемъ форму $ax^2 + bxy + cy^2$ обозначать знакомъ

$$(a,\ b,\ c),$$

причемъ будемъ называть a первымъ коэффиціентомъ, b вторымъ и c третьимъ. Перемѣнную x будемъ называть первою, а y второю.

Во всемъ дальнѣйшемъ мы будемъ предполагать коэффиціенты a, b, c числами цѣлыми безъ общаго дѣлителя. Такія формы назовемъ примитивными.

Gauss пишетъ квадратичныя формы въ видѣ

$$ax^2 + 2bxy + cy^2,$$

такъ что если второй коэффиціентъ печетный, то надо предварительно умножить всю форму на 2. Лишь въ послѣднее время довольно вѣсскія основанія заставляютъ отказаться отъ обозначенія Gauss'a. Послѣ долгихъ колебаній и я въ моей педагогической дѣятельности рѣшилъ также отказаться отъ обозначенія Gauss, такъ что въ дальнѣйшемъ я всюду не буду писать двойки при коэффиціентѣ b.

Если мы перемѣннымъ x и y будемъ приписывать всевозможныя цѣлыя значенія отъ $-\infty$ до $+\infty$, то форма будетъ давать безчисленное множество цѣлыхъ значеній m

$$ax^2 + bxy + cy^2 = m .$$

Напримѣръ, форма $2x^2 + 3y^2$ будетъ давать числа

x	0,	1,	0,	2,	1,	0,	3,	2,	1,	0,	...
y	0,	0,	1,	0,	1,	2,	0,	1,	2,	3,	...
m	0,	2,	3,	8,	5,	12,	18,	11,	14.	27,	...

§ 8. Если надъ перемѣнными x и y произведено линейное преобразованіе вида

$$\left.\begin{aligned} x &= \alpha x_1 + \beta y_1 \\ y &= \gamma x_1 + \delta y_1 \end{aligned}\right| \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}, \qquad (1)$$

то форма (a, b, c) преобразуется въ такую новую

$$a_1 x_1^2 + b_1 x_1 y_1 + c_1 y_1^2$$

гдѣ

$$\begin{aligned} a_1 &= a\alpha^2 + b\alpha\gamma + c\gamma^2 \\ b_1 &= 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta \qquad (2) \\ c_1 &= a\beta^2 + b\beta\delta + c\delta^2 \end{aligned}$$

Если числа α, β, γ, δ цѣлыя, то цѣлымъ значеніямъ x_1, y_1 будутъ соотвѣтствовать также цѣлыя значенія x и y, слѣдовательно, значенія, которыя принимаетъ форма (a_1, b_1, c) при цѣлыхъ значеніяхъ x_1 и y_1 заключаются среди значеній формы (a, b, c). Говорятъ, что форма (a, b, c) *заключаетъ въ себѣ форму* (a_1, b_1, c).

Обозначимъ черезъ ε опредѣлитель преобразованія (1)

$$\varepsilon = \alpha\delta - \beta\gamma .$$

Если опредѣлитель ε есть $= 1$, то мы замѣчаемъ, что всякимъ цѣлымъ значеніямъ первоначальныхъ буквъ x, y соотвѣтствуютъ цѣлыя же значенія новыхъ буквъ x_1, y_1, такъ что обратно форма (a_1, b_1, c_1) будетъ заключать въ себѣ форму (a, b, c). Числа изображаемыя этими обѣими формами одни и тѣже.

Lagrange далъ такимъ двумъ формамъ названіе *эквивалентныхъ*

§ 9. Число

$$D = b^2 - 4ac$$

будемъ называть *опредѣлителемъ* формы.

Необходимо замѣтить, что опредѣлитель формы всегда удовлетворяетъ одному изъ двухъ сравненій

$$D \equiv 1 \pmod 4, \quad D \equiv 0 \pmod 4,$$

судя по тому будетъ ли число b нечетнымъ или четнымъ. Другими словами, D имѣетъ одинаковую четность съ b т. е. оба числа D, b сразу или нечетныя или четныя.

Нетрудно убѣдиться, что, если составимъ опредѣлитель $D_1 = b_1^2 - 4a_1c_1$ преобразованной формы, то на основаніи соотношеній (2) § 8 получимъ

$$D_1 = D(\alpha\delta - \beta\gamma)^2 = D\varepsilon^2$$

то есть приходимъ къ теоремѣ

Опредѣлитель преобразованной формы равенъ опредѣлителю первоначальной умноженному на квадратъ опредѣлителя преобразованія.

§ 10. Если формы эквивалентны, то $\varepsilon^2 = 1$ и, слѣдовательно, $D_1 = D$ т. е. *двѣ эквивалентныя формы имѣютъ одинъ и тотъ же опредѣлитель.*

Обратное заключеніе *несправедливо*, ибо формы могутъ имѣть одинъ и тотъ же опредѣлитель, но могутъ и не быть эквивалентными. Для того, чтобы формы съ общимъ опредѣлителемъ были эквивалентны, необходимо и достаточно, чтобы существовало по крайней мѣрѣ одно преобразованіе вида (1) § 8, у котораго $\alpha\delta - \beta\gamma = \pm 1$, переводящее одну форму въ другую.

§ 11. Слѣдуя Gauss'у, мы будемъ формы называть *proprie*-эквивалентными, если $\alpha\delta - \beta\gamma = +1$ и *improprie*-эквивалентными, если $\alpha\delta - \beta\gamma = -1$.

§ 12. Совокупность формъ даннаго опредѣлителя proprie-эквивалентныхъ между собой называется *классомъ* формъ.

Оказывается, что число различныхъ классовъ формъ даннаго опредѣлителя всегда конечное.

Положительныя формы.

§ 13. Разсмотримъ сначала формы (a, b, c), у которыхъ опредѣлитель *отрицательный* т. е. $D = -d$, гдѣ черезъ d обозначено натуральное число.

Нетрудно убѣдиться, что въ случаѣ отрицательнаго опредѣлителя крайніе коэффиціенты a и c будутъ одного знака, ибо

$$4ac = b^2 + d.$$

Кромѣ того, числа представляемыя формой всѣ того же знака что и крайніе коэффиціенты, ибо

$$4a(a, b, c) = (2ax + by)^2 + dy^2.$$

Очевидно, что *двѣ эквивалентныя формы должны имѣть крайніе коэффиціенты одного и того же знака,* ибо числа, представляемыя обѣими, одинаковы.

Не нарушая общности, мы можемъ ограничиться только разсмотрѣніемъ такъ называемыхъ *положительныхъ* формъ, которыя даютъ числа положительныя. *Отрицательныя* формы получатся черезъ умноженіе положительныхъ на -1.

§ 14. Будемъ положительную квадратичную форму называть приведенною, если будетъ

$$|b| \leqq a \leqq c; \tag{1}$$

какъ слѣдствіе этихъ неравенствъ получаемъ

$$d = 4ac - b^2 \geqslant 4a^2 - a^2$$
$$\geqslant 3a^2,$$

откуда

$$a \leqq \sqrt{\frac{d}{3}}. \tag{2}$$

Докажемъ теперь теорему, что *для всякой формы отрицательнаго опредѣлителя* $-d$ *можно подобрать по крайней мѣрѣ одну ей proprie-эквивалентную приведенную форму.*

§ 15. Не разсматривая значеній $x = 0$, $y = 0$, будемъ числа x и y предполагать *взаимно простыми,* ибо иначе можно было бы квадратъ ихъ общаго множителя вынести за скобки во всей формѣ.

Такимъ образомъ, если мы положимъ одну перемѣнную равной нулю, то другую надо положить равной 1, ибо можно сказать, что значенія $x = \delta$, $y = 0$ имѣютъ общаго дѣлителя δ.

Итакъ, давая всевозможныя указанныя значенія числамъ x и y, мы будемъ получать различныя значенія m формы.

Такъ какъ всѣ значенія цѣлыя положительныя числа не равныя нулю, то одно изъ нихъ a' будетъ наименьшее.

Можетъ случиться, что наименьшихъ будетъ нѣсколько.

Однимъ словомъ можно сказать, что всякое другое значеніе m формы будетъ удовлетворять неравенству $m \geqslant a'$.

Пусть наименьшее значеніе a' форма принимаетъ при $x = \alpha$, $y = \gamma$, т. е.

$$a' = a\alpha^2 + b\alpha\gamma + c\gamma^2.$$

Такъ какъ числа α, γ взаимно простыя, то можно подобрать два цѣлыхъ числа β и δ, чтобы было

$$\alpha\delta - \beta\gamma = 1.$$

Дѣлаемъ преобразованіе

$$x = \alpha x_1 + \beta y_1, \quad y = \gamma x_1 + \delta y_1,$$

тогда заданная форма (a, b, c) обращается въ такую

$$(a', b', c').$$

Здѣсь надо подчеркнуть ту важную теорему, что *для всякой формы* (a, b, c) *можно подобрать ей proprie-эквивалентную* (a', b', c'), *у которой одинъ изъ крайнихъ коэффиціентовъ будетъ любымъ значеніемъ первой формы.*

Въ данномъ случаѣ у насъ a' есть минимумъ формы.

Если $|b'| \leqslant a'$, то форма уже приведенная. Если же $|b'| > a'$, то дѣлаемъ преобразованіе

$$x = x_1 + \lambda y_1$$

$$y = \qquad y_1,$$

тогда форма (a', b', c') обращается въ такую (a', b_1, c_1), гдѣ

$$b_1 = b' + 2a'\lambda$$

$$c_1 = a'\lambda^2 + b'\lambda + c'.$$

Подбираемъ λ такъ, чтобы b_1 былъ абсолютно малый вычетъ числа b' по модулю $2a'$, то есть чтобы было $|b_1| \leqslant a'$; тогда форма (a', b_1, c_1) будетъ искомая приведенная. Въ самомъ дѣлѣ, не можетъ существовать неравенства $c_1 < a'$, ибо c_1, будучи значеніемъ формы $(x_1 = 0, y_1 = 1)$, не можетъ быть меньше минимума.

§ 16. Посмотримъ, не могутъ ли быть двѣ приведенныя формы proprie эквивалентны между собой.

Итакъ, пусть имѣются двѣ приведенныя proprie эквивалентныя формы (a, b, c), (a', b', c') отрицательнаго опредѣлителя $D = -d$. Обозначая черезъ $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ преобразованіе одной въ другую, получимъ

$$a' = a\alpha^2 + b\alpha\gamma + c\gamma^2 \tag{1}$$

$$b' = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta \tag{2}$$

$$\alpha\delta - \beta\gamma = 1. \tag{3}$$

Изъ равенства (1) слѣдуетъ $4aa' = (2a\alpha + b\gamma)^2 + d\gamma^2$. Такъ какъ коэффиціенты a, a', c, c' можно считать положительными, то на основаніи не-

равенства (2) § 14 мы будемъ имѣть $4aa' \leqq \frac{4}{3} d$ и, слѣдовательно, $\gamma^2 \leqq \frac{4}{3}$. Для γ получаются двѣ возможности I. $\gamma = 0$, II. $\gamma = \pm 1$.

I. $\gamma = 0$. Въ этомъ случаѣ мы получаемъ на основаніи (3) $\alpha = \pm 1$, $\delta = \pm 1$.

Въ обоихъ случаяхъ имѣемъ $a' = a$, $b' - b = \pm 2a\beta$, но $|b| \leqq a$, $|b'| \leqq a' = a$ получимъ $|b' - b| \leqq 2a$.

Итакъ, мы получаемъ одно изъ двухъ: или $b = b'$ и формы *тождественны*, или $b = -b' = \pm a$ въ этомъ случаѣ $c' = c$ и мы получаемъ двѣ эквивалентныя приведенныя формы (a, a, c), $(a, -a, c)$. Двѣ формы (a, b, c) и $(a, -b, c)$ отличающіяся знакомъ второго коэффиціента носятъ названіе *обратныхъ* (oppositae).

II. $\gamma = \pm 1$. Изъ уравненія (1) получимъ

$$a\alpha^2 + c - a' = \pm b\alpha,$$

но c не меньше a, съ другой стороны, не нарушая общности, можемъ предположить, что a' не больше a, ибо любую изъ формъ можно выбрать за первую. Слѣдовательно, c не меньше a' и мы получаемъ $|b\alpha| \geqslant a\alpha^2$. Отсюда, принимая во вниманіе $|b| \leqq a$ получимъ $|\alpha| \geqslant \alpha^2$. Это же возможно только при условіи: или $\alpha = 0$, или $\alpha = \pm 1$. Если $\alpha = 0$, то $a' = c$, но такъ какъ $a' \leqq a$, $a \leqq c$, то получимъ $a' = a = c$.

Изъ (3) имѣемъ $\beta\gamma = -1$, откуда на основаніи равенства (2) получаемъ $b + b' = \pm 2\delta c = \pm 2\delta a$. Итакъ мы получаемъ или $b = b' = \pm a$ и формы *тождественны*, или же $b = -b'$ и формы *обратныя*. Если $\alpha = \pm 1$, то уравненіе (1) даетъ $\pm b = a + c - a'$, но ни a ни c не меньше a', слѣдовательно, $|b| \geqslant a$, $|b| \geqslant c$. Сопоставляя послѣднія неравенства съ тѣми, которыя слѣдуютъ на основаніи приведенности формъ, т. е. съ неравенствами $|b| \leqq a$, $|b| \leqq c$ получаемъ $|b| = a = c$, кромѣ того изъ равенства $\pm b = a + c - a'$ получаемъ $|b| = a'$.

Равенство (2) даетъ $b' = 2a(\alpha\beta + \gamma\delta) + b(\alpha\delta + \beta\gamma)$.

На основаніи (3) и $|b| = a$ получимъ $b' - b = 2a(\alpha\beta + \gamma\delta \pm \beta\gamma)$ и получимъ, какъ раньше, или $b = b'$ и формы тождественны, или $b = -b'$, $|b| = a$ и формы обратныя.

Итакъ, сопоставляя все сказанное, можно высказать такую теорему:

Два единственныхъ случая, въ которыхъ не тождественныя приведенныя формы отрицательнаго опредѣлителя принадлежатъ къ одному классу, суть слѣдующія формы

$$(a, a, c) \text{ и } (a, b, a),$$

которыя переходятъ при помощи подстановокъ

$$\begin{pmatrix} 1, & -1 \\ 0, & 1 \end{pmatrix}, \quad \begin{pmatrix} 0, & -1 \\ 1, & 0 \end{pmatrix}$$

въ слѣдующія

$$(a, -a, c), \quad (a, -b, a).$$

§ 17. Прежде чѣмъ мы пойдемъ дальше, надо обратить вниманіе на весьма важное замѣчаніе Lejeune-Dirichlet, которое состоитъ въ томъ, что вмѣсто формы $ax^2 + bxy + cy^2$ разсматривается корень $\omega = \frac{x}{y}$ квадратнаго уравненія. которое получается отъ приравниванія нулю этой формы, т. е. уравненія

$$a\omega^2 + b\omega + c = 0.$$

Очевидно, что двѣ эквивалентныя формы имѣютъ корни эквивалентные въ смыслѣ данномъ въ предыдущей главѣ.

Особенно просто разсматривается геометрически вопросъ о *приведенныхъ квадратичныхъ ирраціональностяхъ* ω, которыя суть корни приведенныхъ формъ.

Мы имѣемъ

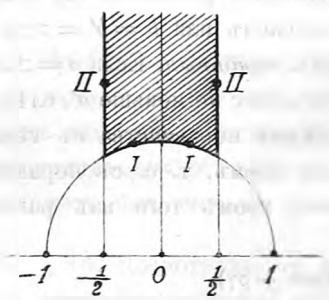
$$\omega = \frac{-b + i\sqrt{d}}{2a} = \xi + i\eta,$$

гдѣ вещественныя числа ξ и η выражаются такъ

$$\xi = -\frac{b}{2a}, \quad \eta = \frac{\sqrt{d}}{2a},$$

причемъ

$$\xi^2 + \eta^2 = \frac{b^2 + 4ac - b^2}{4a^2} = \frac{c}{a}.$$



Условія того, что форма есть приведенная, можно переписать въ такомъ видѣ

$$-\frac{1}{2} \leqslant \xi \leqslant \frac{1}{2}; \quad \xi^2 + \eta^2 \geqslant 1.$$

Приведенныя ирраціональности опредѣляются точками въ области плоскости, заштрихованной на чертежѣ.

Въ каждомъ классѣ формъ получается по одной приведенной формѣ за исключеніемъ двухъ случаевъ § 16, когда двѣ приведенныя формы эквивалентны между собой.

При теперешнихъ обозначеніяхъ мы получаемъ двѣ пары эквивалентныхъ приведенныхъ ирраціональностей

I. $\omega = \xi + i\eta$, $\omega_1 = -\xi + i\eta$ при условіи $\xi^2 + \eta^2 = 1$.

II. $\omega = -\frac{1}{2} + i\eta$, $\omega_1 = +\frac{1}{2} + i\eta$.

Эти исключительные случаи имѣютъ мѣсто на границѣ заштрихованной области.

§ 18. Найдемъ теперь число классовъ формъ даннаго опредѣлителя D. Для этой цѣли достаточно выписать и подсчитать всѣ неэквивалентныя между собой приведенныя формы.

Лучше всего сказанный подсчетъ произвести на численномъ примѣрѣ.

Возьмемъ $D = -163 \equiv 1 \pmod 4$. Основное условіе приведенности есть $|b| < \sqrt{\frac{163}{3}}$. Формула $4ac = b^2 + 163$ показываетъ, что b должно быть нечетнымъ числомъ.

Получаемъ слѣдующія возможныя значенія для b

$$-7, -5, -3, -1, +1, +3, +5, +7.$$

Достаточно взять положительныя значенія.

I. $b = 1$, $4ac = 1^2 + 163 = 4 \cdot 41$, $ac = 41$, $a = 1$, $c = 41$,

получается приведенная форма

$$(1, 1, 41).$$

II. $b = 3$, $4ac = 3^2 + 163 = 4 \cdot 43$, $ac = 43$, $a = 1$, $c = 43$;

нѣтъ приведенной формы,

III. $b = 5$, $4ac = 5^2 + 163 = 4 \cdot 47$, $ac = 47$, $a = 1$, $c = 47$,

нѣтъ приведенной формы.

IV. $b = 7$, $4ac = 7^2 + 163 = 4 \cdot 53$, $ac = 53$, $a = 1$, $c = 53$,

нѣтъ приведенной формы.

Продѣлывая тоже самое съ отрицательными значеніями b, получимъ окончательно двѣ приведенныя формы

$$(1, -1, 41), (1, 1, 41),$$

которыя подходятъ подъ исключительный случай § 16 и, значитъ, эквивалентны между собой. Итакъ, существуетъ только *одинъ классъ* у формъ опредѣлителя -163, то есть, всѣ формы этого опредѣлителя эквивалентны между собой.

§ 19. Случай квадратичныхъ ирраціональностей отрицательнаго опредѣлителя съ однимъ классомъ формъ играетъ извѣстную роль въ современной теоріи чиселъ, а потому скажемъ объ этомъ случаѣ нѣсколько словъ.

Пусть D есть отрицательный нечетный опредѣлитель, обладающій требуемымъ свойствомъ. Полагая $b=1$, получимъ $D=1-4p$. Очевидно, что число p должно быть простымъ, ибо, если $p=p_1p_2$, гдѣ $p_1\leqq p_2$, то существуютъ двѣ приведенныя формы

$$(1,\ 1,\ p_1p_2),\ (p_1,\ 1,\ p_2)$$

даннаго опредѣлителя, не эквивалентныя между собой, слѣдовательно, существуетъ болѣе одного класса формъ даннаго опредѣлителя.

Оказывается, что условіе простоты числа p не есть условіе достаточное.

До настоящаго времени извѣстны только слѣдующія значенія опредѣлителя съ однимъ классомъ формъ

$$p=1,\ 2,\ 3,\ 5,\ 11,\ 17,\ 41$$

$$d=3,\ 7,\ 11,\ 19,\ 43,\ 67,\ 163.$$

Frobenius [1]) заявляетъ, что другихъ значеній не существуетъ до 10000. Онъ приводитъ интересную теорему:

Если положительныя формы опредѣлителя $D=1-4p$ всѣ между собой эквивалентны, то каждое меньшее p^2 число, представляемое этими формами, есть простое.

Такъ, напримѣръ, форма $x^2-xy+41y^2$ при $y=-1$ обращается въ Euler'овское выраженіе x^2+x+41 (см. § 24 гл. I), дающее при $x=0, 1, \ldots 39$ слѣдующія простыя числа

41, 43, 47, 53, 61, 71, 83, 97, 113, 131,
151, 173, 197, 223, 251, 281, 313, 347, 383, 421,
461, 503, 547, 593, 641, 691, 743, 797, 853, 911,
971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523, 1601.

§ 20. Gauss далъ простой алгоритмъ для полученія по заданной формѣ эквивалентной приведенной.

Будемъ разсматривать слѣдующую proprie-эквивалентную подстановку $x=-y'$, $y=x'+by'$. Получаемъ новую форму $(a_1,\ b_1,\ c_1)$, гдѣ

$$a_1=c,\ b_1=-b+2cb,\ c_1=a-bb+cb^2. \qquad (1)$$

Такъ какъ опредѣлитель подстановки есть $+1$, то формы $(a,\ b,\ c)$ и $(a_1,\ b_1,\ c_1)$ proprie-эквивалентны и имѣютъ одинаковые опредѣлители.

---

[1]) *Frobenius.* Ueber quadratische Formen, die viele Primzahlen darstellen. Sitzungsberichte d. k. pr. Ak. d. W. 1912.

Кромѣ того, послѣдній коэффиціентъ первой формы равенъ первому коэффиціенту второй, средніе же коэффиціенты этихъ двухъ формъ удовлетворяютъ сравненію $b + b_1 \equiv 0 \pmod{2c}$.

§ 21. Мы назовемъ *formae contiguae* двѣ формы (a, b, c) и (a_1, b_1, c_1), когда эти формы имѣютъ общій опредѣлитель и кромѣ того

$$c = a_1, \; b + b_1 \equiv 0 \pmod{2c}.$$

Кромѣ того, мы будемъ говорить, что первая форма относительно второй есть *contigua a parte prima*, а вторая относительно первой есть *contigua a parte ultima*.

Такъ, напримѣръ, форма (7, 6, 2) contigua a parte ultima съ формой (3, 8, 7).

Теорема. Формы contiguae всегда proprie-эквивалентны.

Въ самомъ дѣлѣ, первая изъ нихъ переходитъ въ другую при помощи подстановки.

$$x = -y', \; y = x' + \frac{b + b_1}{2c} y'.$$

§ 22. *Формы* (a, b, c) *и* (a_1, b_1, c_1) *будутъ proprie эквивалентны, если*

$$a = a_1, \; b \equiv b_1 \pmod{2a}.$$

Въ самомъ дѣлѣ (a, b, c) proprie-эквивалентна съ формой $(c, -b, a)$, ибо первая переходитъ во вторую при помощи подстановки $x = -y', \; y = x'$; форма же $(c, -b, a)$ contigua a parte prima съ формой (a_1, b_1, c_1).

Подобныя формы (a, b, c) и (a_1, b_1, c_1) мы будемъ называть *параллельными*. Очевидно, что всѣ параллельныя формы получаются изъ одной при помощи подстановки

$$\begin{pmatrix} 1, & k \\ 0, & 1 \end{pmatrix}.$$

§ 23. Нетрудно убѣдиться, что, если мы будемъ составлять для заданной формы (a, b, a') рядъ формъ

$$(a', b', a''), \; (a'' \; b'' \; a'''), \; \ldots,$$

изъ которыхъ каждая есть contigua a parte prima со слѣдующей, причемъ коэффиціенты $b', b'', b''', \ldots$ опредѣляются такъ:

b' абсолютно малый вычетъ числа $-b$ по модулю $2a'$
b'' „ „ „ „ $-b'$ „ „ $2a''$
b''' „ „ „ „ $-b''$ „ „ $2a'''$
. . . . . ;

то послѣ извѣстнаго числа преобразованій дойдемъ до приведенной формы.

Въ самомъ дѣлѣ, такъ какъ абсолютная величина абсолютно малаго вычета не превосходитъ половины модуля, то

$$|b'| \leqq a', \ |b''| \leqq a'', \ |b'''| \leqq a''', \ \ldots$$

Остается показать, что мы непремѣнно придемъ къ такой формѣ

$$(a^{(n)}, \ b^{(n)}, \ a^{(n+1)}),$$

у которой третій коэффиціентъ $a^{(n+1)}$ не меньше перваго $a^{(n)}$. Такая форма будетъ приведенною.

Въ самомъ дѣлѣ, нельзя допустить, чтобы рядъ чиселъ a', a'', a''', ... постоянно убывалъ, ибо существуетъ только конечное число чиселъ меньшихъ a'. Итакъ, примѣняя процессъ составленія формъ contiguarum a parte ultima, мы придемъ окончательно къ приведенной формѣ proprie-эквивалентной съ данной.

При переходѣ отъ каждой формы къ слѣдующей мы пользуемся подстановкой

$$\begin{pmatrix} 0, & -1 \\ 1, & \delta \end{pmatrix},$$

гдѣ δ опредѣляется по формуламъ (1) § 20, слѣдовательно, сопоставляя всѣ эти преобразованія, получимъ окончательную подстановку, приводящую форму въ приведенную.

§ 24. Требуется найдти приведенную форму эквивалентную съ данной

$$(2953, \ 1601, \ 217)$$

опредѣлителя $D = -3$.

Получаемъ рядъ contiguarum a parte ultima

$$(2953, \ 1601, \ 217), \ (217, \ 135, \ 21), \ (21, \ -9, \ 1) \ (1, \ 1, \ 1).$$

Подстановка, переводящая заданную форму въ окончательную, получится отъ перемноженія подстановокъ

$$\begin{pmatrix} 0, & -1 \\ 1, & 4 \end{pmatrix} \begin{pmatrix} 0, & -1 \\ 1, & 3 \end{pmatrix} \begin{pmatrix} 0, & -1 \\ 1, & -4 \end{pmatrix} = \begin{pmatrix} -3, & 13 \\ 11, & -48 \end{pmatrix}.$$

Подобнымъ же образомъ для формы

$$(304, \ 434, \ 155) \qquad (1)$$

получаемъ слѣдующій рядъ формъ

$$(155, \ -124, \ 25), \ (25, \ 24, \ 7), \ (7, \ 4, \ 5), \ (5, \ -4, \ 7), \qquad (2)$$

изъ которыхъ послѣдняя приведенная.

§ 25. Теперь мы въ состояніи рѣшить задачу о представленіи даннаго числа m данной квадратичной формой (a, b, c), то есть, о рѣшеніи въ цѣлыхъ числахъ x, y неопредѣленнаго уравненія

$$ax^2 + bxy + cy^2 = m. \qquad (1)$$

Во всемъ дальнѣйшемъ мы будемъ разсматривать такія представленія чиселъ m формами, когда x и y не имѣютъ общаго дѣлителя.

Предположимъ, что найдена одна пара чиселъ x и y удовлетворяющихъ уравненію (1). По этимъ взаимно простымъ числамъ x и y находимъ два новыхъ ξ и η такихъ, чтобы было $x\eta - y\xi = 1$. Если мы будемъ форму (a, b, c) преобразовывать при помощи подстановки

$$\begin{pmatrix} x, & \xi \\ y, & \eta \end{pmatrix},$$

то мы получимъ новую форму, въ которой на основаніи формулъ (2) § 8 первый коэффиціентъ будетъ не чѣмъ инымъ, какъ заданнымъ числомъ m.

Новая форма будетъ имѣть видъ

$$(m, n, l),$$

гдѣ

$$m = ax^2 + bxy + cy^2$$

$$n = 2ax\xi + b(x\eta + \xi y) + 2cy\eta$$

$$l = a\xi^2 + b\xi\eta + c\eta^2.$$

На основаніи равенства опредѣлителей двухъ формъ получаемъ

$$n^2 - 4ml = D,$$

откуда

$$n^2 \equiv D \pmod{4m}.$$

Теорема. Представить заданной формой можно только такое число m, при которомъ опредѣлитель D есть квадратный вычетъ числа $4m$,

§ 26. Итакъ, предположимъ, что мы желаемъ представить число m формой (a, b, c). Не трудно найти форму (m, n, l), имѣющую съ данной (a, b, c) общій опредѣлитель и у которой первый коэффиціентъ есть число m. Въ самомъ дѣлѣ, если условіе послѣдней теоремы § 25 выполняется, то можно рѣшить квадратное сравненіе

$$x^2 \equiv D \pmod{4m}. \qquad (1)$$

Ищемъ всѣ его рѣшенія. Возьмемъ одно изъ этихъ рѣшеній n. Раздѣляя число $n^2 - D$ на $4m$, получимъ третій коэффиціентъ l формы, и за-

дача сводится къ нахожденію эквивалентной поостановки

$$\begin{pmatrix} x, & \xi \\ y, & \eta \end{pmatrix},$$

переводящей форму (a, b, c) въ форму (m, n, l).

§ 27. Мы оставимъ пока въ сторонѣ задачу нахожденія всѣхъ подстановокъ переводящихъ форму (a, b, c) въ другую (m, n, l) и разсмотримъ задачу нахожденія по крайней мѣрѣ одной такой подстановки.

При помощи вышеуказанныхъ правилъ ищемъ для каждой изъ двухъ формъ приведенныя. Если мы замѣтимъ, что полученныя двѣ приведенныя формы не эквивалентны, то подстановка не существуетъ и наша задача представленія числа формой невозможна при выбранномъ корнѣ n квадратнаго сравненія (1) § 26. Если при всѣхъ корняхъ сравненія (1) § 26 получается отрицательный отвѣтъ, то задача представленія числа формой невозможна. Если же обѣ приведенныя формы совпадаютъ, то мы переходимъ по нашей цѣпи подстановокъ сначала отъ (a, b, c) къ общей приведенной, а потомъ отъ этой послѣдней при помощи обратной цѣпи подстановокъ къ формѣ (m, n, l).

Пусть требуется, напримѣръ, представить число 80 при помощи формы

$$(304, 434, 155).$$

Рѣшаемъ сначала сравненіе (1) § 26

$$x^2 \equiv -124 \pmod{320}.$$

Получаемъ одинъ изъ его корней $x = -46$ и соотвѣтствующую форму

$$(80, -46, 7), \qquad (1)$$

для которой слѣдующая форма contigua a parte ultima будетъ

$$(7, 4, 5). \qquad (2)$$

Далѣе идти не надо, ибо эта форма встрѣчается уже въ цѣпи формъ (2) § 24.

Отъ формы (1) мы переходимъ къ формѣ (2) при помощи подстановки $\begin{pmatrix} 0, & -1 \\ 1, & -3 \end{pmatrix}$, обратная для которой будетъ $\begin{pmatrix} -3, & 1 \\ -1, & 0 \end{pmatrix}$. Сравнивая съ § 24, получаемъ рядъ эквивалентныхъ формъ

$$(304, 434, 115), (155, -124, 25), (25, 24, 7),$$

$$(7, 4, 5), (80, -46, 7).$$

Соотвѣтственныя подстановки

$$\begin{pmatrix}0, & -1\\ 1, & 1\end{pmatrix}\begin{pmatrix}0, & -1\\ 1, & -2\end{pmatrix}\begin{pmatrix}0, & -1\\ 1, & 2\end{pmatrix}\begin{pmatrix}-3, & +1\\ -1, & 0\end{pmatrix}$$

въ произведеніи даютъ

$$\begin{pmatrix}-11, & 2\\ 16, & -3\end{pmatrix},$$

откуда получаемъ искомое представленіе числа 80

$$80 = 304 . (-11)^2 + 434 . (-11) . 16 + 155 . 16^2.$$

Формы неопредѣленныя.

§ 28. Теперь перейдемъ къ гораздо болѣе трудной теоріи квадратичныхъ формъ *положительнаго опредѣлителя.*

Если число m выражается формой (a, b, c), гдѣ $D = b^2 - 4ac > 0$, то имѣемъ

$$4am = (2ax + by)^2 - Dy^2.$$

При $y = 0$, а x отличномъ отъ нуля мы имѣемъ $4am > 0$. Если же положимъ $x = -b$, $y = 2a$, то будемъ имѣть $4am < 0$. Другими словами, формы положительнаго опредѣлителя могутъ давать числа обоихъ знаковъ, поэтому такія формы носятъ названіе *неопредѣленныхъ* въ отличіе отъ формъ отрицательнаго опредѣлителя, дающихъ числа съ однимъ опредѣленнымъ знакомъ и называемыхъ поэтому *опредѣленными.*

Формъ съ опредѣлителемъ *равнымъ нулю* мы не будемъ разсматривать.

§ 29. Для упрощенія теоріи будемъ, по примѣру Lejeune-Dirichlet, разсматривать не формы, а ихъ ирраціональные корни ω

$$a\omega^2 + b\omega + c = 0 .$$

Если мы въ ирраціональномъ корнѣ $\omega = \dfrac{-b + \sqrt{D}}{2a}$ измѣнимъ знакъ у радикала $\sqrt{D}$, то получимъ другой корень ω' того же уравненія (1). Этотъ другой корень ω' мы будемъ называть *величиною сопряженною* относительно ирраціональности ω.

Вещественную квадратичную ирраціональность ω будемъ называть приведенною, если она есть положительное число большее единицы, а сопряженная съ нею ирраціональность отрицательная правильная дробь, то есть, если существуютъ неравенства

$$-1 < \omega' < 0 , \quad 1 < \omega .$$

Форму, корнемъ которой является такое приведенное число, мы будемъ называть также *приведенною*.

§ 30. Будемъ раскладывать въ непрерывную дробь какую нибудь вещественную квадратичную ирраціональность. Получимъ безконечную непрерывную дробь

$$\omega = (a_0, a_1, a_2, \ldots a_{n-1}, \omega_n),$$

гдѣ полное частное ω_n есть, очевидно, квадратичная ирраціональность эквивалентная числу ω.

Если число ω отрицательное, то a_0 будетъ отрицальное цѣлое число, а всѣ остальныя неполныя частныя отличныя отъ нуля положительныя цѣлыя числа.

Покажемъ, что, продолжая достаточно далеко разложеніе, мы придемъ къ такому числу ω_n, которое вмѣстѣ со всѣми слѣдующими будетъ приведеннымъ.

Въ самомъ дѣлѣ, мы имѣемъ

$$\omega = \frac{P_n\omega_n + P_{n-1}}{Q_n\omega_n + Q_{n-1}}. \tag{1}$$

Первое свойство, быть числомъ положительнымъ и большимъ единицы, величина ω_n получаетъ уже начиная съ $n = 1$. Докажемъ теперь, что при достаточно большомъ значеніи числа n будутъ имѣть мѣсто слѣдующія неравенства

$$\omega_n' < 0, \quad \omega_n' + 1 > 0,$$

гдѣ подъ ω_n' мы разумѣемъ величину, сопряженную съ ω_n.

Рѣшимъ уравненіе (1) относительно ω_n

$$\omega_n = \frac{Q_{n-1}\omega - P_{n-1}}{-Q_n\omega + P_n} = -\frac{Q_{n-1}}{Q_n} \cdot \frac{\omega - \frac{P_{n-1}}{Q_{n-1}}}{\omega - \frac{P_n}{Q_n}}. \tag{2}$$

Измѣнимъ знакъ квадратнаго радикала на обратный, тогда ирраціональныя числа замѣнятся сопряженными и мы получимъ

$$\omega_n' = -\frac{Q_{n-1}}{Q_n} \cdot \frac{\omega' - \frac{P_{n-1}}{Q_{n-1}}}{\omega' - \frac{P_n}{Q_n}}. \tag{3}$$

Что касается числителя и знаменателя послѣдней дроби

$$\omega' - \frac{P_{n-1}}{Q_{n-1}}, \quad \omega' - \frac{P_n}{Q_n},$$

то эти два выраженія стремятся при возрастаніи n къ одному и тому же предѣлу $\omega' - \omega$, отличному отъ нуля; слѣдовательно, при достаточно большомъ значеніи n числитель и знаменатель дроби (3) получаютъ знакъ числа $\omega' - \omega$, значитъ, величина ω_n' при достаточно большомъ числѣ n дѣляется отрицательной.

Остается теперь показать, что при достаточно большомъ значеніи n будетъ имѣть мѣсто неравенство $\omega' + 1 > 0$.

Въ самомъ дѣлѣ, замѣняя въ равенствѣ (2) D на $-D$, получимъ

$$\omega_n' = \frac{Q_{n-1}\omega' - P_{n-1}}{-Q_n\omega' + P_n} = -\frac{Q_{n-1}}{Q_n} - \frac{(-1)^n}{Q_n(Q_n\omega' - P_n)}$$

и, наконецъ,

$$\omega_n' + 1 = \frac{1}{Q_n}\left\{Q_n - Q_{n-1} - \frac{(-1)^n}{Q_n\omega' - P_n}\right\}.$$

Разность $Q_n - Q_{n-1}$ есть положительное цѣлое число, другая же дробь при достаточно большомъ значеніи n будетъ правильная и, значитъ, будетъ положительнымъ число $\omega_n' + 1$.

Итакъ, мы дѣйствительно убѣждаемся, что, начиная съ нѣкотораго значенія n и для всѣхъ слѣдующихъ, числа ω_n будутъ приведенныя.

§ 31. Относительно приведенныхъ квадратичныхъ ирраціональностей можно указать нѣсколько важныхъ предложеній.

Теорема I. Если число ω приведенное, то будетъ приведеннымъ также число $-\frac{1}{\omega}$.

Въ самомъ дѣлѣ, ω' число отрицательное и по абсолютной величинѣ меньше единицы, слѣдовательно, число $-\frac{1}{\omega'}$ положительное и больше единицы; тогда какъ сопряженное $-\frac{1}{\omega}$ будетъ отрицательнымъ и меньшимъ единицы по абсолютной величинѣ.

Теорема II. Если мы обозначимъ черезъ α наибольшее цѣлое число, заключающееся въ приведенной квадратичной ирраціональности ω и напишемъ равенство

$$\omega = \alpha + \frac{1}{\omega_1},$$

то ирраціональность ω_1 будетъ также приведенная.

Въ самомъ дѣлѣ, α есть наибольшее цѣлое число въ ω, слѣдовательно, $\frac{1}{\omega_1}$ есть правильная положительная дробь, значитъ $\omega_1 > 1$. Далѣе

$\omega_1 = \frac{1}{\omega - \alpha}$, слѣдовательно, сопряженная величина ω_1' выразится формулой $\omega_1' = \frac{1}{\omega' - \alpha}$, но ω' есть число отрицательное, поэтому ω_1' будетъ число отрицательное, меньшее по абсолютной величинѣ единицы, ибо численная величина знаменателя $\omega' - \alpha$ больше α ($\alpha > 0$, ибо ω число приведенное). Итакъ, ω_1 есть приведенное число.

Теорема III. Если въ равенствѣ $\omega = \alpha + \frac{1}{\omega_1}$ *оба числа* ω *и* ω_1 *приведенныя, то число* α *должно быть непремѣнно цѣлой частью числа* ω.

Въ самомъ дѣлѣ, если $\alpha > \omega$, то ω_1 число отрицательное и не можетъ быть приведеннымъ. Если же $\alpha + 1 < \omega$, то, подставляя въ это неравенство вмѣсто ω его величину, получимъ $\alpha + 1 < \alpha + \frac{1}{\omega_1}$, откуда $1 < \frac{1}{\omega_1}$ и, значитъ, $\omega_1 < 1$, что невозможно.

Теорема IV. Если въ равенствѣ $\omega = \alpha + \frac{1}{\omega_1}$ *оба числа* ω *и* ω_1 *приведенныя, то они другъ друга вполнѣ опредѣляютъ.*

Въ самомъ дѣлѣ, если дано число ω, то α должно быть цѣлой его частью и ω_1 будетъ первымъ полнымъ частнымъ, такъ что число ω_1 будетъ вполнѣ опредѣлено.

Покажемъ теперь, что съ другой стороны и число ω_1 опредѣляетъ вполнѣ число ω.

Перепишемъ наше равенство въ такомъ видѣ

$$-\frac{1}{\omega_1'} = \alpha + \frac{1}{\left(-\frac{1}{\omega'}\right)}.$$

Если числа ω и ω_1 приведенныя, то таковыми же будутъ и числа $-\frac{1}{\omega_1'}$, $-\frac{1}{\omega'}$, слѣдовательно, α окажется цѣлою частью числа $-\frac{1}{\omega_1'}$. Если же задано ω_1, то задано и число $-\frac{1}{\omega_1'}$. Такимъ образомъ по нашему послѣднему равенству получается опредѣленное значеніе для числа $-\frac{1}{\omega'}$, а, значитъ, и для числа ω.

§ 32. Та часть разложенія въ непрерывную дробь всякой квадратичной ирраціональности, въ которой числа ω приведенныя, обладаетъ такимъ свойствомъ, что каждое число ω_n опредѣляетъ всю эту часть разложенія, т. е. какъ слѣдующія ω_n, такъ и предыдущія.

§ 33. Покажемъ теперь, что приведенныхъ ирраціональностей конечное число.

Будемъ въ уравненіи

$$a\omega^2 + b\omega + c = 0 \qquad (1)$$

считать коэффиціентъ b числомъ положительнымъ.

На основаніи неравенствъ, опредѣляющихъ приведенную ирраціональность, оба корня уравненія (1) должны быть разныхъ знаковъ и, слѣдовательно, должны быть разныхъ знаковъ два коэффиціента a и c. Отсюда

$$D = b^2 - 4ac > b^2 .$$

Или, обозначая черезъ $\sqrt{D}$ ариѳметическій корень, получимъ

$$0 < b < \sqrt{D} .$$

Отсюда неравенства $|\omega| > 1$, $|\omega'| < 1$ даютъ

$$\left|\frac{-b-\sqrt{D}}{2a}\right| > 1 , \quad \left|\frac{-b+\sqrt{D}}{2a}\right| < 1 ,$$

то есть,

$$0 < \frac{\sqrt{D}-b}{|2a|} < 1 < \frac{\sqrt{D}+b}{|2a|}$$

или

$$0 < \sqrt{D} - b < |2a| < \sqrt{D} + b . \qquad (1)$$

Будемъ форму (a, b, c) положительнаго опредѣлителя называть *приведенною*, если ея коэффиціенты удовлетворяютъ неравенству (1).

Такое опредѣленіе приведенности формы шире чѣмъ данное раньше опредѣленіе приведенности числа, ибо для приведенности числа мы требовали не неравенства $|\omega| > 1$, $|\omega'| < 1$, а болѣе опредѣленныя неравенства $\omega > 1$, $-1 < \omega' < 0$. Во всякомъ случаѣ, всякая приведенная ирраціональность будетъ корнемъ приведенной формы и, если мы докажемъ конечность числа приведенныхъ формъ, то тѣмъ самымъ получимъ конечность числа приведенныхъ ирраціональностей.

Замѣтимъ, что неравенства (1) для коэффиціента a влекутъ за собою какъ слѣдствіе подобныя же неравенства для коэффиціента c, то есть

$$0 < \sqrt{D} - b < |2c| < \sqrt{D} + b . \qquad (3)$$

Въ самомъ дѣлѣ, мы имѣемъ тождество

$$\frac{\sqrt{D}-b}{2a} = \frac{-4ac}{\sqrt{D}+b} \cdot \frac{1}{2a} = \frac{-2c}{\sqrt{D}+b} ,$$

откуда

$$\frac{\sqrt{D}-b}{|2a|}=\frac{|2c|}{\sqrt{D}+b},\quad \frac{\sqrt{D}+b}{|2a|}=\frac{|2c|}{\sqrt{D}-b};$$

изъ послѣднихъ формулъ ясно, что неравенства (2) имѣютъ своими слѣдствіями неравенства (3) и обратно.

Обозначая $\lambda=\left[\sqrt{D}\right]$, получаемъ для b единственно возможныя значенія

$$b=1,\ 2,\ 3,\ \ldots\ \lambda \qquad (4)$$

съ тѣмъ однако ограниченіемъ, что при четномъ опредѣлителѣ D необходимо для b брать только четныя числа, а при нечетномъ D только нечетныя.

Коэффиціенты a и c получаются по формулѣ

$$\frac{D-b^2}{4}=|a|.|c|,$$

причемъ на основаніи (2) будемъ имѣть

$$\frac{\lambda-b+1}{2}\leqslant|a|\leqslant\frac{\lambda+b}{2}. \qquad (5)$$

Коэффиціентъ c удовлетворяетъ тѣмъ же неравенствамъ.

Получается конечное число возможныхъ случаевъ, ибо, во первыхъ, для b существуетъ конечное число (4) значеній, во вторыхъ, получается для всякаго b конечное число разложеній $\frac{D-b^2}{4}$ на два множителя. Изъ этихъ множителей годятся только такіе, которые удовлетворяютъ неравенствамъ (5) и, наконецъ, надо откинуть тѣ, при которыхъ a, b, c имѣютъ общаго дѣлителя.

Возьмемъ, напримѣръ, опредѣлитель $D=173$.

$\lambda=\left[\sqrt{173}\right]=13$

$b=1,\ 3,\ 5,\ 7,\ 9,\ 11,\ 13.$

Будемъ вычислять выраженіе $\frac{D-b^2}{4}$; получимъ таблицу

b	$\frac{D-b^2}{4}$
1	$43=1.43$
3	$41=1.41$
5	$37=1.37$
7	$31=1.31$
9	$23=1.23$
11	$13=1.13$
13	$1=1.1$

Такъ какъ должны удовлетворяться неравенства (5), то оказывается возможнымъ только послѣдній случай $b = 13$. Мы получаемъ только двѣ приведенныя формы

$$(1, 13, -1), (-1, 13, 1).$$

§ 34. Приведемъ здѣсь кстати двѣ теоремы Frobenius'a изъ цитированной выше статьи. Предположимъ, что обстоятельство, встрѣтившееся въ примѣрѣ предыдущаго параграфа, имѣетъ мѣсто, то есть, $\frac{1}{4}(D - z^2)$ число простое при всѣхъ нечетныхъ положительныхъ $z < \sqrt{D}$.

Тогда будутъ имѣть мѣсто слѣдующія теоремы:

Теорема I. Если $D = p^2 + 1$, *то всякое число абсолютно меньшее чѣмъ* $(2p - 3)$, *опредѣляемое формой* $(1, p, -1)$, *есть простое, если только не дѣлится на* p.

Удовлетворяютъ условіямъ теоремы числа

$$p = 3, 5, 7, 13, 17.$$

Теорема II. Если $D = p(p + 4)$, *то всякое число абсолютно меньшее чѣмъ* $(2p - 1)^2$, *опредѣляемое формой* $(1, p, -p)$ *есть простое, если только не дѣлится на* p *и на* $p + 4$.

Удовлетворяютъ условіямъ теоремы числа

$$p = 1, 3, 7, 19.$$

Frobenius'y не удалось найти для $D < 10000$ другихъ значеній, удовлетворяющихъ требованіямъ двухъ этихъ теоремъ.

§ 35. Въ § 33 показано, что существуетъ конечное число приведенныхъ неопредѣленныхъ формъ даннаго положительнаго опредѣлителя D. Отсюда вытекаетъ, что существуетъ конечное число приведенныхъ ирраціональностей, которыя являются корнями приведенныхъ формъ.

Предположимъ, что выписаны всѣ приведенныя ирраціональности даннаго опредѣлителя.

Будемъ которую нибудь изъ нихъ ω_1 раскладывать въ непрерывную дробь. Послѣдовательныя полныя частныя $\omega_2, \omega_3, \omega_4, \ldots$ будутъ также приведенными числами.

Такъ какъ разложеніе ирраціональнаго числа безконечное, а приведенныхъ ирраціональностей конечное число, то отсюда вытекаетъ, что по

крайней мѣрѣ одно изъ полныхъ частныхъ должно повториться при дальнѣйшемъ разложеніи и непрерывная дробь оказывается періодическою, ибо за повторившимся полнымъ частнымъ ω_k должно слѣдовать повтореніе слѣдующаго ω_{k+1}; а такъ какъ и предыдущее полное частное ω_{k-1} на основаніи IV § 31 должно повториться, то, слѣдовательно, должно повториться и первое полное частное ω_1, т. е. само раскладываемое въ дробь число.

Всякое приведенное квадратичное число раскладывается въ чистую періодическую непрерывную дробь.

§ 36. Изъ всего предыдущаго вытекаетъ какъ слѣдствіе знаменитая теорема Lagrange'a.

Всякая квадратичная ирраціональность, т. е. вещественный, ирраціональный корень квадратнаго уравненія съ цѣлыми коэффиціентами раскладывается въ періодическую непрерывную дробь.

Неприведенная ирраціональность раскладывается въ *смѣшанную* періодическую дробь, причемъ періодъ начнется съ того мѣста, съ котораго полныя частныя дѣлаются приведенными.

Примѣромъ такого разложенія неприведенной ирраціональности является, извѣстное изъ элементарнаго курса алгебры, разложеніе корня квадратнаго изъ цѣлаго числа.

Покажемъ, что ирраціональность $\omega = \sqrt{D}$ есть квадратичная опредѣлителя $4D$. Мы предполагаемъ, конечно, что D не есть квадратъ цѣлаго числа. Въ самомъ дѣлѣ ω есть корень квадратичной формы $x^2 - Dy^2$, опредѣлитель которой есть $4D$.

Ирраціональность ω не приведенная, ибо другой корень формы

$$\omega' = -\sqrt{D} < -1.$$

Начнемъ разложеніе ω въ непрерывную дробь

$$\omega = \alpha_0 + \frac{1}{\omega_1}.$$

Ирраціональность ω_1 будетъ уже приведенною, ибо $\omega_1 > 1$, а

$$\omega'_1 = \frac{1}{\omega' - \alpha_0} = \frac{1}{-\sqrt{D} - \alpha_0},$$

послѣдняя же величина есть отрицательная правильная дробь. Итакъ, періодъ начинается уже со второго звена.

Для примѣра разложимъ въ непрерывную дробь $\sqrt{14}$.

$$\sqrt{14} = 3 + \frac{1}{\omega_1},\quad \omega_1 = \frac{1}{\sqrt{14}-3} = \frac{\sqrt{14}+3}{5} = 1 + \frac{1}{\omega_2}$$

$$\omega_2 = \frac{5}{\sqrt{14}-2} = \frac{\sqrt{14}+2}{2} = 2 + \frac{1}{\omega_3}$$

$$\omega_3 = \frac{2}{\sqrt{14}-2} = \frac{\sqrt{14}+2}{5} = 1 + \frac{1}{\omega_4}$$

$$\omega_4 = \frac{5}{\sqrt{14}-3} = \frac{\sqrt{14}+3}{1} = 6 + \frac{1}{\omega_1}.$$

Если мы введемъ знакъ смѣшанной періодической дроби

$$\alpha_0, \alpha_1, \ldots \alpha_{k-1}(\alpha_k, \alpha_{k+1}, \ldots \alpha_l),$$

гдѣ $\alpha_0, \alpha_1, \ldots \alpha_{k-1}$ обозначаетъ часть дроби до періода, а $\alpha_k, \alpha_{k+1}, \ldots \alpha_l$ періодъ, то можемъ написать въ нашемъ примѣрѣ

$$\sqrt{14} = 3, (1, 2, 1, 6).$$

Въ концѣ книги дана таблица разложеній въ непрерывную дробь для всѣхъ чиселъ D до 100.

§ 37. Въ § 35 мы видѣли, что всякое приведенное число ω_1 приводитъ къ періоду

$$[\omega_1, \omega_2, \omega_3, \ldots \omega_v] \qquad (1)$$

также приведенныхъ чиселъ. Если такимъ образомъ будутъ исчерпаны всѣ приведенныя числа даннаго опредѣлителя, то говорятъ, что въ этомъ случаѣ всѣ приведенныя числа образуютъ одинъ періодъ.

Если же кромѣ чиселъ (1) существуетъ по крайней мѣрѣ одно новое приведенное число ω_1', то, раскладывая его въ непрерывную дробь, получимъ новый періодъ

$$[\omega_1', \omega_2', \omega_3', \ldots \omega_\mu'].$$

Продолжая разсужденіе далѣе, мы расположимъ всѣ приведенныя числа въ конечное число періодовъ.

§ 38. *Теорема. Всѣ числа періода эквиваленты между собой и обратно, два эквивалентныхъ между собой приведенныхъ числа даннаго опредѣлителя не могутъ попасть въ разные періоды, и должны заключаться въ одномъ изъ нихъ.*

Первая часть этого предложенія очевидна на основаніи эквивалентности непрерывной дроби со всѣми ея полными частными. Что же касается доказательства, что всякія два эквивалентныхъ приведенныхъ числа должны непремѣнно попасть въ одинъ періодъ, то допустимъ обратное, а именно, что два эквивалентныхъ приведенныхъ числа принадлежатъ разнымъ періодамъ. Тогда разлагая достаточно далеко оба эти числа въ непрерывную дробь, мы должны были бы придти къ одинаковому полному частному на основаніи теоремы § 24 главы X. Итакъ, приходимъ къ противорѣчію, а именно, что два различные періода имѣютъ общее звено, что невозможно, ибо всякое звено опредѣляетъ весь періодъ.

§ 39. Опредѣляя *классъ* квадратичныхъ ирраціональностей какъ совокупность ирраціональностей эквивалентныхъ между собой (не отличая эквивалентности proprie отъ эквивалентности improprie) придемъ къ предложенію: *число классовъ квадратичныхъ ирраціональностей равно числу періодовъ.*

Мы вели всѣ разсужденія относительно ирраціональностей положительнаго опредѣлителя при помощи ихъ разложенія въ непрерывную дробь. Таковъ былъ путь Lagrange'a. Gauss въ сочиненіи „Disquisitiones arithmeticae“ разсматриваетъ не сами ирраціональности, а формы, корнями которыхъ эти ирраціональности являются.

Постепенному разложенію ирраціональности въ непрерывную дробь $\alpha_0, \alpha_1, \alpha_2, \ldots$ соотвѣтствуетъ преобразованіе формы, имѣющей корнемъ $\frac{x}{y}$ эту ирраціональность въ новыя эквивалентныя формы при помощи подстановокъ

$$\begin{pmatrix} \alpha_0, & 1 \\ 1, & 0 \end{pmatrix}, \begin{pmatrix} \alpha_1, & 1 \\ 1, & 0 \end{pmatrix}, \ldots \quad (1)$$

Такимъ образомъ получается рядъ эквивалентныхъ формъ, который доводитъ всегда до приведенной формы, если заданная не была таковою. Такъ какъ опредѣлители подстановокъ (1) равны -1, то двѣ послѣдовательныя формы получаются improprie-эквивалентныя.

Если мы желаемъ сохранить Gauss'ово опредѣленіе *класса* формъ (см. § 12), какъ *совокупности формъ proprie-эквивалентныхъ между собой*, то придется въ цѣпи формъ, получаемыхъ процессомъ непрерывной дроби, брать формы *черезъ одну.*

Если число звеньевъ періода непрерывной дроби *четное*, то изъ каждаго періода ирраціональностей получится *два класса* формъ.

§ 40. Разсмотримъ теперь образованіе періодовъ формъ по Gauss'у. Для этого воспользуемся тѣмъ же способомъ преобразованія формъ, кото-

рый мы употребляли для положительныхъ формъ, т. е. составленіемъ формъ contiguarum a parte ultima.

Итакъ будемъ преобразовывать форму (a, b, a') при помощи подстановки $\begin{pmatrix} 0, & -1 \\ 1, & \delta \end{pmatrix}$ въ (a', b', a''), причемъ $b' \equiv -b \pmod{2a'}$. Нетрудно показать, что существуетъ *только одно* значеніе b', удовлетворяющее условіямъ

$$\sqrt{D} - |2a'| < b' < \sqrt{D}, \tag{1}$$

ибо придется искать b' среди чиселъ

$$\lambda + 1 - |2a'|, \lambda + 2 - |2a'|, \ldots \lambda - 1, \lambda$$

дающихъ полную систему вычетовъ по модулю $2a'$.

Докажемъ, что составляя указаннымъ образомъ послѣдовательныя формы contiguae a parte ultima

$$(a, b, a'), (a', b', a''), (a'', b'', a'''), \ldots \tag{2}$$

мы обязательно придемъ къ приведенной формѣ. Покажемъ, что форма (a', b', a'') уже будетъ приведенная, если $|a''| \geqslant |a'|$.

Въ самомъ дѣлѣ, равенство $D = b'^2 - 4a'a''$ можно будетъ переписать такъ

$$\frac{\sqrt{D} - b'}{2a'} = \frac{-2a''}{\sqrt{D} + b'}.$$

Взявъ отъ обѣихъ частей абсолютныя величины, мы получимъ на основаніи (1)

$$\frac{\sqrt{D} - b'}{|2a'|} = \frac{|2a''|}{|\sqrt{D} + b'|}, \ldots \tag{3}$$

Откуда, съ одной стороны мы имѣемъ

$$0 < \sqrt{D} - b' < |2a'| \leqslant |2a''|, \tag{4}$$

съ другой стороны на основаніи (3) можно будетъ написать

$$|2a''| < |\sqrt{D} + b'|; \tag{5}$$

сравнивая съ (4), получимъ

$$\sqrt{D} - b' < |\sqrt{D} + b'|.$$

Это неравенство требуетъ, чтобы b' было положительнымъ, и, значитъ, сопоставляя (4) и (5), получимъ

$$0 < \sqrt{D} - b' < |2a'| \leqq |2a'| < \sqrt{D} + b'$$

и форма оказывается приведенной.

Въ рядѣ формъ (2) коэффиціенты a', a'', a''', ... $a^{(n)}$, $a^{(n+1)}$... не могутъ постоянно убывать по абсолютной величинѣ, ибо существуетъ конечное число цѣлыхъ чиселъ меньшихъ даннаго $|a'|$. Такимъ образомъ мы видимъ, что долженъ наступить моментъ, когда будетъ имѣть мѣсто неравенство

$$|a^{(n)}| \leqq |a^{(n+1)}|$$

и форма будетъ приведенная.

Наше теперешнее доказательство не отличается по существу отъ доказаннаго въ § 30. Изложенный способъ Gauss'a найти приведенную форму progrie-эквивалентную съ заданной имѣетъ даже нѣкоторое преимущество въ вычислительномъ отношеніи, не говоря уже о томъ, что получается одинъ и тотъ же пріемъ для случая положительнаго опредѣлителя какъ и для случая отрицательнаго, не смотря на глубокую разницу двухъ теорій.

Недостатокъ этого пріема тотъ, что приведенная форма можетъ появиться раньше, ибо *достаточное* свойство $|a^{(n)}| \leqq |a^{(n+1)}|$ вовсе *не необходимо* для существованія приведенности формы.

§ 40. Какъ и слѣдовало ожидать, начиная уже съ первой приведенной формы всѣ слѣдующія будутъ приведенными. Дадимъ непосредственное доказательство этого предложенія, не ссылаясь на непрерывныя дроби. Покажемъ, что если форма (a, b, a') приведенная, то и форма (a', b', a''), составленная по правиламъ § 39, причемъ удовлетворено неравенство (1) § 39, будетъ приведенная.

Прежде всего убѣждаемся, что $b' > 0$. Въ самомъ дѣлѣ пусть будетъ $b' = -b + \delta|2a'|$. Покажемъ, что должно быть $\delta \geqq 1$. Допустимъ обратное $\delta < 1$, тогда $b' \leqq -b$ и на основаніи (5) § 33 получимъ

$$b' \leqq -b < \lambda - |2a'|,$$

что противорѣчитъ удовлетворенному нами неравенству (1) § 39. Если мы къ b' прибавимъ $|2a'|$, то очевидно, получимъ число большее λ т. е.

$$\lambda + 1 \leqq -b + (\delta + 1)|2a'|,$$

отсюда

$$0 < \lambda + 1 - b \leqq -2b + (\delta + 1)|2a'|,$$

или

$$0 < -b + \frac{\delta + 1}{2}|2a'| \leqq b'.$$

Итакъ b' число положительное.

На основаніи (1) § 39 получается сразу первое условіе приведенности новой формы (a', b', a'')

$$\sqrt{D} - b' < |2a'|.$$

Перейдемъ теперь къ доказательству неравенства

$$|2a'| < \sqrt{D} + b'.$$

Мы имѣемъ очевидное неравенство

$$(1 - \delta)|2a'| < \sqrt{D} - b$$

откуда получаемъ требуемое $|2a'| < \sqrt{D} + b'$.

Итакъ, въ нашей цѣпи формъ за каждою приведенною слѣдуютъ далѣе все приведенныя. Эта цѣпь приведенныхъ формъ должна быть чистою періодическою, ибо каждый элементъ этой цѣпи вполнѣ опредѣляетъ рядомъ стоящіе по обѣ стороны элементы.

Итакъ, приведенныя формы даннаго опредѣлителя распредѣляются по періодамъ.

Доказательство § 38 достаточно, чтобы считать справедливою слѣдующую теорему.

Двѣ proprie-эквивалентныя приведенныя формы положительнаго опредѣлителя принадлежатъ одному и тому же періоду. Двѣ формы не могутъ быть proprie-эквивалентными, если онѣ не принадлежатъ къ одному и тому же періоду.

§ 41. Итакъ, мы видимъ, что у насъ получены всѣ данныя для рѣшенія вопроса объ эквивалентности двухъ формъ.

$$(a, b, c), (a_1, b_1, c_1)$$

положительнаго опредѣлителя. Составляемъ для каждой изъ заданныхъ формъ цѣпь contiguarum a parte ultima; если мы придемъ къ разнымъ періодамъ, то заданныя формы не эквивалентны: если же періоды будутъ одинаковы, то есть, будутъ состоять изъ тѣхъ же приведенныхъ формъ, то заданныя формы эквивалентны. Для составленія подстановки, переводящей первую форму во вторую ищемъ ближайшую общую приведенную форму (α, β, γ). Придется перемножить подстановки цѣпи, переводящія первую форму (a, b, c) въ приведенную (α, β, γ) и отъ послѣдней вернуться по второй цѣпи ко второй формѣ (a_1, b_1, c_1).

Лучше всего пояснить сказанное на примѣрѣ.

Требуется узнать эквивалентны ли формы

$$(360, -175, 21), (12040, -10465, 2274)$$

одного и того же опредѣлителя $D = 385$.

Составляемъ формы contiguae a parte ultima съ первой, получаемъ

$$(360, -175, 21), (21, 7, -4)$$

далѣе идутъ уже приведенныя, образующія періодъ изъ двѣнадцати слѣдующихъ формъ

$$(-4, 17, 12), (12, 7, -7), (-7, 7, 12), (12, 17, -4)$$

$$(-4, 15, 10), (10, 5, -9), (-9, 13, 6), (6, 11, -11)$$

$$(-11, 11, 6), (6, 13, -9), (-9, 5, 10), (10, 15, -4)$$

далѣе идетъ опять первая форма періода.

Подстановки, переводящія эти формы каждую въ слѣдующую, суть

$$\begin{pmatrix}0, & -1\\ 1, & -4\end{pmatrix}, \begin{pmatrix}0, & -1\\ 1, & -3\end{pmatrix}, \begin{pmatrix}0, & -1\\ 1, & -1\end{pmatrix}, \begin{pmatrix}0, & -1\\ 1, & -1\end{pmatrix}, \begin{pmatrix}0, & -1\\ 1, & 1\end{pmatrix}, \begin{pmatrix}0, & -1\\ 1, & -4\end{pmatrix}, \begin{pmatrix}0, & -1\\ 1, & 1\end{pmatrix},$$

$$\begin{pmatrix}0, & -1\\ 1, & -1\end{pmatrix}, \begin{pmatrix}0, & -1\\ 1, & 2\end{pmatrix}, \begin{pmatrix}0, & -1\\ 1, & -1\end{pmatrix}, \begin{pmatrix}0, & -1\\ 1, & 2\end{pmatrix}, \begin{pmatrix}0, & -1\\ 1, & -1\end{pmatrix}, \begin{pmatrix}0, & -1\\ 1, & 1\end{pmatrix}.$$

Продѣлаемъ то же самое для другой формы.

Получаемъ цѣпь формъ

$$(12040, -10465, 2274), (2274, -3179, 1111),$$

$$(1111, -1265, 360), (360, -175, 21).$$

Далѣе продолжать не надо, ибо послѣдняя форма совпадаетъ съ первою заданною.

Соотвѣтственныя подстановки суть

$$\begin{pmatrix}0, & -1\\ 1, & -3\end{pmatrix}, \begin{pmatrix}0, & -1\\ 1, & -2\end{pmatrix}, \begin{pmatrix}0, & -1\\ 1, & -2\end{pmatrix}.$$

Первая заданная форма, очевидно, переходитъ во вторую при помощи подстановки

$$\begin{pmatrix}-2, & 1\\ -1, & 0\end{pmatrix}\begin{pmatrix}-2, & 1\\ -1, & 0\end{pmatrix}\begin{pmatrix}-3, & 1\\ -1, & 0\end{pmatrix} = \begin{pmatrix}-7, & 3\\ -5, & 2\end{pmatrix}$$

или, что одно и тоже,

$$x = -7x' + 3y',\ y = -5x' + 2y'.$$

§ 42. Если найдены надежныя правила для узнаванія эквивалентности двухъ заданныхъ формъ положительнаго опредѣлителя, то тѣмъ самымъ рѣшается вопросъ о представленіи числа заданною формой. Рѣшеніе буквально то же, что и для случая отрицательнаго опредѣлителя.

Лучше всего пояснить дѣло на примѣрѣ.

Требуется представить число $m = 7409$ формой $(21, 15, -7)$ опредѣлителя $D = 813$.

Испытываемъ прежде всего, будетъ ли число D квадратичнымъ вычетомъ числа $4m$, для этой цѣли пробуемъ рѣшать квадратное сравненіе.

$$n^2 \equiv 813 \pmod{29636}, \qquad (1)$$

гдѣ $29636 = 4.7409$.

Раскладываемъ по таблицѣ A [1]) число 7409 на простые множители $7409 = 31.239$. Сравненіе (1) распадается на три

$$n^2 \equiv 1 \pmod 4;\ n^2 \equiv 813 \equiv 7 \pmod{31};\ n^2 \equiv 813 \equiv 96 \pmod{239}.$$

Второе сравненіе рѣшается сразу по таблицѣ индексовъ C. Получаемъ $n \equiv 10, 21 \pmod{31}$. Третье сравненіе положеніемъ $n = 4n'$ приводится къ $n'^2 \equiv 6 \pmod{239}$ $\left(\frac{6}{239}\right) = \left(\frac{2}{239}\right)\left(\frac{3}{239}\right) = \left(\frac{3}{239}\right) = -\left(\frac{239}{3}\right) = -\left(\frac{2}{3}\right) = 1$. Итакъ, третье сравненіе также рѣшается. Примѣнимъ къ нему способъ Коркина.

Надо рѣшить сравненіе $x^2 \equiv 6 \pmod{239}$. Здѣсь $a=6$, $q=2$, $N=119$, $N_1 = 59$, $\tau = 1$, $\sigma = 1$.

$$\Omega^2 \equiv 6^{119} \pmod{239},\ x\Omega \equiv 6^{60}.$$

Составляемъ вычеты степеней числа 6

$$6^2 \equiv 36,\ 6^4 \equiv 101,\ 6^8 \equiv 163,\ 6^{16} \equiv 40;$$

дальше не надо идти, ибо $6^{17} \equiv 1$. Дѣло упрощается, ибо получаемъ $\Omega^2 \equiv 1$ и $\Omega = 1$; такъ что $x \equiv 6^{60} \equiv 6^9 \equiv 22$. Получаемъ $n' = 22$, значитъ, $n = 4n' = 88$.

Итакъ, мы приходимъ къ слѣдующимъ сравненіямъ

$$n \equiv 1,\ 3 \pmod 4;\ n \equiv 10,\ 21 \pmod{31};\ n \equiv 88,\ 151 \pmod{239}.$$

---

[1]) См. таблицы въ концѣ книги.

Удовлетворяя всѣмъ этимъ сравненіямъ по правиламъ § 16 гл. III, получимъ окончательно восемь рѣшеній сравненія (1).

$$4629,\ 6365,\ 8453,\ 10189,\ 19447,\ 21183,\ 23271,\ 25007$$

и, слѣдовательно, восемь формъ

$$\begin{array}{l|l} (7409,\ 4629,\ 723) & (7409,\ 19447,\ 12761) \\ (7409,\ 6365,\ 1367) & (7409,\ 21183,\ 15141) \\ (7409,\ 8453,\ 2411) & (7409,\ 23271,\ 18273) \\ (7409,\ 10189,\ 3503) & (7409,\ 25007,\ 21101) \end{array} \qquad (2)$$

Чтобы рѣшить вопросъ о представленіи числа 7409 заданною формой надо будетъ рѣшить вопросъ, эквивалентна ли заданная форма этимъ послѣднимъ. Если эквивалентность будетъ существовать, то подстановка, переводящая заданную форму въ эквивалентную

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$$

дастъ искомое представленіе

$$7409 = 21\alpha^2 + 15\alpha\gamma - 7\gamma^2. \qquad (3)$$

Такъ какъ заданная форма приведенная, то получаемъ ея періодъ

$$(21,\ 15,\ -7),\ (-7,\ 27,\ 3),\ (3,\ 27,\ -7),\ (-7,\ 15,\ 21),\ (21,\ 27,\ -1),$$
$$(-1,\ 27,\ 21).$$

Подстановки суть

$$\begin{pmatrix} 0, & -1 \\ 1, & -3 \end{pmatrix},\ \begin{pmatrix} 0, & -1 \\ 1, & 9 \end{pmatrix},\ \begin{pmatrix} 0, & -1 \\ 1, & -3 \end{pmatrix},\ \begin{pmatrix} 0, & -1 \\ 1, & 1 \end{pmatrix},\ \begin{pmatrix} 0, & -1 \\ 1, & 27 \end{pmatrix}$$

причемъ послѣдняя переходитъ въ первую при помощи подстановки $\begin{pmatrix} 0, & -1 \\ 1, & 1 \end{pmatrix}$.

Составимъ для формъ (2) цѣпи contiguarum.

I. (7409, 4629, 723), (723, —291, 29), (29, 1, —7), (—7, 27, 3).

Подстановки суть

$$\begin{pmatrix} 0, & -1 \\ 1, & 3 \end{pmatrix},\ \begin{pmatrix} 0, & -1 \\ 1, & -5 \end{pmatrix},\ \begin{pmatrix} 0, & -1 \\ 1, & -2 \end{pmatrix}.$$

II. (7409, 6365, 1367), (1367, —897, 147), (147, 15, —1), (—1, 27, 21).

Подстановки

$$\begin{pmatrix}0, & -1\\ 1, & 2\end{pmatrix}, \begin{pmatrix}0, & -1\\ 1, & -3\end{pmatrix}, \begin{pmatrix}0, & -1\\ 1, & -21\end{pmatrix}.$$

III. (7409, 8453, 2411), (2411, —3631, 1367), (1367, — 1837, 617), (617, — 631, 161), (161, —13, —1), (—1, 27, 21).

Подстановки

$$\begin{pmatrix}0, & -1\\ 1, & 1\end{pmatrix}, \begin{pmatrix}0, & -1\\ 1, & -2\end{pmatrix}, \begin{pmatrix}0, & -1\\ 1, & -2\end{pmatrix}, \begin{pmatrix}0, & -1\\ 1, & -2\end{pmatrix}, \begin{pmatrix}0, & -1\\ 1, & -7\end{pmatrix}.$$

IV. (7409, 10189, 3503), (3503, —3183, 723), (723, —1155, 461), (461, —689, 257), (257, —339, 111), (111, —105, 23), (23, 13, —7), (—7, 15, 21).

Подстановки

$$\begin{pmatrix}0, & -1\\ 1, & 1\end{pmatrix}, \begin{pmatrix}0, & -1\\ 1, & -3\end{pmatrix}, \begin{pmatrix}0, & -1\\ 1, & -2\end{pmatrix}, \begin{pmatrix}0, & -1\\ 1, & -2\end{pmatrix}, \begin{pmatrix}0, & -1\\ 1, & -2\end{pmatrix}, \begin{pmatrix}0, & -1\\ 1, & -2\end{pmatrix},$$

$$\begin{pmatrix}0, & -1\\ 1, & -2\end{pmatrix}.$$

V. (7409, 19447, 12761), (12761, —19447, 7409), (7409, —10189, 3503).

Подстановки

$$\begin{pmatrix}0, & -1\\ 1, & 0\end{pmatrix}, \begin{pmatrix}0, & -1\\ 1, & -2\end{pmatrix}.$$

VI. (7409, 21183, 15141), (15141, —21183, 7409), (7409, —8453, 2411).

Подстановки

$$\begin{pmatrix}0, & -1\\ 1, & 0\end{pmatrix}, \begin{pmatrix}0, & -1\\ 1, & -2\end{pmatrix}.$$

VII. (7409, 23271, 18273), (18273, —23271, 7409), (7409, — 6365, 1367).

Подстановки

$$\begin{pmatrix}0, & -1\\ 1, & 0\end{pmatrix}, \begin{pmatrix}0, & -1\\ 1, & -2\end{pmatrix}.$$

VIII. (7409, 25007, 21101), (21101, —25007, 7409), (7409, —4629, 723).

Подстановки

$$\begin{pmatrix} 0, & -1 \\ 1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 0, & -1 \\ 1, & -2 \end{pmatrix}.$$

Покажемъ теперь, какъ найти α и γ, удовлетворяющія уравненію (3). Беремъ случай I и смотримъ, какъ можно перейти отъ формы (21, 15, —7) къ формѣ (7409, 4629, 723). Ближайшая общая въ обѣихъ цѣпяхъ приведенная форма есть (—7, 27, 3). Мы должны взять подстановку $\begin{pmatrix} 0, & -1 \\ 1, & -3 \end{pmatrix}$, переводящую форму (21, 15, — 7) въ (— 7, 27, 3) и далѣе надо взять въ обратномъ порядкѣ обратныя подстановки случая I. Получаемъ

$$\begin{pmatrix} 0, & -1 \\ 1, & -3 \end{pmatrix}\begin{pmatrix} -2, & 1 \\ -1, & 0 \end{pmatrix}\begin{pmatrix} -5, & 1 \\ -1, & 0 \end{pmatrix}\begin{pmatrix} 3, & 1 \\ -1, & 0 \end{pmatrix} = \begin{pmatrix} -16, & -5 \\ -18, & -6 \end{pmatrix}.$$

Значитъ

$$\alpha = -16, \quad \gamma = -19.$$

и, дѣйствительно, получается тождество

$$7409 = 21.16^2 + 15.16.19 - 7.19^2.$$

Подобнымъ же образомъ другіе случаи даютъ

II. $\alpha = 152, \quad \gamma = -145.$

III. $\alpha = 51, \quad \gamma = -44.$

IV. $\alpha = -999, \quad \gamma = 964.$

Остальные четыре случая не даютъ новыхъ рѣшеній, ибо получаются рѣшенія, отличающіяся только знакомъ $(-\alpha, -\gamma)$ отъ четырехъ уже найденныхъ. Это обстоятельство происходитъ отъ того, что уже на третьемъ звенѣ получается обратная форма одной изъ первыхъ четырехъ: такъ что можно примѣнить подстановку $\begin{pmatrix} 1, & 0 \\ 0, & -1 \end{pmatrix}$, чтобы связать цѣпи четырехъ послѣднихъ случаевъ съ цѣпями первыхъ четырехъ.

Если мы продолжимъ составленіе цѣпей формъ до появленія приведенной формы, то мы убѣдимся, что всѣ формы (2) propriе-эквивалентны формѣ (21, 15, —7) и, слѣдовательно, принадлежатъ къ одному съ нею классу.

Къ этому классу принадлежатъ, очевидно, всѣ выписанныя нами contiguae.

Характернымъ является присутствіе въ этомъ классѣ обратныхъ формъ напримѣръ,

$$(7409,\ 4629,\ 723) \text{ и } (7409,\ -4629,\ 723). \qquad (4)$$

Мы найдемъ подстановку съ опредѣлителемъ $+1$, переводящую формы (4) одну въ другую, если доведемъ для обѣихъ формъ цѣпи contiguarum до общей приведенной. Съ другой стороны, очевидно, что формы (4) переходятъ одна въ другую при помощи подстановки

$$\begin{pmatrix} 1, & 0 \\ 0, & -1 \end{pmatrix}$$

опредѣлителя -1. Итакъ, формы (4) таковы, что онѣ какъ proprie такъ и improprie эквивалентны между собой.

Форма anceps.

§ 43. Теперь мы должны оставить теорію формъ положительнаго опредѣлителя и обратиться къ нѣкоторымъ важнымъ пунктамъ теоріи, не зависящимъ отъ знака опредѣлителя.

Въ предыдущемъ параграфѣ мы видѣли примѣръ двухъ формъ, которыя были эквивалентны какъ proprie такъ и improprie.

Остановимся нѣсколько подробнѣе на этомъ случаѣ.

Пусть форма (a, b, c) переходитъ въ форму (a_1, b_1, c_1) при помощи двухъ подстановокъ S и T, изъ которыхъ первая proprie-эквивалентна, а вторая improprie.

Тогда очевидно, что первая переходитъ въ самое себя при помощи двухъ improprie-эквивалентныхъ подстановокъ

$$ST^{-1} \text{ и } TS^{-1},$$

т. е. получаемъ теорему:

Если двѣ формы какъ proprie такъ и improprie эквивалентны между собой, то каждая изъ нихъ сама себѣ improprie эквивалентна.

§ 44. Если въ нѣкоторомъ классѣ формъ заключаются двѣ обратныя между собой формы (a, b, c) и $(a, -b, c)$, то каждая форма этого класса сама себѣ improprie-эквивалентна.

Въ самомъ дѣлѣ, пусть будетъ (A, B, C) произвольная форма класса. Обозначимъ черезъ S proprie-эквивалентную подстановку, при помощи которой форма (A, B, C) переходитъ въ (a, b, c), а черезъ S_1 proprie-эквивалентную подстановку, при помощи которой форма (A, B, C) переходитъ въ $(a, -b, c)$. Замѣчая, что (a, b, c) переходитъ въ

$a, -b, c$) при помощи подстановки $\begin{pmatrix} 1, & 0 \\ 0, & -1 \end{pmatrix}$ получимъ, что форма ($A. B, C$) переходитъ въ самое себя при помощи подстановки

$$S\begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}S_1^{-1},$$

которая imprpriе эквивалентна, что и требовалось доказать.

Классъ, всѣ формы котораго сами себѣ imprpriе эквивалентны называется anceps.

Обыкновенно форма (a, b, c) и ей обратная ($a, -b, c$) попадаютъ въ два различные класса, которые носятъ названіе *обратныхъ* другъ относительно друга.

Если обратные классы совпадаютъ въ одинъ, то этотъ классъ будетъ anceps.

§ 45. Классъ формъ примѣра, разобраннаго въ § 42, очевидно, *anceps*. Найдемъ imprpriе эквивалентную подстановку, переводящую основную форму (21, 15, —7) самое въ себя. Лучше всего поступить такъ; возьмемъ обратную форму (21, —15, —7), она не приведенная, ибо второй коэффиціентъ отрицательный.

Слѣдующая contigua (—7, 15, 3) уже приведенная. Если мы возьмемъ слѣдующую послѣдовательность формъ

(21, 15, —7), (—7, 27, 3), (3, 27, —7), (—7, 15, 21), (21, —15, —7),

(21, 15, —7).

то подстановки въ произведеніи дадутъ

$$\begin{pmatrix} 0, & -1 \\ 1, & -3 \end{pmatrix}\begin{pmatrix} 0, & -1 \\ 1, & -9 \end{pmatrix}\begin{pmatrix} 0, & -1 \\ 1, & -3 \end{pmatrix}\begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}\begin{pmatrix} 1, & 0 \\ 0, & -1 \end{pmatrix} = \begin{pmatrix} -28, & 9 \\ -87, & 28 \end{pmatrix}$$

и, дѣйствительно, непосредственное вычисленіе повѣряетъ, что подстановка

$$x = -28x' + 9y'$$

$$y = -87x' + 28y'$$

переводитъ форму (21, 15, —7) въ самое себя.

Въ нашей подстановкѣ первый коэффиціентъ (—28) и четвертый (+28) одинаковы по абсолютной величинѣ и разные по знаку. Это свойство общее.

Теорема. Если improprie-эквивалентная подстановка $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ *переводитъ форму въ самое себя, то имѣетъ мѣсто равенство* $\delta = -\alpha$.

Если форма переходитъ въ самое себя, то изъ формулъ (2) § 8 получимъ

$$a\alpha^2 + b\alpha\gamma + c\gamma^2 = a \tag{1}$$

$$2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta = b \tag{2}$$

кромѣ того

$$\alpha\delta - \beta\gamma = -1 \tag{3}$$

изъ (3) получаемъ $\beta\gamma = \alpha\delta + 1$ и подставляемъ въ (2), тогда будетъ

$$a\alpha\beta + b\alpha\delta + c\gamma\delta = 0 .$$

Это послѣднее и (1) можно будетъ переписать такъ

$$a\alpha\beta + \delta(b\alpha + c\gamma) = 0 , \quad a(\alpha^2 - 1) + \gamma(b\alpha + c\gamma) = 0 .$$

Исключая $b\alpha + c\gamma$ получимъ

$$\alpha\beta\gamma = \delta(\alpha^2 - 1)$$

откуда на основаніи (3) выходитъ

$$\delta = -\alpha .$$

§ 45. Особенно важенъ случай формы, переходящей въ самое себя при помощи подстановки $\begin{pmatrix}\alpha, & \beta\\ \gamma, & -\alpha\end{pmatrix}$, у которой $\gamma = 0$. Получаемъ тогда $\alpha^2 = 1$, откуда $\alpha = \pm 1$.

Будемъ называть *формой* anceps такую, которая переходитъ въ самое себя при помощи подстановки $\begin{pmatrix}1, & \beta\\ 0, & -1\end{pmatrix}$. Уравненіе (2) въ этомъ случаѣ даетъ $b = a\beta$, т. е. форма anceps есть такая, у которой второй коэффиціентъ дѣлится на первый.

Теорема. Въ классѣ anceps существуетъ безчисленное множество формъ anceps.

Пусть нѣкоторая форма F класса anceps переходитъ въ самое себя при помощи improprie эквивалентной подстановки $\begin{pmatrix}\alpha, & \beta\\ \gamma, & -\alpha\end{pmatrix}$, такъ что

$$\alpha^2 + \gamma\beta = 1 .$$

Покажемъ, что можно найти proprie эквивалентную подстановку $\begin{pmatrix}\lambda, & \mu\\ \nu, & \rho\end{pmatrix}$, переводящую F въ искомую форму anceps Φ.

Эта форма Φ переходитъ въ самое себя при помощи improprie эквивалентной подстановки

$$\begin{pmatrix} \rho, & -\mu \\ -\nu, & \lambda \end{pmatrix} \begin{pmatrix} \alpha, & \beta \\ \gamma, & -\alpha \end{pmatrix} \begin{pmatrix} \lambda, & \mu \\ \nu, & \rho \end{pmatrix},$$

которую можно будетъ написать окончательно такъ

$$\begin{pmatrix} (\quad \rho\alpha - \mu\gamma)\lambda + (\quad \rho\beta + \alpha\mu)\nu, & (\quad \rho\alpha - \mu\gamma)\mu + (\quad \rho\beta + \alpha\mu)\rho \\ (-\nu\alpha + \lambda\gamma)\lambda + (-\nu\beta - \alpha\lambda)\nu, & (-\nu\alpha + \lambda\gamma)\mu + (-\nu\beta - \alpha\lambda)\rho \end{pmatrix}. \qquad (1)$$

Для того, чтобы форма Φ была anceps, необходимо, чтобы третій коэффиціентъ равнялся нулю, то есть

$$(-\nu\alpha + \lambda\gamma)\lambda + (-\nu\beta - \alpha\lambda)\nu = 0$$

или

$$\lambda^2\gamma - 2\lambda\nu\alpha - \nu^2\beta = 0. \qquad (2)$$

Если $\gamma = 0$, то изслѣдованіе излишне, ибо сама форма F есть anceps. Если же γ не $= 0$, то умножимъ на него (2) и примемъ во вниманіе $\alpha^2 + \beta\gamma = 1$.

$$\lambda^2\gamma^2 - 2\lambda\gamma\nu\alpha + \nu^2\alpha^2 = \nu^2; \qquad (3)$$

ν не равно нулю, ибо иначе на основаніи (2) было бы $\gamma = 0$.

Дѣлимъ на ν^2 уравненіе (3). Получимъ $(\omega\gamma - \alpha)^2 = 1$, гдѣ $\omega = \frac{\lambda}{\nu}$

Далѣе имѣемъ $\omega\gamma - \alpha = \pm 1$ или

$$\frac{\lambda}{\nu} = \frac{\alpha \pm 1}{\gamma}.$$

Вслѣдствіе эквивалентности подстановки числа λ и ν взаимно простыя. Значитъ, для полученія ихъ достаточно при помощи сокращенія привести дробь $\frac{\alpha \pm 1}{\gamma}$ къ простѣйшему виду. Числитель и знаменатель этой уже сокращенной дроби и будутъ давать λ и ν. Когда λ и ν найдены, то μ и ρ получаются по уравненію $\lambda\rho - \mu\nu = 1$.

Послѣдняя формула дастъ безчисленное множество значеній для μ и ρ по формуламъ

$$\mu + \lambda k, \quad \rho + \nu k$$

при произвольномъ k. Очевидно, что получится безчисленное множество формъ anceps, происходящихъ при помощи подстановки

$$\begin{pmatrix} \lambda, & \mu + k\lambda \\ \nu, & \rho + k\nu \end{pmatrix} = \begin{pmatrix} \lambda, & \mu \\ \nu, & \rho \end{pmatrix} \begin{pmatrix} 1, & k \\ 0, & 1 \end{pmatrix}.$$

Всѣ эти формы получаются изъ одной при помощи подстановки $\begin{pmatrix} 1, & k \\ 0, & 1 \end{pmatrix}$. Сопоставляя съ § 21, мы замѣчаемъ, что всѣ такія формы ancеps параллельны между собой.

Итакъ, существуетъ двѣ системы параллельныхъ формъ ancеps, опредѣляемыхъ двумя пропорціями

$$\frac{\lambda}{\nu} = \frac{\alpha + 1}{\gamma}, \quad \frac{\lambda}{\nu} = \frac{\alpha - 1}{\gamma}.$$

Примѣняя къ численному примѣру § 47, получимъ

$$\frac{\lambda}{\nu} = \frac{-28 + 1}{-87} = \frac{9}{29}, \quad \frac{\lambda}{\nu} = \frac{-28 - 1}{-87} = \frac{1}{3}.$$

Въ первомъ случаѣ подстановка $\begin{pmatrix} 9, & 4 \\ 29, & 13 \end{pmatrix}$ переводитъ форму $(21, 15, -7)$ въ форму ancеps $(-271, -271, -87)$.

Во второмъ случаѣ подстановка $\begin{pmatrix} 1, & 0 \\ 3, & 1 \end{pmatrix}$ даетъ форму ancеps $(3, 27, -7)$.

Уравненіе Pell'a.

§ 46. На основаніи соображеній предыдущихъ параграфовъ можно для формъ положительнаго опредѣлителя найти безчисленное множество подстановокъ, переводящихъ форму въ самое себя. Въ самомъ дѣлѣ, пусть задана форма f. Составимъ цѣпь contiguarum. Пусть S обозначаетъ произведеніе всѣхъ подстановокъ цѣпи, переводящихъ форму f въ первую приведенную φ_1. Обозначимъ черезъ Σ_k произведеніе всѣхъ подстановокъ цѣпи между первымъ появленіемъ формы φ_1 и ея $k+1$-мъ появленіемъ послѣ k періодовъ. Очевидно, что форма f будетъ переходить въ самое себя отъ подстановки

$$S\Sigma_k S^{-1}, \tag{1}$$

ибо подстановка S переводитъ форму f въ φ_1, подстановка Σ_k оставляетъ φ_1 безъ перемѣны, а подстановка S^{-1} переводитъ обратно φ_1 въ f.

Различнымъ значеніямъ k будутъ соотвѣтствовать безчисленное множество подстановокъ (1).

§ 47. Не ограничиваясь однимъ знакомъ опредѣлителя разберемъ вопросъ о преобразованіи формы въ самое себя въ самомъ общемъ видѣ.

Итакъ, пусть подстановка $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ переводитъ форму (a, b, c) въ самое себя

$$a\alpha^2 + b\alpha\gamma + c\gamma^2 = a \tag{1}$$

$$2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta = b \tag{2}$$

$$\alpha\delta - \beta\gamma = 1 \tag{3}$$

изъ уравненія (3) подставляемъ $\alpha\delta = 1 + \beta\gamma$ въ (2)

$$a\alpha\beta + b\beta\gamma + c\gamma\delta = 0\,. \tag{4}$$

Рѣшая уравненія (1) и (4) относительно двухъ величинъ $a\alpha + b\gamma$ и $c\gamma$ получимъ

$$a\alpha + b\gamma = a\delta\,, \quad c\gamma = -a\beta$$

что даетъ пропорцію

$$\frac{\alpha - \delta}{-b} = \frac{\gamma}{a} = \frac{\beta}{-c} = u\,,$$

гдѣ раціональное число u обозначаетъ общую величину отношеній. Получаемъ

$$\alpha - \delta = -bu\,, \quad \gamma = au\,, \quad \beta = -cu\,.$$

Число u должно быть цѣлое, ибо три числа a, b, c не имѣютъ общаго дѣлителя, три же числа $\alpha - \delta$, γ, β должны быть цѣлыя.

Разсмотримъ теперь число $\alpha + \delta$

$$(\alpha + \delta)^2 = (\alpha - \delta)^2 + 4\alpha\delta = b^2u^2 + 4(1 + \beta\gamma) = b^2u^2 + 4 - 4acu^2 = Du^2 + 4\,.$$

Обозначая $\alpha + \delta = t$, получаемъ

$$t^2 - Du^2 = 4\,. \tag{5}$$

Итакъ, задача привелась къ нахожденію рѣшеній въ цѣлыхъ числахъ t и u уравненія (5), которое носитъ названіе уравненія Pell'a.

§ 48. Если опредѣлитель D число положительное, то уравненіе (5) § 47 должно имѣть безчисленное число цѣлыхъ рѣшеній, ибо каждая подстановка $\begin{pmatrix}\alpha, & \beta\\ \nu, & \delta\end{pmatrix}$, переводящая форму въ самое себя, даетъ числа t и u, а такихъ подстановокъ безчисленное множество.

Такъ напримѣръ, мы найдемъ подстановку, переводящую форму $(21, 15, -7)$ въ самое себя, если перемножимъ подстановки

$$\begin{pmatrix}0, & -1\\ 1, & -3\end{pmatrix}\begin{pmatrix}0, & -1\\ 1, & 9\end{pmatrix}\begin{pmatrix}0, & -1\\ 1, & -3\end{pmatrix}\begin{pmatrix}0, & -1\\ 1, & 1\end{pmatrix}\begin{pmatrix}0, & -1\\ 1, & 27\end{pmatrix}\begin{pmatrix}0, & -1\\ 1, & 1\end{pmatrix}=$$

$$=\begin{pmatrix}-1027, & 1064\\ -3192, & -3307\end{pmatrix}.$$

Раздѣляя -3192 на 21, получимъ $u=-152$. Кромѣ того $t=\alpha+\delta=-1027-3307=-4334$. Итакъ, получаемъ рѣшеніе $t=4334$, $u=152$ Pell'ева уравненія

$$t^2-813u^2=4.$$

Подстановка $\begin{pmatrix}-28, & 9\\ -87, & 28\end{pmatrix}$, найденная нами, imrgrie-эквивалентна. Можно было бы ожидать, что получится prgrie-эквивалентная подстановка черезъ возвышеніе въ квадратъ; но такимъ образомъ мы не придемъ къ рѣшенію уравненія Pell'a, ибо квадратъ всякой imrgrie-эквивалентной подстановки, переводящей форму въ самое себя, есть $\begin{pmatrix}1, & 0\\ 0, & 1\end{pmatrix}=1$.

§ 49. Въ случаѣ отрицательнаго опредѣлителя число рѣшеній уравненія Pell'a будетъ *конечное*.

Если $D=-d$, то уравненіе Pell'a будетъ имѣть видъ

$$t^2+du^2=4.$$

Если $d>4$, то очевидно, имѣютъ мѣсто только 2 рѣшенія

$$t=2,\ u=0;\quad t=-2,\ u=0.$$

Если $d=4$, то получаются 4 рѣшенія

$$t=\ \ 2,\ \ u=0;\quad t=0,\quad u=\ \ 1$$

$$t=-2,\ \ u=0;\quad t=0,\quad u=-1.$$

Если $d=3$, то получаются 6 рѣшеній

$$t=\ \ 2,\ \ u=0;\quad t=\ \ 1,\ \ u=1;\quad t=\ \ 1,\ \ u=-1$$

$$t=-2,\ \ u=0;\quad t=-1,\ \ u=1;\quad t=-1,\ \ u=-1.$$

Случаи $d=1;2$ невозможны, ибо $D\equiv 0,\ 1\pmod 4$.

§ 50. Рѣшая $\alpha-\delta=-bu$, $\alpha+\delta=t$ относительно α и δ, получимъ подстановку

$$\alpha = \frac{t - bu}{2}, \quad \beta = -cu$$

$$\gamma = au, \quad \delta = \frac{t + bu}{2}.$$

Покажемъ, что для α и δ получаются всегда цѣлыя значенія, т. е., что числа $t - bu$ и $t + bu$ четныя.

Если D четное, то b четное, а на основаніи уравненія Pell'a и t четное. Если D нечетное, то всѣ три числа t, b, u нечетныя, или только одно изъ нихъ b нечетное. Итакъ, всякому рѣшенію уравненія Pell'a соотвѣтствуетъ подстановка преобразующая форму въ самое себя.

§ 51. Итакъ, займемся рѣшеніемъ уравненія

$$t^2 - Du^2 = 4 \qquad (D > 0) \tag{1}$$

въ цѣлыхъ числахъ. Если D четное число, то какъ мы видѣли $D = 4d$, гдѣ d цѣлое положительное число.

Число t должно быть четнымъ $t = 2v$ и мы приходимъ къ рѣшенію уравненія

$$v^2 - du^2 = 1. \tag{2}$$

Обращаясь къ разсмотрѣнію уравненія (1) въ случаѣ D нечетнаго, мы видимъ, что оно можетъ рѣшаться въ нечетныхъ числахъ t и u только тогда, когда $D \equiv 5 \pmod 8$, ибо квадратъ всякаго нечетнаго числа сравнимъ съ единицей по модулю 8 (см. § 12 гл. V).

Если же $D \equiv 1 \pmod 8$, то оба числа t и u должны быть четными. Подставляя тогда $t = 2v$, $u = 2w$, получимъ

$$v^2 - Dw^2 = 1. \tag{3}$$

Если $D \equiv 5 \pmod 8$, то нечетныя рѣшенія уравненія (1) не всегда возможны и, слѣдовательно, когда такія рѣшенія невозможны, надо разсматривать четныя рѣшенія, т. е. уравненіе (3).

Резюмируя сказанное мы видимъ, что всегда рѣшеніе уравненія Pell'a сводится къ уравненію

$$x^2 - Dy^2 = 1. \tag{4}$$

Только иногда, въ случаѣ $D \equiv 5 \pmod 4$, возможно нахожденіе нечетныхъ рѣшеній уравненія (1).

Разсмотримъ болѣе подробно уравненіе (4) и скажемъ лишь нѣсколько словъ о рѣшеніи (1) въ нечетныхъ числахъ.

§ 52. Перепишемъ уравненіе (4) § 51 такъ

$$\frac{x}{y} - \sqrt{D} = \frac{1}{y(x + y\sqrt{D})}$$

получаемъ неравенство

$$0 < \frac{x}{y} - \sqrt{D} < \frac{1}{2y^2}$$

показывающее (см. § 15 гл. X), что величина $\frac{x}{y}$ должна быть подходящей дробью въ разложеніи $\sqrt{D}$ въ непрерывную.

Итакъ, пусть задано разложеніе

$$\sqrt{D} = a_0 + \frac{1}{a_1} + \cdots + \frac{1}{a_{n-1} + \frac{1}{a_n} + \cdots}$$

причемъ мы знаемъ, что періодъ начинается со второго неполнаго частнаго a_1.

Такъ какъ $\frac{x}{y} > \sqrt{D}$, то за $\frac{x}{y}$ надо выбрать четную подходящую дробь. Пусть будетъ

$$x = P_n, \; y = Q_n,$$

гдѣ *n число четное*. Согласно обозначеніямъ главы X дробь $\frac{P_n}{Q_n}$ есть та, которая имѣетъ послѣднее неполное частное a_{n-1}.

Итакъ, пусть P_n и Q_n есть найденное рѣшеніе уравненія Pell'a

$$P_n^2 - DQ_n^2 = 1. \qquad (1)$$

Произведемъ слѣдующія выкладки

$$P_n - Q_n\sqrt{D} = \frac{1}{P_n + Q_n\sqrt{D}} = \frac{Q_{n+1}P_n - Q_nP_{n+1}}{P_n + Q_n\sqrt{D}} =$$

$$= \frac{Q_{n+1}(P_n + Q_n\sqrt{D}) - Q_n(P_{n+1} + Q_{n+1}\sqrt{D})}{P_n + Q_n\sqrt{D}} =$$

$$= Q_{n+1} - Q_n(P_{n+1} + Q_{n+1}\sqrt{D})(P_n - Q_n\sqrt{D}) =$$

$$= Q_{n+1} - Q_n[a + \sqrt{D}],$$

гдѣ цѣлое число $a = P_nP_{n+1} - Q_{n+1}Q_nD$.

Послѣднее уравненіе даетъ

$$P_n = Q_{n+1} - Q_n a . \tag{2}$$

Умножая на P_n и принимая во вниманіе (1), получимъ

$$1 + DQ_n^2 = Q_{n+1}P_n - Q_n P_n a ,$$

или

$$DQ_n^2 = Q_n P_{n+1} - Q_n P_n a ,$$

то есть,

$$DQ_n = P_{n+1} - P_n a . \tag{3}$$

Умножая (2) на $-\sqrt{D}$ и складывая съ уравненіемъ (3), получимъ

$$-\sqrt{D}(P_n - \sqrt{D}\,Q_n) = P_{n+1} - Q_{n+1}\sqrt{D} - a(P_n - Q_n\sqrt{D})$$

или иначе

$$P_{n+1} - Q_{n+1}\sqrt{D} + (\sqrt{D} - a)[P_n - Q_n\sqrt{D})] = 0 ,$$

откуда

$$P_{n+1} + P_n(\sqrt{D} - a) = \sqrt{D}[Q_{n+1} + Q_n(\sqrt{D} - a)]$$

или окончательно

$$\sqrt{D} = \frac{P_{n+1} + P_n(\sqrt{D} - a)}{Q_{n+1} + Q_n(\sqrt{D} - a)} .$$

Если ввести обозначеніе

$$\omega = \frac{1}{\sqrt{D} - a} ; \quad \sqrt{D} = a + \frac{1}{\omega} ,$$

то получимъ

$$\sqrt{D} = \frac{P_{n+1}\omega + P_n}{Q_{n+1}\omega + Q_n} .$$

Итакъ, ω есть полное частное, представляющее величину всей не прерывной дроби, слѣдующей послѣ неполнаго частнаго a_n. Величина ω будетъ, слѣдовательно, положительною неправильною дробью, то есть

$$a = [\sqrt{D}] = a_0 , \quad \sqrt{D} = a_0 + \frac{1}{\omega} .$$

Оказывается, что величина ω представляетъ правильную періодическую часть разложенія и должна начинаться съ начала котораго нибудь изъ періодовъ, то есть должна начинаться непремѣнно съ неполнаго частнаго a_1. Если мы начнемъ съ перваго появленія a_1, то получимъ

$$P_0 = 1 , \quad Q_0 = 0 .$$

т. е. тривіальное рѣшеніе.

Если мы начнемъ ω со второго появленія a_1, то получимъ настоящее рѣшеніе

$$P_n,\ Q_n,$$

которое будетъ наименьшее въ положительныхъ числахъ, ибо, если мы начнемъ ω съ третьяго и дальнѣйшаго появленія a_1, то числа P_n и Q_n будутъ уже больше. Такъ какъ n есть число звеньевъ въ періодѣ непрерывной дроби, а это число мы предположили четнымъ, то періодъ надо брать съ четнымъ числомъ звеньевъ, такъ что если въ періодѣ нечетное число звеньевъ, то надо брать всякій разъ появленіе a_1 черезъ два періода, пропуская по одному разу a_1.

Такъ напримѣръ, возьмемъ случай $D=41$.

Разлагая въ непрерывную дробь, получимъ

$$\sqrt{41}=6,(2,\ 2,\ 12).$$

Для полученія наименьшаго рѣшенія уравненія $x^2-41y^2=1$ придется взять два періода

$$\frac{P_{n+1}}{Q_{n+1}}=6,\ 2,\ 2,\ 12,\ 2,\ 2,\ 12,\ \frac{P_n}{Q_n}=6,\ 2,\ 2,\ 12,\ 2,\ 2,$$

откуда

$$P_n=2049,\ Q_n=320.$$

Въ концѣ книги дана таблица наименьшихъ рѣшеній уравненія Pell'a для всѣхъ значеній D до 100.

§ 53. Покажемъ, какъ по наименьшему положительному рѣшенію Pell'ева уравненія получить всѣ остальныя его рѣшенія.

Возвышая обѣ части уравненія

$$(x+y\sqrt{D})(x-y\sqrt{D})=1$$

въ нѣкоторую степень n, гдѣ n натуральное число, получимъ

$$(x+y\sqrt{D})^n(x-y\sqrt{D})^n=1.$$

Отдѣлимъ раціональную часть отъ ирраціональной въ выраженіи

$$(x+y\sqrt{D})^n=X_n+Y_n\sqrt{D}$$

гдѣ

$$X_n=x^n+\frac{n(n-1)}{1.2}x^{n-2}y^2D+\ldots,$$

$$Y_n=\frac{n}{1}x^{n-1}y+\frac{n(n-1)(n-2)}{1.2.3}x^{n-3}y^3D+\ldots$$

X_n, Y_n суть цѣлыя числа, удовлетворяющія уравненію

$$X_n^2 - DY_n^2 = 1 .$$

Числа X_n, Y_n дадутъ новое рѣшеніе въ положительныхъ числахъ Pell'ева уравненія. Если x, y были наименьшимъ рѣшеніемъ, то покажемъ что числами X_n и Y_n исчерпываются всѣ положительныя рѣшенія уравненія Pell'a. Допустимъ обратное, что существуетъ рѣшеніе t, u, причемъ $t + u\sqrt{D}$ не совпадаетъ съ $(x + y\sqrt{D})^n$. Такъ какъ $(x + y\sqrt{D})^n$ возрастаетъ съ возрастаніемъ n, то число $t + u\sqrt{D}$ должно попасть между двумя послѣдовательными значеніями $(x + y\sqrt{D})^n$

$$(x + y\sqrt{D})^n < t + n\sqrt{D} < (x + y\sqrt{D})^{n+1}$$

умножая всѣ три части неравенства на положительное число $(x - y\sqrt{D})^n$ получимъ

$$1 < (t + u\sqrt{D})(x - y\sqrt{D})^n < x + y\sqrt{D}$$

или, обозначая $(t + u\sqrt{D})(x - y\sqrt{D})^n = \xi + \eta\sqrt{D}$, получимъ

$$1 < \xi + \eta\sqrt{D} < x + y\sqrt{D} .$$

что невозможно, ибо x, y есть наименьшее рѣшеніе.

§ 54. Обращаемся теперь къ разсмотрѣнію уравненія

$$x^2 - Dy^2 = 4 .$$

въ нечетныхъ числахъ при условіи $D \equiv 5 (\mathrm{mod}\ 8)$.

Пусть разложеніе числа $\sqrt{D}$ будетъ

$$\sqrt{D} = a_0, \ a_1, \ a_2, \ \ldots \ a_{n-1}, \ \omega_n ,$$

гдѣ ω_n полное частное, имѣющее, какъ извѣстно, видъ

$$\omega_n = \frac{\sqrt{D} + \alpha_n}{\beta_n} ,$$

гдѣ α_n, β_n цѣлыя положительныя числа

Получаемъ

$$\sqrt{D} = \frac{P_n(\sqrt{D} + \alpha_n) + \beta_n P_{n-1}}{Q_n(\sqrt{D} + \alpha_n) + \beta_n Q_{n-1}} .$$

Сравнивая раціональную часть и ирраціональную, получимъ

$$P_n = Q_n\alpha_n + Q_{n-1}\beta_n \qquad (1)$$

$$DQ_n = P_n\alpha_n + P_{n-1}\beta_n \qquad (2)$$

Умножимъ (1) на P_n, а (2) на $-Q_n$ и сложимъ, тогда получимъ

$$P_n^2 - DQ_n^2 = (-1)^n \beta_n .$$

Получается такое правило для рѣшенія уравненія $x^2 - Dy^2 = \pm 4$ въ нечетныхъ числахъ:

1. *Если среди чиселъ* β_n *не встрѣчается* 4, *то уравненіе невозможно.*

2. *Если въ первый разъ появляется* $\beta_n = 4$, *то уравненіе возможно, причемъ при* n *нечетномъ возможны оба уравненія* $x^2 - Dy^2 = -4$, $x^2 - Dy^2 = 4$, *а при* n *четномъ только уравненіе* $x^2 - Dy^2 = 4$.

Я привожу въ концѣ книги таблицу Cayley рѣшеній $x^2 - Dy^2 = \pm 4$ для всѣхъ значеній D до 1000.

§ 55. Въ §§ 48, 49 мы показали связь между рѣшеніями уравненія Pell'a и числомъ различныхъ подстановокъ, переводящихъ форму даннаго опредѣлителя D въ самое себя.

Въ случаѣ отрицательнаго опредѣлителя число такихъ подстановокъ конечно и равно числу рѣшеній Pell'ева уравненія (см. § 49).

Посмотримъ, сколькими различными подстановками можно перевести форму f въ ей эквивалентную f_1. Если намъ одна такая подстановка S извѣстна, то всѣ подстановки вида

$$\Sigma S, \tag{1}$$

гдѣ Σ переводитъ форму f въ самое себя, будутъ, очевидно, также переводить f въ f_1.

Покажемъ теперь, что обратно всякая подстановка S_1, переводящая форму f въ f_1 имѣетъ видъ (1). Въ самомъ дѣлѣ, подстановка $S_1 S^{-1}$ оставляетъ безъ перемѣны функцію f, ибо первый множитель переводитъ f въ f_1, а второй S^{-1} возвращаетъ обратно къ формѣ f. Итакъ, $S_1 S^{-1} = \Sigma$, откуда $S_1 S^{-1} S = \Sigma S$ или $S_1 = \Sigma S$, что и требовалось доказать.

§ 56. Докажемъ теперь теоремы, приведенныя въ §§ 1, 2.

Разсмотримъ представленіе простого числа p формой $x^2 + y^2 = (1, 0, 1)$ опредѣлителя -4.

Должно имѣть мѣсто сравненіе

$$n^2 \equiv -4 \pmod{4p} \tag{1}$$

полагая $n = 2n'$, получимъ

$$n'^2 \equiv -1 \pmod{p} .$$

Для того чтобы это сравненіе было возможно, необходимо

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1 ,$$

то есть простое число p должно быть вида $4h + 1$.

Сравненіе (1) имѣетъ два корня n_1 и n_2 и мы получаемъ двѣ формы (p, n_1, l_1), (p, n_2, l_2).

На основаніи соображеній § 14 мы имѣемъ въ данномъ случаѣ только одну приведенную форму $(1, 0, 1)$, такъ что всѣ формы опредѣлителя -4 образуютъ одинъ классъ и всѣ эквивалентны между собой. Отсюда мы видимъ, что существуютъ подстановки переводящія форму $(1, 0, 1)$ въ обѣ формы (p, n_1, l_1), (p, n_2, l_2). Принимая во вниманіе, что число рѣшеній уравненія Pell'a въ данномъ случаѣ есть 4, получаемъ максимальное число сказанныхъ подстановокъ $4.2 = 8$. Значитъ таково должно быть максимальное число представленій числа p формой $(1, 0, 1)$.

Съ другой стороны, по одному представленію x, y числа p формой $x^2 + y^2$ получимъ 8 другихъ

$$(\pm x, \pm y), (\pm y, \pm x). \qquad (2)$$

Другихъ представленій, слѣдовательно, быть не можетъ. Но такъ какъ при возвышеніи въ квадратъ знаки x и y не играютъ роли, то приходится всѣ 8 представленій (2) считать за *одно*, и теорема Euler'a доказана.

Подобнымъ же образомъ докажемъ теоремы § 2.

Композиція формъ.

§ 57. Мы упомянемъ теперь объ одномъ изъ важнѣйшихъ открытій Gauss'a въ теоріи квадратичныхъ формъ, открытіи, которое было прообразомъ позднѣйшей теоріи умноженія идеальныхъ чиселъ. Lejeune-Dirichlet и позднѣйшіе авторы значительно упростили теорію Gauss'a.

Gauss устанавливаетъ взглядъ на классы формъ даннаго опредѣлителя, какъ на абелеву группу относительно нѣкотораго дѣйствія, которое онъ назвалъ *композиціей формъ*.

Двѣ формы (a_1, b_1, c_1) и (a_2, b_2, c_2) одного и того же опредѣлителя мы назовемъ *согласными*, если общій наибольшій дѣлитель трехъ чиселъ a_1, a_2, $\frac{b_1 + b_2}{2}$ есть 1. Число $\frac{b_1 + b_2}{2}$, конечно, всегда цѣлое, ибо на основаніи равенства опредѣлителей обѣихъ формъ получается одинаковая четность вторыхъ коэффиціентовъ b_1, и b_2.

Возьмемъ произвольно два класса формъ K_1 и K_2.

Покажемъ, что можно выбрать на безчисленное множество способовъ по одной формѣ изъ каждаго изъ этихъ классовъ такъ, чтобы эти двѣ формы были согласны. Беремъ произвольно форму (a_1, b_1, c_1) изъ класса K_1. Беремъ также произвольную форму (a', b', c') класса K_2. Вслѣдствіе

ея примитивности (см. § 7) можно подставить такія значенія x и y, чтобы форма (a', b', c') давала число взаимно простое съ a_1. Въ самомъ дѣлѣ, разложимъ a_1 на простые множители и пусть одинъ изъ этихъ множителей будетъ p.

Такъ какъ форма (a', b', c') примитивная, то по крайней мѣрѣ одинъ изъ коэффиціентовъ не дѣлится на p. Если этотъ коэффиціентъ есть a', то мы возьмемъ $x \equiv 1 \pmod p$ $y \equiv 0 \pmod p$; если онъ есть b', то возьмемъ $x \equiv 1 \pmod p$ $y \equiv 1 \pmod p$; если онъ есть c', то возьмемъ $x \equiv 0 \pmod p$ $y \equiv 1 \pmod p$. Если мы продѣлаемъ то же самое относительно другихъ простыхъ множителей q, r, ... числа a_1 и удовлетворимъ всѣмъ написаннымъ сравненіямъ, то получимъ значенія x и y, дающія формѣ значеніе a_2 взаимно простое съ a_1. Дѣлаемъ подстановку, чтобы форма (a', b', c') перешла въ эквивалентную (a_2, b_2, c_2), имѣющую первый коэффиціентъ a_2 взаимно простой съ a_1. Очевидно, что формы (a_1, b_1, c_1) и (a_2, b_2, c_2) согласныя.

Итакъ, если взять согласныя формы (a_1, b_1, c_1), (a_2, b_2, c_2) то можно найти число B удовлетворяющее тремъ сравненіямъ

$$B \equiv b_1 \pmod{2a_1}, \quad B \equiv b_2 \pmod{2a_2}, \quad B^2 \equiv D \pmod{4a_1a_2}. \tag{1}$$

Въ самомъ дѣлѣ, изъ первыхъ двухъ сравненій получимъ

$$(B - b_1)(B - b_2) \equiv 0 \pmod{4a_1a_2},$$

далѣе

$$B^2 - (B - b_1)(B - b_2) \equiv D \pmod{4a_1a_2}$$

или окончательно

$$\frac{b_1 + b_2}{2} B \equiv \frac{D + b_1b_2}{2} \pmod{2a_1a_2}.$$

Число $\frac{D + b_1b_2}{2}$ цѣлое вслѣдствіе одинаковой четности трехъ чиселъ D, b_1, b_2.

Для нахожденія числа B придется удовлетворить тремъ сравненіямъ первой степени

$$\begin{gathered} a_2B \equiv a_2b_1 \pmod{2a_1a_2}, \quad a_1B \equiv a_1b_2 \pmod{2a_1a_2} \\ \frac{b_1 + b_2}{2} B \equiv \frac{D + b_1b_2}{2} \pmod{2a_1a_2}. \end{gathered} \tag{2}$$

Покажемъ прежде всего, что они совмѣстны между собой. Если мы исключимъ B изъ первыхъ двухъ, то получимъ $a_1a_2 (b_1 - b_2) \equiv 0 \pmod{2a_1a_2}$, что, дѣйствительно, имѣетъ мѣсто, ибо число $b_1 - b_2$ четное.

Подобнымъ же образомъ провѣримъ совмѣстность перваго съ третьимъ.

Итакъ, долженъ существовать одинъ классъ чиселъ B по модулю $2a_1a_2$, удовлетворяющій сравненіямъ (2), а, слѣдовательно и сравненіямъ (1).

Подбираемъ [1]) три цѣлыхъ числа ξ, η, ζ такія, чтобы было

$$a_1\xi + a_2\eta + \frac{b_1+b_2}{2}\zeta = 1 .$$

Получимъ

$$B \equiv a_1b_2\xi + a_2b_1\eta + \frac{D+b_1b_2}{2}\zeta \pmod{2a_1a_2} .$$

§ 58. На основаніи третьяго сравненія (1) § 57 число $B^2 - D$ дѣлится на $4a_1a_2$. Обозначимъ черезъ C результатъ этого дѣленія, такъ что $D = B^2 - 4a_1a_2C$.

Въ классѣ K_1 существуетъ форма (a_1, B, a_2C) параллельная на основаніи перваго сравненія (1) § 57 формѣ (a_1, b_1, c_1), а во второмъ классѣ K_2 форма (a_2, B, a_1c). Gauss'ова композиція формъ основана на тождествѣ

$$(a_1x_1^2 + Bx_1y_1 + a_2Cy_1^2)(a_2x_2^2 + Bx_2y_2 + a_1Cy_2^2) =$$

$$= a_1a_2X^2 + BXY + CY^2, \qquad (1)$$

гдѣ

$$X = x_1x_2 - Cy_1y_2, \quad Y = \frac{1}{2}[(2a_1x_1 + By_1)y_2 + (2a_2x_2 + By_2)y_1] .$$

Проще всего провѣрить справедливость тождества (1), если сначала провѣрить такое тождество

$$[2a_1x_1 + (B + \sqrt{D})y_1][2a_2x_2 + (B + \sqrt{D})y_2] =$$

$$= 2a_1a_2X + (B + \sqrt{D})Y \qquad (2)$$

а потомъ тождество (2) умножить на сопряженное съ нимъ, то есть, получающееся изъ него черезъ замѣну $+\sqrt{D}$ на $-\sqrt{D}$.

---

[1]) Если даны три числа a, b, c, то можно подобрать три цѣлыхъ числа x, y, z такимъ образомъ, чтобы было

$$ax + by + cz = \mu$$

гдѣ μ есть общій наибольшій дѣлитель a, b, c. Пусть наибольшій общій дѣлитель чиселъ a и b будетъ ν, тогда при помощи алгоритма Эвклида мы получимъ два цѣлыхъ числа u и v такихъ, чтобы было $au + bv = \nu$. Такъ какъ общій наибольшій дѣлитель ν и c есть μ, то мы получаемъ числа t и z такъ, чтобы было $\nu t + cz = \mu$. Окончательно $x = ut$, $y = vt$.

Форму $(a_1a_2,\ B,\ C)$ согласно Gauss'у называютъ *происходящею отъ композиціи двухъ заданныхъ* $(a_1,\ b_1,\ c_1)$ и $(a_2,\ b_2,\ c_2)$.

Замѣчательно, что если формы подлежащія композиціи пробѣгаютъ два опредѣленныхъ класса K_1 и K_2, то форма получающаяся въ результатѣ композиціи будетъ пробѣгать вполнѣ опредѣленный классъ K_3. Не останавливаясь на доказательствѣ этого предложенія отошлемъ читателя къ литературѣ вопроса.

Gauss. Disquisitiones arithmeticae §§ 234—244.

Lejeune-Dirichlet. De formarum binarium secundi gradus compositione 1851. Ges. Werke Bd. II, S. 105 –114.

Dirichlet-Dedekind. Vorlesungen uber Zahlentheorie, 4 Aufl. § 145.

Mertens. Ueber die Komposition der binären quadratischen Formen 1895 Sitrungsb. d. Wiener Akademie Bd. 104.

Dedekind. Ueber binäre trilineare Formen. Crelles Journ. Bd. 129. 1905.

Weber. Ueber die Komposition der quadratischen Formen. Götting. Nachr. 1907.

I. de Seguier. Formes quadratiques et multiplication complexe. Berlin 1894.

Weber. Lehrbuch der Algebra Bd. III.

Bernais. Ueber die Darstellung von positiven ganzen Zahlen durch die primitiven binären quadratischen Formen einer nicht quadratischen Diskriminante. Göttingen (Diss.) 1912.

На основаніи сказаннаго мы видимъ, что композиція формъ даетъ въ сущности композицію классовъ, которую можно обозначить символически

$$K_1K_2 = K_3.$$

Покажемъ, что классы образуютъ относительно композиціи абелеву группу.

Коммутативный и ассоціативный законы, очевидно, имѣютъ мѣсто. Остается только убѣдиться въ существованіи единицы группы и обратнаго элемента.

Очевидно, что групповой *единицей* будетъ тотъ классъ $K_0 = 1$, въ которомъ представляется формой число 1. Возьмемъ $a_2 = 1$, тогда мы замѣчаемъ, что форма $(a_1,\ B,\ C)$, компонированная съ $(1,\ B,\ a_1\ C)$ даетъ $(a_1,\ B,\ C)$, т. е. $K_1K_0 = K_1$.

Обратный классъ для класса, къ которому принадлежитъ форма $(a,\ b,\ c)$, будетъ тотъ, въ составъ котораго входитъ обратная форма

$(a, -b, c)$ или prorpiе-эквивалентная съ нею форма (c, b, a). Очевидно, что отъ композиціи формы (a, b, c) съ формой (c, b, a) получается форма $(ac, b, 1)$, принадлежащая къ единичному классу. Итакъ, обратный элементъ нашей группы есть тотъ обратный классъ, о которомъ мы говорили въ § 43.

Основанія теоріи группъ, изложенныя нами въ главѣ VI, показываютъ, что существуетъ только одинъ классъ, представляющій единицу группы. Этотъ классъ слѣдуя Gauss'у называютъ *главнымъ*. Мы его будемъ обозначать знакомъ 1. Подобнымъ же образомъ для каждаго класса K существуетъ одинъ ему обратный K^{-1}.

Классъ ancerps A совпадаетъ со своимъ обратнымъ т. е.

$$A^2 = 1.$$

§ 59. Мы обозначаемъ композицію классовъ знакомъ алгебраическаго умноженія. Gauss употреблялъ для этой цѣли знакъ сложенія, такъ что вмѣсто A^2 онъ писалъ $A + A = 2A$, поэтому, слѣдуя его терминологіи говорятъ и теперь, что классъ A^2 происходитъ отъ *удвоенія* класса A. Равенство (3) можетъ быть высказано на словахъ такъ: *классъ ancerps есть тотъ, который при удвоеніи даетъ главный.*

Если мы будемъ удваивать классы не ancerps, то будутъ получаться классы, не совпадающіе съ главнымъ.

Совокупность классовъ ancerps образуетъ подгруппу, ибо изъ $A^2 = 1$, $A_1{}^2 = 1$ получается $(AA_1)^2 = 1$.

Обозначимъ черезъ g индексъ этой подгруппы $\mathfrak{A}$, тогда вся группа классовъ разбивается на g сопряженныхъ системъ

$$\mathfrak{A},\ \mathfrak{A}K_1,\ \mathfrak{A}K_2,\ \ldots\ \mathfrak{A}K_{g-1}. \qquad (1)$$

Удваивая классы (1) получаемъ классы

$$1,\ K_1{}^2,\ K_2{}^2,\ \ldots\ K^2{}_{g-1}. \qquad (2)$$

Покажемъ, что классы (2) образуютъ группу.

Для этой цѣли покажемъ, что всѣ они различны, ибо если $K_2{}^2 = K_1{}^2$, то $(K_2K_1{}^{-1})^2 = 1$, то есть $K_2K_1{}^{-1} = A$, гдѣ A есть ancerps. Мы получаемъ $K_2 = AK_1$, что невозможно, ибо, раскладывая на сопряженныя системы, мы предполагаемъ, что K_2 не заключается въ системѣ $\mathfrak{A}K_1$.

Группа (2) порядка g есть, очевидно, нѣкоторая подгруппа $\mathfrak{G}$ группы классовъ съ индексомъ m. Разобьемъ всю группу классовъ на сопряженныя системы относительно подгруппы $\mathfrak{G}$.

$$\mathfrak{G},\ \mathfrak{G}L_1,\ \mathfrak{G}L_2,\ \ldots\ \mathfrak{G}L_{m-1}. \qquad (3)$$

Системы (3) Gauss называетъ *родами* (Genera) формъ, причемъ подгруппу $\mathfrak{G}$ называетъ *главнымъ родомъ*.

Обозначая черезъ h число всѣхъ классовъ, а черезъ i число классовъ ancеps, получимъ на основаніи (1) и (3).

$$h = ig = gm$$

откуда $i = m$ т. е. *число родовъ равно числу классовъ ancеps.*

Оказывается, что число родовъ имѣетъ всегда видъ 2^{μ}, гдѣ μ цѣлое число, зависящее отъ числа простыхъ множителей входящихъ въ составъ опредѣлителя D.

ГЛАВА XII.

Общая теорія алгебраическихъ чиселъ.

§ 1. Если мы обратимъ вниманіе на простѣйшее поле, поле раціональныхъ чиселъ, то мы замѣчаемъ, что числа его распадаются на двѣ категоріи: числа *цѣлыя* и числа *дробныя*. Цѣлыя числа суть тѣ, надъ которыми оперируетъ главнымъ образомъ элементарная теорія чиселъ. Числа дробныя происходятъ отъ дѣленія чиселъ цѣлыхъ.

§ 2. Оказалось важнымъ и необходимымъ сдѣлать нѣчто подобное для произвольнаго числового поля. Kronecker называетъ Integritätsbereich совокупность чиселъ поля, которыя можно назвать по аналогіи съ раціональнымъ полемъ *цѣлыми числами поля*. Integritätsbereich надо подобрать такимъ образомъ, чтобы возможно большая аналогія связывала новыя цѣлыя числа съ элементарными раціональными цѣлыми числами. Остальныя числа поля, которыя можно называть дробными, должны получаться изъ цѣлыхъ черезъ дѣленіе.

Особенно важнымъ оказалось разсмотрѣніе *алгебраическихъ полей* (глава VII) и, слѣдовательно, разсмотрѣніе, такъ называемыхъ чиселъ *цѣлыхъ алгебраическихъ*.

Не сразу было найдено въ наукѣ современное опредѣленіе понятія о цѣломъ алгебраическомъ числѣ. Должны были предшествовать изслѣдованія, выяснившія важность новаго понятія и давшія возможность шагъ за шагомъ придти къ построенію его.

Первый шагъ введенія чиселъ алгебраическихъ сдѣланъ былъ Gauss'омъ, который сталъ разсматривать *цѣлыя комплексныя числа* вида

$$A + Bi,$$

гдѣ $i = \sqrt{-1}$, а A и B обыкновенныя цѣлыя раціональныя числа. Gauss, очевидно, разсматривалъ поле, получаемое отъ присоединенія къ раціональному полю корня i алгебраическаго уравненія $i^2 + 1 = 0$.

Слѣдуя Gauss'у, надо считать элементы

$$x + iy$$

этого поля цѣлыми, если x и y числа цѣлыя, и дробными въ обратномъ случаѣ.

Такъ напримѣръ, для Gauss'ова поля число $2 + 3i$ есть цѣлое, тогда какъ число $\frac{3}{4} + \frac{1}{2}i$ дробное. Gauss ввелъ цѣлыя комплексныя числа, имѣя вполнѣ опредѣленную цѣль, обобщить данный имъ законъ взаимности съ квадратичныхъ вычетовъ на вычеты четвертой степени или, какъ онъ называлъ, на *биквадратичные вычеты*. Gauss замѣтилъ, что нельзя провести настоящей аналогіи, если остаться при прежнихъ цѣлыхъ раціональныхъ числахъ.

Gauss'овы числа обратили на себя особенное вниманіе математиковъ. Eisenstein доказалъ оставшійся у Gauss'а не доказаннымъ во всѣхъ частяхъ законъ взаимности для биквадратичныхъ вычетовъ. Онъ далъ, основываясь на небольшой замѣткѣ Jacobi, законъ взаимности для кубическихъ вычетовъ, для чего пришлось разсматривать поле чиселъ

$$x + \alpha y$$

гдѣ x и y раціональныя числа, символъ же α опредѣляетъ мнимый корень уравненія $\alpha^3 - 1 = 0$.

Lejeune-Dirichlet еще болѣе обратилъ вниманіе математиковъ на пользу введенія чиселъ алгебраическихъ своими знаменитыми изслѣдованіями о квадратичныхъ формахъ съ мнимыми (Gauss'овыми) коэффиціентами.

Дальнѣйшій толчекъ въ пользу теоріи чиселъ алгебраическихъ дали знаменитыя изслѣдованія Kummer'а о задачѣ Fermat'а, упомянутой въ § 34 главы I. Kummer'у приходилось обобщить Gauss'а и Eisenstein'а въ въ томъ смыслѣ, что онъ разсматривалъ поля, получаемыя отъ присоединенія къ раціональному полю корней двучленныхъ уравненій

$$x^n - 1 = 0.$$

Тутъ Kummer'у помогли геніальныя изслѣдованія Gauss'а, изложенныя подъ названіемъ *дѣленія круга* въ его „Disquisitiones arithmeticae".

Съ тѣхъ поръ поля, получаемыя отъ присоединенія корней двучленныхъ уравненій, называются *полями дѣленія круга*.

3. Когда желали обобщить изслѣдованія указанныхъ авторовъ на случай произвольнаго алгебраическаго поля чиселъ

$$\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_{n-1} x^{n-1} \qquad (1)$$

тогда сначала было дано такое опредѣленіе цѣлаго числа въ этомъ полѣ:

Число (1) будетъ цѣлымъ числомъ поля, если всѣ раціональные коэффиціенты a_0, a_1, ... a_{n-1} *суть числа цѣлыя раціональныя.*

Хотя получились хорошія обобщенія, но вскорѣ обнаружилось, что указанная такимъ образомъ совокупность цѣлыхъ чиселъ не можетъ считаться настоящимъ Integritätsbereich'омъ поля.

По терминологіи Dedekind'а получается такимъ образомъ *порядокъ въ полѣ* (Zahlring), который только въ извѣстныхъ случаяхъ совпадаетъ съ настоящимъ Integritätsbereich'омъ.

Оказалось, что въ случаѣ квадратичнаго поля, а также поля дѣленія круга это совпаденіе имѣетъ мѣсто.

§ 4. Чтобы дать настоящее опредѣленіе, нынѣ принятое, цѣлости алгебраическаго числа, надо разсмотрѣть уравненіе, которому оно удовлетворяетъ.

Такъ, напримѣръ, Gauss'ово число $x = 4 + i5$ удовлетворяетъ уравненію $(x-4)^2 + 5^2 = 0$, или что одно и тоже

$$x^2 - 8x + 41 = 0.$$

Оказалось, что для „*цѣлости*“ алгебраическаго числа характерна нецѣлость его коэффиціентовъ, а *равенство единицѣ* старшаго коэффиціента уравненія, которому оно удовлетворяетъ, *при цѣлости другихъ* коэффиціентовъ этого уравненія.

Перейдемъ поэтому къ изложенію настоящей теоріи цѣлыхъ алгебраическихъ чиселъ.

§ 5. Всякое *раціональное число* можно разсматривать какъ корень уравненія первой степени.

$$a_0 x + a_1 = 0$$

съ цѣлыми коэффиціентами a_0 и a_1; если коэффиціентъ a_0 при неизвѣстномъ x есть единица, то x обращается въ цѣлое число.

§ 6. Мы повторимъ, что *алгебраическимъ* числомъ называется всякій корень уравненія

$$a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_{n-1} x + a_n = 0$$

гдѣ коэффиціенты a_0, a_1, a_2, ... a_{n-1}, a_n суть числа цѣлыя. Эти коэффиціенты можно считать не имѣющими общаго дѣлителя.

Если коэффиціентъ a_0 при старшей степени есть единица, то корень x уравненія носитъ названіе *цѣлаго алгебраическаго числа.*

§ 7. Цѣлыя алгебраическія числа заключаютъ, какъ частный случай, обыкновенныя цѣлыя числа. Эти послѣднія мы будемъ называть поэтому *цѣлыми раціональными числами.*

Можно доказать, что *если цѣлое алгебраическое число есть раціональное, то оно будетъ цѣлымъ раціональнымъ.*

Въ самомъ дѣлѣ, пусть $x = \frac{u}{v}$, гдѣ u и v суть взаимно простыя цѣлыя раціональныя числа, удовлетворяетъ уравненію

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n = 0,$$

гдѣ a_1, a_2, $\ldots$ a_n цѣлыя раціональныя числа; получаемъ

$$u^n + a_1 u^{n-1} v + a_2 u^{n-2} v^2 + \ldots + a_n v^n = 0.$$

Отсюда видимъ, что всякій простой дѣлитель числа v долженъ входить множителемъ въ число u^n, а, слѣдовательно, и въ число u. Итакъ, мы видимъ, что x не должно имѣть другого знаменателя v кромѣ единицы.

§ 8. *Сумма, разность и произведеніе двухъ цѣлыхъ алгебраическихъ чиселъ есть также цѣлое число.*

Пусть два числа α и β опредѣляются уравненіями

$$\begin{aligned} \alpha^\mu + a_1 \alpha^{\mu-1} + \ldots + a_{\mu-1}\alpha + a_\mu = 0 \\ \beta^\nu + b_1 \beta^{\nu-1} + \ldots + b_{\nu-1}\alpha + b_\nu = 0. \end{aligned} \tag{1}$$

Обозначимъ черезъ ω одно изъ трехъ чиселъ $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$. Положимъ $\mu\nu = m$ и разсмотримъ m величинъ

$$\alpha^r \beta^s$$

$$r = 0, 1, 2, \ldots \mu - 1; \quad s = 0, 1, 2, \ldots \nu - 1.$$

Пусть эти величины будутъ

$$\omega_1, \omega_2, \omega_3, \ldots \omega_m. \tag{2}$$

На основаніи уравненій (1) можно будетъ представить произведенія

$$\omega\omega_1, \omega\omega_2, \omega\omega_3, \ldots \omega\omega_m$$

линейно черезъ величины (2), т. е.

$$\omega\omega_p = c_{p,1}\omega_1 + c_{p,2}\omega_2 + \ldots c_{p,m}\omega_m \tag{3}$$

$$(p = 1, 2, 3, \ldots m),$$

гдѣ $c_{p,q}$ суть цѣлыя раціональныя числа.

Исключая изъ уравненій (3) числа $\omega_1, \omega_2, \ldots \omega_m$, получимъ

$$\begin{vmatrix} c_{1,1}-\omega, & c_{1,2}, & \ldots & c_{1,m} \\ c_{2,1}, & c_{2,2}-\omega, & \ldots & c_{2,m} \\ \ldots & \ldots & \ldots & \ldots \\ c_{m,1}, & c_{m,2}, & \ldots & c_{m,m}-\omega \end{vmatrix} = 0.$$

Это уравненіе въ раскрытомъ видѣ будетъ

$$\omega^m + C_1\omega^{m-1} + C_2\omega^{m-2} + \ldots + C_m = 0,$$

гдѣ $C_1, C_2, C_3 \ldots C_m$ суть цѣлыя раціональныя числа.

Итакъ, мы видимъ, что ω есть цѣлое число.

§ 9. *Если въ уравненіи*

$$x^\nu + \alpha_1 x^{\nu-1} + \ldots + \alpha_{\nu-1}x + \alpha_\nu = 0 \qquad (1)$$

всѣ коэффиціенты $\alpha_1, \alpha_2, \ldots \alpha_\nu$ *суть цѣлыя алгебраическія числа, то и* x *будетъ цѣлое алгебраическое число.*

По предположенію числа $\alpha_1, \alpha_2, \ldots \alpha_\nu$ удовлетворяютъ извѣстнымъ уравненіемъ съ цѣлыми коэффиціентами. Обозначимъ совокупность этихъ уравненій черезъ Σ.

Подставимъ въ лѣвую часть уравненія (1) всевозможныя комбинаціи корней этихъ уравненій Σ и перемножимъ полученныя выраженія. Получимъ уравненіе, въ которомъ въ первой части будетъ цѣлая функція отъ x съ коэффиціентомъ равнымъ единицѣ при высшей степени x. Остальные коэффиціенты будутъ симметрическія функціи отъ корней всѣхъ уравненій Σ. Очевидно съ одной стороны, что эти коэффиціенты выразятся раціонально черезъ коэффиціенты уравненій Σ, т. е. будутъ числами раціональными; съ другой стороны, эти коэффиціенты суть цѣлыя симметрическія функціи отъ корней уравненій Σ, т. е. отъ цѣлыхъ алгебраическихъ чиселъ, слѣдовательно, они будутъ цѣлыми алгебраическими числами. Итакъ мы видимъ, что эти коэффиціенты суть цѣлыя раціональныя числа. Значитъ x будетъ цѣлымъ алгебраическимъ числомъ.

§ 10. Если уравненіе $F(x) = 0$, которое опредѣляетъ цѣлое алгебраическое число α приводимо въ раціональномъ полѣ, то будетъ существовать неприводимый множитель $f(x)$ съ раціональными коэффиціентами, который имѣетъ корнемъ α. Уравненіе

$$f(x) = 0$$

можно будетъ написать такъ

$$x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots + p_n = 0,$$

гдѣ p_1, p_2, $\ldots p_n$ числа раціональныя.

Каждый изъ корней α уравненія $F(x) = 0$, есть цѣлое алгебраическое число, слѣдовательно, корни уравненія $f(x) = 0$ суть числа цѣлыя, ибо эти корни суть нѣкоторые изъ корней уравненія $F(x) = 0$.

Коэффиціенты p_1, p_2, $\ldots p_n$ получаются изъ корней только при помощи дѣйствій сложенія и умноженія. Слѣдовательно, эти коэффиціенты должны быть цѣлыми алгебраическими числами; но эти коэффиціенты числа раціональныя, слѣдовательно, они суть цѣлые раціональные. Мы приходимъ къ теоремѣ.

Всякое цѣлое алгебраическое число есть корень неприводимаго уравненія съ цѣлыми раціональными коэффиціентами причемъ коэффиціентъ при старшей степени равенъ единицѣ.

Назовемъ для сокращенія *примарною* цѣлую функцію съ цѣлыми коэффиціентами, у которой старшій коэффиціентъ равенъ единицѣ.

Попутно получаемъ доказательство знаменитой теоремы Gauss'a.

Раціональный [1]) *дѣлитель примарной функціи съ коэффиціентомъ равнымъ единицѣ у старшаго члена есть функція примарная.*

§ 11. *Всякое алгебраическое число ω можетъ быть умноженіемъ на нѣкоторое натуральное число обращено въ цѣлое алгебраическое.*

Если алгебраическое число ω не цѣлое, то оно удовлетворяетъ уравненію

$$\omega^n + A_1\omega^{n-1} + \ldots + A_n = 0, \qquad (1)$$

гдѣ раціональные коэффиціенты A_1, A_2, $\ldots A_n$ не всѣ цѣлые. Обозначая черезъ a общаго знаменателя всѣхъ дробныхъ коэффиціентовъ, можно представить уравненіе (1) въ такомъ видѣ

$$(a\omega)^n + A_1 a(a\omega)^{n-1} + A_2 a^2(a\omega)^{n-2} + \ldots + A_n a^n = 0$$

и, слѣдовательно, число $a\omega$ будетъ цѣлымъ алгебраическимъ.

§ 12. Если цѣлое алгебраическое число α есть произведеніе двухъ цѣлыхъ алгебраическихъ чиселъ β и γ, т. е. $\alpha = \beta\gamma$, то говорятъ, что число α *дѣлится* на число β, а число β называютъ *множителемъ* или *дѣлителемъ* числа α, или иначе, говорятъ, что число β входитъ множителемъ въ число α. Если мы цѣлыя алгебраическія числа не подвергнемъ

[1]) Съ раціональными коэффиціентами.

никакимъ ограниченіямъ, то у насъ не получится аналогіи съ теоріей дѣлимости цѣлыхъ раціональныхъ чиселъ.

Въ самомъ дѣлѣ, если α цѣлое алгебраическое число, то очевидно, что и $\sqrt{\alpha}$ будетъ цѣлымъ алгебраическимъ числомъ. Съ другой стороны $\sqrt{\alpha}$ будетъ дѣлителемъ числа α, и значитъ, въ общей области всѣхъ чиселъ алгебраическихъ существуетъ неограниченная разложимость на множители, такъ что аналогія съ цѣлыми раціональными числами падаетъ, ибо не будетъ существовать самаго важнаго понятія, понятія о простомъ числѣ, не разложимомъ далѣе на множители. Для достиженія аналогіи съ раціональными числами надо разсматривать поле.

Фундаментальный базисъ.

§ 13. Обозначимъ черезъ Ω раціональное поле. Присоединимъ къ нему нѣкоторое цѣлое алгебраическое число θ, тогда поле $\Omega(\theta)$ будетъ представлять совокупность чиселъ вида

$$\omega = x_0 + x_1\theta + x_2\theta^2 + \ldots + x_{n-1}\theta^{n-1},$$

гдѣ n есть степень неприводимаго въ Ω уравненія, которому удовлетворяетъ алгебраическое число θ.

Будемъ раціональные коэффиціенты $x_0, x_1, x_2 \ldots x_{n-1}$ называть *координатами* числа ω. Числами поля $\Omega(\theta)$ степени n можно заполнить плотнымъ [1]) образомъ n-мѣрное пространство. Для квадратичнаго поля можно разсматривать плоскость, для кубическаго трехмѣрное пространство.

§ 14. Посмотримъ какимъ точкамъ пространства соотвѣтствуютъ цѣлыя алгебраическія числа.

Нетрудно убѣдиться, что при цѣлыхъ координатахъ число ω будетъ цѣлымъ алгебраическимъ, ибо если θ цѣлое число, то и степени $\theta^2, \theta^3, \ldots \theta^{n-1}$ будутъ также цѣлыми.

Совокупность точекъ n-мѣрнаго пространства, имѣющихъ цѣлыя координаты, мы назовемъ *основною точечной сѣтью*. На плоскости получимъ вершины квадратовъ, стороны которыхъ равны единицѣ и на которые разбита вся плоскость прямыми, параллельными осямъ координатъ.

Основная точечная сѣть даетъ возможность разбить все пространство на равновеликіе *основныя ячейки*; эти ячейки суть квадраты при двухмѣрномъ пространствѣ и кубы въ случаѣ трехъ измѣреній.

---

[1]) Не непрерывно, ибо точки съ ирраціональными координатами пропускаются.

§ 15. Итакъ, точки основной сѣти соотвѣтствуютъ цѣлымъ алгебраическимъ числамъ. Оказывается, что и внутрь основныхъ ячеекъ могутъ попадать цѣлыя алгебраическія числа. Лучше всего разобрать вопросъ на случаѣ квадратичнаго поля.

Можно сказать, что всякое квадратичное поле образовано числами

$$\omega = x + \theta y, \qquad (1)$$

гдѣ θ корень квадратнаго уравненія

$$\theta^2 - d = 0,$$

причемъ d цѣлое раціональное число (безразлично положительное или отрицательное), не имѣющее квадратныхъ дѣлителей.

Поставимъ вопросъ, не могутъ ли существовать цѣлыя алгебраическія числа ω при дробныхъ координатахъ x и y. Приведемъ эти координаты къ наименьшему общему знаменателю.

$$x = \frac{\xi}{\zeta}, \quad y = \frac{\eta}{\zeta},$$

гдѣ три числа ξ, η, ζ не имѣютъ общихъ дѣлителей.

Составимъ квадратное уравненіе

$$\omega^2 - A\omega + B = 0,$$

которому удовлетворяетъ число ω.

$$A = \frac{2\xi}{\zeta}, \quad B = \frac{\xi^2 - d\eta^2}{\zeta^2}.$$

Для цѣлости числа ω, должны быть цѣлыми числа A и B.

Числа ξ и ζ должны быть взаимно простыя, ибо допустивъ существованіе у нихъ общаго простого дѣлителя p мы получимъ на основаніи требованія цѣлости числа B и на основаніи недѣлимости на p числа η дѣлимость на p^2 числа d, что противорѣчитъ предположенію. Итакъ единственное возможное предположеніе есть $\zeta = 2$, ибо A должно быть цѣлымъ числомъ. Но тогда $\xi = 2u + 1$; число η должно быть также нечетнымъ $\eta = 2v + 1$, и кромѣ того, очевидно, должно быть

$$d \equiv 1 \pmod 4,$$

ибо число $\frac{\xi^2 - d\eta^2}{4}$ должно быть цѣлымъ.

Итакъ, въ случаѣ $d \equiv 1 \pmod 4$ кромѣ основной сѣти получаемъ сѣть точекъ съ координатами

$$x = \frac{\xi}{\zeta} = \frac{2u+1}{2} = u + \frac{1}{2}, \quad y = v + \frac{1}{2},$$

гдѣ u и v произвольныя цѣлыя числа. Новыя точки даютъ центры основныхъ ячеекъ.

Сказанное можно резюмировать въ такой теоремѣ

Если $d \equiv 2, 3 \pmod 4$, *то всѣ цѣлыя числа поля получаются по формулѣ*

$$x + \theta y,$$

если же $d \equiv 1 \pmod 4$, *то всѣ цѣлыя числа поля получаются по формулѣ*

$$x + y\frac{1+\theta}{2}$$

при цѣлыхъ раціональныхъ x и y.

§ 16. Разсужденія § 15 обобщаются на случай поля произвольной степени.

Въ каждомъ полѣ степени n можно указать такую систему n цѣлыхъ алгебраическихъ чиселъ

$$\omega_1, \omega_2, \ldots \omega_n, \tag{1}$$

что всѣ цѣлыя числа поля получаются по формулѣ

$$x_1\omega_1 + x_2\omega_2 + \ldots + x_n\omega_n$$

при цѣлыхъ раціональныхъ значеніяхъ координатъ x_i.

Система чиселъ (1) образуетъ такъ называемый *фундаментальный базисъ* поля.

§ 17. Нахожденіе фундаментальнаго базиса въ общемъ случаѣ представляетъ трудную задачу.

Проф. А. Марковъ далъ видъ фундаментальнаго базиса для поля, зависящаго отъ корня уравненія $x^3 = A$.

Чтобы образовать всѣ цѣлыя алгебраическія числа, зависящія отъ $\sqrt[3]{A}$, *прежде всего надо выдѣлить изъ* A *квадратные множители (предполагается, что* A *не содержитъ кубическихъ множителей), т. е. представить* A *подъ видомъ* a^2b. *Тогда, подразумѣвая подъ* x, y, z *произвольныя цѣлыя раціональныя числа, всѣ цѣлыя числа, зависящія отъ* $\sqrt[3]{A}$, *можно представить подъ видомъ*

$$x + y\sqrt[3]{a^2b} + z\sqrt[3]{ab^2}$$

при A не $\equiv \pm 1 \pmod 9$ *и подъ видомъ*

$$x\frac{1+b\sqrt[3]{a^2b}+a\sqrt[3]{ab^2}}{3}+y\sqrt[3]{a^2b}+z\sqrt[3]{ab^2}$$

при $A \equiv \pm 1 \pmod 9$.

Эта теорема доказана И. Ивановымъ въ сочиненіи „Цѣлыя комплексныя числа“ СПБ. 1891.

Теорема А. Маркова была обобщена Г. Воронымъ на случай общаго кубическаго поля въ сочиненіи „О цѣлыхъ алгебраическихъ числахъ, зависящихъ отъ корня уравненія 3-й степени“ СПБ. 1894.

Теорему Вороного можно формулировать такъ:

Всякое цѣлое алгебраическое число кубическаго поля имѣетъ видъ

$$x+y\alpha+z\frac{k}{\alpha},$$

гдѣ x, y, z числа цѣлыя раціональныя, α есть нѣкоторое приличнымъ образомъ выбранное изъ поля цѣлое алгебраическое число, а k есть наименьшее натуральное число обращающее число

$$\frac{k}{\alpha}$$

въ цѣлое алгебраическое.

§ 18. Пусть корни основного уравненія, которому удовлетворяетъ число θ, образующее поле $\Omega(\theta)$, будутъ

$$\theta,\ \theta',\ \theta'',\ \ldots \qquad (1)$$

Значенія

$$\omega,\ \omega',\ \omega'',\ \ldots$$

получаемыя изъ $\omega = \varphi(\theta)$ послѣ подстановки вмѣсто θ величинъ (1) носятъ названіе чиселъ *сопряженныхъ* съ числомъ ω.

Возьмемъ фундаментальный базисъ

$$\omega_1,\ \omega_2,\ \ldots\ \omega_n$$

и разсмотримъ квадратъ опредѣлителя

$$\begin{vmatrix} \omega_1 & \omega_2 \ldots \omega_n \\ \omega_1' & \omega_2' \ldots \omega_n' \\ \omega_1'' & \omega'' \ldots \omega_n'' \\ \ldots & \ldots \end{vmatrix} = D.$$

Этотъ квадратъ будетъ симметрическою функціею отъ корней (1) основного уравненія, значитъ онъ будетъ раціональнымъ числомъ. Это раціональное число должно быть обязательно цѣлымъ, ибо опредѣлитель есть цѣлая функціи отъ цѣлыхъ чиселъ поля.

Цѣлое раціональное число D носитъ названіе *основного числа* поля. Минковскій доказалъ, что это число не можетъ равняться 1.

Если поле *простѣйшее*, то есть, если фундаментальный базисъ состоитъ изъ степеней одного и того же числа поля

$$1, \zeta, \zeta^2, \ldots \zeta^{n-1} \tag{2}$$

то квадратъ опредѣлителя обращается [1]) въ дискриминантъ $\Delta(\zeta)$ числа ζ.

Простыя разсужденія приводятъ для всякаго числа ζ поля къ формулѣ

$$\Delta(\zeta) = A^2.D, \tag{3}$$

гдѣ A натуральное число, которое можетъ равняться единицѣ, если (2) будетъ фундаментальнымъ базисомъ. Число A называютъ *индексомъ* числа ζ.

Итакъ, мы видимъ, что основное число есть общій дѣлитель дискриминантовъ всѣхъ ирраціональныхъ чиселъ поля. Дискриминантъ раціональнаго числа есть нуль, ибо для числа раціональнаго числа сопряженныя совпадаютъ съ самимъ числомъ.

Для того, чтобы поле было простѣйшимъ, необходимо, чтобы существовало въ полѣ по крайней мѣрѣ одно число съ индексомъ равнымъ единицѣ.

Такъ, напримѣръ, квадратичное поле всегда простѣйшее, ибо его фундаментальный базисъ

$$1, \zeta$$

гдѣ ζ или θ, или $\frac{1+\theta}{2}$.

Для нѣкоторыхъ полей легко убѣдиться, что они не простѣйшія, ибо существуютъ опредѣленныя простыя числа p, которыя входятъ въ индексы всѣхъ ирраціональныхъ чиселъ поля. Такія простыя числа p называются *особенными* (ausserwesentliche gemeinschaftliche Discriminantenteiler).

Проф. Ермаковъ замѣтилъ, что для кубическаго поля такимъ особеннымъ числомъ можетъ быть только 2. Студентъ Б. Делоне далъ на засѣданіяхъ моего семинара по теоріи чиселъ въ Кіевскомъ Университетѣ очень хорошее доказательство этой теоремы.

---

[1]) Д. Граве. Курсъ алгебраическаго анализа. Кіевъ 1910.

Студентъ Е. Жилинскій [1]) замѣтилъ элегантное общее свойство.

Особенныя простыя числа поля меньше степени поля.

§ 19. Теорема. *Всякое цѣлое число* ω *области* $\Omega(\theta)$ *можетъ быть представлено въ видѣ*

$$\omega = \frac{\varphi(\theta)}{F'(\theta)},$$

гдѣ

$$F(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a^{n-1}x + a_n = 0 \qquad (1)$$

есть неприводимое уравненіе съ цѣлыми коэффиціентами, которому удовлетворяетъ цѣлое число θ, *а*

$$\varphi(\theta) = b_0 + b_1\theta + \ldots + b_{n-1}\theta^{n-1},$$

гдѣ всѣ координаты $b_0, b_1, \ldots b_{n-1}$ *суть числа цѣлыя раціональныя.*

Для доказательства теоремы докажемъ такую лемму.

Лемма. *Выраженія*

$$\sum \frac{\theta^\mu}{F'(\theta)} = S_\mu,$$

гдѣ сумма распространяется на всѣ корни θ *уравненія* $F(x) = 0$, *равны нулю, когда* $\mu \leqq n-2$ *и числа цѣлыя раціональныя при* $\mu > n-2$.

Для доказательства этой леммы покажемъ сначала, что при произвольной функціи $\psi(x)$ степени не выше $n-2$, будетъ имѣть мѣсто равенство

$$\sum \frac{\psi(\theta)}{F'(\theta)} = 0.$$

Обозначая черезъ $\theta_1, \theta_2, \ldots \theta_n$ корни уравненія $F(x) = 0$, мы замѣчаемъ, что подлежитъ доказательству равенство

$$\frac{\psi(\theta_1)}{F'(\theta_1)} + \frac{\psi(\theta_2)}{F'(\theta_2)} + \ldots + \frac{\psi(\theta_n)}{F'(\theta_n)} = 0. \qquad (2)$$

Такъ какъ функція $F(x)$ неприводимая, то она не имѣетъ кратныхъ корней и, слѣдовательно, производная не можетъ равняться нулю ни при какомъ корнѣ θ.

---

[1]) E. v. Zylinski. Ueber die ausserwesentlichen gemeinschaftlichen Discriminantenteiler Math. Ann. 1912.

Будемъ раскладывать по формулѣ Лагранжа на частныя дроби выраженіе

$$\frac{x\psi(x)}{F(x)}.$$

Получимъ тождество

$$\frac{\theta_1\psi(\theta_1)}{F'(\theta_1)(x-\theta_1)}+\frac{\theta_2\psi(\theta_2)}{F'(\theta_2)(x-\theta_2)}+\cdots+\frac{\theta_n\psi(\theta_n)}{F'(\theta_n)(x-\theta_n)}=\frac{x\psi(x)}{F(x)}.$$

Подставляя въ послѣднее тождество $x=0$, получимъ тождество (2), которое мы хотѣли доказать. Такъ какъ функція $\psi(x)$ есть совершенно произвольная функція степени не выше $n-2$, то мы имѣемъ право въ равенство (2), вмѣсто функціи $\psi(x)$, подставлять слѣдующія простѣйшія

$$1,\ x,\ x^2,\ x^3,\ \ldots,\ x^{n-2}.$$

Мы замѣчаемъ, что будутъ равны нулю всѣ выраженія

$$S_0,\ S_1,\ S_2,\ \ldots,\ S_{n-2}.$$

Нетрудно видѣть, что $S_{n-1}=1$. Въ самомъ дѣлѣ, раздѣляя x^{n-1} на производную

$$F'(x)=nx^{n-1}+\ldots,$$

получаемъ въ частномъ $\frac{1}{n}$ и остатокъ $\psi(x)$ степени не выше $n-2$, такъ что

$$\frac{x^{n-1}}{F'(x)}=\frac{1}{n}+\frac{\psi(x)}{F'(x)},$$

или

$$S_{n-1}=\sum\frac{\theta^{n-1}}{F'(\theta)}=\sum\frac{1}{n}+\sum\frac{\psi(\theta)}{F'(\theta)},$$

но

$$\sum\frac{1}{n}=1$$

и

$$\sum\frac{\psi(\theta)}{F'(\theta)}=0.$$

Чтобы убѣдиться, что для всѣхъ значеній μ большихъ $n-1$ S_μ будетъ цѣлое раціональное число, найдемъ рекуррентное соотношеніе, свя-

зывающее $n+1$ послѣдовательныхъ чиселъ

$$S_{\nu+n},\ S_{\nu+n-1},\ S_{\nu+n-2},\ \ldots\ S_{\nu}.$$

Очевидно имѣетъ мѣсто соотношеніе

$$\sum \frac{\theta^{\nu}F(\theta)}{F'(\theta)} = 0, \tag{3}$$

ибо выраженіе $F(\theta)$ равно нулю при всякомъ корнѣ. Раскрывая это выраженіе, имѣемъ

$$\sum \frac{\theta^{\nu}}{F'(\theta)}\left[\theta^{n} + a_1\theta^{n-1} + a_2\theta^{n-2} + \ldots + a_{n-1}\theta + a_n\right] = 0,$$

откуда получимъ, очевидно,

$$S_{\nu+n} + a_1 S_{\nu+n-1} + a_2 S_{\nu+n-2} + \ldots + a_{n-1}S_{\nu+1} + a_n S_{\nu} = 0. \tag{4}$$

При всякомъ цѣломъ положительномъ значеніи ν равенство (4) имѣетъ мѣсто. Будемъ подставлять вмѣсто ν рядъ значеній $0, 1, 2, \ldots$. Получаемъ, принимая во вниманіе

$$S_{n-1} = 1,\ S_{n-2} = 0,\ \ldots,\ S_0 = 0,$$

слѣдующій рядъ равенствъ

$$\begin{aligned}
&S_n + a_1 = 0,\\
&S_{n+1} + a_1 S_n + a_2 = 0,\\
&S_{n+2} + a_1 S_{n+1} + a_2 S_n + a_3 = 0,\\
&\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

Эти уравненія даютъ возможность вычислять послѣдовательно выраженія S_n, S_{n+1}, ... и т. д. Получаемъ

$$S_n = -a_1,\ S_{n+1} = -a_2 + a_1^2, \text{ и т. д.}$$

Такъ какъ всѣ коэффиціенты a_1, a_2 и т. д. числа цѣлыя раціональныя, то, слѣдовательно, и всѣ S_n, S_{n+1}, и т. д. будутъ цѣлыми раціональными.

Приступаемъ теперь къ доказательству теоремы. Принимая во вниманіе выраженіе S_{μ}, разсмотрѣнное выше, получаемъ рядъ равенствъ

$$\left.\begin{aligned}
&\sum\omega = \sum\frac{b_0 + b_1\theta + \ldots + b_{n-1}\theta^{n-1}}{F'(\theta)} = b_{n-1}\\
&\sum\theta\omega = S_n b_{n-1} + b_{n-2}\\
&\sum\theta^2\omega = S_{n+1}b_{n-1} + b_{n-2}S_n + b_{n-3}\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}\right\} \quad \ldots\ldots (5)$$

Но ω число цѣлое; значитъ, всѣ сопряженныя значенія ω будутъ также цѣлыми, и суммы

$$\sum\omega,\ \sum\theta.\omega,\ \sum\theta^2.\omega,\ \ldots$$

должны быть цѣлыми алгебраическими числами. Но, такъ какъ формулы (5) показываютъ, что эти суммы должны равняться раціональнымъ числамъ, то, слѣдовательно, эти суммы должны быть цѣлыми раціональными. Итакъ, мы видимъ, что цѣлыми раціональными должны быть всѣ коэффиціенты b_{n-1}, b_{n-2}, ... и т. д. ибо всѣ числа S_n, S_{n-1}, ... и т. д. суть числа цѣлыя раціональныя.

Доказанную нами теорему не слѣдуетъ понимать въ томъ смыслѣ, что, обратно, при всевозможныхъ цѣлыхъ коэффиціентахъ b_0, b_1 и т. д. получаются непремѣнно цѣлыя числа.

Мы видимъ, что всякое цѣлое число области $\Omega(\theta)$ можетъ быть представлено въ слѣдующемъ видѣ

$$\frac{b_0 + b_1\theta + b_2\theta^2 + \ldots + b_{n-1}\theta^{n-1}}{n\theta^{n-1} + (n-1)a_1\theta^{n-2} + (n-2)a_2\theta^{n-3} + \ldots + a^n{}_{-1}}. \qquad (1)$$

Если мы хотимъ выраженіе (1) привести къ простѣйшему виду, т. е. избавиться отъ знаменателя, то надо будетъ умножить числителя и знаменателя на всѣ сопряженныя значенія знаменателя, т. е. разсмотрѣть выраженіе [1])

$$\frac{\psi(\theta)F'(\theta_1).F'(\theta_2)\ldots F'(\theta_{n-1})}{F'(\theta).F'(\theta_1)F'(\theta_2)\ldots F'(\theta_{n-1})}.$$

Изъ элементарнаго курса алгебры извѣстно, что

$$F'(\theta).F'(\theta_1)\ldots F'(\theta_{n-1}) = (-1)^{\frac{n(n-1)}{2}}D,$$

гдѣ D есть не что иное, какъ дискриминантъ уравненія $F(x) = 0$. Этотъ дискриминантъ есть цѣлая функція отъ коэффиціентовъ a_1, a_2 и т. д. съ

---

[1]) Теперь мы обозначимъ корни уравненія (1) черезъ

$$\theta,\ \theta_1,\ \theta_2,\ \theta_{n-1}.$$

цѣлыми коэффиціентами; значитъ, есть нѣкоторое цѣлое число. Выраженіе же

$$F'(\theta_1) \cdot F'(\theta_2) \ldots F'(\theta_{n-1})$$

есть цѣлая симметрическая функція съ цѣлыми коэффиціентами отъ корней уравненія

$$\frac{F(x)}{x-\theta} = 0;$$

но это послѣднее уравненіе, какъ не трудно видѣть, имѣетъ видъ

$$x^{n-1} + (a_1 + \theta)x^{n-2} + (a_2 + a_1\theta + \theta^2)x^{n-3} + \ldots = 0,$$

т. е. его коэффиціенты суть цѣлыя функціи θ съ цѣлыми коэффиціентами. Резюмируя все сказанное, мы видимъ, что цѣлое алгебраическое число (1) можно представить въ такомъ видѣ

$$\frac{X(\theta)}{D},$$

гдѣ функція $X(\theta)$ цѣлая функція съ цѣлыми коэффиціентами. Будемъ дѣлить $X(x)$ на $F(x)$. Обозначимъ черезъ $X_1(x)$ и $X_2(x)$ частное и остатокъ отъ дѣленія; такъ какъ коэффиціентъ при старшей степени x въ дѣлителѣ $F(x)$ есть 1, то всѣ коэффиціенты функцій $X_1(x)$ и $X_2(x)$ будутъ числа цѣлыя раціональныя. Подставляя корень θ функціи $F(x)$ въ тождество

$$X(x) = F(x)X_1(x) + X_2(x),$$

получимъ

$$X(\theta) = X_2(\theta),$$

и мы получаемъ окончательно слѣдующее выраженіе:

$$\frac{X(\theta)}{D} = \frac{X_2(\theta)}{D} = \frac{c_0 + c_1\theta + c_2\theta^2 + \ldots + c_{n-1}\theta^{n-1}}{D},$$

гдѣ числа $c_0, c_1, \ldots$ цѣлыя раціональныя. Отсюда получается слѣдующая теорема:

Координаты всякаго цѣлаго алгебраическаго числа должны имѣть видъ:

$$\frac{c_0}{D}, \frac{c_1}{D}, \ldots \frac{c_{n-1}}{D},$$

гдѣ числа $c_0, c_1, \ldots c_{n-1}$ *цѣлыя раціональныя или* 0.

Итакъ, мы видимъ, что, если коэффиціенты цѣлаго алгебраическаго числа суть числа дробныя раціональныя, то въ знаменатели этихъ чиселъ могутъ входить только простые множители дискриминанта.

Алгебраическія единицы.

§ 20. Произведеніе

$$\zeta\zeta'\zeta''\ldots$$

всѣхъ сопряженныхъ величинъ алгебраическаго числа ζ называется *нормой* числа ζ. Будемъ обозначать норму знакомъ $N(\zeta)$.

Очевидно, что норма цѣлаго числа есть цѣлое раціональное число, равное взятому съ тѣмъ или другимъ знакомъ послѣднему члену уравненія

$$\zeta^n + q_1\zeta^{n-1} + q_2\zeta^{n-2} + \ldots + q_n = 0,$$

опредѣляющаго ζ, т. е.

$$N(\zeta) = \pm q_n.$$

Если $q_n = 1$, то число ζ называется *алгебраической единицей.*

Итакъ, алгебраическая единица опредѣляется уравненіемъ

$$|N(\zeta)| = 1.$$

§ 21. Посмотримъ, къ чему приводится нахожденіе алгебраическихъ единицъ въ квадратичномъ полѣ.

Будемъ искать цѣлое число $x + \zeta y$ квадратичнаго поля по уравненію

$$N(x + \zeta y) = (x + \zeta y)(x + \zeta' y) = x^2 + (\zeta + \zeta')xy + \zeta\zeta' y^2 = \pm 1. \quad (1)$$

1. Случай $d \equiv 2, 3 \pmod 4$; $\zeta = 0$, $\zeta' = -0$ уравненіе (1) дастъ

$$x^2 - dy^2 = \pm 1.$$

2. Случай $d \equiv 1 \pmod 4$; $\zeta = \frac{1+0}{2}$, $\zeta' = \frac{1-0}{2}$ уравненіе (1) дастъ

$$x^2 + xy + \frac{1-d}{4}y^2 = \pm 1$$

$$(2x + y)^2 - dy^2 = \pm 4$$

$$\xi^2 - d\eta^2 = \pm 4.$$

Итакъ, нахожденіе алгебраическихъ единицъ въ квадратичномъ полѣ равносильно съ рѣшеніемъ уравненія Pell'a.

§ 22. Заслуга нахожденія алгориѳма для вычисленія алгебраическихъ единицъ въ кубическомъ полѣ принадлежитъ выдающемуся русскому математику Г. Вороному, изложившему свой способъ въ трактатѣ „Объ одномъ обобщеніи алгориѳма непрерывныхъ дробей“ Варшава 1896.

Преждевременная смерть прекратила научную дѣятельность, носившую отпечатокъ геніальности. Долгъ русскихъ ученыхъ продолжить изслѣдованія Вороного, ибо все говоритъ въ пользу возможности дальнѣйшихъ обобщеній на поля высшихъ степеней.

Идеальныя числа.

§ 23. Теперь мы желаемъ дать читателю возможность понять въ краткомъ изложеніи сущность понятія объ идеальномъ числѣ, о которомъ мы много разъ раньше уже упоминали.

Разсмотримъ совокупность всѣхъ отличныхъ отъ нуля цѣлыхъ алгебраическихъ чиселъ нѣкотораго поля $\Omega(\vartheta)$. Эти числа, очевидно, образуютъ безконечную группу G относительно умноженія. Если мы примемъ въ соображеніе очевидное равенство

$$N(\alpha\beta) = (\alpha\beta)(\alpha\beta)'(\alpha\beta)'' \ldots = (\alpha\alpha'\alpha'' \ldots)(\beta\beta'\beta'' \ldots) = N(\alpha)N(\beta),$$

то замѣтимъ, что произведеніе двухъ единицъ ε и ε_1 должно быть также единицей, ибо

$$N(\varepsilon\varepsilon_1) = N(\varepsilon)N(\varepsilon_1) = (\pm 1)(\pm 1) = \pm 1 .$$

Итакъ всѣ алгебраическія единицы поля образуютъ подгруппу E группы G. Подгруппа E дастъ возможность разложить группу G на сопряженныя системы

$$E,\ \alpha E,\ \beta E,\ \gamma E,\ \ldots$$

гдѣ α, β, γ ... различныя отличныя отъ единицъ цѣлыя алгебраическія числа поля.

Система αE состоитъ изъ чиселъ вида $\alpha\varepsilon$, которыя получаются отъ умноженія числа α на всевозможныя алгебраическія единицы ε.

Нормы всѣхъ чиселъ αE одинаковы по абсолютной величинѣ, ибо

$$N(\alpha\varepsilon) = N(\alpha)N(\varepsilon) = \pm N(\alpha) .$$

Устанавливая дѣлимость цѣлыхъ алгебраическихъ чиселъ поля, мы не будемъ различать чиселъ каждой изъ системъ αE, βE, γE, ... такъ

что два числа отличающіяся между собой множителемъ равнымъ алгебраической единицѣ будемъ считать за одно.

Если норма числа α есть натуральное простое число p, то такое число α не можетъ далѣе раскладываться на два цѣлыхъ алгебраическихъ множителя, ибо произведеніе отличныхъ отъ единицы нормъ этихъ множителей не можетъ давать простого числа.

Подобнымъ же образомъ, если

$$|N(\alpha)| = pq,$$

гдѣ p и q различныя простыя натуральныя числа, то число α можетъ раскладываться только на произведеніе такихъ двухъ множителей β и γ, которые удовлетворяютъ равенствамъ

$$|N(\beta)| = p, \quad |N(\gamma)| = q.$$

§ 24. Уже на примѣрѣ квадратичныхъ полей было замѣчено явленіе, отличавшее, повидимому, теорію дѣлимости цѣлыхъ алгебраическихъ чиселъ отъ дѣлимости чиселъ натуральныхъ. Это явленіе состояло въ возможности разложенія цѣлаго алгебраическаго числа нѣсколькими различными способами на простые, или лучше сказать, далѣе неразложимые множители.

Простой примѣръ разъяснитъ дѣло.

Возьмемъ поле $\Omega(\theta)$, гдѣ θ есть корень уравненія

$$\theta^2 + 5 = 0.$$

Число 21 разлагается въ этомъ полѣ двумя способами на множители

$$21 = 3.7 = (1 + 2\theta)(1 - 2\theta). \qquad (1)$$

Нетрудно показать, что всѣ четыре множителя

$$3, \quad 7, \quad 1 + 2\theta, \quad 1 - 2\theta \qquad (2)$$

далѣе не разлагаются, ибо ихъ нормы равны

$$3^2, \quad 7^2, \quad 21, \quad 21$$

и если бы множители (2) разлагались далѣе, то они могли бы имѣть множителями лишь числа, нормы которыхъ суть 3 и 7.

Уравненія

$$x^2 + 5y^2 = 3, \quad x^2 + 5y^2 = 7$$

не имѣютъ рѣшеній въ цѣлыхъ раціональныхъ числахъ, слѣдовательно, не существуетъ чиселъ съ нормами 3 и 7. Число 21 разложилось двумя различными способами на неразложимые далѣе множители.

Kummer предлагаетъ разсматриваемый примѣръ объяснить такъ.

Число 21 есть произведеніе четырехъ *идеальныхъ* несуществующихъ на самомъ дѣлѣ простыхъ чиселъ

$$21 = \alpha\beta\gamma\delta .$$

Эти идеальные множители, группируясь въ произведенія по два, даютъ существующія числа, такъ напримѣръ, для нашего случая

$$\alpha\beta = 3 , \quad \gamma\delta = 7$$

$$\alpha\gamma = 1 + 2\theta , \quad \beta\delta = 1 - 2\theta .$$

Введеніе такихъ идеальныхъ множителей не нарушитъ реальности теоріи, если мы условимся эти числа не разсматривать отдѣльно, а всегда вводить въ разсмотрѣніе парами, дающими существующія числа.

Если бы числа α, β, γ, δ были обыкновенныя простыя цѣлыя раціональныя числа, то дѣлимость числа

$$\beta\delta\omega$$

на числа $\alpha\beta$ выразила бы дѣлимость натуральнаго числа ω на простое число α. По аналогіи съ этимъ говорятъ, что цѣлое алгебраическое число ω дѣлится на идеальнаго множителя α, если число

$$(1 - 2\theta)\omega$$

дѣлится на число 3. Обозначивъ $\omega = x + \theta y$, получимъ

$$(1 - 2\theta)(x + \theta y) = 3(\xi + \theta\eta) ,$$

гдѣ ξ и η числа цѣлыя раціональныя. Сравнивъ обѣ части, получимъ

$$x + 10y = 3\xi$$

$$y - 2x = 3\eta .$$

Отсюда получимъ

$$x + 10y \equiv 0 \pmod 3$$

$$y - 2x \equiv 0 \pmod 3 .$$

Эти два сравненія равносильны одному слѣдующему

$$x + y \equiv 0 \pmod 3 .$$

Откуда

$$x = -y + 3z .$$

Общій видъ цѣлаго числа ω поля, дѣлящагося на идеальнаго множителя α, будетъ

$$\omega = -y + 3z + \theta y = 3z + (-1 + \theta)y , \qquad (1)$$

гдѣ z и y суть произвольныя цѣлыя раціональныя числа.

Числа вида (1), очевидно, воспроизводятся черезъ сложеніе и вычитаніе.

Если бы множитель α былъ существующимъ числомъ, то общій видъ числа ω дѣлящагося на α былъ бы

$$\omega = \alpha z + \alpha\theta y ,$$

гдѣ z и y также произвольныя цѣлыя раціональныя числа. При существующемъ числѣ α имѣетъ мѣсто свойство, состоящее въ томъ, что, если ω дѣлится на α, то дѣлится на α и число

$$\omega\rho ,$$

гдѣ ρ произвольное цѣлое алгебраическое число.

Покажемъ, что числа вида (1), дѣлящіяся на идеальнаго множителя α, обладаютъ тѣми же свойствами, а именно, всякое число вида (1) отъ умноженія на произвольное цѣлое число области даетъ число того же вида. Провѣримъ сказанное на нашемъ примѣрѣ. Умножимъ $\omega = 3z + (-1 + \theta)y$ на число $\rho = \xi + \theta\eta$, гдѣ ξ и η цѣлыя раціональныя числа

$$\omega\rho = 3z\xi - y\xi - 5y\eta + \theta(\xi y + 3z\eta - \eta y) =$$

$$= 3z\xi - y\xi - 5y\eta + (-1 + \theta)(\xi y + 3z\eta - \eta y) + \xi y + 3\eta z - \eta y =$$

$$= 3(z\xi + \eta z - 2y\eta) + (-1 + \theta)(\xi y + 3z\eta - \eta y) =$$

$$= 3Z + (-1 + \theta)Y ,$$

гдѣ

$$Z = z\xi + \eta z - 2\eta y$$

$$Y = \xi y + 3\eta z - \eta y .$$

Такъ какъ Z и Y суть цѣлыя раціональныя числа, то мы видимъ, что число $\omega\rho$ имѣетъ также видъ (1), слѣдовательно, дѣлится на идеальнаго множителя α.

Dedekind предложилъ называть *идеаломъ*, соотвѣтствующимъ идеальному числу α, совокупность чиселъ $3z + (-1 + \theta)y$.

Каждому числу α, существующему или идеальному, Dedekind сопоставляетъ идеалъ. Получаются для всѣхъ полей законы дѣлимости идеаловъ, совпадающіе съ законами дѣлимости въ области цѣлыхъ раціональныхъ чиселъ.

Оказалось, что можно не вводить предварительно никакихъ несуществующихъ чиселъ, а прямо оперировать съ идеалами какъ совокупностями чиселъ существующихъ. Поэтому Dedekind въ основу своей теоріи прямо кладетъ слѣдующее опредѣленіе идеала.

Идеаломъ называется совокупность цѣлыхъ чиселъ поля, обладающая слѣдующими свойствами.

I. *Числа этой совокупности воспроизводятся черезъ сложеніе и вычитаніе.*

II. *Черезъ умноженіе любого числа идеала на произвольное цѣлое алгебраическое число даннаго поля получаемъ новое число, принадлежащее тому же идеалу.*

§ 25. Чтобы показать на простомъ примѣрѣ существованіе идеаловъ въ любомъ полѣ разсмотримъ совокупность чиселъ поля

$$\beta\omega, \qquad (1)$$

дѣлящихся на цѣлое алгебраическое число β этого поля. Здѣсь ω пробѣгаетъ всю совокупность цѣлыхъ чиселъ поля. Очевидно, что совокупность чиселъ (1) есть идеалъ. Такіе идеалы болѣе простого вида Dedekind называетъ *главными* [1]).

Главный идеалъ (1) считается соотвѣтствующимъ числу существующему β. Идеалы не главные соотвѣтствуютъ Kummer'овымъ идеальнымъ числамъ.

Относительно нѣкоторыхъ полей обнаруживается фактъ, что всѣ идеалы такихъ полей главные.

Таковы, напримѣръ, поле Gauss'овыхъ чиселъ $A + Bi$ и Eisenstein'овское поле трисекціи круга.

Въ поляхъ, гдѣ всѣ идеалы главные, цѣлыя числа обладаютъ всѣми законами дѣлимости, такъ что нѣтъ надобности вводить идеальныя числа.

На этомъ я покончу краткое изложеніе общей теоріи алгебраическихъ чиселъ, отсылая для дальнѣйшаго изученія къ моей книгѣ „Теорія идеаловъ“.

§ 26. Считаю необходимымъ сообщить о движеніи впередъ теоріи идеаловъ за послѣдній періодъ времени.

Въ 1882 году Kronecker опубликовалъ мемуаръ „Grundzüge einer arithmetischen Theorie der algebraischen Grössen. Въ этомъ мемуарѣ авторъ

---

[1]) Терминъ взятъ изъ Gauss'овой теоріи квадратичныхъ формъ.

указываетъ новый путь для рѣшенія тѣхъ же вопросовъ. Kronecker вводитъ въ разсмотрѣніе раціональныя функціи отъ любого числа перемѣнныхъ независимыхъ съ коэффиціентами, принадлежащими къ данному полю. Этотъ мемуаръ, подобно многому, что написано этимъ выдающимся германскимъ математикомъ, мало доступенъ для читающихъ по характеру изложенія. Ученикъ и послѣдователь Kronecker'a Weber далъ общедоступное изложеніе идей своего учителя во второмъ томѣ книги „Lehrbuch der Algebra".

Другому ученику Kronecker'a Hensel'ю наука обязана рѣшеніемъ вопросовъ о разложеніи на идеальные множители особенныхъ чиселъ поля (см. § 18). Эти вопросы представили въ свое время особенное затрудненіе.

Крупнымъ явленіемъ въ разсматриваемой области было появленіе въ 1897 г. фундаментальнаго сочиненія D. Hilbert'a „Die Theorie der algebraischen Zahlkörper, Bericht erstattet der Deutschen Mathematiker-Vereinigung". Это замѣчательное сочиненіе представляетъ полное изложеніе теоріи алгебраическихъ чиселъ съ главнѣйшими ея приложеніями. Оно изобилуетъ новыми весьма важными результатами и ставитъ новыя задачи. Вопросы, поставленные Hilbert'омъ, служили предметомъ изслѣдованія его учениковъ.

§ 26. Исторія теоріи идеальныхъ чиселъ заключаетъ почетную страницу, относящуюся къ русской наукѣ.

Въ 1874 появилось замѣчательное сочиненіе Е. Золотарева „Теорія цѣлыхъ комплексныхъ чиселъ съ приложеніемъ къ интегральному исчисленію".

Въ этомъ сочиненіи была дана новая самостоятельная теорія идеальныхъ чиселъ, основанная на функціональныхъ сравненіяхъ, и приложена къ рѣшенію одного вопроса интегральнаго исчисленія.

Внезапная смерть въ возрастѣ 33 лѣтъ отъ несчастнаго случая лишила русскую науку въ лицѣ Золотарева одного изъ крупнѣйшихъ ея представителей.

Ученикъ Золотарева А. Марковъ опубликовалъ работу, посвященную памяти учителя, и относящуюся къ полю зависящему отъ корня уравненія $x^3 = A$.

Н. Ивановъ сопоставилъ теорію Золотарева съ теоріей Dedekind'a въ сочиненіи „Цѣлыя комплексныя числа" СПБ. 1891 г.

Въ заключеніе я упомяну еще объ одной теоріи идеальныхъ чиселъ, принадлежащей Ю. Сохоцкому и изложенной имъ въ статьѣ „Принципъ наибольшаго дѣлителя" СПБ.

Теорія Сохоцкаго была положена Воронымъ въ основу его замѣчательныхъ изслѣдованій объ общемъ кубическомъ полѣ.

ГЛАВА XIII.

Исчисленіе матрицъ.

§ 1. Совокупность n^2 чиселъ, расположенныхъ въ слѣдующей квадратной схемѣ:

$$\begin{Vmatrix} a_{11}a_{12} \ldots a_{1n} \\ a_{21}a_{22} \ldots a_{2n} \\ \ldots\ldots\ldots \\ a_{n1}a_{n2} \ldots a_{nn} \end{Vmatrix} = \| a_{ik} \|$$

образуютъ такъ называемую *квадратную матрицу* порядка n. Cayley [1]) первый обратилъ вниманіе на то обстоятельство, что матрицу можно разсматривать какъ одно *комплексное* число. Можно установить правила сложенія и умноженія матрицъ, откуда появится новая алгебра дѣйствій надъ матрицами.

§ 2. Будемъ разсматривать всю совокупность W комплексныхъ чиселъ обыкновенной алгебры, кромѣ этихъ чиселъ будемъ разсматривать *всевозможныя* матрицы порядка n, элементами которыхъ являются числа W. Эти матрицы вмѣстѣ съ числами W образуютъ новую совокупность предметовъ M, въ составъ которой входитъ совокупность W какъ часть. Для сокращенія рѣчи будемъ называть числа W *величинами скалярными*, а матрицы *величинами комплексными*.

§ 3. Будемъ обозначать матрицы большими готическими буквами

$$\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \ldots$$

---

[1]) Cayley. Coll. math papers 2, 475.

Опредѣленіе равенства двухъ матрицъ. Двѣ матрицы

$$\mathfrak{A} = \| a_{ik} \| \quad \text{и} \quad \mathfrak{B} = \| b_{ik} \|$$

называются равными, если каждый изъ n^2 элементовъ матрицы $\mathfrak{A}$ равенъ соотвѣтственному элементу матрицы $\mathfrak{B}$, то есть $\mathfrak{A} = \mathfrak{B}$, если

$$a_{ik} = b_{ik} \quad (i, k = 1, 2, \ldots n).$$

Опредѣленіе нуля. Матрица $\mathfrak{A}$ называется нулемъ тогда и только тогда, когда всѣ ея элементы равны нулю, т. е. $\mathfrak{A} = 0$, если

$$a_{ik} = 0 \quad (i, k = 1, 2, \ldots n).$$

§ 4. *Опредѣленіе сложенія матрицъ.* По соотвѣтственнымъ элементамъ a_{ik} и b_{ik} двухъ произвольно взятыхъ матрицъ $\mathfrak{A}$ и $\mathfrak{B}$ составляемъ элементъ

$$s_{ik} = a_{ik} + b_{ik}$$

новой матрицы $\mathfrak{S}$. Эту матрицу $\mathfrak{S}$ называютъ суммой $\mathfrak{A}$ и $\mathfrak{B}$ и пишутъ

$$\mathfrak{S} = \mathfrak{A} + \mathfrak{B}.$$

Такимъ образомъ мы приходимъ къ слѣдующему опредѣленію сложенія матрицъ:

Подъ суммой двухъ матрицъ разумѣется такая новая, элементы которой суть суммы соотвѣтственныхъ элементовъ слагаемыхъ матрицъ.

§ 5. Правило вычитанія матрицъ получается какъ слѣдствіе изъ опредѣленія сложенія.

Разностью двухъ матрицъ будетъ такая новая, элементы которой суть разности соотвѣтственныхъ элементовъ обѣихъ заданныхъ.

§ 6. Итакъ, мы видимъ, что матрицы представляютъ относительно сложенія абелеву группу, ибо изъ опредѣленія сложенія вытекаетъ существованіе какъ перестановочнаго

$$\mathfrak{A} + \mathfrak{B} = \mathfrak{B} + \mathfrak{A},$$

такъ и сочетательнаго

$$(\mathfrak{A} + \mathfrak{B}) + \mathfrak{C} = \mathfrak{A} + (\mathfrak{B} + \mathfrak{C})$$

законовъ.

Единицей группы является матрица равная нулю.

Обратнымъ элементомъ группы для каждой матрицы $\mathfrak{A}$ является матрица, элементы которой получаются отъ умноженія на -1 элементовъ матрицы $\mathfrak{A}$.

§ 7. Приступая къ умноженію матрицъ, разсмотримъ сначала умноженіе матрицы на скалярную величину и поставимъ такое опредѣленіе:

Опредѣленіе. Подъ произведеніемъ $k.\mathfrak{A}$ или $\mathfrak{A}.k$ *матрицы* $\mathfrak{A}$ *на скалярную величину* k *разумѣется матрица, каждый элементъ которой происходитъ отъ умноженія на* k *соотвѣтствующаго элемента матрицы* $\mathfrak{A}$.

Умноженіе на скалярную величину удовлетворяетъ законамъ перестановочному и распредѣлительному

$$k\mathfrak{A} = \mathfrak{A}k$$

$$k\mathfrak{A} + k\mathfrak{B} = k(\mathfrak{A} + \mathfrak{B})$$

$$k\mathfrak{A} + l\mathfrak{A} = (k + l)\mathfrak{A},$$

гдѣ k и l скалярныя величины.

Мы будемъ употреблять обозначеніе

$$-\mathfrak{A} = (-1)\mathfrak{A}.$$

§ 8. Переходимъ теперь къ опредѣленію умноженія двухъ матрицъ, причемъ возьмемъ правило умноженія изъ теоріи опредѣлителей.

Опредѣленіе умноженія. Подъ произведеніемъ $\mathfrak{AB}$ *двухъ матрицъ* $\mathfrak{A}$ *и* $\mathfrak{B}$ *разумѣется такая новая матрица, у которой элементъ* (i, j), *стоящій на пересѣченіи* i*-ой горизонтали съ* j*-ой колонной, получается черезъ умноженіе каждаго элемента* i*-ой горизонтали* $\mathfrak{A}$ *на соотвѣтственный элементъ* j*-ой колонны* $\mathfrak{B}$ *и сложеніе полученныхъ отдѣльныхъ произведеній.*

Такъ, напримѣръ, элементъ (i, j) въ произведеніи $\mathfrak{A}.\mathfrak{B}$ будетъ

$$a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots + a_{in}b_{nj}. \qquad (1)$$

Подобнымъ же образомъ тотъ же элементъ (i, j) произведенія $\mathfrak{BA}$ будетъ

$$b_{i1}a_{1j} + b_{i2}a_{2j} + \ldots + b_{in}a_{nj}. \qquad (2)$$

Такъ какъ въ общемъ случаѣ числа (1) и (2) неодинаковы, то мы получаемъ теорему:

Умноженіе матрицъ есть дѣйствіе вообще говоря неперестановочное, т. е.

$$\mathfrak{AB} \neq \mathfrak{BA}.$$

§ 9. Хотя умноженіе матрицъ обладаетъ законами сочетательнымъ и распредѣлительнымъ

$$(\mathfrak{AB})\mathfrak{C} = \mathfrak{A}(\mathfrak{BC})$$

$$\mathfrak{A}(\mathfrak{B} + \mathfrak{C}) = \mathfrak{AB} + \mathfrak{AC}.$$

Но совокупность M скалярныхъ величинъ и матрицъ не будетъ *полемъ*. Отличнымъ отъ свойствъ поля является неперестановочность умноженія. Еще болѣе важное отличіе отъ поля представляетъ то обстоятельство, что произведеніе нѣсколькихъ матрицъ можетъ равняться нулю, тогда какъ ни одинъ изъ множителей не равенъ нулю. Въ этомъ мы можемъ убѣдиться на слѣдующемъ простомъ примѣрѣ

$$\begin{Vmatrix} a_{11} & a_{12} & 0 \\ a_{21} & a_{22} & 0 \\ a_{31} & a_{32} & 0 \end{Vmatrix} \cdot \begin{Vmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ b_{31} & b_{32} & b_{33} \end{Vmatrix} = \begin{Vmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{Vmatrix} = 0 .$$

Получаемъ теорему:

Произведеніе двухъ матрицъ можетъ равняться нулю, когда оба множителя отличны отъ нуля.

§ 10. Мы будемъ матрицу $\mathfrak{A} = \| a_{ik} \|$ называть *особенною*, если *равенъ нулю* опредѣлитель $| a_{ik} |$, составленный изъ ея элементовъ.

Для *неособенныхъ* матрицъ получаемъ теорему:

Опредѣлитель произведенія двухъ матрицъ равенъ произведенію опредѣлителей множителей.

§ 11. Матрицу $\mathfrak{A}$ мы будемъ называть *дѣлителемъ нуля*, если можно подобрать такую отличную отъ нуля матрицу $\mathfrak{B}$, что будетъ или $\mathfrak{AB} = 0$ или $\mathfrak{BA} = 0$.

Нетрудно доказать теорему:

Дѣлителемъ нуля можетъ быть только особенная матрица.

§ 12. Въ теоріи опредѣлителей горизонтали и колонны могли быть замѣняемы одни другими. При матрицахъ происходитъ другое. Двѣ матрицы

$$\mathfrak{A} = \begin{Vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{Vmatrix}, \quad \mathfrak{A}' = \begin{Vmatrix} a_{11} & a_{21} & \dots & a_{n1} \\ a_{12} & a_{22} & \dots & a_{n2} \\ \dots & \dots & \dots & \dots \\ a_{1n} & a_{2n} & \dots & a_{nn} \end{Vmatrix},$$

обладающія свойствомъ, что горизонтали одной совпадаютъ съ колоннами другой называются *сопряженными*. Сопряженныя матрицы имѣютъ одинаковыхъ опредѣлителей, но сами, вообще говоря, *неравны* между собой.

Если $\mathfrak{A} = \mathfrak{A}'$, то есть, если матрица $\mathfrak{A}$ равна своей сопряженной $\mathfrak{A}'$, то она должна быть *симметричною*, т. е.

$$a_{ik} = a_{ki} .$$

§ 13. Замѣняя колонны горизонталями и обратно, мы получимъ равенство

$$(\mathfrak{AB})' = \mathfrak{B}'\mathfrak{A}',$$

выражающее теорему.

Сопряженная величина произведенія матрицъ равна произведенію сопряженныхъ величинъ множителей, причемъ ихъ надо перемножать въ обратномъ порядкѣ.

§ 14. Поясним основанія, которыми руководился Cayley при установленіи правила умноженія матрицъ. Онъ имѣлъ въ виду теорію линейныхъ преобразованій. Сдѣлаемъ наше поясненіе на случаѣ трехъ перемѣнныхъ. Пусть разсматриваются два линейныхъ преобразованія.

$$\begin{aligned} x_1' &= a_{11}x_1 + a_{12}x_2 + a_{13}x_3 \qquad & x_1'' &= b_{11}x_1' + b_{12}x_2' + b_{13}x_3' \\ x_2' &= a_{21}x_1 + a_{22}x_2 + a_{23}x_3 \quad , & x'' &= b_{21}x_1' + b_{22}x_2' + b_{23}x_3' \\ x_3' &= a_{31}x_1 + a_{32}x_2 + a_{33}x_3 \qquad & x_3'' &= b_{31}x_1' + b_{32}x_2' + b_{33}x_3' \end{aligned}$$

Эти преобразованія можно символически обозначить такъ

$$x' = \mathfrak{A}(x) \quad , \quad x'' = \mathfrak{B}(x'),$$

гдѣ $\mathfrak{A}$ и $\mathfrak{B}$ суть матрицы коэффиціентовъ a_{ik} и b_{ik}. Подставимъ въ выраженія x_1'', x_2'', x_3'' вмѣсто x_1', x_2', x_3' ихъ выраженія черезъ x_1, x_2, x_3; получимъ

$$\begin{aligned} x_1'' = {} & (a_{11}b_{11} + a_{21}b_{12} + a_{31}b_{13})x_1 + \\ & + (a_{12}b_{11} + a_{22}b_{12} + a_{32}b_{13})x_2 + \\ & + (a_{13}b_{11} + a_{23}b_{12} + a_{33}b_{13})x_3 \\ x_2'' = {} & (a_{11}b_{21} + a_{21}b_{32} + a_{31}b_{23})x_1 + \\ & + (a_{12}b_{21} + a_{22}b_{22} + a_{32}b_{23})x_2 + \\ & + (a_{13}b_{21} + a_{23}b_{22} + a_{33}b_{23})x_3 \\ x_3'' = {} & (a_{11}b_{31} + a_{21}b_{32} + a_{31}b_{33})x_1 + \\ & + (a_{12}b_{31} + a_{22}b_{32} + a_{32}b_{33})x_2 + \\ & + (a_{13}b_{31} + a_{23}b_{32} + a_{33}b_{33})x_3. \end{aligned}$$

Матрица послѣдняго преобразованія, конечно, есть

$$\mathfrak{BA},$$

и мы получаемъ

$$x'' = \mathfrak{BA}(x).$$

§ 15. Посмотримъ теперь, можно ли матрицы разсматривать, какъ группу относительно умноженія.

Сочетательный законъ имѣетъ мѣсто. Необходимо убѣдиться въ существованіи *единицы* группы и *обратнаго элемента.*

Будемъ разсматривать матрицы въ связи съ линейными преобразованіями.

Очевидно, что будетъ единицей *мультипликативной* группы матрица тождественнаго преобразованія

$$x_1' = x_1,\ x_2' = x_2,\ \ldots\ x_n' = x_n$$

т. е. матрица

$$I = \begin{Vmatrix} 1\ 0\ 0\ \ldots\ldots\ 0 \\ 0\ 1\ 0\ \ldots\ldots\ 0 \\ 0\ 0\ 1\ \ldots\ldots\ 0 \\ \ldots\ldots\ldots\ldots \\ 0\ 0\ 0\ \ldots\ldots\ 1 \end{Vmatrix},$$

у которой діагональными элементами являются единицы, а остальные элементы равны нулю.

Для полученія матрицы обратной относительно матрицы $\mathfrak{A}$ поступимъ такъ. Напишемъ линейное преобразованіе

$$\begin{aligned} x_1' &= a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_n' &= a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n \end{aligned} \qquad (1)$$

съ коэффиціентами матрицы $\mathfrak{A}$. Чтобы получить обратную матрицу, надо составить линейное преобразованіе обратное преобразованію (1), то есть рѣшимъ уравненія (1) относительно $x_1, x_2, \ldots x_n$. Мы замѣчаемъ прежде всего, что для существованія обратной матрицы необходима возможность рѣшенія уравненій (1) т. е. *необходимо, чтобы матрица* $\mathfrak{A}$ *была неособенною.*

Итакъ мультипликативную группу образуютъ только неособенныя матрицы.

Итакъ, предполагая матрицу $\mathfrak{A}$ неособенною, рѣшимъ уравненія (1) относительно $x_1, x_2, \ldots x_n$

$$x_1 = \frac{A_{11}}{a} x_1' + \frac{A_{21}}{a} x_2' + \ldots + \frac{A_{n1}}{a} x_n'$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$x_n = \frac{A_{1n}}{a} x_1' + \frac{A_{2n}}{a} x_2' + \ldots + \frac{A_{nn}}{a} x_n',$$

гдѣ a отличный отъ нуля опредѣлитель матрицы $\mathfrak{A}$, а A_{ik} его миноры. Итакъ, обратная матрица $\mathfrak{A}^{-1}$ будетъ

$$\mathfrak{A}^{-1} = \left\| \begin{array}{ccc} \frac{A_{11}}{a}, & \frac{A_{21}}{a}, & \ldots \frac{A_{n1}}{a} \\ \ldots\ldots\ldots\ldots & & \\ \frac{A_{1n}}{a}, & \frac{A_{2n}}{a}, & \ldots \frac{A_{nn}}{a} \end{array} \right\|.$$

Замѣчая, что неособенныя матрицы образуютъ мультипликативную группу, мы получаемъ (см. гл. VI § 7, 8)

$$I\mathfrak{A} = \mathfrak{A}I = \mathfrak{A} \qquad (2)$$

$$\mathfrak{A}^{-1}\mathfrak{A} = \mathfrak{A}\mathfrak{A}^{-1} = I$$

при всякой матрицѣ $\mathfrak{A}$. Формула (2) остается справедливой также и при особенной матрицѣ $\mathfrak{A}$.

§ 16. Скажемъ теперь о дѣленіи матрицъ, какъ объ операціи обратной умноженію. Вслѣдствіе неперестановочности умноженія можетъ существовать два способа дѣленія, которые мы назовемъ *правымъ* и *лѣвымъ* дѣленіемъ. Подъ частнымъ отъ дѣленія матрицы $\mathfrak{A}$ на $\mathfrak{B}$ можно разумѣть корень одного изъ двухъ уравненій

$$\mathfrak{A} = \mathfrak{B}\mathfrak{X}\ , \quad \mathfrak{A} = \mathfrak{Y}\mathfrak{B}.$$

Дѣленіе возможно, только когда дѣлитель $\mathfrak{B}$ есть неособенная матрица. Тогда мы получаемъ

$$\mathfrak{X} = \mathfrak{B}^{-1}\mathfrak{A}\ , \quad \mathfrak{Y} = \mathfrak{A}\mathfrak{B}^{-1}.$$

§ 17. Скажемъ теперь о степеняхъ матрицы съ цѣлыми показателями. Если m есть натуральное число, то мы опредѣлимъ

$$\mathfrak{A}^m = \mathfrak{A} \cdot \mathfrak{A} \cdot \mathfrak{A} \ldots \mathfrak{A}$$

какъ произведеніе m множителей равныхъ $\mathfrak{A}$.

Если $\mathfrak{A}$ неособенная матрица, то выраженіе съ цѣлымъ отрицательнымъ показателемъ или же съ показателемъ равнымъ нулю можно опредѣлить формулами

$$\mathfrak{A}^{-m} = (\mathfrak{A}^{-1})^m, \quad \mathfrak{A}^0 = I.$$

Итакъ, получаются формулы

$$\mathfrak{A}^p . \mathfrak{A}^q = \mathfrak{A}^q \mathfrak{A}^p = \mathfrak{A}^{p+q}, \quad (\mathfrak{A}^p)^q = \mathfrak{A}^{pq},$$

справедливыя всегда при натуральныхъ значеніяхъ p и q. Если показатели могутъ быть отрицательные, тогда надо матрицу $\mathfrak{A}$ предполагать неособенною.

§ 18. Покажемъ, что скалярныя величины можно замѣнить матрицами, которыя мы будемъ называть *скалярными*, такъ что наша совокупность M будетъ исключительно состоять изъ матрицъ скалярныхъ и нескалярныхъ. Введеніе скалярныхъ матрицъ даетъ возможность установить правило сложенія скалярной величины и матрицы.

Скалярною мы будемъ называть матрицу

$$\mathfrak{K} = \begin{Vmatrix} k & 0 & 0 & \dots & 0 \\ 0 & k & 0 & \dots & 0 \\ 0 & 0 & k & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & k \end{Vmatrix} = kI$$

и будемъ ее считать равносильною числу k, причемъ будемъ въ формулахъ матрицу $\mathfrak{K}$ замѣнять просто числомъ k, не придерживаясь строго требованія писать около множителя k матрицу I.

Сравнивая съ правиломъ умноженія матрицы $\mathfrak{A}$ на скалярное число k, получимъ

$$\mathfrak{K}\mathfrak{A} = \mathfrak{A}\mathfrak{K} = k\mathfrak{A}. \tag{1}$$

Кромѣ того скалярныя матрицы несомнѣнно образуютъ поле, какъ и соотвѣтствующія имъ числа, ибо

$$\mathfrak{K} + \mathfrak{L} = \mathfrak{L} + \mathfrak{K} = (k + l)I$$

$$\mathfrak{K}\mathfrak{L} = \mathfrak{L}\mathfrak{K} = lkI$$

и т. д.

§ 10. Скалярныя матрицы обладаютъ важнымъ свойствомъ (1) *перестановочности съ любой матрицей* $\mathfrak{A}$.

Вниманіе самыхъ выдающихся математиковъ было обращено на нахожденіе общаго вида матрицъ перестановочныхъ между собой и въ частности перестановочныхъ съ данной.

Очевидно, что двѣ матрицы

$$k_0 + k_1\mathfrak{A} + k_2\mathfrak{A}^2 + \ldots + k_p\mathfrak{A}^p$$

$$l_0 + l_1\mathfrak{A} + l_2\mathfrak{A}^2 + \ldots + l_s\mathfrak{A}^s$$

раціонально выраженныя черезъ третью $\mathfrak{A}$ перестановочны. Повидимому съ небольшими ограниченіями можно утверждать, что таковъ самый общій видъ перестановочныхъ матрицъ.

Frobenius'y [1]) принадлежатъ важныя изслѣдованія по этому вопросу.

Для случая матрицъ второго порядка существуетъ теорема, что общій видъ матрицы перестановочной съ данною $\mathfrak{A}$ есть $k_0 + k_1\mathfrak{A}$.

Въ самомъ дѣлѣ, пусть задана матрица

$$\mathfrak{A} = \begin{Vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{Vmatrix}$$

Ищемъ четыре числа x_1, x_2, y_1, y_2 такихъ, чтобы было

$$\begin{Vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{Vmatrix} \cdot \begin{Vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{Vmatrix} = \begin{Vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{Vmatrix} \cdot \begin{Vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{Vmatrix}.$$

Получаемъ четыре уравненія

$$a_1x_1 + a_2y_1 = x_1a_1 + x_2b_1, \quad a_1x_2 + a_2y_2 = x_1a_2 + x_2b_2$$

$$b_1x_1 + b_2y_1 = y_1a_1 + y_2b_1, \quad b_1x_2 + b_2y_2 = y_1a_2 + y_2b_2.$$

Первое и четвертое уравненія даютъ

$$x_2b_1 = a_2y_1,$$

откуда

$$x_2 = a_2k_1, \quad y_1 = b_1k_1,$$

---

[1]) *Frobenius.* Ueber vertauschbare Matricen. S. B. A. 1896, 1910.

гдѣ k_1 произвольное число. Подставляя въ уравненія второе или третье, получимъ

$$x_1 + b_2 k_1 = y_2 + a_1 k_1 ,$$

или иначе

$$x_1 - a_1 k_1 = y_2 - b_2 k_1 = k_0 ,$$

гдѣ k_0 произвольное число, отсюда

$$x_1 = k_0 + k_1 a_1 , \quad y_2 = k_0 + k_1 b_2 .$$

Итакъ, искомая матрица

$$\left\| \begin{matrix} x_1 & x_2 \\ y_1 & y_2 \end{matrix} \right\| = \left\| \begin{matrix} k_0 + k_1 a_1 , & k_1 a_2 \\ k_1 b_1 , & k_0 + k_1 b_2 \end{matrix} \right\| = \left\| \begin{matrix} k_0 & 0 \\ 0 & k_0 \end{matrix} \right\| + k_1 \left\| \begin{matrix} a_1 & a_2 \\ b_1 & b_2 \end{matrix} \right\| = k_0 + k_1 \mathfrak{A} .$$

Что и требовалось показать.

§ 20. Покажемъ еще одинъ примѣръ матрицы перестановочной съ данной. Будемъ называть *взаимною* относительно $\mathfrak{A}$ такую новую матрицу $\mathfrak{A}$, которая получается изъ $\mathfrak{A}$ *замѣной* элементовъ $\mathfrak{A}$ ихъ соотвѣтственными минорами (алгебраическими дополненіями) и *составленіемъ* отъ полученной матрицы ей сопряженной. Другими словами, элементъ a_{ik} матрицы $\mathfrak{A}$ замѣняется элементомъ A_{ki} въ матрицѣ $\mathfrak{A}$.

На основаніи извѣстныхъ соображеній теоріи опредѣлителей мы получимъ

$$\mathfrak{A} . \mathfrak{A} = \mathfrak{A} . \mathfrak{A} = aI , \quad \mathfrak{A} = a\mathfrak{A}^{-1} ,$$

гдѣ a опредѣлитель матрицы $\mathfrak{A}$.

§ 21. Говорятъ, что матрица *ранга* r, если существуетъ *по крайней мѣрѣ одинъ отличный отъ нуля* опредѣлитель порядка r этой матрицы, тогда какъ всѣ опредѣлители высшаго порядка равны нулю.

Такъ, напримѣръ, матрица

$$\left\| \begin{matrix} a_1\alpha_1 , & a_1\alpha_2 , & a_1\alpha_3 \\ a_2\alpha_1 , & a_2\alpha_2 , & a_2\alpha_3 \\ a_3\alpha_1 , & a_3\alpha_2 , & a_3\alpha_3 \end{matrix} \right\|$$

имѣетъ *первый* рангъ.

Матрица, всѣ элементы которой равны нулю имѣетъ рангъ *нуль*.

Рангъ матрицы совпадаетъ съ ея порядкомъ, если опредѣлитель *неравенъ нулю*.

§ 22. Посмотримъ, что можно сказать о рангѣ произведенія двухъ матрицъ, зная ранги множителей. Прежде всего надо обратить вниманіе на то обстоятельство, что рангъ произведенія не опредѣляется рангами множителей, что можно видѣть на самыхъ простыхъ примѣрахъ. Такъ, напримѣръ, въ § 9 мы видѣли, что произведеніе двухъ матрицъ *второго* и *перваго* ранговъ давало матрицу *нулевого* ранга. Нетрудно построить примѣръ, гдѣ произведеніе матрицъ *второго* и *перваго* ранговъ дастъ матрицу *перваго* ранга

$$\begin{Vmatrix} a_1 & a_2 & 0 \\ b_1 & b_2 & 0 \\ c_1 & c_2 & 0 \end{Vmatrix} \cdot \begin{Vmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{Vmatrix} = \begin{Vmatrix} 0 & 0 & a_2 \\ 0 & 0 & b_2 \\ 0 & 0 & c_2 \end{Vmatrix}.$$

§ 23. *Теорема. Рангъ произведенія двухъ множителей не можетъ быть болье ранга каждаго изъ множителей.*

Возьмемъ двѣ матрицы

$$\mathfrak{A} = \begin{Vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{Vmatrix}, \quad \mathfrak{B} = \begin{Vmatrix} b_{11} & \dots & b_{1n} \\ \dots & \dots & \dots \\ b_{n1} & \dots & b_{nn} \end{Vmatrix}.$$

Пусть рангъ матрицы $\mathfrak{A}$ есть k. Покажемъ, что всѣ опредѣлители порядка $k+1$ въ обоихъ произведеніяхъ

$$\mathfrak{AB}\ ,\ \mathfrak{BA}$$

равны нулю. Въ самомъ дѣлѣ, каждый изъ такихъ опредѣлителей можно представить въ видѣ суммы опредѣлителей порядка $k+1$ составленныхъ изъ элементовъ матрицы $\mathfrak{A}$ съ коэффиціентами заключающими b_{ik}. Но каждый изъ послѣднихъ опредѣлителей или тождественно обращается въ нуль или же уничтожается какъ опредѣлитель порядка $k+1$ матрицы, рангъ которой есть k, и теорема доказана.

§ 24. Покажемъ, что отъ умноженія на *неособенную* матрицу рангъ не мѣняется.

Пусть рангъ матрицы $\mathfrak{A}$ есть k, а матрица $\mathfrak{B}$ неособенная. Обозначимъ черезъ l рангъ произведенія $\mathfrak{AB}$. На основаніи § 23 имѣемъ $l \leqq k$. Такъ какъ матрица $\mathfrak{B}$ неособенная, то существуетъ обратная ей $\mathfrak{B}^{-1}$. Равенство

$$(\mathfrak{AB})\mathfrak{B}^{-1} = \mathfrak{A}$$

даетъ $k \leqq l$ и мы получаемъ $l = k$, что и требовалось показать.

§ 25. Будемъ называть *элементарными операціями* слѣдующія преобразованія матрицъ:

1) Перестановка двухъ горизонталей или двухъ колоннъ.

2) Умноженіе всѣхъ элементовъ одной горизонтали (колонны) на одинъ и тотъ же неравный нулю множитель.

3) Прибавленіе, на произвольный множитель умноженной, горизонтали (колонны) къ другой горизонтали (колоннѣ).

Двѣ матрицы называются *эквивалентными*, если одна получается изъ другой при помощи ряда элементарныхъ операцій.

§ 26. Чтобы составить себѣ болѣе ясное представленіе объ эквивалентности матрицъ, достаточно принять въ соображеніе слѣдующіе факты.

Каждая изъ элементарныхъ операцій можетъ быть замѣнена умноженіемъ слѣва или справа данной матрицы на нѣкоторую неособенную матрицу. Эту неособенную матрицу легко подобрать нѣсколько видоизмѣняя единичную матрицу I.

Отсюда слѣдуетъ, что если двѣ матрицы $\mathfrak{A}$ и $\mathfrak{B}$ эквивалентны, то можно всегда подобрать двѣ новыя $\mathfrak{P}$, $\mathfrak{Q}$ неособенныя такъ, чтобы было

$$\mathfrak{PAQ} = \mathfrak{B}.$$

Весьма важно обратить вниманіе на теорему.

Необходимымъ и достаточнымъ условіемъ эквивалентности двухъ матрицъ одного и того же порядка является равенство ихъ рангов.

Необходимость теоремы слѣдуетъ изъ § 24.

Достаточность слѣдуетъ изъ того обстоятельства, что всякую матрицу ранга k можно при помощи элементарныхъ операцій привести къ виду

$$\left\| \begin{array}{cccccc} 1 & 0 & 0 & \dots & 0 & 0 \dots 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \dots 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \dots 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & 0 \dots 0 \\ 0 & 0 & 0 & \dots & 0 & 0 \dots 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & 0 \dots 0 \end{array} \right\|,$$

причемъ всѣ элементы матрицы нули кромѣ k равныхъ единицъ, стоящихъ на верху главной діагонали.

§ 27. Мы теперь обращаемся къ основной теоремѣ теоріи матрицъ, которая была извѣстна еще Hamilton'y и Cayley [1]), но доказана во всей общности Pasch'омъ [2]).

Если элементы нѣкоторой матрицы суть функціи отъ перемѣнной независимой λ, то такія матрицы мы будемъ называть *функціональными матрицами* или короче λ-матрицами.

Мы обратимъ особенное вниманіе на такую λ-матрицу, которая получается изъ данной числовой матрицы $\mathfrak{A}$ черезъ вычитаніе перемѣнной λ изъ всѣхъ элементовъ главной діагонали

$$\begin{Vmatrix} a_{11}-\lambda, & a_{12}, & a_{13} \ldots & a_{1n} \\ a_{21}, & a_{22}-\lambda, & a_{23}, \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1}, & a_{n2} & a_{n3} \ldots & a_{nn}-\lambda \end{Vmatrix}.$$

Опредѣлитель этой матрицы есть, очевидно, полиномъ n-ой степени относительно λ, который мы обозначимъ черезъ

$$\varphi(\lambda) = p_0\lambda^n + p_1\lambda^{n-1} + \ldots + p_{n-1}\lambda + p_n,$$

гдѣ p_n есть опредѣлитель матрицы $\mathfrak{A}$, а $p_0 = (-1)^n$.

Уравненіе

$$\varphi(\lambda) = 0$$

носитъ названіе *характеристическаго* относительно матрицы $\mathfrak{A}$.

Введемъ теперь символъ $\varphi(\mathfrak{A})$, подъ которымъ мы будемъ разумѣть матрицу, опредѣляемую символически равенствомъ

$$\varphi(\mathfrak{A}) = p_0\mathfrak{A}^n + p_1\mathfrak{A}^{n-1} + \ldots + p_{n-1}\mathfrak{A} + p_nI;$$

здѣсь скалярныя величины $p_0, p_1, \ldots p_{n-1}, p_n$ надо замѣнить скалярными матрицами и произвести умноженія и сложенія по правиламъ дѣйствій съ матрицами.

Теорема. Всякая матрица $\mathfrak{A}$ есть символическій корень ея характеристическаго уравненія, т. е. имѣетъ мѣсто слѣдующее символическое равенство

$$\varphi(\mathfrak{A}) = 0.$$

---

[1]) *Cayley.* Coll. math. papers 2. 482.

[2]) *Pasch.* Math. Ann. Bd. 38. S. 48

Frobenius. Journ. f. r. u. ang. Math. 84, 11. Sitzungsb. d. Berl. Akad, (1896) 606.

Пусть $\mathfrak{L}$ обозначаетъ характеристическую λ-матрицу

$$\mathfrak{L} = \mathfrak{A} - \lambda I.$$

Составимъ для нея взаимную $\boldsymbol{\Lambda}$, которая будетъ, очевидно, также λ-матрица, причемъ каждый ея элементъ, будучи миноромъ первоначальной, будетъ полиномомъ относительно λ степени не выше $n-1$, т. е.

$$\boldsymbol{\Lambda} = \mathfrak{L}_{n-1}\lambda^{n-1} + \mathfrak{L}_{n-2}\lambda^{n-2} + \ldots + \mathfrak{L}_0, \tag{1}$$

гдѣ $\mathfrak{L}_{n-1}, \mathfrak{L}_{n-2}, \ldots \mathfrak{L}_0$ суть обыкновенныя матрицы, составленныя изъ элементовъ $\mathfrak{A}$.

Переписавъ функцію $\varphi(\lambda)$ такъ

$$\varphi(\lambda) = k_n\lambda^n + k_{n-1}\lambda^{n-1} + \ldots + k_0, \tag{2}$$

получимъ на основаніи формулъ § 20

$$(\mathfrak{A} - \lambda I)\boldsymbol{\Lambda} = \mathfrak{A}\boldsymbol{\Lambda} - \lambda\boldsymbol{\Lambda} = \varphi(\lambda) I.$$

Раскладывая въ обѣихъ частяхъ послѣдняго уравненія $\boldsymbol{\Lambda}$ и $\varphi(\lambda)$ по степенямъ λ на основаніи (1) и (2) и сравнивая коэффиціенты у одинаковыхъ степеней, получимъ рядъ символическихъ уравненій

$$\begin{aligned}
&\mathfrak{A}\mathfrak{L}_0 &&= k_0 I\\
&\mathfrak{A}\mathfrak{L}_1 - \mathfrak{L}_0 &&= k_1 I\\
&\ldots\ldots\ldots\ldots\ldots\\
&\mathfrak{A}\mathfrak{L}_{n-1} - \mathfrak{L}_{n-2} &&= k_{n-1} I\\
&\quad - \mathfrak{L}_{n-1} &&= k_n I.
\end{aligned}$$

Умножая эти уравненія по порядку на $I, \mathfrak{A}, \mathfrak{A}^2, \ldots \mathfrak{A}^n$ и складывая мы замѣчаемъ, что лѣвая часть обращается въ нуль, правая же часть даетъ

$$k_0 I + k_1\mathfrak{A} + k_2\mathfrak{A}^2 + \ldots + k_n\mathfrak{A}^n = 0,$$

то есть $\varphi(\mathfrak{A}) = 0$, что и требовалось доказать.

§ 28. Мы выведемъ изъ послѣдней теоремы важныя для теоріи чиселъ слѣдствія.

Пусть матрица $\mathfrak{A}$ имѣетъ элементами положительныя или отрицательныя цѣлыя числа или нули. Очевидно тогда, что такую матрицу можно разсматривать съ точки зрѣнія дѣйствій надъ матрицами за *цѣлое алгебраическое число*, ибо она удовлетворяетъ символически уравненію степени n

$$\varphi(\mathfrak{A}) = 0,$$

у котораго всѣ коэффиціенты *цѣлые* и старшій равенъ единицѣ.

Предполагая функцію $\varphi(\lambda)$ неприводимою, мы приходимъ къ построенію *поля* изъ матрицъ вида

$$x_0 + x_1\mathfrak{A} + x_2\mathfrak{A}^2 + \ldots + x_{n-1}\mathfrak{A}^{n-1},$$

гдѣ $x_0, x_1, x_2, \ldots x_{n-1}$ раціональныя числа. Это поле изоморфно съ полемъ, получающимся отъ присоединенія къ полю раціональныхъ чиселъ корня λ уравненія $\varphi(\lambda) = 0$.

Сопоставленіе матрицъ алгебраическимъ числамъ поля производится просто на основаніи такого разсужденія.

Пусть фундаментальный базисъ (см. гл. XII § 16) поля степени n будетъ

$$\omega_1, \omega_2, \ldots \omega_n;$$

возьмемъ произвольное число ξ поля, тогда всѣ числа

$$\xi\omega_1, \xi\omega_2, \ldots \xi\omega_n,$$

какъ числа поля, должны выражаться черезъ базисъ съ цѣлыми координатами

$$\xi\omega_1 = a_{11}\omega_1 + a_{12}\omega_2 + \ldots + a_{1n}\omega_n$$

$$\xi\omega_2 = a_{21}\omega_1 + a_{22}\omega_2 + \ldots + a_{2n}\omega_n$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\xi\omega_n = a_{n1}\omega_1 + a_{n2}\omega_2 + \ldots + a_{nn}\omega_n.$$

Очевидно, что алгебраическому числу ξ можно сопоставить матрицу

$$\mathfrak{A} = \begin{Vmatrix} a_{11} \ldots a_{1n} \\ \ldots\ldots\ldots \\ a_{n1} \ldots a_{nn} \end{Vmatrix},$$

тѣмъ болѣе, что матрица $\mathfrak{A}$ удовлетворяетъ *символически* тому же уравненію, которому удовлетворяетъ *обыкновеннымъ образомъ* число ξ.

Замѣняя алгебраическія числа матрицами, получаемъ вычислительный пріемъ, который нельзя игнорировать при бѣдности относительно алгоритмовъ теоріи алгебраическихъ чиселъ.

§ 29. По поводу алгебраическихъ матрицъ приведемъ здѣсь кстати интересную теорему Smith'a [1]), воспользовавшись для ея доказательства принципомъ Dedekind'a (см. гл. II § 31).

[1]) Stephen Smith. Proc. of the London's Math. Soc. VII Mai 1876.

Обозначимъ черезъ (n, N) общій наибольшій дѣлитель двухъ цѣлыхъ чиселъ n и N: тогда дѣло идетъ о матрицѣ

$$\left\| \begin{array}{l} (1,1)(1,2)(1,3)\ldots \\ (2,1)(2,2)(2,3)\ldots \\ (3,1)(3,2)(3,3)\ldots \\ \ldots\ldots\ldots\ldots \end{array} \right\| = \left\| \begin{array}{l} 1\ 1\ 1\ 1\ 1\ 1\ldots. \\ 1\ 2\ 1\ 2\ 1\ 2\ldots. \\ 1\ 1\ 3\ 1\ 1\ 3\ldots. \\ 1\ 2\ 1\ 4\ 1\ 2\ldots. \\ 1\ 1\ 1\ 1\ 5\ 1\ldots. \\ 1\ 2\ 3\ 2\ 1\ 6\ldots. \\ \ldots\ldots\ldots\ldots \end{array} \right\|$$

Теорема Smith'a состоитъ въ томъ, что опредѣлитель послѣдней матрицы, составленный изъ n первыхъ горизонталей и колоннъ, равенъ

$$\varphi(1)\varphi(2)\ldots\varphi(n),$$

гдѣ $\varphi(n)$ Euler'ова функція (см. гл. II § 23).

Введемъ для доказательства такую новую числовую функцію $\rho(n, N)$, которую опредѣлимъ равенствомъ

$$\rho(n, N) = \varphi(n),$$

когда N дѣлится на n и равенствомъ

$$\rho(n, N) = 0,$$

если N не дѣлится на n.

Будемъ имѣть соотношеніе

$$\sum_d \rho(d, N) = (n, N), \qquad (1)$$

гдѣ сумма распространена на всѣхъ дѣлителей d числа n.

Настолько просто убѣдиться на основаніи формулы (1) § 26 гл. II въ справедливости формулы (1), что мы на этомъ останавливаться не будемъ. Примѣняя принципъ Dedekind'a, получимъ

$$\rho(n, N) = (n, N) - \sum\left(\frac{n}{p}, N\right) + \sum\left(\frac{n}{pp_1}, N\right). \qquad (2)$$

гдѣ p, p_1 . . . суть простые множители числа n.

Если у насъ разсматривается опредѣлитель

$$K_n = \left| \begin{array}{l} (1,1)(1,2)(1,3)\ldots(1,n) \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ (n,1)(n,2)(n,3)\ldots(n,n) \end{array} \right|,$$

го, прибавляя къ послѣдней (нижней) n-ой горизонтали другія горизонтали, имѣющія нумерами

$$\frac{n}{p}, \frac{n}{p_1}, \frac{n}{p_2}, \ldots \frac{n}{pp_1}, \frac{n}{pp_2}, \frac{n}{p_1p_2}, \ldots \frac{n}{pp_1p_2}, \ldots$$

умноженныя всякій разъ на $+1$ или на -1, судя по формулѣ (2), мы обратимъ послѣднюю горизонталь въ такую

$$\rho(n,1),\ \rho(n,2),\ \rho(n,3),\ \ldots\ \rho(n,n-1),\ \rho(n,n)$$

или, что одно и тоже, въ такую

$$0 \qquad 0 \qquad 0 \quad \ldots \quad 0 \qquad \varphi(n).$$

Отсюда

$$K_n = \varphi(n) K_{n-1}$$

и теорема доказана.

ГЛАВА XIV.

Числа Bernoulli.

§ 1. Въ предыдущей главѣ мы разсматривали символическія дѣйствія надъ матрицами.

Въ этой главѣ я желаю обратить вниманіе на пользу символическаго исчисленія для теоріи чиселъ вообще [1]). Для этой цѣли я выберу предметомъ изученія замѣчательныя числа, введенныя въ науку Bernoulli. Эти числа получили особенное значеніе въ XIX столѣтіи въ изслѣдованіяхъ Kummer'a, связанныхъ съ великой теоремой Fermat'a, гдѣ выяснилась ихъ глубокая связь со свойствами поля дѣленія круга.

§ 2. Будемъ называть *первою конечною разностью* функціи $f(x)$ выраженіе

$$\Delta f(x) = f(x+1) - f(x).$$

Разсмотримъ случай, когда такая первая разность есть цѣлая функція, т. е.

$$\Delta f(x) = f(x+1) - f(x) = a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n \qquad (1)$$

подставляя въ равенство (1) вмѣсто x числа $1, 2, 3, \ldots x-1$ и складывая, получимъ

$$f(x) - f(1) = a_0 S_n + a_1 S_{n-1} + a_2 S_{n-2} + \ldots + a_n S_0, \qquad (2)$$

---

[1]) Можно рекомендовать для болѣе подробнаго знакомства съ приложеніемъ символическаго исчисленія къ теоріи чиселъ Bernoulli курсъ теоріи чиселъ Lucas (Theorie de Nombres) и *Чезаро*. Элементарный учебникъ алгебраическаго анализа. 1913. Переводъ съ примѣчаніями проф. Поссе.

гдѣ

$$S_n = 1^n + 2^n + 3^n + \ldots + (x-1)^n.$$

Вмѣсто формулы (2) напишемъ новую

$$f(x) - f(1) \doteqdot a_0 S^n + a_1 S^{n-1} + a_2 S^{n-2} + \ldots + a_n S^0; \qquad (3)$$

эта формула представляетъ такъ называемую символическое равенство, причемъ знакъ $\doteqdot$ этого символическаго равенства показываетъ, что для полученія изъ него настоящаго равенства надо въ правой части показатели надъ буквой S замѣнить нижними значками. Принимая во вниманіе формулу (1), можно будетъ формулу (3) переписать такъ

$$f(x) - f(1) \doteqdot f(S+1) - f(S). \qquad (4)$$

Знака символическаго равенства мы не будемъ однако далѣе писать, ибо будетъ всегда ясно, какое написано равенство *обыкновенное* или *символическое*.

§ 3. Полагая въ равенствѣ (4) § 2 $f(x) = x^n$, получимъ

$$x^n - 1 = (S+1)^n - S^n.$$

Замѣняя символическое равенство обыкновеннымъ получимъ

$$x^n - 1 = nS_{n-1} + \frac{n(n-1)}{1.2} S_{n-2} + \frac{n(n-1)(n-2)}{1.2.3} S_{n-3} + \ldots \qquad (1)$$

Обозначаемъ

$$C_n^k = \frac{n(n-1)(n-2)\ldots(n-k+1)}{1.2.3\ldots k}.$$

Примѣняя формулу (1) къ значеніямъ показателя n, $n-1$, $n-2$, получимъ рядъ уравненій

$$x^n - 1 = C_n^1 S_{n-1} + C_n^2 S_{n-2} + C_n^3 S_{n-3} + \ldots$$

$$x^{n-1} - 1 = C_{n-1}^1 S_{n-2} + C_{n-1}^2 S_{n-3} + \ldots$$

$$x^{n-2} - 1 = C_{n-2}^1 S_{n-3} + \ldots$$

. . . . . .

Рѣшая эти уравненія какъ линейныя относительно S_{n-1}, S_{n-2}, . . . получимъ

$$1.2.3\ldots nS_{n-1}=\begin{vmatrix} x^n & C_n^2 & C_n^3 & \ldots & C_n^{n-1} & 1 \\ x^{n-1} & C_{n-1}^1 & C_{n-1}^2 & \ldots & C_{n-1}^{n-2} & 1 \\ x^{n-2} & 0 & C_{n-2}^1 & \ldots & C_{n-2}^{n-3} & 1 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ x^2 & 0 & 0 & \ldots & C_2^1 & 1 \\ x & 0 & 0 & \ldots & 0 & 1 \end{vmatrix}. \qquad (2)$$

Раскрывая этотъ опредѣлитель по элементамъ первой колонны, мы получимъ

$$nS_{n-1}=x^n+n.\mathfrak{B}_1x^{n-1}+\frac{n(n-1)}{1.2}\mathfrak{B}_2x^{n-2}+\frac{n(n-1)(n-2)}{1.2.3}\mathfrak{B}_3x^{n-3}+ \\ +\ldots+n\mathfrak{B}_{n-1}x. \qquad (3)$$

Числа $\mathfrak{B}_1, \mathfrak{B}_2, \mathfrak{B}_3, \ldots \mathfrak{B}_{n-1}$ оказываются независимыми отъ n и зависящими только отъ своего значка.

Дадимъ болѣе простой способъ послѣдовательнаго вычисленія коэффиціентовъ $\mathfrak{B}_k$.

Формулу (3) можно замѣнить слѣдующей символической

$$nS_{n-1}=(x+\mathfrak{B})^n-\mathfrak{B}^n. \qquad (4)$$

Взявъ первую разность отъ обѣихъ частей послѣдней формулы, получимъ

$$nx^{n-1}=(x+\mathfrak{B}+1)^n-(x+\mathfrak{B})^n. \qquad (5)$$

Подставляя сюда $x=0$, получимъ при $n>1$ рекурентную формулу

$$(\mathfrak{B}+1)^n-\mathfrak{B}^n=0, \qquad (6)$$

дающую возможность послѣдовательно вычислять коэффиціенты $\mathfrak{B}_n$.

Полагая въ (6) $n=2$, получимъ

$$2\mathfrak{B}^1+1=0 \quad \text{или} \quad 2\mathfrak{B}_1+1=0, \quad \mathfrak{B}_1=-\frac{1}{2}.$$

Полагая въ (6) $n=3$, получимъ

$$3\mathfrak{B}^2+3\mathfrak{B}^1+1=0, \quad 3\mathfrak{B}_2+3\mathfrak{B}_1+1=0, \quad \mathfrak{B}_2=\frac{1}{6}.$$

Полагая въ (6) $n=4$, получимъ

$$4\mathfrak{B}^3+6\mathfrak{B}^2+4\mathfrak{B}^1+1=0, \quad 4\mathfrak{B}_3+6\mathfrak{B}_2+4\mathfrak{B}_1+1=0,$$

откуда $\mathfrak{B}_3=0$.

Итакъ, получаются слѣдующія значенія первыхъ коэффиціентовъ

$$\mathfrak{B}_1 = -\frac{1}{2},\ \mathfrak{B}_2 = \frac{1}{6},\ \mathfrak{B}_3 = 0,\ \mathfrak{B}_4 = -\frac{1}{30},\ \mathfrak{B}_5 = 0,\ \mathfrak{B}_6 = \frac{1}{42},\ \mathfrak{B}_7 = 0,$$

$$\mathfrak{B}_8 = -\frac{1}{30},\ \text{и т. д.}$$

§ 4. Числа $\mathfrak{B}_k$ съ нечетными значками оказываются равными нулю. Въ этомъ очень просто убѣдиться изъ такихъ соображеній.

Полагая $x = -1$ въ формулѣ (5) § 3, получимъ

$$\mathfrak{B}^n - (\mathfrak{B} - 1)^n = n(-1)^{n-1}.$$

Складывая съ формулой (6) § 3, получимъ

$$(\mathfrak{B} + 1)^n - (\mathfrak{B} - 1)^n = n(-1)^{n-1}. \qquad (1)$$

Полагая далѣе $x = -\frac{1}{2}$ въ формулѣ (5) § 3 получимъ

$$(2\mathfrak{B} + 1)^n - (2\mathfrak{B} - 1)^n = 2n(-1)^{n-1}. \qquad (2)$$

Изъ равенствъ (1) и (2) получаемъ окончательно

$$(2\mathfrak{B} + 1)^n - (2\mathfrak{B} - 1)^n - 2[(\mathfrak{B} + 1)^n - (\mathfrak{B} - 1)^n] = 0,$$

то есть однородное линейное соотношеніе, связывающее рядъ первыхъ по порядку коэффиціентовъ $\mathfrak{B}_k$ со значками одинаковой четности. При n четномъ получается однородное линейное соотношеніе, связывающее $\frac{n}{2}$ первыхъ $\mathfrak{B}_k$ съ нечетными значками.

Очевидно, что, если нѣсколько первыхъ такихъ коэффиціентовъ равны нулю, то будетъ равенъ нулю и всякій слѣдующій.

§ 5. Обыкновенно разумѣютъ подъ названіемъ *чисель Bernoulli* [1]) числа B_k опредѣляемыя равенствомъ

$$(-1)^{k-1} B_k = \mathfrak{B}_{2k}.$$

---

[1]) Марковъ. Исчисленіе конечныхъ разностей.

Формула (3) § 3 даетъ двѣ слѣдующія

$$1^{2n}+2^{2n}+\ldots+(x-1)^{2n}=\frac{x^{2n+1}}{2n+1}-\frac{x^{2n}}{2}+\frac{B_1}{2}C^1_{2n}x^{2n-1}-$$
$$-\frac{B_2}{4}C^3_{2n}x^{2n-3}+\ldots+(-1)^{n-1}\frac{B_n}{2n}C^{2n-1}_{2n}.x,$$
$$1^{2n+1}+2^{2n+1}+\ldots+(x-1)^{2n+1}=\frac{x^{2n+2}}{2n+2}-\frac{x^{2n+1}}{2}+ \tag{1}$$
$$+\frac{B_1}{2}C^1_{2n+1}x^{2n}-\frac{B_2}{4}C^3_{2n+1}x^{2n-2}+\ldots+(-1)^{n-1}\frac{B_n}{2n}C^{2n-1}_{2n+1}x^2.$$

Разсматривая послѣднія формулы, мы замѣчаемъ, что послѣдній членъ съ самой меньшею степенью x будетъ:

въ выраженіи S_{2n} . . . . . $(-1)^{n-1}B_nx$

въ выраженіи S_{2n+1} . . . . . $(-1)^{n-1}\frac{2n+1}{2}B_nx^2$.

§ 6. Покажемъ теперь, что числа Bernoulli всѣ *положительныя* и *безпредѣльно возрастаютъ* съ возрастаніемъ значка. Для этой цѣли выведемъ одну весьма важную формулу

$$(1^p+2^p+\ldots+x^p)^2=1^{2p}+2^{2p}+\ldots+x^{2p}+$$
$$+2\{1^p.0^p+2^p.1^p+3^p(1^p+2^p)+4^p(1^p+2^p+3^p)+\ldots\},$$

то есть

$$(\sum x^p)^2=\sum x^{2p}+2\sum_{y=1}^{y=x}y^p(\sum y^p-y^p).$$

Здѣсь подъ знакомъ $\sum q^p$ разумѣется $1^p+2^p+\ldots+q^p$.

Но

$$\sum y^p-y^p=\frac{y^{p+1}}{p+1}-\frac{y_p}{2}+\frac{B_1}{2}C^1_py^{p-1}-\ldots$$

Слѣдовательно, получаемъ

$$(\sum x^p)^2=\sum x^{2p}+2\left\{\frac{\sum x^{2p+1}}{p+1}-\frac{1}{2}\sum x^{2p}+\frac{B_1}{2}C^1_p\sum x^{2p-1}-\ldots\right\}$$

Примѣняя къ четному значенію $p=2n$, получимъ

$$(\sum x^{2n})^2 = \frac{2}{2n+1}\sum x^{4n+1} + C_{2n}^1 \frac{B_1}{1}\sum x^{4n-1} - C_{2n}^3 \frac{B_2}{2}\sum x^{4n-3} +$$

$$+ \ldots + (-1)^{n-1}\frac{B_n}{n} C_{2n}^{2n-1}\sum x^{2n+1}$$

$$B_n^2 = -\frac{2}{2n+1}\frac{4n+1}{2} B_{2n} + C_{2n}^1 \frac{4n-1}{2} B_1 B_{2n-1} +$$

$$+ C_{2n}^3 \frac{4n-3}{4} B_2 B_{2n-2} + \ldots + (2n+1)B_n^2,$$

или окончательно

$$\frac{4n+1}{2n+1} B_{2n} = \frac{4n-1}{2} C_{2n}^1 . B_1 B_{2n-1} + \frac{4n-3}{4} C_{2n}^3 B_2 B_{2n-2} + \ldots + 2n B_n^2. \quad (1)$$

Эта формула показываетъ, что, если положительны числа B_1, B_2, $\ldots B_{2n-1}$, то будетъ положительно также число B_{2n}. Для нечетнаго значка $2n+1$ будетъ существовать подобная же формула; такимъ образомъ мы видимъ, что всѣ числа Bernoulli положительны. Покажемъ теперь, что они безпредѣльно возрастаютъ. На основаніи формулы (1) мы имѣемъ

$$\frac{4n+1}{2n+1} B_{2n} > \frac{4n-1}{2}\frac{2n}{1} B_1 B_{2n-1}.$$

Подобнымъ же образомъ для нечетнаго значка

$$\frac{4n+3}{2n+2} B_{2n+1} > \frac{4n+1}{2}\frac{2n+1}{1} B_1 B_{2n}.$$

Обѣ послѣднія формулы можно замѣнить одной общей

$$B_p > \frac{2p-1}{2p+1}\frac{p(p+1)}{1.2} B_1 B_{p-1}.$$

Какое бы ни было задано число α, начиная съ извѣстнаго p будетъ

$$B_p > \alpha B_{p-1}.$$

§ 7. Формула (2) § 3 даетъ

$$1.2.3 \ldots n\mathfrak{B}_{n-1} = (-1)^{n-1}\begin{vmatrix} C_n^2, & C_n^3, & C_n^4 & \ldots & 1 \\ C_{n-1}^1, & C_{n-1}^2, & C_{n-1}^3 & \ldots & 1 \\ 0, & C_{n-2}^1, & C_{n-2}^3 & \ldots & 1 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0, & 0, & 0, & \ldots C_2^1, & 1 \end{vmatrix},$$

откуда мы видимъ, что число $1.2.3 \ldots n\mathfrak{B}_{n-1}$ есть цѣлое число.

§ 8. Числа Bernoulli суть, какъ мы видимъ, положительныя, безпредѣльно возрастающія, дробныя числа.

J. Adams [1]) далъ таблицу первыхъ 62 чиселъ Bernoulli B_k. Эта таблица продолжена Серебренниковымъ [2]) до B_{90}. Небольшую таблицу чиселъ Bernoulli мы приводимъ въ концѣ книги.

Теорема Staudt'a.

§ 9. Покажемъ теперь, что всѣ числа Bernoulli суть дѣйствительно дробныя. Для этой цѣли докажемъ весьма важную теорему Staudt'a [3]).

Теорема. Дробная часть B_k *равна произведенію* $(-1)^k$ *на сумму всѣхъ дробей вида*

$$\frac{1}{\lambda},$$

гдѣ λ *простое число, при которомъ* $2k \equiv 0 \pmod{\lambda - 1}$.

Напримѣръ

$$B_5 = 1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{11}, \quad B_8 = 6 + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{17}.$$

Мы докажемъ эту теорему изъ разсмотрѣнія выраженія Bernoulli'его числа черезъ конечныя разности.

§ 10. Если мы положимъ для сокращенія

$$\begin{aligned} f(x+1) - f(x) &= \Delta f(x) \\ \Delta f(x+1) - \Delta f(x) &= \Delta^2 f(x) \\ \Delta^2 f(x+1) - \Delta^2 f(x) &= \Delta^3 f(x) \\ &\cdots\cdots\cdots\cdots \end{aligned} \tag{1}$$

то выраженія

$$\Delta f(x),\ \Delta^2 f(x),\ \Delta^3 f(x),\ \ldots$$

представляютъ такъ называемыя *конечныя разности перваго, второго, третьяго и т. д. порядка отъ функціи* $f(x)$.

---

[1]) J. Adams. Journ. f. r. u. ang. Math. B. 85.

[2]) Серебренниковъ. Таблица первыхъ 90 чиселъ Бернулли. Зап. С.-Пет. Ак. Н. 1905.

[3]) Staudt. Journ. f. r. u. ang. Math. B. 21. S. 72.

Не трудно изъ равенствъ (1) вывести формулу Newton'a [1])

$$f(x+n) = f(x) + C_n^1 \Delta f(x) + C_n^2 \Delta^2 f(x) + \ldots + C_n^n \Delta^n f(x),$$

полагая въ ней $x = 1$, $n = x - 1$, получимъ

$$f(x) = f(1) + \frac{x-1}{1} \Delta f(1) + \frac{(x-1)(x-2)}{1.2} \Delta^2 f(1) +$$

$$+ \frac{(x-1)(x-2)(x-3)}{1.2.3} \Delta^3 f(1) + \ldots$$

Примѣняя эту формулу къ функціи x^n, получимъ

$$x^n = 1^n + \frac{x-1}{1} \Delta 1^n + \frac{(x-1)(x-2)}{1.2} \Delta^2 1^n +$$

$$+ \frac{(x-1)(x-2)(x-3)}{1.2.3} \Delta^3 1^n + \ldots; \qquad (2)$$

суммируя далѣе по x отъ 1 до $x-1$, будемъ имѣть

$$S_n = x - 1 + \frac{(x-1)(x-2)}{1.2} \Delta 1^n + \frac{(x-1)(x-2)(x-3)}{1.2.3} \Delta^2 1^n + \ldots,$$

собирая въ обѣихъ частяхъ коэффиціентъ при x въ первой степени, получимъ

$$\mathfrak{B}_n = 1 - \left(\frac{1}{1} + \frac{1}{2}\right) \Delta 1^n +$$

$$+ \left(\frac{1}{1} + \frac{1}{2} + \frac{1}{3}\right) \Delta^2 1^n - \left(\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4}\right) \Delta^3 1^n + \ldots, \qquad (3)$$

собирая въ обѣихъ частяхъ равенства (2) коэффиціентъ при первой степени x, получимъ

$$0 = \Delta 1^n - \left(\frac{1}{1} + \frac{1}{2}\right) \Delta^2 1^n + \left(\frac{1}{1} + \frac{1}{2} + \frac{1}{3}\right) \Delta^3 1^n + \ldots, \qquad (4)$$

вычитая далѣе (4) изъ (3), получимъ окончательно

$$\mathfrak{B}_n = 1 - \frac{\Delta 1^n}{2} + \frac{\Delta^2 1^n}{3} - \frac{\Delta^3 1^n}{4} + \frac{\Delta^4 1^n}{5} - \ldots$$

---

[1]) *Марковъ*. Исчисленіе конечныхъ разностей. I-ая часть, глава II.

Очевидно, достаточно разсмотрѣть случай четнаго $n = 2k$, тогда формула будетъ

$$(-1)^{k-1}B_k = 1 - \frac{\Delta 1^{2k}}{2} + \frac{\Delta^2 1^{2k}}{3} - \frac{\Delta^3 1^{2k}}{4} + \frac{\Delta^4 1^{2k}}{5} - \ldots$$

Остается доказать, что будетъ

$$\Delta^{\lambda-1}1^{2k} \equiv -1 \pmod{\lambda},$$

если λ простое число, при которомъ $2k \equiv 0 \pmod{\lambda - 1}$; и

$$\Delta^{\lambda-1}1^{2k} \equiv 0 \pmod{\lambda}$$

во всѣхъ остальныхъ случаяхъ.

Въ самомъ дѣлѣ, разсмотримъ сравненіе

$$F(x) \equiv 0 \pmod{\lambda}. \tag{1}$$

Подобно тому какъ было показано для простого модуля (см. § 27 гл. III), можно понизить степень сравненія ниже λ и въ случаѣ составного λ. Пусть γ есть наибольшій изъ показателей простыхъ множителей числа λ, т. е. если $\lambda = p_1^{\omega_1}p_2^{\omega_2}p_3^{\omega_3}\ldots$, то γ есть наибольшій изъ показателей $\omega_1, \omega_2, \omega_3, \ldots$ Пусть кромѣ того $\psi(\lambda)$ есть наименьшее кратное чиселъ $\varphi(p_1^{\omega_1})$, $\varphi(p_2^{\omega_2})$, $\varphi(p_3^{\omega_3})\ldots$, тогда будемъ имѣть сравненіе

$$x^\gamma(x^{\psi(\lambda)} - 1) \equiv 0 \pmod{\lambda}$$

справедливое при всѣхъ значеніяхъ x. Если x дѣлится на простое p_i, то x^γ дѣлится на $p_i^{\omega_i}$, если же x взаимно простое съ $p_i^{\omega_i}$, то $x^{\psi(\lambda)} - 1$ дѣлится на $p_i^{\omega_i}$.

Дѣлимъ $F(x)$ на $x^\gamma(x^{\psi(\lambda)} - 1)$ и обозначимъ остатокъ отъ этого дѣленія черезъ $f(x)$. Имѣемъ тождество

$$F(x) = x^\gamma(x^{\psi(\lambda)} - 1)\Phi(x) + f(x),$$

откуда получаемъ тождественное сравненіе

$$F(x) \equiv f(x) \pmod{\lambda}$$

и, слѣдовательно, сравненіе (1) равносильно такому

$$f(x) \equiv 0 \pmod{\lambda}, \tag{2}$$

степень котораго не выше

$$\psi(\lambda) + \gamma - 1.$$

Для составного числа кромѣ $\lambda = 4$ имѣемъ

$$\psi(\lambda) + \gamma - 1 < \lambda - 1$$

и, слѣдовательно,

$$\Delta^{\lambda-1} F(x) \equiv \Delta^{\lambda-1} f(x) \equiv 0 (\mathrm{mod}\, \lambda) .$$

При $\lambda = 4$ получаемъ

$$\Delta^{\lambda-1} 1^{2k} = \Delta^3 1^{2k} = 4^{2k} - 3 . 3^{2k} + 3 . 2^{2k} - 1^{2k} \equiv 0 (\mathrm{mod}\, 4) .$$

Если λ нечетное простое число, то будемъ дѣлить $2k$ на $\lambda - 1$ и обозначимъ остатокъ отъ этого дѣленія черезъ σ, причемъ, если дѣленіе совершается безъ остатка, то мы будемъ предполагать $\sigma = \lambda - 1$.

Если $\sigma < \lambda - 1$, то получаемъ тождество

$$\Delta^{\lambda-1} x^{2k} \equiv \Delta^{\lambda-1} x^{\sigma} \equiv 0 (\mathrm{mod}\, \lambda) .$$

Если же $\sigma = \lambda - 1$, то

$$\Delta^{\lambda-1} x^{2k} \equiv \Delta^{\lambda-1} x^{\lambda-1} \equiv 1 . 2 . 3 \ldots (\lambda - 1) \equiv -1 (\mathrm{mod}\, \lambda) .$$

При $\lambda = 2$ получаемъ

$$\Delta 1^{2k} = 2^{2k} - 1^{2k} \equiv -1 (\mathrm{mod}\, 2)$$

и теорема Staudt'a доказана вполнѣ.

§ 11. Изъ теоремы Staudt'a слѣдуетъ между прочимъ, что знаменатель всякаго числа Bernoulli дѣлится на 6.

Теоремы Adams'a-Вороного.

§ 12. Въ цитированной выше (въ § 8) статьѣ Adams'a авторъ даетъ безъ доказательства слѣдующія свойства чиселъ Bernoulli: онъ говоритъ *„Я доказалъ, что, если n простое число большее 3, то числитель n-го числа Bernoulli будетъ дѣлиться на n“.*

„Я также замѣтилъ, что если p такой простой дѣлитель числа n, который не входитъ множителемъ въ знаменатель n-го числа Bernoulli, то числитель этого числа дѣлится на p“.

Вороной [1]) доказалъ предложеніе болѣе общее:

„Если число m, значекъ m-го числа Bernoulli, имѣетъ дѣлителемъ число $k = p_1^{\alpha} p_2^{\beta} \ldots p_l^{\lambda}$, гдѣ p_1, p_2, p_l простыя числа, не дѣлящія знаменатель m-го числа Bernoulli, то числитель его будетъ дѣлиться на k.

[1]) Вороной. Сообщенія Харьковскаго Математическаго Общества. 1890.

§ 13. Пусть a и N цѣлыя положительныя взаимно простыя числа. Обозначимъ черезъ

$$r_1, r_2, \ldots r_{N-1} \tag{1}$$

остатки отъ дѣленія на N чиселъ

$$1.a, 2.a, 3a, \ldots (N-1)a;$$

числа (1) представляютъ изъ себя рядъ чиселъ $1, 2, \ldots N-1$ только иначе расположенныхъ

$$a - N\left[\frac{a}{N}\right] = r_1, \; 2a - N\left[\frac{2a}{N}\right] = r_2, \ldots (N-1)a - N\left[\frac{(N-1)a}{N}\right] = r_{N-1}.$$

Возвышая эти равенства въ степень m, получимъ сравненія по модулю N^2

$$a^m - mNa^{m-1}\left[\frac{a}{N}\right] \equiv r_1^m \pmod{N^2}$$

$$2^m a^m - mN2^{m-1}a^{m-1}\left[\frac{2a}{N}\right] \equiv r_2^m \pmod{N^2}$$

. . . . . .

$$(N-1)^m a^m - mN(N-1)^{m-1}a^{m-1}\left[\frac{(N-1)a}{N}\right] \equiv r_{N-1}^m \pmod{N^2}.$$

Складывая всѣ эти сравненія почленно, найдемъ

$$a^m S_m(N-1) - ma^{m-1}N\sum_{i=1}^{N-1} i^{m-1}\left[\frac{ia}{N}\right] \equiv S_m(N-1) \pmod{N^2}$$

$$(a^m - 1)S_m(N-1) \equiv ma^{m-1}N\sum i^{m-1}\left[\frac{ia}{N}\right] \pmod{N^2}.$$

При $m > 1$ можно будетъ написать также сравненіе

$$(a^m - 1)S_m(N) \equiv ma^{m-1}N\sum i^{m-1}\left[\frac{ia}{N}\right] \pmod{N^2},$$

которое мы будемъ употреблять при четномъ значеніи m, т. е. писать

$$(a^{2m} - 1)S_{2m}(N) \equiv 2ma^{2m-1}N\sum i^{2m-1}\left[\frac{ia}{N}\right] \pmod{N^2}. \tag{2}$$

§ 14. Возьмемъ равенство (1) § 5, которое въ примѣненіи къ случаю $x = N$ перепишемъ такъ

$$S_{2m}(N) = \frac{N^{2m+1}}{2m+1} + \frac{N^{2m}}{2} + \frac{2m}{1.2} B_1 N^{2m-1} -$$

$$- \frac{2m(2m-1)(2m-2)}{1.2.3.4} B_2 N^{2m-3} + \ldots + (-1)^{m-2} \frac{2m(2m-1)\ldots 4}{1.2\ldots(2m-2)} B_{m-1} N^3 +$$

$$+ (-1)^{m-1} B_m N, \qquad (1)$$

обозначая $B_m = \frac{P_m}{Q_m}$, не трудно убѣдиться въ справедливости сравненія

$$Q_m S_{2m}(N) \equiv (-1)^{m-1} P_m N \pmod{N^2}. \qquad (2)$$

Для доказательства справедливости послѣдняго сравненія замѣтимъ, что въ равенствѣ (1) можно считать всѣ члены правой части кромѣ послѣдняго сравнимыми съ нулемъ по модулю N^2.

На основаніи сказаннаго въ главѣ о приложеніяхъ конечнаго поля дробность входящихъ въ уравненіе (1) величинъ не можетъ служить препятствіемъ для разсмотрѣнія ихъ по модулю N^2. Необходимо лишь убѣдиться, что, если мы обозначимъ черезъ λ наибольшаго изъ показателей простыхъ чиселъ входящихъ въ знаменатель нѣкотораго общаго члена второй части (1)

$$(-1)^{m-\mu-1} \frac{2m(m-1)\ldots(2m-2\mu+1)}{1.2\ldots 2\mu} \cdot \frac{B_{m-\mu}}{2\mu+1} N^{2\mu+1} \qquad (3)$$

то послѣ откидыванія множителя N^λ останется степень N съ показателемъ не меньшимъ 2.

Въ самомъ дѣлѣ, знаменатель члена (3) состоитъ изъ знаменателя $Q_{m-\mu}$ числа Bernoulli и изъ числа $2\mu+1$. Такъ какъ по теоремѣ Staudt'a всѣ простые множители входятъ въ первой степени въ знаменателяхъ чиселъ Bernoulli, то высшій предѣлъ для числа λ будетъ

$$\lambda = 1 + \nu,$$

гдѣ ν высшій изъ показателей числа $2\mu+1$. Мы получимъ высшій предѣлъ для числа ν, если предположимъ, что $2\mu+1$ есть степень самаго меньшаго нечетнаго простого числа 3.

$$3^\mu = (1+2)^\mu > 1 + 2\mu,$$

значитъ $\nu \leqq \mu$, гдѣ знакъ равенства можетъ быть при $\mu = 1$. Итакъ, откидывая степень N^λ, гдѣ $\lambda \leqq 1 + \mu$ получимъ степень N съ показателемъ

не меньшимъ μ. Такъ какъ при $\mu = 1$ можетъ получаться первая степень, то предпослѣдній членъ требуетъ особеннаго разсмотрѣнія. Въ самомъ дѣлѣ, этотъ членъ есть

$$(-1)^{m-2}\frac{2m(2m-1)}{1.2}\cdot\frac{B_{m-1}}{3}N^3.$$

Здѣсь знаменатель Bernoulli'ева числа уничтожаетъ первую степень N, множитель же 3 не играетъ роли, ибо онъ пропадаетъ отъ умноженія всего уравненія на Q_m (см. § 11).

Итакъ, сравненіе (2) справедливо. Умножая обѣ части сравненія (2) § 13, на Q_m и пользуясь сравненіемъ (2) § 14, получимъ

$$P_m(a^{2m}-1)N \equiv (-1)^{m-1}2ma^{2m-1}NQ_m\sum i^{2m-1}\left[\frac{ia}{N}\right] \pmod{N^2}$$

или, сокращая на N, получаемъ окончательно

$$P_m(a^{2m}-1) \equiv (-1)^{m-1}2ma^{2m-1}Q_m\sum i^{2m-1}\left[\frac{ia}{N}\right] \pmod{N}$$

Примѣняя послѣднее сравненіе къ случаю $N = m$, получимъ

$$P_m(a^{2m}-1) \equiv 0 \pmod{m}. \qquad (4)$$

§ 15. Возьмемъ сравненіе (4) § 14 и предположимъ, что число m имѣетъ дѣлителя

$$k = p_1^{\alpha}p_2^{\beta}\ldots p_l^{\lambda}$$

такого, что относительно простыхъ чиселъ $p_1, p_2 \ldots p_l$ существуетъ свойство не дѣлимости числа $2m$ на числа $p_1 - 1$, $p_2 - 1$, $\ldots p_l - 1$. Другими словами, простыя числа p_1, p_2, $\ldots p_l$ не входятъ въ составъ Q_m.

Пусть a_1 первообразный корень простого числа p_1. Въ такомъ случаѣ, не можетъ имѣть мѣста сравненіе

$$a_1^{2m} - 1 \equiv 0 \pmod{p_1}.$$

Поэтому, на основаніи сравненія (4) § 14 получаемъ

$$P_m \equiv 0 \pmod{p_1^{\alpha}}.$$

Поступая подобнымъ же образомъ, докажемъ

$$P_m \equiv 0 \pmod{p_2^{\beta}}, \quad \ldots \quad P_m \equiv 0 \pmod{p_l^{\lambda}},$$

откуда окончательно

$$P_m \equiv 0 \pmod{k},$$

и теорема Вороного доказана.

Числа Genocchi и Euler'a.

§ 16. Разсмотримъ теперь знакоперемѣнныя суммы одинаковыхъ степеней цѣлыхъ чиселъ.

Предположимъ число x четнымъ

$$m[1^{m-1} + 2^{m-1} + \ldots + (x-1)^{m-1}] = (x + \mathfrak{B})^m - \mathfrak{B}^m. \qquad (1)$$

Примѣнимъ эту формулу къ случаю $\frac{x}{2}$

$$m\left[1^{m-1} + 2^{m-1} + \ldots + \left(\frac{x}{2} - 1\right)^{m-1}\right] = \left(\frac{x}{2} + \mathfrak{B}\right)^m - \mathfrak{B}^m. \qquad (2)$$

Умножая (2) на 2^m и вычитая изъ (1), получимъ

$$m[1^{m-1} - 2^{m-1} + 3^{m-1} - 4^{m-1} + \ldots + (x-1)^{m-1}] =$$

$$= (x + \mathfrak{B})^m - \mathfrak{B}^m - 2^m\left(\frac{x}{2} + \mathfrak{B}\right)^m + 2^m\mathfrak{B}^m. \qquad (3)$$

Составляемъ коэффиціентъ при x^{m-k}

$$C_m{}^k\mathfrak{B}^k - 2^m\frac{1}{2^{m-k}}C_m{}^k\mathfrak{B}^k = C_m{}^k\mathfrak{B}_k(1 - 2^k).$$

Введемъ по примѣру Genocchi [1]) новыя числа, связанныя съ числами Bernoulli при помощи формулъ

$$2(1 - 2^k)\mathfrak{B}_k = G_k. \qquad (4)$$

Формула (3) даетъ

$$2m[1^{m-1} - 2^{m-1} + 3^{m-1} + \ldots + (x-1)^{m-1}] = (x + G)^m - G^m. \qquad (5)$$

На основаніи формулы (4) мы замѣчаемъ, что числа Genocchi съ нечетными значками равны нулю, числа же съ четными значками опредѣляются по формулѣ

$$G_{2k} = (-1)^{k-1}2(1 - 2^{2k})B_k.$$

Числа G_{2k} очевидно цѣлыя, ибо для всякаго нечетнаго простого множителя p знаменателя B_k имѣетъ мѣсто сравненіе $2k \equiv 0 \pmod{p-1}$ а, слѣдовательно, и сравненіе $2^{2k} \equiv 1 \pmod{p}$.

---

[1]) Genocchi. Annali di Tortolini t. III 1852.

§ 17. Выведемъ нѣкоторыя символическія формулы, относящіяся къ числамъ Genocchi.

Прежде всего имѣемъ символическое равенство

$$\frac{1}{2} G^m = \mathfrak{B}^m - (2\mathfrak{B})^m ,$$

откуда

$$\frac{1}{2} f(G) = f(\mathfrak{B}) - f(2\mathfrak{B}) , \tag{1}$$

гдѣ $f(x)$ цѣлая функція $\sum a_n x^n$.

Умножая формулу (5) § 3 на a_n и суммируя, получимъ

$$f'(x) = f(x + \mathfrak{B} + 1) - f(x + \mathfrak{B}) . \tag{2}$$

На основаніи той же формулы (5) § 3 мы можемъ написать

$$x^m = \frac{(x + 1 + \mathfrak{B})^{m+1} - (x + \mathfrak{B})^{m+1}}{m + 1}$$

$$(x + 1)^m = \frac{(x + 2 + \mathfrak{B})^{m+1} - (x + 1 + \mathfrak{B})^{m+1}}{m + 1} ,$$

отсюда, складывая, получимъ

$$x^m + (x + 1)^m = \frac{(x + 2 + \mathfrak{B})^{m+1} - (x + \mathfrak{B})^{m+1}}{m + 1} .$$

Такъ какъ въ этой формулѣ x совершенно произволенъ, то подставимъ вмѣсто него символическую величину $2\mathfrak{B}$, и мы будемъ имѣть

$$(2\mathfrak{B})^m + (2\mathfrak{B} + 1)^m = \frac{[2(\mathfrak{B}' + 1) + \mathfrak{B}]^{m+1} - [2\mathfrak{B}' + \mathfrak{B}]^{m+1}}{m + 1} . \tag{3}$$

Во второй части равенства приходится ввести вмѣсто знака $\mathfrak{B}$ новой введенной символической величины знакъ $\mathfrak{B}'$, ибо тамъ уже находится другая символическая величина $\mathfrak{B}$; хотя обѣ величины $\mathfrak{B}$ и $\mathfrak{B}'$ равносильны, но при символическихъ дѣйствіяхъ надо производить выкладъ отдѣльно относительно знака $\mathfrak{B}'$.

Принимая во вниманіе, что

$$(\mathfrak{B}' + 1)^k - \mathfrak{B}'^k \begin{cases} = 0 \text{ при } k > 1 \\ = 1 \text{ при } k = 1 , \end{cases}$$

мы замѣчаемъ, что во второй части формулы (3) остается только одинъ членъ

$$2\mathfrak{B}^m ,$$

и мы получаемъ

$$(2\mathfrak{B})^m + (2\mathfrak{B}+1)^m = 2\mathfrak{B}^m,$$

откуда

$$f(2\mathfrak{B}) + f(2\mathfrak{B}+1) = 2f(\mathfrak{B}). \qquad (4)$$

Подставляемъ въ (2) $x = 0$

$$f(\mathfrak{B}+1) - f(\mathfrak{B}) = f'(0)$$

и вычитаемъ (4)

$$[f(\mathfrak{B}+1) - f(2\mathfrak{B}+1)] + [f(\mathfrak{B}) - f(2\mathfrak{B})] = f'(0).$$

Принимая же во вниманіе (1) получимъ окончательно

$$f(G+1) + f(G) = 2f'(0).$$

Примѣнимъ эту формулу къ функціи $f(x) = x^m(x-1)^m$, получимъ

$$G^m(G+1)^m + G^m(G-1)^m = 0.$$

Эту формулу можно упростить, написавъ

$$G^m(G+1)^m = 0, \qquad (5)$$

принимая въ соображеніе, что числа Genocchi съ нечетными значками n равны нулю при $n > 1$.

На основаніи формулы (4) § 16 получимъ

$$G_0 = 0,\ G_1 = 1,\ G_2 = -1,$$

слѣдующія числа получаются изъ формулы (5), полагая послѣдовательно $m = 2, 3, 4, \ldots$

$$G_4 = 1,\ G_6 = -3,\ G_8 = 17,\ G_{10} = -155,\ G_{12} = 2073.$$

Формула (5) учитъ, что всѣ числа Genocchi съ четными значками суть числа *цѣлыя и нечетныя*.

§ 18. Въ связи съ числами G_k находятся числа Euler'a E_k, опредѣляемыя символически

$$2mE^{m-1} = (2G+1)^m.$$

Не трудно убѣдиться, что числа Euler'a удовлетворяютъ рекурентному соотношенію

$$(E+1)^m + (E-1)^m = 0.$$

Давая m различныя по порядку значенія, получимъ

$E_{2n+1} = 0$

$E_0 = 1,\ E_2 = -1,\ E_4 = 5,\ E_6 = -61,\ E_8 = 1385,\ E_{10} = -50521, \ldots$

Для болѣе подробнаго изученія этихъ вопросовъ можно рекомендовать—Lucas. Theorie des nombres.

§ 19. Скажемъ теперь нѣсколько словъ о цѣлыхъ частяхъ Bernoulli'евыхъ чиселъ.

Возьмемъ формулу

$$(-1)^n B_n = A_n + \frac{1}{2} + \frac{1}{\alpha} + \frac{1}{\beta} + \ldots + \frac{1}{\lambda}, \qquad (1)$$

гдѣ α, β, . . . λ соотвѣтственныя нечетныя простыя числа.

Сообщимъ элементарныя соображенія Hermite'a, относящіяся къ нахожденію рекурентной формулы для чиселъ A_n.

Соотношеніе

$$(1 + \mathfrak{B})^{2n+1} - \mathfrak{B}^{2n+1} = 0$$

даетъ

$$1 + (2n+1)\mathfrak{B}_1 + C^2_{2n+1}\mathfrak{B}_2 + C^4_{2n+1}\mathfrak{B}_4 + C^6_{2n+1}\mathfrak{B}_6 + \ldots = 0 .$$

Эту формулу перепишемъ въ такомъ видѣ

$$C^2_{2n+1}B_1 - C^4_{2n+1}B_2 + C^6_{2n+1}B_3 - \ldots + (-1)^{n-1}C^{2n}_{2n+1}B_n = n - \frac{1}{2}.$$

Примѣняя формулу (1) получимъ

$$C^2_{2n+1}\left[A_1 + \frac{1}{2} + \frac{1}{3}\right] +$$

$$+ C^4_{2n+1}\left[A_2 + \frac{1}{2} + \frac{1}{3} + \frac{1}{5}\right] +$$

$$+ C^6_{2n+1}\left[A_3 + \frac{1}{2} + \frac{1}{3} + \frac{1}{7}\right] +$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$+ C^{2n}_{2n+1}\left[A_n + \frac{1}{2} + \frac{1}{\alpha} + \ldots + \frac{1}{\lambda}\right] + n - \frac{1}{2} = 0 . \qquad (2)$$

Покажемъ, что всѣ дроби сокращаются. Разсмотримъ сначала дробь $\frac{1}{2}$. Въ первую часть уравненія (2) входитъ выраженіе

$$\frac{1}{2}\left[C^2_{2n+1} + C^4_{2n+1} + \ldots + C^{2n}_{2n+1} - 1\right] = \frac{2^{2n} - 2}{2} = 2^{2n-1} - 1 \quad [1]).$$

---

[1]) Сумма биноміальныхъ коэффиціентовъ четнаго порядка равна суммѣ коэффиціентовъ нечетнаго порядка.

Покажемъ, что будетъ цѣлымъ числомъ выраженіе

$$\sigma(p) = \frac{1}{p}\left[C_{2n+1}^{p-1} + C_{2p+1}^{2(p-1)} + C_{2n+1}^{3(p-1)} + \ldots\right].$$

Въ самомъ дѣлѣ, разсмотримъ въ числовомъ полѣ $G[p]$ уравненіе

$$x^{p-1} = 1, \qquad (3)$$

пусть ω обозначаетъ корень этого уравненія.

Будемъ имѣть на основаніи § 25 гл. III.

$$\sum(1+\omega)^{2n+1} = (p-1)\left|1 + C_{2n+1}^{p-1} + C_{2n+1}^{2(p-1)} + \ldots\right|,$$

гдѣ сумма распространена на всѣ корни уравненія (3).

Но мы имѣемъ кромѣ того

$$\sum(1+\omega)^{2n+1} + 1^{2n+1} = 0,$$

ибо нечетное число $2n+1$ не дѣлится на $p-1$, и когда ω пробѣгаетъ элементы $1, 2, 3, \ldots p-1$, удовлетворяющіе уравненію (3), величины 1 и $1+\omega$ пробѣгутъ ту же совокупность.

Итакъ

$$C_{2n+1}^{p-1} + C_{2n+1}^{2(p-1)} + \ldots \equiv 0 (\mathrm{mod}\, p).$$

Значитъ $\sigma(p)$ есть число цѣлое.

Мы получаемъ окончательно формулу Hermite'a

$$C_{2n+1}^{2}A_1 + C_{2n+1}^{4}A_2 + \ldots + C_{2n+1}^{2n}A_n + n + 2^{2n-1} - 1 + \sum\sigma(p) = 0.$$

ГЛАВА XV.

О задачѣ Fermat'a.

§ 1. Частный случай $n = 2$ въ Діофантовомъ уравненіи

$$x^n + y^n = z^n$$

представляетъ задачу нахожденія прямоугольнаго треугольника, катеты и гипотенуза котораго выражаются цѣлыми числами. Уже въ древности были извѣстны рѣшенія: $3^2 + 4^2 = 5^2$, $5^2 + 12^2 = 13^2$, . . .

Не трудно найти всѣ возможныя рѣшенія уравненія

$$x^2 + y^2 = z^2. \quad (1)$$

Euler предложилъ для этой цѣли слѣдующія разсужденія. Введемъ вмѣсто z новую неизвѣстную u, полагая

$$z = y + u;$$

тогда уравненіе (1) обратится въ такое

$$x^2 = 2uy + u^2. \quad (2)$$

Положимъ $u = q^2 r$, гдѣ q^2 наибольшій квадратъ, заключающійся въ u, такъ что r заключаетъ простые множители въ первыхъ степеняхъ. Уравненіе показываетъ, что x^2 дѣлится на q^2, значитъ x должно дѣлиться на q, и мы имѣемъ право написать

$$x = qm,$$

отсюда уравненіе (2) приводится къ слѣдующему

$$m^2 = 2ry + q^2 r^2. \quad (3)$$

итакъ m^2 дѣлится на r, но r не имѣетъ кратныхъ множителей, значитъ m дѣлится на r, то есть

$$m = pr .$$

Сопоставляя всѣ полученныя формулы, приходимъ къ выводу, что

$$x = pqr , \; y = \frac{1}{2} r(p^2 - q^2) , \; z = \frac{1}{2} r(p^2 + q^2) . \qquad (4)$$

Не трудно убѣдиться, что необходимо положить $r = 2$.

Въ самомъ дѣлѣ, три числа x, y, z, можно считать взаимно простыми и значитъ для r возможны только два значенія 1 и 2. Но значеніе $r = 1$ надо откинуть, такъ какъ формула $y = \frac{1}{2}(p^2 - q^2)$ требовала бы предположить, что p и q или оба четныя, или оба нечетныя и тогда y выходитъ четнымъ числомъ намъ же достаточно предположить число y нечетнымъ. Итакъ получаются окончательно формулы

$$x = 2pq , \; y = p^2 - q^2 , \; z = p^2 + q^2$$

въ которыхъ p и q взаимно простыя, изъ которыхъ одно четное, а другое нечетное.

§ 2. Для доказательства великой теоремы Фермата, что уравненіе $x^n + y^n = z^n$ невозможно при $n > 2$ достаточно убѣдиться, что оно невозможно когда $n = 4$ и когда n есть нечетное простое число.

Мы ограничимся въ нашемъ элементарномъ курсѣ доказательствомъ случая $n = 4$.

Euler показываетъ, что уже уравненіе

$$\alpha^4 + \beta^4 = c^2 \qquad (1)$$

невозможно въ цѣлыхъ отличныхъ отъ нуля числахъ.

Конечно достаточно доказать невозможность уравненія (1) въ числахъ взаимнопростыхъ.

Уравненіе (1) переписанное въ видѣ

$$(\alpha^2)^2 + (\beta^2)^2 = c^2$$

является частнымъ случаемъ, разобраннаго въ предыдущемъ параграфѣ, и мы имѣемъ

$$\alpha^2 = 2pq , \; \beta^2 = p^2 - q^2 , \; c = p^2 + q^2 ;$$

второе изъ этихъ уравненій имѣетъ опять видъ

$$q^2 + \beta^2 = p^2 ,$$

такъ какъ β должно быть нечетнымъ, то мы получаемъ

$$q = 2tu, \quad \beta = t^2 - u^2, \quad p = t^2 + u^2;$$

подобно числамъ p и q должны быть взаимно простыми числа t и u. Вставляя полученныя значенія p и q въ $\alpha^2 = 2pq$, будемъ имѣть

$$\left(\frac{\alpha}{2}\right)^2 = tu(t^2 + u^2)$$

три числа t, u, $t^2 + u^2$ суть взаимно простыя, значитъ всѣ они должны быть полными квадратами, то есть

$$t = \alpha_1^2, \quad u = \beta_1^2, \quad t^2 + u^2 = c_1^2. \tag{2}$$

Числа α_1, β_1, c_1, всѣ три отличны отъ нуля, ибо иначе было бы равно нулю и число $\alpha = 2\alpha_1\beta_1c_1$.

Уравненія (2) даютъ

$$\alpha_1^4 + \beta_1^4 = c_1^2. \tag{3}$$

Мы пришли къ новому рѣшенію уравненія (1) съ числами меньшими. Въ самомъ дѣлѣ

$$c = p^2 + q^2 = (t^2 + u^2)^2 + 4t^2u^2 = c_1^4 + 4t^2u^2,$$

то есть

$$c > c_1^4 \quad \text{или} \quad c_1 < \sqrt[4]{c}.$$

Продолжая разсуждать аналогично, мы будемъ приходить къ новымъ рѣшеніямъ

$$\alpha_2^4 + \beta_2^4 = c_2^2, \quad \alpha_3^4 + \beta_3^4 = c_3^2 \ldots$$

гдѣ числа

$$c, \ c_1, \ c_2, \ c_3, \ \ldots$$

идутъ убывая, пока не дойдемъ до невозможнаго уравненія

$$\alpha_k^4 + \beta_k^4 = 1,$$

ибо оба числа α_k и β_k отличны отъ нуля.

§ 3. Въ высшей степени важно подчеркнуть тотъ фактъ, что во всѣхъ извѣстныхъ до сихъ поръ доказательствахъ теоремы Fermat'a приходится задачу разбивать на двѣ. Доказывать сначала невозможность уравненія

$$x^p + y^p = z^p$$

въ томъ случаѣ, когда всѣ три числа x, y, z не дѣлятся на простого показателя p. Этотъ случай мы будемъ называть первой половиной задачи. Второй половиной мы будемъ называть разборъ случая, когда одно изъ чиселъ x, y, z дѣлится на p.

Характернымъ является, что во всѣхъ доказательствахъ Euler'a, Dirichlet, Lamé и Kummer'a первая половина задачи допускаетъ прямое доказательство. Вторая же половина требуетъ рекурентнаго способа доказательства, аналогичнаго тому, которое мы привели для случая $n = 4$. То есть, предполагается существованіе одного рѣшенія, тогда приходятъ путемъ умозаключеній къ необходимости новаго рѣшенія въ меньшихъ числахъ.

§ 4. Въ послѣднее время молодому нѣмецкому ученому Wieferich'у удалось свести первую половину задачи къ весьма важному критеріуму.

Теорема Wieferich'a. Если уравненіе $x^p + y^p = z^p$ *рѣшается въ цѣлыхъ числахъ не дѣлящихся на* p, *то имѣетъ мѣсто сравненіе*

$$2^{p-1} \equiv 1 \pmod{p^2}.$$

Мнѣ извѣстно, что послѣднее сравненіе никогда не имѣетъ мѣста, слѣдовательно, первая половина задачи Fermat'a можетъ считаться рѣшенной.

§ 5. Что касается второй половины задачи, то тутъ не извѣстно иныхъ путей кромѣ изслѣдованій по Kummer'у. Повидимому усилія должны быть направлены къ устраненію ограниченій Kummer'овскаго доказательства.

ЧИСЛОВЫЯ ТАБЛИЦЫ.

A.

Таблицы дѣлителей цѣлыхъ чиселъ

отъ 1 до 107999 *).

Способъ употребленія.

Каждая таблица (латинскія цыфры) расположена на трехъ страницахъ (буквы a, b, c) и въ началѣ каждой указаны наименьшее и наибольшее число, дѣлителя котораго можно найти изъ таблицы. Въ таблицахъ помѣщены только числа не дѣлящіяся на 2, 3 и 5; поэтому эти множители, если они входятъ въ составъ испытываемаго числа, слѣдуетъ предварительно выдѣлить простымъ дѣленіемъ.

Пусть требуется опредѣлить простые дѣлители числа не превосходящаго 107999 (не дѣлящагося на 2, 3 и 5).

Разбиваемъ это число справа на лѣво на грани, по двѣ цыфры въ каждой. Въ соотвѣтствующей таблицѣ находимъ вертикальный столбецъ, верхнее число котораго отвѣчаетъ второй грани разложенія, и горизонтальный столбецъ, крайнее лѣвое число котораго отвѣчаетъ первой грани. Если на пересѣченіи этихъ двухъ столбцовъ—пустое мѣсто, то испытываемое число—простое; въ противномъ случаѣ оно имѣетъ дѣлителемъ число стоящее на пересѣченіи. Выдѣляя дѣленіемъ найденнаго дѣлителя, если онъ существуетъ, къ частному примѣняемъ снова тѣ же правила. Будемъ такимъ образомъ идти впередъ до тѣхъ поръ, пока одно изъ частныхъ не будетъ простымъ числомъ.

Примѣры:

1) Дано число 31331; требуется разложить его на простые множители. Разбиваемъ сначала число на грани: 3 | 13 | 31. Изъ таблицы IV b. находимъ множителя 17. Выдѣляя его изъ испытываемаго числа, получаемъ: $31331 : 17 = 1843$. Для 18 | 43 изъ таблицы I a. находимъ множителя 19. Отсюда имѣемъ: $1843 : 19 = 97$. Но изъ той же таблицы I a. видно, что число 97—простое; слѣдовательно, искомое разложеніе будетъ: $31331 = 17.19.97$.

2) Для числа 83339 изъ таблицы X c. находимъ сразу, что оно простое.

---

*) Эти таблицы перепечатаны изъ: „Table des diviseurs pour tous les nombres des 1-e, 2-e et 3-e million, ou plus exactement, depuis la 3036000. avec les nombres premiers qui s'y trouvent“ par I. Ch. Burckhardt. Paris 1817.

	00	03	06	09	12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57	60	63	66	69	72	75	78	81	84	87
01	—	7	—	17	—	19	—	11	7	37	—	—	13	47	—	7	—	—	11	—	17	—	7	67	19	13	29	—	31	7
07	—	—	—	—	17	11	13	7	29	—	31	—	—	—	7	—	11	—	—	13	—	7	—	—	—	—	37	11	7	—
11	—	—	13	—	7	—	—	—	—	—	—	7	23	—	—	13	17	19	7	—	—	—	11	—	—	7	73	—	13	31
13	—	—	—	11	—	17	7	—	19	—	23	—	—	7	11	—	—	—	—	29	7	59	17	31	—	11	13	7	47	—
17	—	—	—	7	—	37	23	29	—	11	7	31	—	—	—	—	—	7	—	—	11	—	13	—	7	—	—	—	19	23
19	—	11	—	—	23	7	17	13	41	—	—	—	7	—	—	—	61	—	—	7	13	71	—	11	—	73	7	23	—	—
23	—	17	7	13	—	—	—	11	—	7	—	—	—	—	41	—	7	47	11	59	19	—	37	7	31	—	—	—	—	11
29	—	7	17	—	—	11	31	—	7	—	13	—	19	—	—	7	11	23	61	17	—	—	7	13	—	—	—	11	—	7
31	—	—	—	7	—	—	—	—	11	—	7	—	—	—	—	23	—	7	—	11	37	13	19	29	7	17	41	47	—	—
37	—	—	7	—	—	29	11	—	—	7	—	47	—	31	19	13	7	11	—	—	—	—	—	7	—	—	17	79	11	—
41	—	11	—	—	17	23	7	—	—	—	—	13	11	7	—	19	47	53	—	—	7	17	29	11	13	—	—	7	23	—
43	—	7	—	23	11	—	19	—	7	13	17	—	—	—	—	7	29	37	—	—	—	—	7	53	—	19	11	17	—	7
47	—	—	—	—	29	7	—	19	—	41	11	—	7	—	31	—	37	—	13	7	—	11	17	—	—	—	7	—	—	—
49	7	—	11	13	—	—	43	7	31	—	—	17	41	11	7	—	13	19	—	—	23	7	61	—	11	—	47	29	7	13
53	—	—	—	—	7	—	17	—	11	—	43	7	13	59	—	29	23	—	7	11	—	—	—	17	—	7	—	31	79	—
59	—	—	—	7	—	—	11	17	—	31	7	—	—	37	—	47	43	7	53	13	73	—	—	—	7	—	29	41	11	19
61	—	19	—	31	13	7	—	—	23	11	—	—	7	17	—	—	—	13	43	7	11	—	—	—	53	—	7	—	—	—
67	—	—	23	—	7	—	—	11	—	—	—	7	19	—	17	—	31	—	7	73	—	—	59	—	13	7	—	—	—	11
71	—	7	11	—	31	—	—	13	7	17	37	—	—	11	—	7	—	—	—	29	13	23	7	—	11	67	17	—	43	7
73	—	—	—	7	19	11	—	41	—	47	7	—	—	29	—	17	11	7	13	23	—	—	—	19	7	—	—	11	37	31
77	7	13	—	—	—	19	—	7	—	—	17	11	—	41	7	23	—	31	—	53	59	7	11	—	19	—	—	13	7	67
79	—	—	7	11	—	—	—	—	37	7	—	31	13	23	11	19	7	—	—	—	—	—	—	7	29	11	—	—	61	—
83	—	—	—	—	—	—	7	37	13	11	—	17	29	7	—	—	19	71	—	—	7	13	41	—	—	—	—	7	17	—
89	—	—	13	23	—	7	—	11	19	—	—	—	7	—	—	13	—	—	11	7	—	—	—	29	37	—	7	19	13	11
91	7	17	—	—	—	37	31	7	47	—	11	—	—	13	7	—	67	29	17	—	—	—	7	—	—	23	—	13	—	7	59
97	—	—	17	—	—	—	7	13	11	—	19	43	—	7	—	—	59	—	23	11	7	—	37	—	—	71	53	7	29	19

	01	04	07	10	13	16	19	22	25	28	31	34	37	40	43	46	49	52	55	58	61	64	67	70	73	76	79	82	85	88
01	—	—	—	7	—	—	—	31	41	—	7	19	—	—	11	43	13	7	—	—	—	37	—	—	7	11	—	59	—	13
03	—	13	19	17	—	7	11	—	—	—	29	41	7	—	13	—	—	11	—	7	17	19	—	47	67	—	7	13	11	—
07	—	11	7	19	—	—	—	—	23	7	13	—	11	—	59	17	7	41	—	—	31	43	19	7	—	—	—	29	47	—
09	—	—	-	—	7		23	47	13	53	—	7	—	19	31	11	--	—	7	37	41	13	—	43	—	7	11	—	67	23
13	—	7	23	—	13	—	—	—	7	29	11	—	47	—	19	7	17	13	37	—	—	11	7	—	71	23	41	43	—	7
19	7	—	—	—	—	—	19	7	11	—	—	13	—	—	7	31	—	17	—	11	29	7	—	—	13	19	—	-	7	—
21	11	—	7	—	—	—	17	—	—	7	—	11	61	—	29	--	7	23	—	—	—	—	11	7	—	—	89	—	—	—
27	—	7	—	13	—	—	41	17	7	11	53	23	—	—	—	7	13	—	—	—	11	—	7	—	17	29	--	19	—	7
31	—	—	17	—	11	7	—	23	—	19	31	47	7	29	61	11	—	—	—	7	--	59	53	79	—	13	7	—	19	—
33	7	—	—	—	31	23	—	7	17	—	13	—	—	37	7	41	—	—	11	19	—	7	—	13	—	17	—	—	7	11
37	—	19	11	17	7	—	13	—	43	—	—	7	37	11	—	—	—	—	7	13	17	41	—	31	11	7	—	—	—	—
39	—	—	—	—	13	11	7	—	—	17	43	19	—	7	—	—	11	13	29	—	7	47	23	—	41	—	17	7	—	—
43	11	—	—	7	17	31	29	—	—	—	7	11	19	13	43	—	—	7	23	—	—	17	11	—	7	—	13	—	—	37
49	—	—	7	—	19	17	—	13	—	7	47	—	23	—	—	—	7	29	31	—	11	—	17	7	—	—	—	73	83	—
51	—	11	—	—	7	13	—	—	—	—	23	7	11	—	19	—	—	59	7	—	—	—	43	11	—	7	—	37	17	53
57	—	—	—	7	23	—	19	37	—	—	7	—	13	—	—	—	—	7	—	—	47	11	29	—	7	13	73	23	43	17
61	7	—	—	—	—	11	37	7	13	—	29	—	—	31	7	59	11	—	67	—	61	7	—	23	17	47	19	11	7	—
63	—	—	7	—	29	—	13	31	11	7	—	—	53	17	—	—	7	19	—	11	—	23	—	7	37	79	—	—	—	—
67	—	—	13	11	—	—	7	—	17	47	—	—	—	7	11	13	—	23	19	—	7	29	67	37	53	11	31	7	13	—
69	13	7	—	—	37	—	11	—	7	19	—	—	—	13	17	7	—	11	—	—	31	—	7	—	—	—	13	—	11	7
73	—	11	—	29	—	7	—	—	31	13	19	23	7	—	—	—	—	—	—	7	—	—	13	11	73	—	7	—	—	19
79	—	—	19	13	7	23	—	43	—	—	11	7	—	--	29	—	13	—	7	—	37	11	—	—	47	7	79	17	23	13
81	—	13	11	23	—	41	7	—	29	43	—	59	19	7	13	31	17	—	—	—	7	—	—	73	11	—	23	7	—	83
87	11	—	—	—	19	7	—	—	13	—	—	11	7	61	41	43	—	17	37	7	23	13	11	19	83	—	7	—	31	—
91	—	—	7	—	13	19	11	29	—	7	—	—	17	—	—	—	7	11	—	43	41	-	—	7	19	—	61	—	11	17
93	—	17	13	—	7	—	—	—	—	11	31	7	—	—	23	13	—	67	7	71	11	43	—	41	—	7	—	—	13	—
97	—	7	—	—	11	—	—	—	7	—	23	13	—	17	—	7	19	—	29	—	—	73	7	47	13	43	11	—	—	7
99	—	—	17	7	—	—	—	11	23	13	7	—	29	—	53	37	—	7	11	17	—	67	13	31	7	—	19	43	—	11

	02	05	08	11	14	17	20	23	26	29	32	35	38	41	44	47	50	53	56	59	62	65	68	71	74	77	80	83	86	89
03	7	—	11	—	23	13	—	7	19	—	—	31	—	11	7	—	—	—	13	—	—	7	—	—	11	—	53	19	7	29
09	11	—	—	—	—	—	7	—	—	—	—	11	13	7	—	17	—	—	71	19	7	23	11	—	31	13		7	—	59
11	—	7	—	11	17	29	—	—	7	41	13	—	37	—	11	7	—	47	31	23	—	17	7	13	—	11	—	—	79	7
17	7	11	19	—	13	17	—	7	—	—	—	—	11	23	7	53	29	13	41	61	—	7	17	11	—	—	—	—	7	37
21	13	—	—	19	7	—	43	11	—	23	—	7	—	13	—	—	—	17	7	31	—	—	19	—	41	7	13	53	37	11
23	—	—	—	—	—	—	7	23	43	37	11	13	—	7	—	—	—	—	—	—	7	11	—	17	13	—	71	7	—	—
27	—	17	—	7	—	11	—	13	37	—	7	—	43	—	19	29	11	7	17	—	13	61	—	—	7	—	23	11	—	79
29	—	23	—	—	—	7	—	17	11	29	—	—	7	—	43	—	47	73	13	7	—	—	—	—	17	59	7	—	—	—
33	—	13	7	11	—	—	19	—	—	7	53	—	—	—	11	—	7	—	43	17	23	47	—	7	—	11	29	13	89	—
39	—	7	—	17	—	37	—	—	7	—	41	—	11	—	23	7	—	19	—	—	17	13	7	11	43	71	—	31	53	7
41	—	—	29	7	11	—	13	—	19	17	7	—	23	41	—	11	71	7	—	13	79	31	—	37	7	—	11	19	—	—
47	13	—	7	31	—	—	23	—	—	7	17	—	—	11	—	47	7	—	—	19	—	—	41	7	11	61	13	17	—	23
51	—	19	23	—	—	17	7	—	11	13	—	53	—	7	—	—	—	—	—	11	7	—	13	—	—	23	83	7	41	—
53	11	7	—	—	—	—	—	13	7	—	—	11	—	—	61	7	31	53	—	—	13	—	7	23	29	—	—	—	17	7
57	—	—	—	13	31	7	11	—	—	—	—	—	7	—	—	67	13	11	—	7	—	79	—	17	—	—	—	7	61	11	13
59	7	13	—	19	—	—	29	7	—	11	—	—	17	—	7	—	—	23	—	59	11	7	19	—	—	—	—	13	7	17
63	—	—	—	—	7	41	—	17	—	—	13	7	—	23	—	11	61	31	7	67	—	—	—	13	17	7	11	—	—	—
69	—	—	11	7	13	29	—	23	17	—	7	43	53	11	41	19	37	7	—	47	—	—	—	67	7	17	—	—	—	—
71	—	—	13	—	—	7	19	—	—	—	—	—	7	43	17	13	11	41	53	7	—	—	—	71	31	19	7	11	13	—
77	—	—	—	11	7	—	31	—	—	13	29	7	—	—	11	17	—	19	7	43	—	—	13	—	—	7	41	—	—	47
81	—	7	—	—	—	13	—	—	7	11	17	—	—	37	—	7	—	—	13	—	11	—	7	43	—	31	—	17	—	7
83	—	11	—	7	—	—	—	—	—	19	7	—	11	47	—	—	13	7	—	31	61	29	—	11	7	43	59	83	19	13
87	7	—	—	—	—	—	—	7	—	29	19	17	13	53	7	—	—	—	11	—	—	7	71	—	—	13	—	—	7	11
89	17	19	7	29	—	—	—	—	—	7	11	37	—	59	67	—	7	17	—	53	19	11	83	7	—	—	—	—	—	89
93	—	—	19	—	—	11	7	—	—	41	37	—	17	7	—		11	—	—	13	7	19	61	—	59	—	—	7	—	17
99	13	—	29	11	—	7	—	—	—	—	—	59	7	13	11	—	—	—	41	7	—	—	—	23	—	11	7	37	—	—

l c.

	90	93	96	99	1 02	05	08	11	14	17	20	23	26	29	32	35	38	41	44	47	50	53	56	59	62	65	68	71	74	77
01	—	71	—	—	101	—	7	17	13	—	11	—	—	7	43	23	37	59	—	61	7	11	—	—	17	29	53	7	—	31
07	—	41	13	—	59	7	101	29	11	23	—	31	7	—	47	13	—	—	—	7	43	—	—	—	19	17	7	—	13	—
11	—	—	7	11	—	23	19	41	—	7	—	13	—	—	11	59	7	103	—	47	17	61	67	7	13	11	—	71	23	89
13	—	67	—	23	7	—	11	—	101	13	41	7	—	37	73	—	19	11	7	—	—	—	13	—	31	7	17	109	11	—
17	71	7	59	47	17	13	29	—	7	—	61	109	11	—	—	7	41	19	13	—	—	17	7	11	—	83	67	—	—	7
19	29	—	—	7	11	67	31	—	19	—	7	97	—	—	—	11	13	7	—	41	23	—	—	—	7	—	11	17	—	13
23	7	—	—	—	—	17	79	7	—	19	11	—	13	—	7	—	23	29	—	—	83	7	17	—	—	13	—	—	7	37
29	—	19	—	—	53	—	7	31	11	37	23	—	73	7	—	83	—	71	47	11	7	—	—	17	—	—	—	7	29	—
31	11	7	—	—	13	—	—	—	7	—	53	11	17	67	101	7	—	13	—	—	—	—	7	89	—	61	—	37	—	7
37	7	—	23	19	29	41	—	7	—	11	—	13	—	17	7	—	101	67	—	—	11	7	19	—	13	23	113	—	7	—
41	—	—	31	—	7	83	37	13	17	59	—	7	—	—	—	11	—	79	7	—	13	23	—	19	109	7	11	61	107	113
43	—	—	—	61	—	13	7	11	—	—	—	—	47	7	17	29	109	—	11	23	7	67	—	107	37	71	—	7	—	11
47	83	13	11	7	—	53	—	71	—	17	7	—	—	11	13	19	61	7	—	—	41	103	—	37	7	—	17	13	73	—
49	—	—	—	—	37	7	19	—	107	31	—	53	7	23	—	17	11	—	—	7	101	—	—	41	—	13	7	11	—	—
53	11	47	7	37	—	61	—	19	13	7	17	11	—	—	29	—	7	—	97	—	—	13	11	7	—	—	19	17	31	41
59	—	7	13	23	—	—	—	—	7	11	31	17	—	—	—	7	—	—	19	—	11	—	7	—	71	29	23	—	13	7
61	13	11	—	7	31	59	—	—	73	19	7	47	11	13	89	71	83	7	—	29	—	—	—	11	7	—	13	131	19	—
67	—	17	7	—	—	—	—	13	—	7	11	83	53	—	—	—	7	31	17	—	13	11	—	7	—	—	101	—	—	109
71	47	—	19	13	—	11	7	—	—	79	—	89	—	7	23	41	11	37	29	—	7	19	—	—	53	73	—	7	—	13
73	43	7	17	—	—	97	83	—	7	61	—	—	19	—	13	7	—	—	41	11	—	—	7	—	—	—	47	13	101	7
77	29	—	—	11	43	7	73	—	23	—	13	—	7	19	11	—	—	—	31	7	—	—	61	13	41	11	7	89	—	29
79	7	83	—	17	19	71	11	7	13	—	47	—	31	—	7	37	—	11	—	—	17	7	—	19	73	59	—	41	7	23
83	31	11	23	67	7	19	—	53	—	—	43	7	11	—	37	17	—	13	7	—	—	—	—	11	19	7	—	—	—	—
89	61	41	—	7	—	—	—	67	—	—	7	13	—	31	97	107	17	7	—	23	79	11	29	59	7	53	—	—	—	—
91	—	—	11	97	41	7	—	19	—	13	107	—	7	11	—	—	29	23	43	7	—	—	13	—	11	47	7	—	—	—
97	11	—	—	13	7	—	17	—	—	47	—	7	—	41	—	—	13	—	7	—	31	89	11	17	43	7	61	29	—	13

	91	94	97	1 00	03	06	09	12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57	60	63	66	69	72	75	78
01	19	7	89	73	—	—	11	23	7	—	—	—	13	—	47	7	—	11	17	19	—	—	7	—	—	13	—	103	11	7
03	—	—	31	7	—	23	—	17	—	11	7	79	—	—	53	61	—	7	—	113	11	73	41	13	7	—	—	23	19	
07	7	23	17	—	11	—	13	7	37	—	—	19	97	—	7	11	—	—	89	13	—	7	113	—	23	—	11	—	7	—
09	—	97	7	—	13	103	—	11	17	7	—	—	71	—	—	31	7	13	11	59	29	19	23	7	47	17	37	—	—	11
13	13	—	11	17		—	7	—	29	—	—	—	—	7	—	—	—	61	23	—	7	—	19	67	11	37	13	7	83	47
19	11	—	—	43	17	7	61	13	—	53	—	11	7	47	19	—	31	59	—	7	13	17	11	83	—	—	7	67	—	103
21	7	—	—	11	—	13	67	7	41	—	17	—	—	29	7	53	—	—	13	—	—	7	79	37	19	11	—	17	7	71
27	—	11	71	37	23	—	7	103	—	—	67	17	11	7	—	—	19	41	73	—	7	—	—	11	29	13	—	7	17	—
31	23	—	37	7	—	—	17	11	13	—	7	31	29	83	—	43	—	7	11	—	—	13	—	17	7	—	—	—	47	11
33	—	—	—	79	—	7	13	47	19	—	11	—	7	—	67	—	—	43	—	7	37	11	—	—	—	—	7	19	89	17
37	—	—	7	—	—	11	—	17	83	7	53	—	47	—	—	13	7	23	—	37	—	43	—	7	17	127	—	11	13	—
39	13	—	—	—	7	—	—	—	11	—	61	7	—	13	—	23	53	29	7	11		—	—	43	—	7	13	—	—	—
43	41	7	—	11	—	29	31	—	7	13	—	23	—	—	11	7	73	—	—	—	19	—	7	61	59	11	—	43	53	7
49	7	11	—	13	79	23	—	7	—	17	—	59	11	—	7	—	13	—	—	31	—	7	—	11	—	—	17	47	7	13
51	—	13	7	19	11	—	47	—	—	7	29	—	41	31	13	11	7	—	—	—	109	—	19	7	83	—	11	13	—	—
57	—	7	11	89	—	—	—	—	7	71	—	—	—	11	19	7	17	53	—	83	23	13	7	—	11	—	31	—	97	7
61	—	—	43	—	13	7	97	—	11	29	—	17	7	37	31	19	23	13	—	7	—	—	—	—	—	—	7	41	17	53
63	7	—	13	29	43	—	19	7	31	—	—	11	—	—	7	13	—	17	—	89	59	7	11	—	—	19	—	61	7	—
67	89	—	—	—	7	—	11	19	43	—	23	7	17	73	—	79	—	11	7	-	29	—	—	—	13	7	19	31	11	17
69	53	17	—	—	—	47	7	59	23	11	43	37	113	7	29	—	61	19	17	—	7	31	13	—	—	79	71	7	—	107
73	—	—	29	7	11	13	—	—	71	31	7	—	53	17	43	11	89	7	13	107	—	—	—	—	7	—	11	23	—	61
79	67	—	7	—	97	59	—	—	—	7	19	—	13	11	17	—	7	109	61	—	43	23	31	7	11	13	—	37	—	19
81	—	19	—	17	7	11	79	29	37	109	13	7	—	103	—	—	—	11	—	7	23	17	113	43	13	—	7	—	11	—	—
87	—	53	—	7	13	—	—	—	—	—	7		19	23	11	—	71	7	29	—	—	17	—	—	7	11	—	59	43	31
91	7	—	—	—	—	—	29	7	67	11	73	—	—	13	7	—	17	31	—	—	11	7	—	—	37	—	13	—	7	—
93	29	11	7	—	19	17	—	23	—	7	89	13	11	—	59	—	7	—	—	53	—	—	17	7	13	—	—	—	73	29
97	17	—	97	23	37	19	7	11	—	—	—	—	67	7	—	—	—	17	11	—	7	—	—	—	19	59	23	7	—	11
99	—	7	41	—	—	13	17	—	7	73	11	29	—	—	—	7	—	79	13	47	—	11	7	17	23	—	89	—	—	7

II b.

	92	95	98	1 01	04	07	10	13	16	19	22	25	28	31	34	37	40	43	46	49	52	55	58	61	64	67	70	73	76	79
03	—	13	—	—	101	7	—	89	41	—	—		7	—	13	71	11	—	17	7	23	37	—	—	47	—	7	11	29	—
09	—	37	17	11	7	—	101	43	13	—	29	7	—	—	11	—	—	41	7	17	67	13	—	89	61	7	73	19	—	—
11	61	—	—	—	29	—	7	—	17	43	—	—	23	7	—	—	—	11	19	13	7	—	97	—	—	17	—	7	11	—
17	13	31	—	67	11	7	23	—	—	17	19	—	7	13	—	11	107	103	47	7	—	59	—	71	—	73	7	—	79	19
21	—	—	7	29	17	71	103	—	—	7	11	19	—	—	—	—	7	—	—	43	31	11	13	7	—	23	—	—	67	—
23	23	89	11	53	7	—	73	13	59	—	17	7	—	11	31	—	37	—	7	—	13	19	—	23	11	7	29	17	—	—
27	—	7	31	13	—	17	—	47	7	—	—	—	101	—	29	7	13	—	—	11	—	—	7	—	—	43	—	—	—	7
29	11	13	—	7	—	—	41	—	29	79	7	11	—	19	13	—	—	7	—	—	97	53	11	127	7	—	—	13	17	—
33	7	—	—	—	—	—	11	7	—	—	13	83	41	23	7	31	—	11	—	109	—	7	71	13	—	29	—	—	7	79
39	—	—	—	—	11	—	7	17	103	—	—	—	37	7	89	11	101	13	—	—	7	41	47	—	17	19	11	7	31	—
41	—	7	13	—	53	23	61	11	7	—	—	—	—	17	—	7	19	—	11	67	—	—	7	—	41	—	—	—	13	7
47	7	—	43	73	31	11	—	7	19	13	37	—	29	—	7	59	11	—	97	—	79	7	13	67	—	—	—	11	7	131
51	11	—	—	—	7	13	43	—	61	17	—	7	71	—	—	—	—	113	7	—	101	—	11	31	—	7	17	—	19	29
53	19	41	59	11	—	—	7	—	43	—	—	—	—	7	11	17	13	31	—	19	7	103	83	29	—	11	—	7	127	13
57	—	19	—	7	—	31	—	41	—	11	7	29	13	59	—	—	—	7	—	—	11	47	101	107	7	13	37	17	—	—
59	47	11	—	—	—	7	—	37	89	—	13	19	7	—	43	—	17	83	107	7	—	—	—	11	109	—	7	—	—	—
63	59	73	7	—	—	47	13	11	107	7	—	17	19	—	—	—	7	53	11	13	—	79	29	7	101	—	113	97	17	11
69	13	7	71	—	19	11	—	—	7	—	—	—	17	13	—	7	11	—	—	—	—	—	7	19	43	41	13	11	—	7
71	73	17	—	7	37	—	—	83	11	—	7	13	61	—	19	47	—	7	17	11	—	23	59	103	7	31	43	29	41	—
77	—	61	7	—	—	13	11	31	—	7	—	—	79	—	—	23	7	11	13	17	—	37	—	7	—	19	—	—	11	—
81	—	11	41	—	47	—	7	19	—	—	—	23	11	7	13	—	—	73	53	71	7	—	—	11	—	97	19	7	—	—
83	—	7	—	17	11	41	—	—	7	23	71	—	13	—	97	7	—	19	—	—	17	—	7	—	53	13	11	—	—	7
87	37	—	—	61	—	7	—	59	13	—	11	41	7	—	—	17	—	—	19	7	—	11	—	—	—	—	7	—	23	—
89	7	43	11	23	17	—	13	7	—	19	—	—	—	11	7	—	73	—	37	13	—	7	—	—	11	103	23	—	7	—
93	—	53	13	—	7	43	—	—	11	67	19	7	—	79	103	13	17	37	7	11	41	31	23	—	—	7	—	—	13	19
99	17	29	19	7	—	—	11	—	—	13	7	43	—	67	—	—	23	7	—	53	—	19	13	97	7	107	—	127	11	41

II c.

	1 80	83	86	89	92	95	1 98	2 01	04	07	10	13	16	19	22	25	28	31	34	37	40	43	46	49	52	55	58	61	64	67
01	47	—	11	41	7	—	—	—	23	127	—	7	—	11	149	—	151	13	7	137	—	19	73	37	11	7	—	43	17	—
07	11	—	23	7	—	—	29	—	—	—	7	11	17	19	53	71	—	7	89	151	—	109	11	—	7	23	131	—	—	17
11	7	—	37	—	—	109	11	7	—	139	—	101	—	—	7	—	—	11	41	131	13	7	—	29	17	97	53	—	7	—
13	—	—	7	—	—	13	—	—	137	7	—	—	—	17	97	47	7	29	13	23	11	41	151	7	19	31	83	—	61	—
17	43	13	—	—	11	29	7	—	17	—	—	—	—	7	13	11	—	—	—	37	7	—	103	—	151	17	11	7	—	—
19	37	7	43	—	—	131	—	11	7	—	—	—	13	23	17	7	19	61	11	—	—	83	7	—	—	13	—	—	29	7
23	67	73	11	127	47	7	43	—	13	17	—	—	7	11	71	101	29	19	59	7	—	13	—	—	11	—	7	151	—	—
29	11	—	13	23	7	59	79	—	31	19	17	7	43	—	—	13	37	101	7	61	—	—	11	97	—	7	23	17	13	—
31	13	23	31	11	—	—	7	41	—	—	—	83	97	7	11	—	17	—	—	19	7	29	—	107	23	11	13	7	—	—
37	17	11	—	29	—	7	83	13	107	89	109	19	7	—	37	31	41	17	23	7	13	—	71	11	—	—	7	59	—	—
41	—	—	7	13	71	—	—	11	—	7	53	—	17	37	23	—	7	73	11	—	29	101	41	7	43	—	—	—	137	11
43	—	13	103	19	7	—	—	—	—	—	11	7	23	—	13	—	53	—	7	—	—	11	19	—	—	7	43	13	31	47
47	—	7	29	—	19	11	89	—	7	—	13	—	—	17	—	7	11	79	—	—	139	97	7	13	—	59	—	11	53	7
49	—	59	17	7	—	113	23	—	11	—	7	37	—	47	19	—	73	7	131	11	—	13	157	61	7	29	—	79	—	23
53	7	—	23	11	13	—	—	7	113	—	37	131	59	29	7	19	—	13	47	—	67	7	89	—	—	11	103	—	7	31
59	—	11	47	—	—	—	7	19	41	—	—	13	11	7	—	17	—	—	—	23	7	—	—	11	13	61	19	7	—	—
61	—	7	—	67	11	31	—	—	7	13	—	41	—	—	113	7	—	19	29	—	—	17	7	109	—	—	11	—	47	7
67	7	—	11	13	—	17	—	7	97	19	—	23	47	11	7	—	13	—	31	—	41	7	17	—	11	37	—	137	7	13
71	17	—	—	61	7	—	31	23	11	—	19	7	13	127	—	—	—	71	7	11	—	—	—	—	37	7	41	—	103	19
73	11	19	71	—	—	23	7	—	59	—	13	11	—	7	—	—	89	—	—	—	7	—	11	13	127	107	—	7	23	41
77	—	17	19	7	37	—	11	—	—	79	7	—	53	—	—	107	—	7	17	13	—	19	—	—	7	—	113	—	11	—
79	101	—	—	—	13	7	103	17	—	11	107	—	7	31	—	67	137	13	53	7	11	—	23	—	17	—	7	47	—	61
83	13	31	7	41	11	—	59	—	—	7	29	—	—	13	—	11	7	97	23	17	—	37	—	7	131	—	11	—	71	—
89	—	7	11	17	—	19	—	13	7	—	—	73	23	11	31	7	47	—	83	—	13	29	7	—	11	—	—	—	—	7
91	79	53	—	7	101	11	—	61	31	17	7	—	109	—	—	19	11	7	13	37	—	—	—	67	7	157	17	11	59	73
97	—	—	7	11	23	—	101	19	103	7	17	—	13	—	11	59	7	—	—	53	—	31	—	7	41	11	19	17	—	127

III a.

	1 81	84	87	90	93	96	1 99	2 02	05	08	11	14	17	20	23	26	29	32	35	38	41	44	47	50	53	56	59	62	65	68
01	23	—	—	—	—	17	7	—	13	11	—	—	—	7	29	97	—	—	71	—	7	13	17	23	—	—	59	7	—	—
03	43	7	59	31	97	—	13	89	7	71	47	17	11	—	—	7	37	—	19	13	—	23	7	11	—	—	—	—	17	7
07	19	79	13	83	43	7	17	11	—	—	—	—	7	59	—	13	—	23	11	7	—	—	31	17	—	29	7	73	13	11
09	7	41	53	—	—	—	43	7	—	—	11	79	17	13	7	23	31	—	—	29	—	7	—	89	—	—	13	—	7	17
13	59	—	—	—	7	11	—	17	73	13	43	7	—	—	53	—	11	139	7	—	—	—	13	—	17	7	—	11	—	—
19	—	113	—	7	—	23	—	—	17	109	7	—	37	97	11	—	13	7	29	—	89	—	19	127	7	11	—	157	23	13
21	—	13	97	23	139	7	11	73	—	47	—	31	7	19	13	—	—	11	43	7	—	—	59	131	—	—	7	13	11	—
27	—	—	61	53	7	19	—	113	13	59	37	7	—	—	83	11	101	—	7	—	23	13	79	29	19	7	11	—	41	139
31	—	7	—	—	13	67	19	—	7	37	11	29	31	—	137	7	23	13	—	—	59	11	7	—	73	19	—	17	43	7
33	—	—	11	7	—	29	31	—	—	83	7	—	103	11	23	13	17	7	101	—	—	53	—	—	7	—	—	37	13	—
37	7	103	41	—	61	73	—	7	11	67	23	13	—	—	7	—	—	19	—	11	—	7	29	—	13	31	37	—	7	47
39	11	—	7	79	83	41	127	37	19	7	—	11	—	—	89	—	7	17	—	31	101	—	11	7	—	—	—	19	—	—
43	—	—	—	137	23	13	7	31	—	19	—	41	17	7	—	—	—	11	13	113	7	—	109	79	—	—	—	7	11	17
49	—	19	—	43	11	7	—	—	—	—	—	89	7	17	—	11	53	67	—	7	19	23	—	37	—	13	7	—	139	—
51	7	—	17	—	37	43	71	7	—	29	13	19	—	—	7	—	59	—	11	17	—	7	53	13	101	113	—	—	7	11
57	67	—	—	17	13	11	7	47	61	—	—	43	—	7	79	139	11	13	—	—	7	37	19	—	—	—	101	7	—	107
61	11	—	73	7	19	—	—	—	29	23	7	11	47	13	59	17	—	7	—	107	37	61	11	19	7	67	13	—	—	—
63	41	37	29	11	17	7	—	23	—	31	—	13	7	—	11	131	—	43	—	7	73	17	—	71	13	11	7	—	101	—
67	37	59	7	23	107	71	41	13	131	7	61	—	—	—	—	19	7	53	—	29	11	43	—	7	—	—	23	—	31	67
69	—	11	137	—	7	13	19	—	67	41	—	7	11	29	—	—	103	—	7	—	—	—	17	11	23	7	—	109	163	97
73	17	7	—	—	—	103	—	11	7	—	31	109	—	—	13	7	—	17	11	—	23	—	7	—	—	—	19	13	—	7
79	7	17	89	—	—	11	—	7	13	—	—	47	29	—	7	—	11	—	17	—	—	7	71	31	41	—	83	11	7	—
81	—	—	7	—	—	—	13	17	11	7	59	—	23	71	—	37	7	31	—	11	—	—	—	7	17	61	—	41	19	—
87	13	7	—	—	—	—	11	—	7	—	—	—	—	13	61	7	127	11	103	—	19	47	7	—	53	17	13	97	11	7
91	—	11	19	17	—	7	—	103	59	13	—	—	7	—	—	—	83	—	31	7	17	19	13	11	—	23	7	61	—	—
93	7	—	—	61	11	47	—	7	—	17	—	—	19	—	7	11	—	—	—	—	13	7	—	23	67	—	11	—	7	—
97	31	53	—	13	7	—	—	—	43	—	11	7	71	19	—	—	13	—	7	23	—	11	137	—	109	7	—	—	—	13
99	—	13	11	71	19	—	7	53	—	—	17	—	—	7	13	—	109	23	—	—	7	—	—	19	11	31	—	7	67	37

	1 82	85	88	91	94	1 97	2 00	03	06	09	12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57	60	63	66	69
03	109	—	—	7		17	83	79	11	—	7		—	23	43	73	—	7	—	11	—	107	17	13	7	—	—	29	37	—
09	131	83	7	97	13	—	11	23	37	7	127	137	113	—	—	—	7	11	—	—	43	—	—	7	—	47	31	—	11	71
11	—	107	13	29	7	23	—	19	—	11	—	7	17	—	73	13	—	—	7	—	11	127	43	—	—	7	19	83	13	17
17	—	—	31	7	—	—	37	11	53	13	7	—	—	17	29	—	—	7	11	—	61	—	13	—	7	—	—	—	43	11
21	7	—	11	—	—	13	—	7	17	—	—	—	—	11	7	—	—	—	13	19	53	7	—	—	11	17	—	—	7	—
23	—	—	7	13	—	11	—	—	41	7	19	—	139	—	17	31	7	83	—	47	—	137	103	7	—	29	53	11	79	13
27	11	97	67	31	—	—	7	—	—	17	—	11	13	7	41	—	—	—	—	71	7	—	11	—	47	13	17	7	—	—
29	—	7	19	11	—	109	—	29	7	—	13	—	83	—	11	7	—	41	—	—	—	19	7	13	59	11	—	113	31	7
33	—	43	37	19	—	7	13	—	47	11	17	61	7	—	—	127	31	—	—	7	11	—	19	41	29	—	7	17	—	23
39	13	—	—	—	7	—	29	11	—	—	67	7	—	13	19	—	—	—	7	37	—	53	59	23	—	7	13	—	17	11
41	17	—	83	—	—	19	7	—	—	43	11	13	—	7	—	—	—	17	47	89	7	11	—	31	13	—	—	7	—	29
47	71	17	47	41	—	7	—	—	11	—	—	29	7	—	—	23	19	37	13	7	—	—	—	—	—	—	7	—	—	—
51	—	13	7	11	53	—	—	47	107	7	79	23	—	17	11	—	7	19	67	43	—	—	—	7	31	11	109	13	29	—
53	—	—	17	107	7	—	11	—	19	23	53	7	13	—	—	61	—	11	7	17	79	43	29	—	—	7	—	19	11	—
57	—	7	109	—	—	23	31	—	7	19	29	—	11	—	17	7	—	—	41	—	127	13	7	11	—	43	71	—	19	7
59	19	67	—	7	11	—	13	—	73	—	7	—	—	—	37	11	—	7	59	13	17	41	—	139	7	—	11	43	53	—
63	7	19	13	—	—	—	—	7	—	—	11	—	—	37	7	13	—	61	—	31	19	7	23	—	—	—	67	41	7	59
69	—	31	—	29	—	53	7	—	11	13	—	—	19	7	—	—	17	—	—	11	7	79	13	—	—	73	131	7	—	149
71	11	7	113	19	—	17	—	13	7	67	89	11	—	—	23	7	—	—	—	—	13	—	7	—	—	—	29	—	149	7
77	7	13	43	127	—	—	17	7	23	11	—	—	131	67	7	—	47	97	—	—	11	7	—	17	73	149	89	13	7	53
81	101	17	79	—	7	131	43	89	—	—	13	7	—	41	—	11	—	103	7	—	—	47	139	13	83	7	11	23	—	—
83	47	—	23	—	—	73	7	11	13	—	—	113	79	7	—	—	41	67	11	29	7	13	149	—	17	19	—	7	—	11
87	—	—	11	7	13	47	53	19	137	31	7	—	43	11	113	—	—	7	—	17	149	23	41	89	7	107	19	—	—	—
89	—	29	13	31	—	7	—	—	17	139	61	—	7	—	43	13	11	19	—	7	107	67	—	—	71	17	7	11	13	137
93	11	—	7	17	101	—	71	—	—	7	107	11	—	—	83	23	7	149	19	—	17	—	11	7	13	—	97	—	—	—
99	29	7	—	73	17	13	101	—	7	11	19	—	61	79	149	7	—	—	13	103	11	17	7	113	43	—	—	—	—	7

III c.

	2 70	73	76	79	82	85	88	91	94	2 97	3 00	03	06	09	12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57
01	13	23	7	—	—	11	83	—	—	7	19	157	71	13	41	17	7	47	—	53	61	—	—	7	23	—	13	11	—	19
07	113	7	19	11	67	29	—	13	7	61	37	—	127	31	11	7	17	97	23	—	13	19	7	41	79	11	—	—	—	7
11	—	31	—	13	—	7	47	43	—	11	—	17	7	—	23	—	13	163	—	7	11	—	19	—	—	—	7	—	17	13
13	7	11	53	103	89	—	—	7	67	43	—	—	11	19	7	—	29	17	—	—	—	7	—	11	—	—	31	13	7	71
17	—	59	—	—	7	—	—	11	23	—	13	7	17	43	19	—	—	—	7	—	137	—	—	13	—	7	37	—	107	11
19	41	17	71	—	—	19	7	37	13	113	11	—	67	7	—	43	47	—	17	—	7	11	—	107	19	—	—	7	—	23
23	61	89	23	7	13	11	19	—	—	—	7	—	113	17	—	29	11	7	—	43	—	47	—	—	7	19	97	11	—	139
29	151	—	7	11	—	47	127	—	—	7	—	13	109	157	11	41	7	19	—	23	—	—	—	7	13	11	29	—	71	—
31	—	151	—	17	7	103	11	—	19	13	59	7	—	—	—	—	139	11	7	71	17	—	13	—	—	7	61	19	11	—
37	19	—	29	7	11	—	—	—	—	131	7	23	—	—	—	11	13	7	163	19	—	17	—	—	7	—	11	41	—	13
41	7	19	131	—	31	—	151	7	59	—	11	—	13	—	7	—	17	—	—	29	19	7	—	—	97	13	—	—	7	103
43	—	37	7	—	61	17	—	151	—	7	13	19	—	11	157	—	7	—	—	137	173	—	17	7	11	—	—	113	23	31
47	17	23	—	—	47	—	7	—	11	151	—	—	19	7	—	—	—	17	71	11	7	—	—	83	23	179	—	7	—	—
49	11	7	43	19	13	—	17	103	7	71	151	11	—	—	—	7	—	13	37	—	—	—	7	17	29	—	—	—	—	7
53	13	17	—	—	19	7	11	—	—	—	41	127	7	13	—	139	53	11	17	7	—	—	73	19	—	109	7	—	11	—
59	—	109	17	73	7	—	—	13	89	—	—	7	23	83	—	11	—	—	7	17	13	—	97	29	—	7	11	—	59	—
61	—	—	139	—	59	13	7	11	17	—	23	97	—	7	43	37	151	29	11	181	7	73	41	—	—	17	71	7	—	11
67	—	—	73	—	23	7	—	—	79	17	107	—	7	173	—	—	11	19	—	7	43	61	131	—	—	13	7	11	29	47
71	11	101	7	83	17	—	—	31	13	7	—	11	—	—	—	131	7	53	19	—	—	13	11	7	43	181	—	—	79	—
73	—	31	—	11	7	—	13	—	—	19	17	7	37	47	11	—	—	—	7	13	—	23	151	53	—	7	43	17	19	83
77	—	7	13	101	—	17	67	163	7	11	19	37	—	—	—	7	127	23	47	73	11	—	7	61	151	71	—	29	13	7
79	13	11	89	7	—	—	—	—	41	97	7	17	11	13	31	23	71	7	—	—	19	29	—	11	7	151	13	127	17	37
83	7	139	19	—	—	101	17	7	—	13	67	23	61	—	7	—	—	—	11	—	—	7	13	17	—	—	—	151	7	11
89	103	61	—	13	—	11	7	17	37	—	—	—	—	7	67	31	11	—	53	—	7	173	59	41	17	—	139	7	23	13
91	—	7	—	23	19	—	167	—	7	31	—	—	47	17	13	7	—	—	—	11	—	—	7	19	53	—	23	13	—	7
97	7	—	—	—	—	—	11	7	13	83	—	113	—	139	7	19	167	11	—	—	23	7	31	—	—	29	—	61	7	—

IV a.

	2 71	74	77	80	83	86	89	92	95	2 98	3 01	04	07	10	13	16	19	22	25	28	31	34	37	40	43	46	49	52	55	58
01	41	11	—	—	7	37	—	—	—	17	31	7	11	29	113	—	19	13	7	—	79	127	67	11	—	7	17	—	131	—
03	—	67	13	41	11	—	7	19	163	—	—	—	—	7	23	11	61	—	—	—	7	—	—	37	—	—	11	7	13	—
07	—	—	103	7	—	—	137	—	19	41	7	13	—	101	—	—	—	7	—	53	—	11	37	31	7	—	67	17	—	61
09	—	—	11	37	—	7	—	—	23	13	—	47	7	11	131	73	17	31	19	7	113	—	13	71	11	53	7	137	—	—
13	19	79	7	109	23	13	29	131	11	7	—	17	—	—	173	101	7	—	13	11	—	—	—	7	—	—	—	23	17	59
19	47	7	53	—	—	—	11	61	7	—	—	19	13	—	—	7	59	11	31	37	—	23	7	—	—	13	—	41	11	7
21	37	17	19	7	127	—	—	—	53	11	7	29	31	67	—	103	137	7	17	23	11	19	—	13	7	89	47	—	—	113
27	—	—	7	—	13	—	—	11	—	7	47	—	—	19	—	—	7	13	11	17	157	—	29	7	—	31	53	—	—	11
31	13	—	11	—	41	—	7	—	—	23	29	—	79	7	17	47	37	167	—	—	7	101	89	—	11	—	13	7	—	—
33	43	7	—	17	29	11	—	23	7	—	—	13	73	—	—	7	11	—	—	—	17	67	7	—	13	59	181	11	—	7
37	11	—	—	23	43	7	19	13	—	—	—	11	7	41	—	17	109	—	—	7	13	29	11	101	—	19	7	167	—	—
39	7	23	—	11	17	13	43	7	109	53	—	61	59	—	7	29	19	103	13	—	31	7	—	—	23	11	—	131	7	—
43	—	13	—	29	7	—	103	—	31	11	43	7	71	37	13	—	17	19	7	—	11	53	41	59	61	7	83	13	—	73
49	17	—	—	7	—	—	—	11	13	19	7	—	97	61	23	—	43	7	11	107	—	13	—	79	7	—	—	101	19	11
51	19	97	—	—	—	7	13	—	29	—	11	37	7	—	107	31	89	—	43	7	—	11	—	17	—	—	7	—	73	—
57	13	—	41	—	7	—	23	17	11	73	53	7	—	13	—	—	—	—	7	11	71	—	—	—	17	7	13	—	31	23
61	157	7	17	11	79	—	—	29	7	13	—	83	19	89	11	7	31	—	—	17	—	—	7	—	—	11	—	37	43	7
63	23	29	—	7	113	—	11	13	17	—	7	41	—	—	79	—	—	7	—	59	13	109	19	23	7	17	—	179	11	—
67	7	11	—	13	19	109	83	7	—	—	97	—	11	47	7	—	13	41	29	23	17	7	—	11	—	—	73	—	7	13
69	101	13	7	—	11	—	59	—	—	7	—	—	29	—	13	11	7	23	—	—	41	—	—	7	—	37	11	13	—	—
73	29	83	—	67	17	53	7	73	—	—	11	31	—	7	137	19	—	59	—	71	7	11	—	13	37	—	41	7	—	29
79	—	—	—	43	13	7	—	19	11	—	103	29	7	—	—	79	113	13	—	7	—	—	17	53	31	—	7	—	47	—
81	7	—	13	—	101	23	73	7	—	—	—	11	—	—	7	13	—	19	31	131	—	7	11	173	—	79	—	—	7	53
87	31	—	37	—	—	—	7	—	—	11	—	43	17	7	—	—	29	83	—	—	7	—	13	89	137	—	59	7	19	17
91	—	37	—	7	11	13	53	17	127	71	7	—	41	—	—	11	—	7	13	31	—	107	—	73	7	113	11	—	—	19
93	71	19	—	13	—	7	79	11	101	167	109	—	7	17	—	41	13	43	11	7	19	—	47	103	163	—	7	29	—	11
97	—	31	7	—	73	—	107	—	17	7	—	—	13	11	—	29	7	—	37	67	89	19	—	7	11	13	79	47	—	—
99	59	107	—	—	7	11	47	83	—	29	13	7	19	137	17	—	11	—	7	167	—	139	73	13	41	7	31	11	97	—

IV b.

	2 72	75	78	81	84	87	90	93	96	2 99	3 02	05	08	11	14	17	20	23	26	29	32	35	38	41	44	47	50	53	56	59
03	11	7	—	157	—	—	13	—	7	17	—	11	—	19	31	7	—	—	—	13	—	—	7	67	—	—	17	43	—	7
09	7	—	—	—	—	19	—	7	29	11	17	—	—	13	7	37	—	—	—	—	11	7	—	23	19	61	13	17	7	149
11	—	11	7	—	-	—	67	—	—	7	—	13	11	53	101	19	7	79	—	—	—	23	—	7	13	103	157	—	149	-
17	17	7	—	31	157	13	—	19	7	—	11	—	—	29	89	7	101	17	13	—	59	11	7	109	127	149	19	—	—	7
21	163	13	43	61	97	7	—	109	19	—	47	23	7	—	13	—	11	—	—	7	139	--	31	149	—	—	7	11	179	17
23	7	17	—	—	43	—	—	7	11	23	—	131	13	—	7	--	31	—	17	11	—	7	149	--	29	13	--	—	7	—
27	19	—	—	11	7	23	—	—	13	—	167	7	29	17	11	—	—	—	7	19	149	13	--	—	173	7	—	—	23	37
29	73	—	17	23	—	—	7	139	—	173	19	—	—	7	53	—	—	11	67	13	7	—	—	—	—	—	23	7	11	19
33	113	11	13	7	—	59	—	—	—	37	7	19	11	163	17	13	103	7	—	—	167	—	23	11	7	47	53	89	13	—
39	—	—	7	19	—	29	71	—	107	7	11	—	—	—	149	17	7	73	127	—	43	11	13	7	—	—	37	—	157	83
41	—	—	11	107	7	41	113	13	—	79	—	7	—	11	23	—	179	—	7	—	13	17	43	—	11	7	67	59	29	127
47	11	13	—	7	—	17	31	—	23	—	7	11	109	—	13	53	73	7	—	47	—	—	11	—	7	—	101	13	43	103
51	7	—	—	—	23	—	11	7	149	61	13	137	—	—	7	—	—	11	103	83	41	7	—	13	47	19	—	23	7	—
53	--	59	7	47	37	—	17	149	13	7	—	—	—	—	71	113	7	—	—	31	11	13	97	7	131	23	—	—	101	157
57	97	17	89	37	11	149	7	31	47	29	79	—	59	7	83	11	—	13	17	—	7	23	—	—	—	—	11	7	181	41
59	—	7	13	29	149	—	—	11	7	—	—	—	—	—	163	7	—	—	11	23	79	37	7	—	17	—	—	19	13	7
63	137	43	11	—	—	7	—	—	—	19	53	13	7	11	73	23	—	—	89	7	29	—	—	127	11	—	7	—	19	—
69	11	19	29	17	7	13	41	43	—	23	—	7	—	71	—	—	—	—	7	—	17	—	11	47	—	7	—	113	53	—
71	—	79	47	11	71	—	7	23	—	17	—	19	—	7	11	—	13	—	37	—	7	59	—	—	—	11	17	7	—	13
77	—	11	61	19	—	7	—	29	59	31	13	—	7	—	—	43	—	—	41	7	107	—	19	11	23	83	7	17	—	—
81	—	—	7	—	19	17	13	11	67	7	107	53	—	—	—	61	7	—	11	13	23	—	17	7	29	—	—	—	31	11
83	—	—	—	—	7	107	127	—	—	—	11	7	89	—	19	37	—	13	7	—	83	11	31	—	—	7	—	41	17	—
87	13	7	79	71	61	11	17	—	7	157	31	73	67	13	23	7	11	139	—	—	—	—	7	17	—	43	13	11	127	7
89	29	47	167	7	31	—	19	—	11	—	7	13	17	—	—	83	—	7	97	11	—	—	—	179	7	19	—	43	89	17
93	7	41	—	11	—	—	47	7	23	89	—	—	—	—	7	—	67	29	—	—	13	7	—	31	17	11	19	—	7	—
99	—	11	23	163	—	31	7	—	17	131	41	37	11	7	13	—	—	179	19	—	7	—	109	11	—	17	—	7	29	—

	3 60	63	66	69	72	75	78	81	84	87	90	93	96	3 99	4 02	05	08	11	14	17	20	23	26	29	32	35	38	41	44	47
01	7	31	17	—	—	—	103	7	11	13	43	—	199	—	7	101	—	23	19	11	97	7	13	—	—	41	—	—	7	—
07	—	—	—	13	29	—	7	53	193	—	19	23	—	7	31	—	13	11	47	179	7	—	137	107	—	139	71	7	11	13
11	—	11	31	7	127	—	—	23	71	—	7	19	11	107	79	17	37	7	—	53	43	29	—	11	7	13	193	—	89	—
13	—	—	19	—	11	7	—	—	107	—	13	—	7	167	—	11	—	—	—	7	—	17	43	13	79	53	7	31	23	61
17	—	23	7	19	—	—	13	47	41	7	11	—	173	179	131	31	7	—	83	13	—	11	19	7	23	—	43	157	—	97
19	181	—	11	—	7	17	59	—	103	31	—	7	—	11	37	—	—	13	7	—	—	101	17	167	11	7	29	—	43	197
23	13	7	53	—	—	157	109	67	7	—	—	—	—	13	19	7	—	17	23	11	—	—	7	—	—	71	13	—	31	7
29	7	17	—	—	59	—	11	7	83	—	31	67	23	—	7	—	—	11	17	—	13	7	47	—	139	19	41	—	7	—
31	137	47	7	—	31	13	—	17	—	7	23	37	—	73	—	—	7	—	13	29	11	—	89	7	17	101	53	—	157	41
37	—	7	—	43	23	—	157	11	7	—	103	139	13	—	—	7	97	31	11	—	127	—	7	—	—	13	59	19	37	7
41	23	—	11	17	167	7	79	43	13	19	—	—	7	11	—	71	—	—	29	7	17	13	—	23	11	—	7	37	19	—
43	7	—	—	—	—	11	13	7	37	17	—	—	29	59	7	—	11	—	—	13	—	7	—	—	83	—	17	11	7	101
47	11	19	13	—	7	—	—	37	—	—	—	7	41	43	167	13	—	23	7	109	19	17	11	67	59	7	163	131	13	29
49	13	163	67	11	193	—	7	—	—	—	17	19	31	7	11	23	—	—	181	83	7	—	—	29	61	11	13	7	—	73
53	31	—	—	7	—	17	—	—	—	11	7	23	19	—	—	107	—	7	—	43	11	41	13	—	7	97	—	67	—	—
59	107	103	7	13	19	23	17	11	—	7	139	—	—	31	127	—	7	79	11	—	137	—	29	7	181	43	61	—	23	11
61	—	13	61	23	7	—	—	31	—	83	11	7	17	89	13	47	29	—	7	—	—	11	37	—	—	7	23	13	173	17
67	—	41	37	7	83	—	19	—	11	—	7	—	—	17	67	113	—	7	—	11	23	13	—	—	7	19	—	29	53	89
71	7	37	—	11	13	—	—	7	17	137	89	—	—	—	7	29	23	13	113	—	—	7	71	97	—	11	19	—	7	—
73	—	—	7	—	—	—	11	59	79	7	41	—	97	71	17	13	7	11	67	37	—	—	139	7	109	—	73	163	11	—
77	43	11	—	103	—	53	7	—	109	17	23	13	11	7	—	—	41	—	19	—	7	31	—	11	13	—	17	7	79	—
79	109	7	43	—	11	—	—	73	7	13	—	53	—	—	47	7	—	—	—	41	29	—	7	—	113	—	11	—	19	7
83	—	—	—	31	23	7	43	—	29	—	11	—	7	—	—	—	—	—	13	7	—	11	—	53	—	41	7	17	—	19
89	151	—	19	47	97	—	—	—	11	79	—	7	13	—	—	37	31	—	7	11	—	19	—	—	73	7	—	—	17	—
91	11	151	—	71	89	—	7	181	61	—	13	11	19	7	43	—	103	17	—	23	7	—	11	13	—	—	—	7	—	47
97	—	17	—	—	13	7	—	—	137	11	—	—	7	23	59	—	—	13	17	7	11	—	—	19	29	—	7	193	—	—

V a.

	3 61	64	67	70	73	76	79	82	85	88	91	94	3 97	4 00	03	06	09	12	15	18	21	24	27	30	33	36	39	42	45	48
01	13	89	7	163	11	19	151	—	—	7	61	31	29	13	191	11	7	—	47	—	—	109	—	7	19	59	11	—	—	71
03	79	59	17	—	7	31	29	11	139	—	—	7	—	109	41	19	—	—	7	17	71	—	—	—	13	7	43	—	191	11
07	—	7	11	23	—	—	—	13	7	151	—	157	59	11	17	7	19	89	—	97	13	—	7	29	11	—	23	—	—	7
09	—	23	—	7	—	11	167	19	97	197	7	—	—	—	173	—	11	7	13	—	17	—	—	41	7	—	19	11	47	—
13	7	13	—	—	—	29	31	7	19	37	—	11	151	—	7	17	163	—	—	—	23	7	11	—	—	—	—	13	7	41
19	19	79	73	—	67	—	7	—	13	11	—	—	—	7	23	151	17	47	—	19	7	13	—	—	—	53	37	7	—	—
21	41	7	—	—	—	17	13	37	7	—	19	79	11	31	61	7	151	—	—	13	73	59	7	11	—	181	167	—	211	7
27	7	73	19	61	163	191	17	7	59	41	11	89	—	13	7	—	—	—	131	151	103	7	—	17	37	—	13	47	7	23
31	—	17	23	19	7	11	83	—	53	13	109	7	67	—	31	41	11	—	7	59	—	151	13	37	—	7	197	11	—	127
33	23	—	109	29	37	—	7	13	11	—	—	47	—	7	53	179	—	—	41	11	7	—	151	23	17	—	—	7	—	107
37	—	83	17	7	—	61	59	—	89	71	7	113	79	—	11	—	13	7	73	17	29	—	—	—	7	11	53	31	—	13
39	71	13	—	—	—	7	11	—	17	—	—	—	7	—	13	—	—	11	—	7	—	31	79	193	19	17	7	13	11	—
43	47	11	7	17	107	—	19	167	—	7	13	—	11	23	—	97	7	—	—	—	17	—	—	7	89	19	—	151	—	—
49	37	7	—	—	13	—	137	23	7	53	11	103	—	29	157	7	—	13	—	—	113	11	7	—	67	—	71	—	—	7
51	—	—	11	7	41	23	—	29	19	—	7	—	127	11	—	13	31	7	37	—	61	—	—	—	7	—	—	17	13	—
57	11	—	7	—	—	—	—	67	—	7	—	11	83	41	—	109	7	—	29	19	—	—	11	7	191	149	113	—	17	31
61	—	19	—	—	—	13	7	—	—	—	—	—	—	7	—	73	—	11	13	41	7	—	61	17	131	—	—	7	11	113
63	29	7	97	13	—	—	—	83	7	11	—	19	17	—	181	7	13	—	89	—	11	—	7	—	103	47	—	—	—	7
67	59	—	—	101	11	7	—	17	—	—	53	61	7	103	37	11	71	29	197	7	149	—	—	—	17	13	7	—	41	—
69	7	—	83	19	—	139	43	7	—	47	13	29	—	17	7	67	53	—	11	149	—	7	19	13	31	—	—	—	7	11
73	61	—	11	131	7	101	13	—	17	—	43	7	31	11	47	89	—	149	7	13	181	—	—	19	11	7	—	—	29	23
79	11	—	—	7	—	41	163	101	173	17	7	11	—	13	149	19	43	7	—	—	—	107	11	23	7	31	13	—	—	—
81	97	191	—	11	29	7	19	—	41	59	—	13	7	149	11	17	107	—	43	7	—	23	179	67	13	11	7	—	109	37
87	—	11	—	—	7	13	—	—	47	37	149	7	11	—	—	23	17	19	7	—	—	—	—	11	43	7	—	67	—	—
91	—	7	—	29	139	—	—	11	7	—	—	17	—	47	13	7	179	157	11	163	31	—	7	41	—	—	—	13	17	7
93	17	—	—	7	61	—	—	149	—	19	7	73	13	—	31	—	—	7	—	—	—	11	—	—	7	13	29	—	19	—
97	7	—	31	—	—	11	—	7	13	97	19	127	17	101	7	—	11	61	—	—	—	7	—	71	—	37	—	11	7	17
99	53	17	7	23	149	—	13	—	11	7	—	—	—	—	71	—	7	—	17	11	19	—	127	7	—	89	23	31	103	59

V b.

	3 62	65	68	71	74	77	80	83	86	89	92	95	3 98	4 01	04	07	10	13	16	19	22	25	28	31	34	37	40	43	46	49
03	41	173	13	11	113	37	7	—	—	—	197	—	53	7	11	13	131	103	—	—	7	19	23	—	—	11	79	7	13	83
09	—	11	—	43	—	7	191	29	—	13	—	—	7	19	17	—	23	101	—	7	—	—	13	11	83	109	7	59	31	—
11	7	29	131	17	11	43	—	7	—	167	113	—	41	—	7	11	—	109	—	—	13	7	31	19	—	—	11	73	7	97
17	—	13	11	—	17	—	7	—	23	—	—	43	29	7	13	19	—	79	—	167	7	17	47	—	11	—	—	7	—	—
21	29	59	—	7	23	67	193	—	11	—	7	—	—	53	83	43	17	7	—	11	—	101	—	13	7	—	—	23	—	29
23	11	—	23	—	—	7	47	19	13	—	61	11	7	—	—	193	—	31	107	7	—	13	11	29	173	23	7	127	—	167
27	17	—	7	137	13	31	11	—	19	7	—	29	—	—	—	139	7	11	—	—	—	23	113	7	—	73	—	19	11	—
29	—	—	13	107	7	29	17	—	—	11	—	7	—	—	—	13	89	37	7	23	11	71	—	17	137	7	—	97	13	179
33	19	7	—	71	11	97	73	—	7	—	—	13	61	67	—	7	37	—	17	19	157	—	7	—	13	101	11	43	—	7
39	7	61	11	—	29	13	—	7	—	23	—	19	—	11	7	—	—	67	13	17	—	7	—	179	11	191	47	101	7	—
41	—	—	7	13	—	11	109	23	17	7	—	—	—	137	37	131	7	—	—	—	53	19	—	7	—	17	—	11	—	13
47	67	7	—	11	—	—	—	31	7	17	13	71	—	19	11	7	—	173	—	—	83	157	7	13	23	11	17	61	—	7
51	—	—	43	97	17	7	13	—	—	11	—	—	7	—	19	—	—	—	—	7	11	17	73	—	—	67	7	—	—	79
53	7	11	137	53	13	19	—	7	—	—	17	37	11	—	7	83	61	13	23	—	29	7	—	11	19	—	—	17	7	—
57	13	139	—	73	7	17	19	11	29	163	37	7	—	13	23	53	—	—	7	—	—	—	17	103	—	7	13	—	—	11
59	101	—	29	—	47	61	7	89	67	—	11	13	23	7	—	—	19	59	—	—	7	11	—	—	13	—	—	7	17	—
63	—	—	191	7	—	11	17	13	23	47	7	—	—	—	43	—	11	7	61	29	13	31	—	17	7	107	139	11	59	—
69	—	13	7	11	89	179	—	17	—	7	107	—	—	—	11	59	7	41	—	—	43	—	163	7	17	11	127	13	19	193
71	19	—	—	—	7	107	11	—	—	—	173	7	13	17	—	—	67	11	7	19	41	—	43	23	29	7	—	—	11	—
77	—	79	—	7	11	37	13	—	—	—	7	19	—	—	17	11	—	7	71	13	67	—	53	—	7	—	11	199	43	41
81	7	157	13	—	37	—	113	7	47	17	11	—	19	23	7	13	—	—	—	—	—	7	137	29	—	—	17	—	7	31
83	13	—	7	19	—	—	—	131	101	7	163	23	—	11	—	17	7	29	73	—	—	97	19	7	11	—	13	—	—	—
87	131	—	—	41	19	29	7	23	11	13	17	31	—	7	—	—	181	—	—	11	7	37	13	19	—	—	—	7	—	—
89	11	7	37	—	—	23	41	13	7	127	101	11	113	—	19	7	17	—	47	199	13	—	7	—	157	—	—	—	23	7
93	—	23	79	13	—	7	11	—	—	—	—	17	7	—	—	19	13	11	173	7	—	191	59	47	23	—	7	103	11	13
99	—	—	—	—	7	—	31	19	—	59	13	7	17	61	—	11	73	—	7	—	—	41	—	13	—	7	11	29	—	17

V c.

	4 50	53	56	59	62	65	68	71	74	77	80	83	86	89	92	95	4 98	5 01	04	07	10	13	16	19	22	25	28	31	34	37
01	11	89	31	197	47	7	17	19	107	—	23	11	7	79	—	59	—	—	13	7	—	29	11	17	—	—	7	—	—	83
07	—	—	59	29	7	—	—	17	—	11	61	7	13	—	—	31	—	89	7	—	11	—	—	—	17	7	—	23	—	43
11	19	7	17	31	11	—	—	—	7	—	41	—	—	59	—	7	—	—	—	17	29	13	7	23	109	—	11	173	—	7
13	—	113	—	7	37	193	13	11	17	—	7	—	173	41	29	67	109	7	11	13	139	23	—	—	7	17	—	—	31	11
17	7	—	11	17	113	181	—	7	—	—	—	19	61	11	7	13	31	23	—	41	17	7	71	193	11	—	—	—	7	—
19	13	—	7	47	—	11	—	—	—	7	31	211	—	13	83	23	7	—	127	67	163	19	41	7	79	29	13	11	—	—
23	11	61	43	19	17	—	7	—	47	13	—	11	—	7	—	—	—	—	—	—	7	17	11	137	—	53	101	7	41	31
29	37	—	103	13	—	7	—	—	43	11	—	31	7	113	19	—	13	—	211	7	11	—	17	—	29	—	7	—	23	13
31	7	11	—	23	83	19	—	7	—	59	43	17	11	167	7	—	—	—	29	97	—	7	—	11	19	131	23	13	7	—
37	29	—	47	71	—	173	7	—	13	—	11	—	17	7	53	—	19	181	31	113	7	11	—	167	—	107	—	7	—	17
41	73	—	—	7	13	11	31	17	—	—	7	—	127	109	41	107	11	7	—	—	43	—	113	—	7	—	53	11	—	61
43	31	—	13	—	131	7	139	—	11	—	107	29	7	17	23	13	—	41	73	7	—	—	43	127	89	—	7	19	13	223
47	107	137	7	11	103	89	79	—	17	7	23	13	—	—	11	—	7	—	61	31	—	—	—	7	13	11	43	—	19	71
49	19	101	191	—	7	—	11	—	23	13	—	7	—	31	17	—	79	11	7	19	71	—	13	—	—	7	41	—	11	59
53	—	7	71	—	23	13	—	61	7	17	29	—	11	—	—	7	—	—	13	—	19	89	7	11	—	—	17	23	—	7
59	7	67	—	—	167	—	47	7	—	163	11	37	13	173	7	—	73	—	—	193	—	7	—	223	—	13	—	17	7	—
61	—	—	7	19	—	101	—	—	31	7	13	137	—	11	—	29	7	103	—	23	—	—	19	7	11	—	—	—	193	37
67	11	7	—	43	13	—	—	101	7	37	71	11	41	23	19	7	47	13	109	—	223	31	7	157	—	—	29	79	127	7
71	13	59	109	—	—	7	11	43	37	23	53	—	7	13	29	19	—	11	41	7	—	47	163	—	167	—	7	—	11	17
73	7	17	—	31	—	—	19	7	29	11	—	13	—	—	7	89	53	131	17	—	11	7	—	—	13	19	37	—	7	—
77	—	—	—	23	7	47	—	13	197	—	131	7	—	17	—	11	—	—	7	—	13	83	31	—	61	7	11	41	53	—
79	61	23	17	—	—	13	7	11	79	—	—	101	—	7	—	43	31	19	11	17	7	191	—	59	23	—	—	7	—	11
83	—	13	11	7	31	37	173	29	103	71	7	—	89	11	13	179	83	7	19	43	23	—	—	227	7	—	—	13	79	—
89	11	—	7	—	41	—	—	—	13	7	19	11	181	—	23	17	7	31	29	—	47	13	11	7	—	43	—	—	89	19
91	67	19	—	11	7	—	13	41	—	—	—	7	23	—	11	101	—	53	7	13	19	17	—	—	—	7	227	43	149	—
97	13	11	—	7	67	17	23	109	—	—	7	—	11	13	—	—	41	7	—	79	37	103	17	11	7	149	13	—	61	23

	4 51	54	57	60	63	66	69	72	75	78	81	84	87	90	93	96	4 99	5 02	05	08	11	14	17	20	23	26	29	32	35	38
01	7	83	23	157	—	—	—	7	—	13	103	29	31	19	7	193	139	17	11	37	137	7	13	149	—	23	—	—	7	11
03	23	—	7	179	19	29	17	13	67	7	11	97	113	—	47	—	7	61	—	101	13	11	149	7	193	41	—	83	—	173
07	43	17	—	13	—	11	7	—	—	—	73	—	53	7	—	113	11	—	17	23	7	—	29	131	19	31	191	7	—	13
09	79	7	43	139	—	127	61	17	7	—	—	—	67	—	13	7	29	23	53	11	—	101	7	—	17	—	157	13	73	7
13	197	—	17	11	29	7	43	31	—	137	13	—	7	23	11	—	19	149	—	7	79	—	—	13	—	11	7	127	59	—
19	—	11	131	17	7	—	—	23	19	—	—	7	11	—	149	29	—	13	7	89	17	—	—	11	113	7	—	19	109	—
21	—	53	13	—	11	23	7	—	—	17	—	41	83	7	31	11	—	—	19	—	7	—	—	—	—	101	11	7	13	107
27	—	—	11	—	—	7	167	83	—	13	17	79	7	11	107	—	—	—	—	7	29	—	13	—	11	—	7	17	—	19
31	—	181	7	191	107	13	71	73	11	7	—	19	—	—	—	31	7	—	13	11	—	—	17	7	43	—	41	—	199	—
33	11	—	19	13	7	—	—	149	—	31	127	7	—	—	—	—	13	191	7	—	—	19	11	61	59	7	43	—	17	13
37	—	7	—	19	—	149	11	—	7	—	37	—	13	—	103	7	—	11	97	29	—	—	7	17	199	13	—	139	11	7
39	—	—	53	7	149	—	73	97	137	11	7	59	17	19	—	—	—	7	—	—	11	—	31	13	7	—	167	—	37	17
43	7	29	149	41	11	—	13	7	—	—	31	193	79	—	7	11	—	47	—	13	199	7	59	71	17	61	11	37	7	23
49	13	47	11	—	—	—	7	37	17	59	89	—	29	7	61	131	199	109	—	—	7	—	—	23	11	17	13	7	—	—
51	163	7	—	—	—	11	29	—	7	109	179	13	—	181	17	7	11	31	—	211	—	23	7	—	13	37	—	11	—	7
57	7	131	—	11	151	13	—	7	19	—	—	47	—	—	7	17	—	29	13	—	—	—	7	73	—	41	11	—	19	7	—
61	—	13	67	—	7	29	151	167	199	11	17	7	—	71	13	53	47	—	7	181	11	—	191	79	—	7	211	13	19	—
63	19	11	—	73	71	—	7	151	—	23	—	—	11	7	—	—	17	—	59	19	7	53	37	11	—	13	—	7	29	61
67	31	19	—	7	199	23	67	11	13	151	7	17	—	139	—	—	29	7	11	—	19	13	—	—	7	—	—	—	17	11
69	17	41	37	23	89	7	13	—	—	—	11	19	7	—	—	—	107	17	61	7	—	11	—	—	—	31	7	—	—	103
73	199	37	7	—	79	11	107	41	113	7	67	—	17	31	97	13	7	—	103	—	73	—	23	7	83	—	—	11	13	17
79	—	7	—	11	19	—	109	—	7	13	—	—	—	17	1	7	23	137	37	83	61	—	7	19	—	11	31	—	131	7
81	—	—	17	7	—	—	11	13	—	—	7	—	—	—	19	—	151	7	—	17	13	—	53	—	7	139	—	—	11	—
87	73	13	7	17	11	—	19	—	23	7	—	—	—	191	13	11	7	—	—	151	17	—	—	7	—	19	11	13	41	—
91	—	—	29	—	23	—	7	19	—	83	11	—	97	7	—	17	—	—	—	—	7	11	67	13	—	—	19	7	—	—
93	43	7	11	—	17	53	—	—	7	47	—	71	59	11	—	7	—	19	—	—	—	13	7	113	11	23	197	137	—	7
97	—	—	41	31	13	7	—	—	11	211	—	—	7	29	47	—	17	13	19	7	—	23	—	59	151	—	7	223	—	—
99	7	173	13	—	—	17	43	7	—	19	157	11	—	37	7	13	—	179	—	23	—	7	11	53	61	151	—	—	7	—

VI b.

01

	4 52	55	58	61	64	67	70	73	76	79	82	85	88	91	94	4 97	5 00	03	06	09	12	15	18	21	24	27	30	33	36	39
03	17	—	163	—	7	—	11	—	181	—	19	7	37	—	127	23	31	11	7	109	—	—	—	—	13	7	—	151	11	19
09	53	17	19	7	11	13	29	—	—	23	7	179	—	—	—	11	43	7	13	—	41	19	103	107	7	—	11	—	—	31
11	29	71	61	13	—	7	53	11	47	—	37	139	7	67	—	—	13	—	11	7	83	—	197	31	17	—	7	89	—	11
17	103	23	—	107	7	11	—	—	17	—	13	7	—	—	—	83	11	67	7	59	—	—	—	13	23	7	—	11	—	—
21	11	7	—	17	61	19	13	79	7	173	—	11	—	—	73	7	—	—	223	13	17	—	7	—	19	—	37	71	29	7
23	41	—	—	7	13	—	59	37	—	17	7	—	—	—	11	19	—	7	23	—	181	67	29	47	7	11	17	—	—	—
27	7	53	—	193	17	—	31	7	97	11	29	—	157	13	7	—	19	59	—	127	11	7	—	—	103	—	13	—	7	—
29	31	11	7	163	29	83	131	19	—	7	17	13	11	73	—	223	7	—	197	—	—	227	—	7	13	67	19	17	—	199
33	—	—	—	—	59	17	7	11	19	—	139	—	47	7	—	41	—	—	11	31	7	29	17	37	—	—	181	7	—	11
39	19	13	23	29	—	7	17	—	—	—	—	—	7	—	13	—	11	71	79	7	—	—	—	17	41	23	7	11	—	—
41	7	—	—	—	—	43	—	7	11	191	19	—	13	157	7	—	163	—	89	11	—	7	47	23	229	13	29	41	7	17
47	—	37	19	—	—	—	7	113	29	—	—	43	—	7	197	—	—	11	—	13	7	19	139	—	179	—	—	7	11	73
51	37	11	13	7	—	—	—	—	17	—	7	47	11	23	—	13	—	7	—	—	53	—	19	11	7	17	—	31	13	—
53	13	—	—	—	11	7	211	—	—	79	73	23	7	13	17	11	—	43	37	7	107	31	—	—	—	71	7	—	—	163
57	167	—	7	101	—	—	—	23	—	7	11	59	—	—	19	—	7	37	179	—	—	11	13	7	—	—	17	229	—	79
59	—	29	11	31	7	19	—	13	—	199	—	7	—	11	—	17	113	—	7	131	13	47	—	43	11	7	97	—	23	—
63	—	7	—	13	97	101	19	—	7	—	17	—	131	211	—	7	13	—	29	11	—	—	7	—	23	19	47	17	103	7
69	7	—	—	137	31	—	11	7	73	—	13	17	—	—	7	157	—	11	23	—	167	7	—	13	71	—	—	83	7	29
71	17	199	7	—	—	—	103	127	13	7	—	—	—	—	61	71	7	17	—	—	11	13	—	7	137	113	73	19	191	31
77	19	7	13	61	—	29	179	11	7	—	23	31	37	—	—	7	—	—	11	19	47	—	7	—	97	89	—	—	13	7
81	—	19	11	—	53	7	23	—	—	—	—	13	7	11	—	67	61	83	59	7	19	—	29	—	11	47	7	—	—	23
83	7	79	17	—	23	11	197	7	41	13	53	19	—	137	7	—	11	—	—	17	—	7	13	—	31	—	109	11	7	37
87	11	—	—	—	7	13	—	—	43	47	109	7	19	101	17	—	—	—	7	67	—	79	11	23	73	7	—	197	37	—
89	—	—	109	11	—	71	7	—	103	37	43	—	—	7	11	—	13	41	173	—	7	23	19	—	—	11	—	7	53	13
93	—	127	—	7	19	73	—	83	37	11	7	—	13	—	43	17	—	7	163	—	11	—	—	19	7	13	—	107	—	—
99	97	—	7	—	—	53	13	11	—	7	—	23	107	—	—	19	7	101	11	13	43	—	—	7	47	37	29	67	—	11

VI c.

	5 40	43	46	49	52	55	58	61	64	67	70	73	76	79	82	85	88	91	94	5 97	6 00	03	06	09	12	15	18	21	24	27
01	—	13	—	7	—	—	41	—	—	—	7	—	—	—	11	19	127	7	191	227	29	47	—	—	7	11	23	13	—	—
07	53	11	7	—	—	47	—	19	13	7	109	17	11	79	—	41	7	—	—	—	23	13	—	7	97	—	19	173	17	73
11	—	—	97	43	13	—	7	11	19	—	47	223	53	7	—	—	23	13	11	29	7	41	—	17	—	—	113	7	139	11
13	—	7	13	89	—	43	—	—	7	—	11	37	17	29	23	7	103	—	19	211	—	11	7	—	41	137	—	179	13	7
17	19	29	—	—	—	7	—	17	—	43	23	13	7	—	—	163	11	31	—	7	—	—	—	—	13	227	7	11	—	59
19	7	—	193	—	—	59	—	7	11	13	19	31	157	17	7	139	131	—	—	11	47	7	13	-	29	—	—	—	7	19
23	89	—	—	11	7	13	—	—	17	131	127	7	29	—	11	43	59	—	7	—	193	179	—	—	—	7	211	23	—	—
29	97	11	—	7	—	—	—	37	73	17	7	—	11	53	—	107	89	7	67	—	—	23	19	11	7	13	17	—	163	149
31	71	—	—	163	11	7	31	-	—	—	13	—	7	19	—	11	—	29	103	7	173	—	—	13	—	37	7	—	149	—
37	—	67	11	137	7	19	—	73	—	—	—	7	—	11	—	—	17	13	7	31	—	—	—	—	11	7	—	—	29	43
41	13	7	101	—	37	—	19	31	7	23	—	17	—	13	139	7	29	—	—	11	—	83	7	149	47	19	13	—	17	7
43	11	31	53	7	—	67	—	23	—	179	7	11	59	—	—	—	19	7	—	—	97	—	11	—	7	—	—	—	41	—
47	7	—	—	23	101	—	11	7	47	—	—	—	17	—	7	127	83	11	—	—	13	7	-	59	73	—	23	29	7	17
49	—	17	7	—	—	13	—	—	19	7	89	—	—	167	31	—	7	—	13	149	11	29	—	7	23	61	127	19	197	131
53	191	13	31	179	11	73	7	233	—	19	59	83	—	7	13	11	229	149	—	—	7	—	131	—	—	—	11	7	19	—
59	—	19	11	—	—	7	83	89	13	211	—	41	7	11	17	31	71	—	37	7	19	13	—	47	11	—	7	61	—	97
61	7	—	47	17	73	11	13	7	131	31	43	19	23	149	7	157	11	67	97	13	17	7	—	—	—	—	—	11	7	—
67	13	—	—	11	17	181	7	—	—	—	149	—	—	7	11	—	37	—	—	59	7	17	19	41	197	11	13	7	—	23
71	139	—	23	7	19	61	—	-	149	11	7	103	101	29	—	37	17	7	—	—	11	73	13	19	7	23	—	—	179	41
73	23	11	—	—	31	7	59	13	—	—	—	—	7	—	19	—	113	47	—	7	13	—	17	11	71	67	7	79	—	—
77	17	—	7	13	167	149	71	11	—	7	—	181	137	—	101	19	7	17	11	23	—	173	47	7	29	139	43	97	—	11
79	41	13	—	—	7	—	17	—	—	—	11	7	—	37	13	—	97	23	7	—	73	11	—	17	233	7	—	13	43	67
83	—	7	149	—	59	11	29	19	7	—	13	—	37	23	167	7	11	—	17	191	—	—	7	13	—	—	19	11	—	7
89	7	137	17	11	13	—	—	7	—	109	—	—	—	103	7	41	—	13	19	17	—	7	—	71	167	11	199	—	7	37
91	—	109	7	127	—	23	11	83	17	7	37	29	31	—	71	13	7	11	41	—	—	131	137	7	—	17	59	—	11	—
97	47	7	83	43	11	53	—	—	7	13	—	—	—	59	97	7	—	—	—	—	19	—	7	181	—	31	11	37	—	7

VII a.

	5 41	44	47	50	53	56	59	62	65	68	71	74	77	80	83	86	89	92	95	5 98	6 01	04	07	10	13	16	19	22	25	28
01	—	—	19	—	17	7	—	43	—	79	11	61	7	31	173	—	—	53	13	7	—	11	101	—	59	229	7	—	—	—
03	7	—	11	13	29	—	—	7	—	43	17	137	19	11	7	—	13	73	157	79	—	7	—	53	11	—	103	17	7	13
07	61	41	227	67	7	17	37	—	11	—	—	7	13	19	199	103	—	—	7	11	—	29	17	—	101	7	31	—	—	181
09	11	—	—	—	19	—	7	—	—	—	13	11	—	7	—	29	—	—	—	—	7	193	11	13	37	—	—	7	17	107
13	53	—	—	7	—	19	11	67	31	—	7	—	—	—	—	—	—	7	—	13	47	—	109	17	7	—	101	—	11	23
19	13	—	7	37	11	—	199	17	—	7	—	67	—	13	29	11	7	—	53	41	79	31	—	7	17	43	11	—	101	—
21	—	—	—	—	7	—	—	11	29	—	239	7	197	17	—	31	—	—	7	163	59	23	41	139	13	7	19	43	103	11
27	113	37	—	7	61	11	—	59	—	—	7	—	—	—	17	23	11	7	13	29	—	—	—	—	7	—	—	11	31	—
31	7	13	229	113	—	—	—	7	—	17	—	11	—	—	7	—	31	61	59	19	157	7	11	—	—	—	17	13	7	83
33	—	29	7	11	—	—	—	53	—	7	19	79	13	131	11	17	7	—	37	—	—	223	—	7	—	11	—	—	—	19
37	43	—	127	47	—	23	7	—	13	11	17	19	—	7	—	191	—	37	29	53	7	13	—	67	83	—	241	7	23	31
39	—	7	19	23	—	—	13	—	7	113	—	71	11	127	227	7	17	—	—	13	—	19	7	11	—	53	23	109	—	7
43	29	—	13	19	—	7	43	11	—	—	—	17	7	—	41	13	—	—	11	7	137	—	19	—	—	—	7	67	13	11
49	173	—	53	—	7	11	—	—	193	13	—	7	17	—	19	223	11	179	7	97	—	—	13	41	31	7	—	11	—	17
51	—	17	—	—	—	19	7	13	11	139	67	73	—	7	23	89	167	193	17	11	7	61	79	—	19	—	41	7	71	—
57	31	13	17	—	197	7	11	101	23	—	61	—	7	—	13	—	19	11	—	7	43	—	—	—	—	—	7	13	11	239
61	41	11	7	—	23	—	107	127	163	7	13	37	11	—	17	—	7	19	—	31	—	103	—	7	43	197	—	23	73	—
63	—	107	23	17	7	—	191	—	13	101	—	7	47	31	—	11	—	—	7	—	17	13	—	227	—	7	11	19	—	37
67	—	7	—	53	13	—	—	—	7	19	11	—	61	—	—	7	—	13	—	131	—	11	7	79	109	—	—	71	19	7
69	19	—	11	7	17	179	97	—	—	29	7	101	41	11	—	13	109	7	71	19	—	17	67	173	7	83	31	73	13	—
73	7	19	—	—	—	—	223	7	11	—	—	13	—	—	7	23	17	—	41	11	19	7	—	157	13	—	29	—	7	—
79	17	157	—	—	79	13	7	167	29	23	—	229	19	7	—	—	—	11	13	—	7	197	—	103	—	37	—	7	11	227
81	—	7	29	13	—	—	17	23	7	11	211	47	—	241	79	7	13	—	—	233	11	31	7	17	—	—	—	61	—	7
87	7	23	—	31	97	233	—	7	71	163	13	—	—	29	7	—	61	101	11	—	139	7	89	13	17	—	—	199	7	11
91	47	29	11	89	7	—	13	181	—	—	—	7	—	11	—	19	—	211	7	13	23	241	31	—	11	7	—	167	—	61
93	—	—	157	37	13	11	7	41	17	—	—	—	—	7	—	—	11	13	23	101	7	—	—	199	29	17	47	7	53	109
97	11	—	37	7	31	—	—	19	—	—	7	11	29	13	23	79	—	7	61	89	17	—	11	107	7	103	13	—	—	—
99	83	—	—	11	—	7	29	—	—	17	47	13	7	—	11	—	41	19	107	7	37	101	163	—	13	11	7	—	59	31

	5 42	45	48	51	54	57	60	63	66	69	72	75	78	81	84	87	90	93	96	5 99	6 02	05	08	11	14	17	20	23	26	29
03	67	—	7	—	17	53	—	13	23	7	—	—	—	97	—	47	7	31	19	37	11	17	41	7	—	—	—	—	—	—
09	151	7	23	—	67	17	—	11	7	—	19	131	—	—	13	7	—	127	11	139	—	—	7	53	—	23	59	13	137	7
11	23	19	59	7	—	—	79	—	—	—	7	17	13	—	—	—	—	7	—	181	19	11	—	23	7	13	—	—	17	53
17	—	—	7	—	151	—	13	199	11	7	29	113	17	89	—	71	7	23	—	11	—	73	61	7	—	—	—	101	—	17
21	59	—	13	11	157	—	7	17	41	—	—	97	67	7	11	13	—	137	—	—	7	—	—	—	17	11	109	7	13	—
23	13	7	73	199	19	103	11	151	7	—	—	23	53	13	37	7	—	11	109	31	—	29	7	19	239	—	13	—	11	7
27	211	11	109	—	43	7	179	23	17	13	89	—	7	37	—	—	67	41	—	7	229	—	13	11	19	17	7	—	—	—
29	7	31	—	29	11	23	43	7	—	—	151	—	—	—	7	11	—	79	—	—	13	7	59	—	47	—	11	157	7	—
33	193	23	—	13	7	—	137	—	—	17	11	7	151	61	71	—	13	—	7	73	29	11	127	113	23	7	17	83	—	13
39	73	—	29	7	—	139	—	53	11	97	7	163	—	47	—	151	43	7	23	11	59	—	83	13	7	107	—	17	—	—
41	11	—	173	67	—	7	—	103	13	—	—	11	7	53	—	—	17	—	19	7	107	13	11	—	—	29	7	31	37	113
47	17	—	13	—	7	107	41	29	37	11	19	7	—	—	211	13	137	17	7	151	11	191	71	47	43	7	—	—	13	19
51	—	7	—	131	11	197	23	37	7	—	—	13	17	—	—	7	—	—	—	—	—	151	7	—	13	—	11	—	31	7
53	227	17	19	7	23	127	—	11	181	13	7	67	—	—	—	41	—	7	11	167	89	19	13	—	7	37	—	23	—	11
57	7	89	11	19	—	13	29	7	53	—	31	—	47	11	7	—	73	—	13	—	—	7	19	23	11	—	—	127	7	157
59	29	—	7	13	31	11	61	—	—	7	—	—	—	19	53	67	7	—	—	17	—	23	—	7	41	151	229	11	—	13
63	11	—	83	—	37	—	7	157	—	—	173	11	13	7	17	—	—	23	—	61	7	71	11	31	—	13	53	7	223	79
69	—	197	—	43	—	7	13	—	61	11	—	23	7	—	59	17	—	—	—	7	11	37	—	—	—	19	7	47	29	—
71	7	11	37	—	13	43	47	7	—	23	—	—	11	—	7	—	19	13	—	—	—	7	29	11	—	223	—	97	7	—
77	—	—	—	23	29	17	7	—	19	227	11	13	31	7	—	53	—	—	83	37	7	11	17	131	13	163	23	7	233	71
81	17	—	—	7	109	11	—	13	—	19	7	71	—	73	—	43	11	7	37	—	13	29	23	193	7	—	—	11	19	—
83	19	—	71	139	113	7	17	—	11	—	—	89	7	83	233	29	—	43	13	7	23	47	107	17	—	31	7	—	—	—
87	—	13	7	11	—	—	—	113	—	7	—	—	107	31	11	—	7	—	17	223	19	43	—	7	—	11	47	13	—	—
89	233	79	131	229	7	47	11	17	83	—	59	7	13	—	23	—	37	11	7	239	—	—	—	43	17	7	29	89	11	—
93	—	7	17	97	211	—	—	—	7	—	23	—	11	—	29	7	—	—	—	17	—	13	7	11	—	61	31	43	71	7
99	7	71	13	17	19	—	—	7	31	—	11	239	—	—	7	13	113	—	—	—	17	7	—	19	89	29	—	23	7	73

	6 30	33	36	39	42	45	48	51	54	57	60	63	66	69	72	75	78	81	84	87	90	93	96	6 99	7 02	05	08	11	14	17
01	251	7	—	—	19	53	11	—	7	—	13	—	—	149	17	7	—	11	73	23	—	37	7	13	—	—	101	97	11	7
07	7	29	—	—	11	251	229	7	—	—	149	61	43	23	7	11	—	13	67	127	151	7	47	53	—	—	11	211	7	—
11	13	—	—	79	7	31	—	—	149	23	11	7	59	13	—	—	19	—	7	—	—	11	151	—	61	7	13	17	—	—
13	61	—	11	—	157	—	7	19	—	—	251	13	29	7	—	181	17	—	37	—	7	—	67	151	11	107	19	7	—	—
17	29	—	—	7	—	149	—	13	11	—	7	17	—	61	—	107	73	7	31	11	13	—	43	139	7	151	23	19	17	29
19	11	23	113	41	149	7	53	—	—	—	107	11	7	—	—	251	—	17	13	7	—	103	11	29	23	97	7	—	—	—
23	19	13	7	97	—	113	11	—	—	7	103	29	17	—	13	—	7	11	53	19	23	181	—	7	—	109	—	13	11	17
29	—	7	—	—	11	173	241	—	7	—	—	19	—	17	23	7	—	193	41	—	—	13	7	—	—	—	11	—	—	7
31	—	—	17	7	—	47	13	11	59	—	7	113	23	—	—	—	29	7	11	13	—	19	179	—	7	251	193	83	61	11
37	13	—	7	17	—	11	23	53	—	7	—	—	37	13	71	—	7	61	—	—	17	—	83	7	—	—	13	11	—	23
41	11	97	23	43	227	233	7	—	31	13	—	11	103	7	19	17	179	—	89	53	7	—	11	—	—	23	—	7	199	—
43	23	7	31	11	17	19	61	13	7	29	211	—	—	—	11	7	—	83	—	—	13	17	7	23	19	11	—	—	—	7
47	67	—	—	13	41	7	19	—	—	11	—	—	7	—	—	—	13	—	—	7	11	31	257	113	199	19	7	—	37	13
49	7	11	—	—	47	17	—	7	—	37	257	43	11	—	7	31	19	23	—	—	29	7	17	11	—	—	—	13	7	157
53	17	—	53	31	7	—	—	11	29	47	13	7	—	23	109	43	—	17	7	197	199	223	—	13	163	7	—	—	—	11
59	—	17	—	7	13	11	79	23	67	19	7	—	191	—	103	—	11	7	17	29	53	43	41	—	7	37	59	11	19	73
61	19	—	13	167	179	7	37	17	11	—	31	—	7	29	—	13	79	—	223	7	—	139	—	43	17	41	7	—	13	—
67	—	—	—	47	7	—	11	—	17	13	—	7	163	167	137	—	—	11	7	—	—	71	13	31	29	7	—	—	11	43
71	59	7	—	17	—	13	—	—	7	89	—	31	11	193	—	7	67	—	13	—	17	—	7	11	—	—	—	131	—	7
73	—	127	41	7	11	31	29	—	233	17	7	—	61	—	—	11	13	7	—	97	—	173	19	167	7	—	—	11	103	—	13
77	7	—	37	—	17	—	—	7	41	—	11	—	13	—	7	—	103	79	—	—	67	7	—	19	31	13	—	109	7	—
79	—	61	7	137	—	—	—	—	—	7	13	41	131	11	19	—	7	29	31	109	37	—	59	7	11	163	—	17	—	179
83	199	241	43	109	—	17	7	—	11	157	—	—	—	7	61	19	—	41	—	11	7	—	17	47	67	—	73	7	—	23
89	13	—	—	61	53	7	11	19	43	—	—	197	7	13	—	—	29	11	—	7	59	—	227	17	—	—	7	257	11	—
91	7	—	—	89	239	—	—	7	79	11	29	13	17	31	7	257	—	19	—	—	11	7	—	—	13	73	—	—	7	17
97	—	—	—	—	113	13	7	11	—	19	157	67	—	7	173	23	43	47	11	89	7	29	—	—	—	227	31	7	19	11

	6 31	34	37	40	43	46	49	52	55	58	61	64	67	70	73	76	79	82	85	88	91	94	6 97	7 00	03	06	09	12	15	18
01	89	13	11	7	—	—	—	113	17	29	7	23	—	11	13	—	—	7	—	107	43	—	47	—	7	17	—	13	127	19
03	—	19	—	29	—	7	41	—	31	23	—	—	7	—	17	67	11	241	61	7	19	—	43	—	229	13	7	11	—	59
07	11	163	7	—	107	23	47	197	13	7	—	11	41	37	—	—	7	—	—	83	29	13	11	7	167	—	17	31	23	—
09	223	—	—	11	7	—	13	61	109	—	—	7	19	113	11	17	59	—	7	13	—	31	—	—	—	7	23	—	43	—
13	—	7	13	—	73	—	139	—	7	11	17	—	—	19	83	7	113	—	131	—	11	41	7	53	—	241	—	17	13	7
19	7	—	—	—	—	19	—	7	—	13	37	17	137	29	7	—	23	—	11	—	—	7	13	—	19	—	—	229	7	11
21	17	—	7	73	131	—	—	13	—	7	11	127	—	—	23	19	7	17	—	—	13	11	113	7	—	—	—	67	37	—
27	—	7	—	43	—	—	—	19	7	—	89	181	53	97	13	7	—	—	17	11	—	—	7	239	—	—	19	13	—	7
31	—	137	101	11	23	7	29	37	19	—	13	—	7	17	11	—	—	31	—	7	73	—	103	13	53	11	7	19	233	109
33	7	229	17	—	—	—	11	7	13	43	41	31	—	—	7	47	—	11	19	17	257	7	137	59	61	23	89	—	7	29
37	19	11	—	—	7	109	—	89	—	—	—	7	11	43	17	239	41	13	7	19	47	23	—	11	37	7	—	—	—	—
39	103	—	13	17	11	37	7	—	—	—	19	29	—	7	—	11	—	—	—	23	7	—	—	—	31	—	11	7	13	19
43	233	—	—	7	37	127	101	53	—	—	7	13	31	—	—	17	—	7	—	43	—	11	97	89	7	41	61	191	29	—
49	—	67	7	19	229	13	107	71	11	7	29	—	—	—	—	61	7	139	13	11	—	37	19	7	103	31	—	—	—	—
51	11	107	37	13	7	17	—	23	—	—	83	7	—	19	47	—	13	131	7	31	—	199	11	—	—	7	—	43	—	13
57	137	23	103	7	139	19	17	—	—	11	7	—	241	—	193	29	—	7	179	37	11	—	79	13	7	—	—	—	163	181
61	7	17	—	29	11	—	13	7	53	67	—	41	101	—	7	11	—	—	17	13	23	7	—	—	71	19	11	—	7	—
63	83	—	7	—	13	—	167	11	—	7	109	—	—	199	31	71	7	13	11	—	—	—	—	7	17	—	29	—	—	11
67	13	—	11	—	191	—	7	—	173	—	127	—	179	7	23	157	—	19	—	17	7	—	—	—	11	—	13	7	59	—
69	181	7	43	79	59	11	—	—	7	199	—	13	23	47	—	7	11	233	191	61	263	127	7	41	13	17	—	11	—	7
73	11	—	—	17	—	7	43	13	23	19	—	11	7	—	89	31	101	67	47	7	13	—	11	79	—	29	7	263	19	41
79	—	13	23	139	7	—	181	29	—	11	—	7	43	—	13	—	—	—	7	—	11	17	—	—	—	7	—	13	31	—
81	23	11	—	—	—	71	7	97	—	—	17	19	11	7	43	53	157	—	—	—	7	—	31	11	—	13	—	7	47	—
87	179	—	227	19	31	7	13	—	—	41	11	17	7	73	79	113	—	23	107	7	43	11	19	109	59	—	7	—	17	—
91	29	173	7	—	19	11	17	109	107	7	—	—	—	23	—	13	7	47	113	—	—	—	101	7	43	223	—	11	13	29
93	13	—	—	107	7	—	103	—	11	131	37	7	17	13	19	139	—	31	7	11	—	—	71	29	—	7	13	—	—	17
97	—	7	131	11	71	31	—	17	7	13	53	29	—	229	11	7	97	163	—	—	—	—	7	191	17	11	—	83	—	7
99	—	—	—	7	—	23	11	13	—	—	7	—	67	17	—	—	53	7	181	—	13	—	223	—	7	19	—	37	11	—

	6 32	35	38	41	44	47	50	53	56	59	62	65	68	71	74	77	80	83	86	89	92	95	6 98	7 01	04	07	10	13	16	19
03	7	11	—	13	—	89	—	7	17	59	239	73	11	—	7	79	13	167	31	—	—	7	29	11	23	17	19	113	7	13
09	31	41	—	—	29	—	7	—	—	17	11	—	—	7	—	—	47	83	19	—	7	11	—	13	181	—	17	7	101	—
11	—	7	11	61	41	163	—	241	7	19	73	227	71	11	—	7	23	—	—	137	67	13	7	—	11	31	—	29	19	7
17	7	19	13	97	37	—	79	7	—	29	23	11	109	41	7	13	17	53	59	—	19	7	11	—	67	—	47	—	7	—
21	191	—	19	37	7	61	11	83	211	—	—	—	7	—	—	—	241	251	11	7	41	—	19	—	—	13	7	29	73	11	23
23	17	139	—	—	23	59	7	—	137	11	47	—	19	7	191	—	—	17	163	157	7	37	13	—	—	197	—	7	67	71
27	23	—	83	7	11	13	—	—	29	—	7	71	17	19	—	11	59	7	13	—	37	251	—	23	7	107	11	—	41	17
29	53	17	29	13	19	7	—	11	—	—	103	—	7	—	—	89	13	—	11	7	107	23	—	19	—	—	7	—	83	11
33	37	—	7	59	—	19	—	79	—	7	107	—	13	11	—	—	7	23	—	29	—	31	—	7	11	13	251	—	—	—
39	11	7	—	31	—	41	13	223	7	233	—	11	89	—	17	7	19	37	—	13	—	—	7	—	—	127	—	—	71	7
41	—	—	—	7	13	101	193	19	41	23	7	—	—	—	11	—	—	7	83	71	17	197	211	—	7	11	19	—	31	—
47	—	11	7	23	17	—	29	101	—	7	31	13	11	83	—	37	7	41	19	—	—	17	—	7	13	263	23	—	—	—
51	19	103	67	—	—	73	7	11	—	—	97	61	—	7	37	—	17	—	11	19	7	157	23	29	—	139	227	7	137	11
53	43	7	—	—	—	13	—	—	7	101	11	—	—	—	—	7	—	29	13	53	23	11	7	31	47	—	41	—	79	7
57	17	13	—	—	43	7	67	—	—	—	59	19	7	—	13	—	11	17	71	7	—	—	—	—	—	173	7	11	131	47
59	7	—	19	83	73	31	17	7	11	71	173	101	13	239	7	—	—	197	—	11	—	7	—	17	—	13	—	—	7	227
63	41	17	—	11	7	—	—	163	13	—	23	7	—	47	11	—	29	137	7	—	—	13	19	—	31	7	179	—	—	—
69	151	11	13	7	23	239	31	131	97	41	7	—	11	—	19	13	43	7	—	17	113	73	109	11	7	—	—	23	13	79
71	13	151	23	—	11	7	—	—	17	37	—	—	7	13	109	11	—	—	43	7	53	29	107	47	19	17	7	149	—	—
77	—	—	11	29	7	211	59	13	—	17	191	7	—	11	—	—	19	101	7	23	13	41	—	—	11	7	17	137	229	167
81	—	7	127	13	17	—	151	—	7	—	79	139	47	—	—	7	13	19	173	11	29	17	7	—	—	37	—	41	43	7
83	11	13	193	7	—	—	37	151	19	—	7	11	—	23	13	—	103	7	—	101	79	149	11	—	7	—	31	13	97	—
87	7	—	29	—	59	17	11	7	—	19	13	—	211	—	7	53	—	11	—	149	193	7	17	13	—	71	67	—	7	—
89	19	—	7	—	—	67	—	23	13	7	151	17	—	—	—	—	7	—	149	19	11	13	47	7	—	29	—	—	17	193
93	167	19	181	23	11	—	7	—	179	—	—	—	151	7	—	11	149	13	73	—	7	—	37	17	157	—	11	7	—	—
99	—	—	11	43	—	7	—	17	—	31	167	13	7	11	—	151	—	—	—	7	23	79	—	—	11	83	7	—	—	—

	7 20	23	26	29	32	35	38	41	44	47	50	53	56	59	62	65	68	71	74	77	80	83	86	89	92	95	7 98	8 01	04	07
01	89	17	79	—	71	31	7	—	47	11	179	257	19	7	181	113	—	—	17	13	7	—	83	—	—	107	—	7	37	—
07	13	—	17	—	19	7	23	11	37	—	107	—	7	13	—	—	89	83	11	7	—	-	—	19	103	43	7	—	—	11
11	107	167	7	—	179	19	31	37	—	7	—	127	—	11	17	—	7	29	199	—	181	—	13	7	11	23	—	—	191	43
13	23	—	—	17	7	11	223	13	—	—	—	7	83	—	—	19	11	59	7	—	13	71	127	23	113	7	—	11	97	—
17	11	7	—	13	211	—	97	137	7	—	—	11	—	89	199	7	13	67	—	23	—	—	7	53	37	131	—	113	29	7
19	—	13	101	7	17	37	—	19	—	—	7	109	—	31	11	—	—	7	-	—	61	17	29	—	7	11	19	13	137	53
23	7	31	—	—	37	—	—	7	19	11	13	—	47	23	7	59	17	233	139	—	11	7	—	13	227	281	—	19	7	89
29	17	151	59	233	13	—	7	11	263	—	—	—	—	7	31	103	—	13	11	19	7	29	61	—	—	67	—	7	—	11
31	—	7	13	—	67	23	17	-	7	—	11	71	53	—	—	7	—	137	—	—	—	11	7	17	—	—	97	227	13	7
37	7	—	19	—	—	151	47	7	11	13	—	—	43	—	7	—	—	—	211	11	73	7	13	193	17	—	29	127	7	—
41	61	—	17	11	7	13	41	151	—	31	—	7	—	—	11	—	43	—	7	17	—	—	19	—	—	7	—	—	257	263
43	—	73	—	13	—	251	7	—	17	41	101	59	67	7	—	—	13	11	43	—	7	157	—	89	109	17	—	7	11	13
47	—	11	—	7	89	—	—	53	109	—	7	—	11	173	19	41	—	7	—	—	17	—	31	11	7	13	—	—	—	—
49	109	71	—	—	11	7	—	—	—	17	13	151	7	53	—	11	31	179	41	7	—	47	—	13	19	—	7	—	—	—
53	—	—	7	—	17	—	13	29	—	7	11	—	—	151	—	37	7	—	73	13	89	11	—	7	41	19	47	—	43	23
59	13	7	113	—	—	17	—	—	7	—	47	179	—	13	—	7	151	19	29	11	—	127	7	23	—	—	13	71	61	7
61	11	269	—	7	61	—	233	—	19	—	7	11	29	37	—	—	101	7	71	—	251	23	11	281	7	—	—	19	17	-
67	19	—	7	131	41	13	—	-	113	7	271	—	17	—	53	23	7	—	13	19	11	—	97	7	31	251	—	—	67	17
71	97	13	—	43	11	—	7	17	—	—	41	23	31	7	13	11	—	—	—	83	7	109	151	157	17	47	11	7	—	37
73	—	7	—	—	47	29	31	11	7	23	37	19	13	17	89	7	—	229	11	—	101	181	7	151	—	13	—	—	—	7
77	—	157	11	—	—	7	—	—	13	37	193	—	7	11	83	73	59	71	—	7	163	13	29	—	11	17	7	—	23	—
79	7	—	—	19	127	11	13	7	71	—	—	43	—	—	7	—	11	113	—	13	—	7	19	—	—	—	23	11	7	—
83	11	—	13	59	7	—	—	31	211	17	—	7	—	—	—	13	—	79	7	—	113	103	11	19	—	7	17	181	13	—
89	—	191	—	7	83	—	37	—	—	11	7	—	—	—	—	19	23	7	—	107	11	43	13	—	7	—	—	17	—	—
91	—	11	157	47	—	7	19	13	163	29	61	—	7	—	23	191	17	—	—	7	13	277	—	11	37	19	7	—	—	173
97	17	13	139	—	7	—	—	—	23	—	11	7	59	—	13	—	131	17	7	—	29	11	—	197	179	7	109	13	101	43

	7 21	24	27	30	33	36	39	42	45	48	51	54	57	60	63	66	69	72	75	78	81	84	87	90	93	96	7 99	8 02	05	08
01	—	7	—	37	23	11	67	—	7	131	13	—	17	—	41	7	11	—	19	—	—	—	7	13	—	—	—	11	79	7
03	—	17	23	7	—	89	263	—	11	19	7	—	—	—	—	—	53	7	17	11	83	13	211	199	7	23	—	139	19	—
07	7	61	—	11	13	—	—	7	—	239	19	—	—	17	7	—	—	13	179	29	37	7	—	41	71	11	—	—	7	19
09	—	19	7	—	—	—	11	—	—	7	—	73	—	29	137	13	7	11	—	17	19	89	31	7	—	—	41	—	11	—
13	37	11	19	—	167	—	7	47	269	79	31	13	11	7	17	23	—	—	—	—	7	19	—	11	13	—	157	7	—	211
19	41	139	—	—	157	7	193	—	43	23	11	53	7	19	167	17	—	37	13	7	191	11	223	31	—	103	7	97	73	—
21	7	—	11	13	17	83	29	7	—	—	43	199	—	11	7	193	13	31	—	59	—	7	—	19	11	—	229	—	7	13
27	11	23	—	103	—	17	7	199	—	—	13	11	41	7	127	19	43	29	—	223	7	—	11	13	23	—	257	7	—	131
31	17	—	257	7	—	29	11	—	—	—	7	—	—	—	37	—	19	7	31	13	23	107	131	—	7	—	67	—	11	—
33	53	113	—	199	13	7	17	19	73	11	—	241	7	139	—	197	107	13	23	7	11	41	43	17	—	-	7	—	29	—
37	13	17	7	—	11	—	107	61	19	7	227	—	53	13	23	11	7	—	17	277	—	—	—	7	—	97	11	19	—	229
39	—	107	—	—	7	211	—	11	131	67	29	7	23	—	97	173	47	—	7	—	—	—	71	—	13	7	—	—	43	11
43	19	7	11	—	71	—	—	13	7	—	163	37	—	11	—	7	—	—	—	17	13	47	7	—	11	73	—	29	239	7
49	7	13	23	17	41	47	73	7	127	29	—	11	211	113	7	—	—	—	—	—	17	7	11	137	—	23	31	13	7	—
51	23	53	7	11	—	—	—	41	—	7	223	197	13	59	11	—	7	67	—	127	31	19	61	7	73	11	17	—	109	233
57	59	7	31	43	109	73	13	—	7	—	17	61	11	19	29	7	41	23	—	13	—	67	7	11	—	—	37	17	—	7
61	—	—	13	—	—	7	—	11	—	—	—	59	7	23	19	13	—	—	11	7	47	31	17	173	61	37	7	83	13	11
63	7	233	—	—	—	19	37	7	173	43	11	17	239	13	7	31	—	—	—	—	—	7	79	—	19	29	13	—	7	—
67	—	—	—	31	7	11	17	23	—	13	—	7	—	29	—	—	11	—	7	—	—	—	13	17	—	7	—	11	—	193
69	—	—	53	89	—	23	7	13	11	—	—	163	17	7	—	43	19	—	—	11	7	131	227	37	139	—	211	7	23	17
73	—	23	61	7	239	—	—	17	—	—	7	71	—	127	11	—	13	7	—	43	—	97	37	107	7	11	—	—	197	13
79	89	11	7	—	—	—	29	—	17	7	13	—	11	—	—	—	7	—	23	47	—	—	—	7	—	17	—	—	19	31
81	19	—	73	107	7	—	167	59	13	103	—	7	—	—	17	11	23	109	7	19	37	13	—	31	163	7	11	43	61	29
87	37	173	11	7	—	31	241	—	—	—	7	19	—	11	—	13	167	7	—	71	41	—	—	—	7	—	—	—	13	47
91	7	71	83	—	79	59	23	7	11	—	17	13	19	—	7	53	—	—	—	11	—	7	—	139	13	—	41	17	7	23
93	11	—	7	19	23	—	61	—	97	7	—	11	—	47	79	271	7	37	31	—	—	53	11	7	—	—	167	23	83	41
97	23	—	—	67	19	13	7	—	—	—	29	17	—	7	241	—	37	11	13	61	7	—	—	19	—	—	—	7	11	—
99	17	7	43	13	29	—	—	191	7	11	139	103	229	—	19	7	13	17	73	—	11	23	7	83	—	—	—	59	—	7

	7 22	25	28	31	34	37	40	43	46	49	52	55	58	61	64	67	70	73	76	79	82	85	88	91	94	7 97	8 00	03	06	09
03	103	—	47	41	11	7	43	67	61	—	157	—	7	—	—	11	—	23	71	7	—	29	—	—	271	13	7	131	—	17
09	163	31	11	29	7	—	13	19	—	173	—	7	41	11	109	79	53	97	7	13	197	—	—	239	11	7	19	—	149	—
11	—	59	17	113	13	11	7	—	—	23	—	—	47	7	43	41	11	13	—	17	7	—	53	—	—	79	29	7	—	—
17	257	127	—	11	—	7	—	—	29	19	—	13	7	103	11	—	—	—	—	7	17	—	269	61	13	11	7	—	19	—
21	—	47	7	—	—	—	—	13	71	7	19	—	—	163	—	17	7	167	—	67	11	233	23	7	43	29	—	31	—	19
23	—	11	—	83	7	13	79	—	—	—	—	7	11	—	—	73	—	—	7	29	19	17	—	11	—	7	43	47	37	—
27	—	7	19	—	101	—	—	11	7	31	—	—	191	269	13	7	17	53	11	149	137	19	7	67	—	61	79	13	—	7
29	—	29	67	7	97	17	181	239	37	—	7	47	13	—	23	277	—	7	149	—	—	11	17	53	7	13	191	—	—	—
33	7	—	173	—	—	11	101	7	13	—	23	—	—	19	7	—	11	17	29	—	—	7	31	—	—	71	163	11	7	—
39	29	17	13	11	23	19	7	79	101	137	—	—	181	7	11	13	41	—	17	59	7	—	—	—	19	11	—	7	13	29
41	13	7	23	—	271	37	11	17	7	—	67	—	149	13	—	7	—	11	—	41	—	—	7	29	17	23	13	—	11	7
47	7	—	97	193	11	29	—	7	17	149	47	31	73	—	7	11	—	—	—	23	13	7	37	—	53	17	11	—	7	61
51	—	—	263	13	7	—	—	149	19	241	11	7	101	271	89	23	13	—	7	—	17	11	29	—	—	7	—	19	—	13
53	—	13	11	191	—	131	7	—	—	17	—	—	—	7	13	—	29	103	19	137	7	—	—	—	11	173	17	7	59	—
57	19	37	41	7	17	—	103	—	11	23	7	—	31	—	101	—	251	7	79	11	139	17	—	13	7	—	223	107	—	73
59	11	—	—	149	—	7	31	23	13	—	17	11	7	—	157	59	263	—	—	7	—	13	11	—	181	47	7	17	79	19
63	127	149	7	23	13	17	11	—	197	7	73	19	107	—	—	29	7	11	37	53	61	251	17	7	229	31	23	—	11	—
69	—	7	—	19	11	71	17	31	7	61	—	13	—	59	47	7	—	—	101	—	23	—	7	17	13	—	11	—	—	7
71	—	31	—	7	—	—	—	11	89	13	7	—	17	19	—	—	37	7	11	103	29	—	13	41	7	241	—	179	—	11
77	—	—	7	13	—	11	—	—	53	7	—	—	23	17	31	—	7	—	173	—	—	—	—	7	19	—	—	11	—	13
81	11	181	31	—	197	89	7	—	17	97	83	11	13	7	—	—	—	223	—	29	7	179	11	—	—	13	73	7	—	47
83	41	7	—	11	—	—	23	—	7	167	13	—	—	29	11	7	19	—	131	—	—	—	7	13	61	11	53	31	—	7
87	—	29	23	163	43	7	13	73	—	11	79	131	7	47	—	31	157	19	—	7	11	89	—	—	101	23	7	—	—	109
89	7	11	—	—	13	113	43	7	19	31	—	269	11	61	7	17	127	13	—	167	79	7	—	11	29	73	283	19	7	—
93	13	229	—	53	7	109	—	11	113	19	17	7	29	13	—	41	—	193	7	23	59	—	—	—	—	7	13	17	19	11
99	197	19	269	7	67	11	—	13	—	37	7	17	71	23	227	61	11	7	—	—	13	53	257	29	7	199	173	11	17	107

IX c.

	8 10	13	16	19	22	25	28	31	34	37	40	43	46	49	52	55	58	61	64	67	70	73	76	79	82	85	88	91	94	97
01	—	11	13	—	7	17	31	—	—	—	167	7	11	59	—	13	239	29	7	277	19	67	17	11	193	7	—	—	13	271
07	59	—	79	7	—	—	17	41	—	13	7	—	19	197	139	37	53	7	71	31	167	11	13	17	7	67	—	—	29	109
11	7	17	—	101	229	11	—	7	239	97	—	59	211	19	7	233	11	—	13	—	—	7	79	—	—	61	—	11	7	283
13	—	31	7	13	19	109	—	17	11	7	29	—	191	—	—	—	7	—	—	11	—	—	—	7	17	—	—	—	—	13
17	—	233	17	11	—	19	7	—	—	—	—	—	13	7	11	—	—	—	103	17	7	—	41	—	19	11	—	7	—	73
19	—	7	—	—	—	179	11	43	7	—	13	—	37	—	31	7	—	11	89	—	173	29	7	13	47	17	—	—	11	7
23	—	11	31	17	—	7	13	101	—	29	73	37	7	163	—	—	19	71	—	7	17	—	—	11	—	—	7	—	223	23
29	13	167	—	—	7	—	113	97	19	101	11	7	—	31	—	31	—	43	7	—	29	11	—	23	83	7	13	19	37	53
31	—	—	11	—	—	—	7	59	—	31	17	13	—	7	29	—	—	—	19	43	7	23	—	—	11	223	211	7	—	61
37	11	163	—	—	—	7	—	—	—	—	19	11	7	157	—	23	—	—	13	7	—	—	11	47	—	29	7	—	17	19
41	—	13	7	67	—	59	11	71	181	7	31	19	53	29	13	113	7	11	—	127	—	167	—	7	—	37	73	13	11	43
43	—	—	19	—	7	197	37	29	—	11	229	7	13	173	—	131	—	—	7	—	11	19	—	—	79	7	—	97	—	17
47	—	7	—	19	11	23	—	17	7	83	—	—	47	—	—	7	—	277	137	223	61	13	7	31	17	—	11	239	23	7
49	—	—	—	7	233	—	13	11	—	89	7	—	—	17	163	—	293	7	11	13	—	113	—	37	7	73	23	59	—	11
53	7	—	11	—	83	31	29	7	17	61	—	67	—	11	7	13	—	101	—	—	263	7	23	281	11	17	—	—	7	—
59	11	—	37	41	43	—	7	137	—	13	—	11	—	7	—	67	23	29	31	101	7	—	11	—	—	19	17	7	—	—
61	103	7	127	11	—	—	41	13	7	—	—	29	31	—	11	7	19	—	—	53	13	199	7	—	—	11	—	163	137	7
67	7	11	—	—	—	—	173	7	19	211	—	239	11	—	7	41	17	199	—	—	83	7	29	11	61	31	—	13	7	—
71	—	—	—	—	7	—	79	11	—	19	13	7	227	31	71	—	43	—	7	—	—	41	—	13	103	7	181	23	17	11
73	17	—	23	—	29	71	7	31	13	—	11	139	—	7	269	83	79	17	43	19	7	11	73	—	41	23	—	7	131	107
77	—	19	—	7	13	11	179	—	—	—	7	—	17	—	53	—	11	7	—	107	19	23	43	—	7	101	31	11	—	17
79	89	17	13	73	—	7	67	223	11	199	83	19	7	—	107	13	157	—	17	7	31	59	—	97	43	283	7	257	13	—
83	—	97	7	11	107	269	—	193	31	7	47	13	19	17	11	23	7	—	197	—	—	—	—	7	13	11	—	101	43	—
89	131	7	—	163	19	13	—	41	7	23	—	—	11	37	17	7	—	79	13	59	73	31	7	11	—	—	103	—	109	7
91	83	199	151	7	11	—	—	23	29	—	7	—	—	—	19	11	13	7	—	229	17	281	—	—	7	—	11	79	—	13
97	—	23	7	167	17	151	19	271	—	7	13	37	—	11	—	—	7	—	67	29	251	17	—	7	11	19	—	191	31	—

X a.

	8 11	14	17	20	23	26	29	32	35	38	41	44	47	50	53	56	59	62	65	68	71	74	77	80	83	86	89	92	95	98
01	—	—	—	43	—	—	7	19	11	47	37	—	—	7	197	—	17	—	—	11	7	71	—	—	—	41	19	7	—	89
03	11	7	—	—	13	17	—	—	7	181	31	11	71	167	—	7	—	13	23	61	—	—	7	—	227	251	—	—	37	7
07	13	127	—	—	—	7	11	—	113	43	151	—	7	13	23	—	271	11	19	7	—	—	229	—	233	—	7	37	11	31
09	7	—	101	—	53	—	17	7	37	11	241	13	23	—	7	59	—	—	—	47	11	7	139	17	13	—	67	—	7	—
13	29	17	41	—	7	—	—	13	23	—	19	7	—	151	—	11	53	73	7	—	13	61	239	283	47	7	11	—	—	19
19	—	13	11	7	263	—	283	—	47	79	7	29	—	11	13	—	151	7	241	17	—	19	—	—	7	23	—	13	—	—
21	23	—	71	—	191	7	101	—	17	109	—	—	7	—	41	—	11	151	31	7	—	—	—	23	—	13	7	11	—	—
27	31	107	—	11	7	53	13	—	101	17	—	7	193	—	11	—	29	23	7	13	151	—	37	19	—	7	17	—	—	43
31	—	7	13	—	17	19	127	—	7	11	—	—	—	23	—	7	—	53	—	31	11	17	7	47	19	263	113	—	13	7
33	13	11	37	7	281	—	239	—	103	—	7	23	11	13	—	19	—	7	—	71	—	—	59	11	7	61	13	17	—	—
37	7	31	—	—	137	17	197	7	—	13	—	—	—	—	7	29	19	83	11	—	79	7	13	—	—	151	—	—	7	11
39	41	—	7	—	—	23	—	13	139	7	11	17	101	277	61	—	7	—	—	37	13	11	—	7	—	137	19	233	17	—
43	53	23	43	13	67	11	7	—	19	—	—	—	83	7	31	—	11	—	37	—	7	—	—	17	23	—	29	7	151	13
49	19	79	—	11	—	7	109	17	29	191	13	—	7	—	11	41	61	—	23	7	—	157	47	13	17	11	7	31	149	—
51	7	47	29	—	—	—	11	7	13	71	19	79	—	17	7	97	23	11	41	—	—	7	—	191	53	—	—	149	7	19
57	—	—	13	31	11	—	7	—	—	—	23	—	131	7	17	11	43	—	101	—	7	19	127	173	149	—	11	7	13	59
61	277	29	—	7	—	131	23	139	—	17	7	13	—	—	—	—	67	7	—	—	43	11	19	107	7	—	17	—	—	23
63	—	—	11	137	23	7	—	53	—	13	—	—	7	11	—	17	31	—	107	7	101	149	13	83	11	—	7	23	—	73
67	23	41	7	—	31	13	163	—	11	7	17	—	29	257	19	—	7	281	13	11	67	47	—	7	97	—	43	17	—	—
69	11	257	—	13	7	19	29	—	193	—	73	7	103	97	—	—	13	—	7	—	61	23	11	—	19	7	—	—	43	13
73	—	7	—	—	—	47	11	—	7	—	41	17	13	241	59	7	149	11	—	109	179	—	7	29	67	13	193	—	11	7
79	7	59	53	211	11	29	13	7	—	37	—	23	17	149	7	11	127	19	—	13	—	7	61	—	—	71	11	73	7	17
81	—	17	7	79	13	89	—	11	19	7	—	—	149	—	—	47	7	13	11	283	—	—	41	7	31	—	101	19	29	11
87	19	7	17	23	—	11	31	37	7	149	29	13	—	—	103	7	11	—	—	17	—	89	7	59	13	131	23	11	101	7
91	11	19	89	103	47	7	37	13	—	—	—	11	7	—	17	—	—	—	131	7	13	—	11	137	157	31	7	29	—	—
93	7	227	263	11	—	13	149	7	179	43	59	19	—	—	7	67	113	—	13	31	17	7	—	—	37	11	—	—	7	241
97	—	13	157	53	7	41	—	31	—	11	269	7	19	43	13	17	23	—	7	113	11	59	—	37	—	7	—	13	—	—
99	—	11	—	19	17	—	7	—	41	53	—	—	11	7	23	43	—	211	—	67	7	17	19	11	109	13	61	7	—	—

X b. X

	8 12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57	60	63	66	69	72	75	78	81	84	87	90	93	96	99
03	—	149	179	7	19	191	—	11	13	—	7	—	137	—	41	—	17	7	11	43	29	13	—	19	7	107	—	—	—	11
09	17	—	7	47	23	11	—	227	—	7	107	—	—	—	223	13	7	17	257	233	37	—	277	7	211	43	—	11	13	—
11	13	37	23	157	7	107	17	—	11	—	—	7	—	13	—	—	—	—	7	11	—	—	—	17	—	7	13	31	—	47
17	241	—	—	7	73	181	11	13	—	31	7	223	89	47	229	—	—	7	37	23	13	—	137	—	7	79	—	—	11	—
21	7	11	17	13	—	—	61	7	—	—	—	—	11	—	7	23	13	37	19	17	—	7	53	11	29	—	—	179	7	13
23	—	13	7	41	11	—	—	97	17	7	—	—	271	23	13	11	7	—	29	—	—	—	31	7	—	17	11	13	19	—
27	43	—	47	17	139	—	7	103	241	23	11	181	—	7	—	59	—	173	—	—	7	11	71	13	—	83	127	7	—	19
29	29	7	11	—	31	—	79	23	7	17	—	137	41	11	—	7	—	131	—	—	19	13	7	—	11	—	17	—	47	7
33	—	—	19	23	13	7	43	167	11	—	131	—	7	—	37	—	227	13	41	7	83	17	—	31	191	89	7	157	—	139
39	—	67	—	—	7	17	11	—	—	—	—	7	43	19	—	83	97	11	7	—	23	—	17	53	13	7	269	41	11	—
41	137	73	223	—	19	97	7	—	—	11	61	17	37	7	43	179	139	—	23	227	7	—	13	19	59	—	—	7	17	53
47	113	—	—	13	29	7	—	11	233	127	—	59	7	—	—	19	13	79	11	7	43	—	107	181	241	—	7	47	157	11
51	31	—	7	113	41	83	53	17	23	7	173	—	13	11	—	—	7	—	73	—	—	29	59	7	11	13	—	199	37	293
53	193	—	—	—	7	11	23	19	—	37	13	7	53	17	—	29	11	—	7	89	—	—	—	13	197	7	19	11	—	23
57	11	7	23	29	—	—	13	—	7	59	109	11	—	31	97	7	47	—	193	13	—	—	7	199	53	17	—	19	—	7
59	23	—	109	7	13	—	—	31	269	113	7	—	—	—	11	191	41	7	19	—	71	—	103	23	7	11	29	193	—	—
63	7	—	71	—	—	—	—	7	—	11	—	103	113	13	7	139	89	67	79	19	11	7	41	131	—	37	13	—	7	—
69	181	—	—	127	—	37	7	11	31	—	17	19	—	7	—	199	—	—	11	—	7	67	—	—	—	29	—	7	—	11
71	67	7	19	—	—	13	—	263	7	131	11	23	—	53	127	7	17	—	13	29	197	11	7	37	—	—	—	—	—	7
77	7	29	41	37	67	23	—	7	11	79	71	83	13	19	7	31	—	17	—	11	—	7	—	—	103	13	281	139	7	—
81	—	23	37	11	7	—	251	199	13	137	271	7	17	103	11	—	59	—	7	—	—	13	—	109	23	7	229	—	—	17
83	—	17	—	—	—	19	7	—	67	—	89	41	29	7	73	109	—	11	17	13	7	—	23	163	19	47	—	7	11	—
87	29	11	13	7	—	—	19	61	53	—	7	251	11	17	—	13	31	7	23	37	191	—	—	11	7	19	—	—	13	29
89	13	83	17	—	11	7	—	—	—	47	31	—	7	13	53	11	19	—	—	7	41	—	179	29	107	—	7	71	—	—
93	—	139	7	—	—	—	—	89	127	7	11	29	23	—	17	—	7	19	—	—	—	11	13	7	—	—	41	—	257	31
99	—	7	—	13	—	—	23	—	7	19	—	31	73	—	193	7	13	—	181	11	—	251	7	89	—	—	139	—	19	7

X c. X

	9 00	03	06	09	12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57	60	63	66	69	72	75	78	81	84	87
01	—	73	7	—	11	37	—	31	—	7	—	13	—	—	—	11	7	—	—	—	—	23	—	7	13	—	11	—	19	89
07	—	7	11	—	223	13	—	—	7	—	17	—	—	11	—	7	113	—	13	—	19	193	7	—	11	281	47	17	—	7
11	—	13	19	—	197	7	—	—	11	83	281	23	7	—	13	29	—	—	73	7	67	19	17	—	41	—	7	13	—	—
13	7	—	31	229	53	—	—	7	—	23	47	11	13	—	7	—	59	227	—	—	—	7	11	199	—	13	—	41	7	—
17	—	37	—	—	7	23	11	251	13	—	191	7	179	19	71	47	53	11	7	—	—	13	79	17	67	7	29	59	11	—
19	—	181	—	23	19	71	7	—	—	11	167	—	17	7	—	31	—	73	—	13	7	61	53	19	191	113	23	7	—	17
23	—	41	13	7	11	19	—	17	29	—	7	—	251	—	59	11	—	7	37	—	131	—	23	103	7	—	11	—	13	269
29	197	59	7	79	—	—	229	181	17	7	41	—	—	11	—	—	7	251	—	29	109	—	13	7	11	17	—	—	—	—
31	—	103	—	—	7	11	131	13	—	47	31	7	109	29	17	—	11	—	7	—	13	—	71	—	—	7	19	11	257	—
37	179	13	233	7	—	239	—	199	23	—	7	—	—	—	11	17	—	7	19	—	137	—	41	31	7	11	227	13	173	—
41	7	61	—	211	23	—	—	7	97	11	13	31	29	—	7	—	—	89	—	19	11	7	241	13	—	103	—	17	7	293
43	127	11	7	199	—	31	29	—	13	7	19	269	11	37	73	—	7	—	—	97	—	13	—	7	47	23	—	—	—	19
47	53	167	—	—	13	43	7	11	193	163	—	17	37	7	79	—	—	13	11	—	7	23	127	29	31	—	—	7	17	11
49	17	7	13	103	—	83	53	43	7	137	11	277	71	—	307	7	—	17	31	23	139	11	7	67	79	—	—	61	13	7
53	—	—	269	19	—	7	31	—	59	—	—	13	7	47	—	23	11	—	53	7	—	—	19	—	13	—	7	11	—	17
59	—	—	—	11	7	13	97	157	—	23	—	7	73	17	11	—	29	43	7	31	—	167	163	—	—	7	—	103	—	61
61	113	109	17	13	263	19	7	23	—	—	29	89	229	7	—	—	13	11	—	17	7	173	—	47	19	—	—	7	11	13
67	—	23	71	17	11	7	—	37	—	—	13	73	7	—	107	11	19	59	—	7	17	29	—	13	23	43	7	89	—	283
71	—	—	7	—	107	—	13	61	89	7	11	—	47	—	31	17	7	19	—	13	23	11	—	7	211	—	—	127	59	43
73	—	—	11	29	7	—	—	—	19	113	163	7	283	11	—	—	—	13	7	—	191	17	277	—	11	7	97	19	—	—
77	13	7	—	—	97	—	79	—	7	19	—	—	113	13	23	7	17	—	307	11	29	—	7	37	89	—	13	31	19	7
79	11	—	—	7	37	17	139	—	—	—	7	11	23	—	29	271	79	7	—	19	—	31	11	—	7	—	—	—	—	—
83	7	19	29	37	—	—	11	7	23	31	—	—	—	—	7	—	239	11	—	—	13	7	109	293	—	—	—	47	7	173
89	—	13	23	—	11	67	7	—	—	—	—	47	19	7	13	11	—	—	17	—	7	113	31	—	271	23	11	7	149	223
91	23	7	89	19	—	—	—	43	11	7	—	127	61	13	193	—	7	31	—	11	—	307	41	7	23	17	13	53	149	—	7
97	7	—	—	—	—	11	13	7	17	71	—	59	43	—	7	—	11	23	29	13	—	7	—	—	149	17	223	11	7	31

90001—98999

9 01	04	07	10	13	16	19	22	25	28	31	34	37	40	43	46	49	52	55	58	61	64	67	70	73	76	79	82	85	88
01	11	—	13	17	7	139	29	137	233	—	157	7	—	23	181	13	43	31	7	—	17	—	11	—	—	7	47	283	13	—
03	13	—	—	11	—	47	7	—	—	17	—	23	—	7	11	—	—	—	43	—	7	149	—	—	—	11	13	7	137	29
07	—	—	61	7	17	101	73	19	—	11	7	—	83	—	—	89	—	7	—	149	11	17	13	—	7	—	19	—	—	—
09	251	11	—	—	—	7	—	13	79	—	17	29	7	—	—	37	107	19	149	7	13	229	97	11	31	—	7	17	23	—
13	97	23	7	13	127	17	107	11	71	7	—	109	31	41	37	—	7	—	11	—	223	67	17	7	23	—	179	—	29	11
19	227	7	83	—	53	11	17	—	7	101	13	—	—	149	257	7	11	—	23	—	277	—	7	13	307	31	—	11	—	7
21	—	19	257	7	29	—	—	—	11	—	7	103	17	167	—	—	23	7	59	11	19	13	311	—	7	41	181	—	83	17
27	—	31	7	227	271	59	11	—	67	7	23	—	19	17	—	13	7	11	—	79	97	211	197	7	—	233	—	—	11	37
31	193	11	—	29	—	—	7	149	17	—	—	13	11	7	—	173	59	—	—	61	7	—	—	11	13	17	—	7	37	23
33	173	7	41	—	11	43	149	—	7	13	—	233	67	—	17	7	—	—	83	47	251	73	7	19	131	89	11	23	—	7
37	23	—	31	59	149	7	89	—	37	17	11	233	7	271	29	101	139	131	13	7	—	11	—	23	19	163	7	193	211	—
39	7	—	11	13	241	—	—	7	29	263	—	41	—	11	7	17	13	—	—	239	127	7	—	—	11	251	37	31	7	13
43	109	149	103	181	7	113	—	—	11	227	17	7	13	157	—	31	19	23	7	11	79	—	89	53	311	7	—	17	—	97
49	—	151	—	7	167	37	11	29	19	—	7	17	241	—	—	—	—	7	—	13	—	43	—	107	7	—	41	19	11	—
51	17	29	151	83	13	7	—	—	—	11	—	113	7	163	—	—	—	13	19	7	11	—	31	37	67	—	7	—	139	41
57	89	17	47	23	7	151	—	11	—	—	19	7	29	—	157	103	269	—	7	—	—	—	—	71	13	7	23	—	67	11
61	29	7	11	41	103	71	—	13	7	—	59	19	—	11	127	7	—	—	—	257	13	—	7	31	11	61	—	97	—	7
63	—	61	17	7	211	11	41	257	151	—	7	—	—	—	197	181	11	7	13	17	23	19	—	29	7	127	163	11	—	109
67	7	13	139	19	—	31	—	7	—	—	151	11	41	109	7	137	23	—	227	37	—	7	11	113	—	101	—	13	7	—
69	37	—	7	11	—	29	—	—	—	7	—	151	13	19	11	41	7	47	—	—	17	—	—	7	—	11	313	—	241	—
73	—	—	43	61	—	—	7	53	13	11	23	211	79	7	19	17	73	—	31	—	7	13	29	—	—	—	—	7	—	—
79	31	173	13	—	23	7	19	11	43	131	—	—	7	—	—	13	17	—	11	7	—	—	—	193	—	19	7	23	13	11
81	7	—	23	—	—	17	59	7	—	293	11	—	191	13	7	73	19	151	—	—	—	7	17	—	—	23	13	29	7	61
87	—	41	—	79	—	277	7	13	11	29	—	—	—	7	37	—	43	—	61	11	7	—	—	17	—	—	—	7	311	—
91	—	17	163	7	59	—	67	41	53	19	7	—	71	37	11	23	13	7	17	—	43	47	151	79	7	11	29	227	19	13
93	19	13	—	71	—	7	11	17	—	—	41	—	7	23	13	—	—	11	109	7	29	—	43	151	17	211	7	13	11	—
97	—	11	7	—	—	47	—	—	29	7	13	—	11	73	—	281	7	233	—	17	19	—	—	7	—	151	43	—	—	—
99	—	—	29	—	7	107	197	23	13	—	—	7	97	—	—	11	—	157	7	41	—	13	—	89	173	7	11	—	43	—

	9 02	05	08	11	14	17	20	23	26	29	32	35	38	41	44	47	50	53	56	59	62	65	68	71	74	77	80	83	86	89
03	—	7	—	17	13	—	—	241	7	61	11	—	19	139	67	7	--	13	—	29	17	11	7	—	257	41	23	197	151	7
09	7	29	71	31	17	293	—	7	11	53	83	13	—	—	7	—	—	191	67	11	23	7	131	19	13	199	—	37	7	—
11	11	—	7	179	—		101	—	37	7	17	11	-	—	19	53	7	—	23	—	—	103	11	7	29	—	—	17	31	—
17	—	7	197	13	113	41	19	—	7	11	31	17	23	—	263	7	13	—	—	—	11	—	7	—	61	19	—	—	17	7
21	83	131	—	—	11	7	17	19	23	—	73	41	7	—	—	11	—	199	—	7	—	263	—	17	37	13	7	—	—	31
23	7	—	—	293	—	37	23	7	—	43	13	—	17	61	7	—	167	19	11	—	—	7	—	13	—	79	83	—	7	11
27	—	—	11	—	7	29	13	17	—	—	53	7	—	11	—	—	—	—	7	13	41	—	—	—	11	7	61	—	—	—
29	23	—	61	—	13	11	7	127	211	19	—	—	101	7	89	43	11	13	—	—	7	83	37	23	--	—	167	7	19	—
33	11	—	—	7	—	—	—	—	17	199	7	11	103	13	—	61	29	7	—	23	—	37	11	137	7	17	13	107	53	19
39	—	37	7	—	61	199	31	13	—	7	—	89	107	23	—	211	7	—	59	197	11	19	179	7	139	43	17	29	—	—
41	31	11	—	—	7	13	—	107	—	—	—	7	11	47	—	17	101	67	7	37	157	29	113	11	—	7	—	43	—	163
47	—	--	—	7	19	23	83	—	—	41	7	139	13	31	—	—	17	7	101	—	109	11	—	19	7	13	—	—	23	—
51	7	23	47	—	109	11	—	7	13	—	—	17	—	—	7	41	11	97	—	229	29	7	—	—	19	239	71	11	7	53
53	17	83	7	—	—	—	13	—	11	7	—	—	127	—	29	19	7	17	41	11	101	—	23	7	—	67	31	59	47	--
57	43	137	13	11	—	—	7	—	-	—	—	—	17	7	11	13	19	167	23	—	7	—	—	—	41	11	—	7	13	17
59	13	7	43	—	—	89	11	19	7	—	179	—	47	13	59	7	23	11	17	—	—	223	7	—	—	29	13	41	11	7
63	—	11	—	—	—	7	43	—	19	13	—	—	7	17	—	193	—	47	271	7	—	61	13	11	—	59	7	19	—	—
69	19	41	89	13	7	163	23	—	—	31	11	7	37	—	17	97	13	—	7	19	—	11	157	—	29	7	281	—	—	13
71	—	13	11	17	23	—	7	71	—	239	19	137	—	7	13	—	—	283	29	—	7	269	73	—	11	—	101	7	79	19
77	11	53	19	73	17	7	—	—	13	109	37	11	7	41	—	—	31	127	241	7	43	13	11	—	107	—	7	—	101	29
81	—	239	7	19	13	—	11	—	—	7	—	—	269	53	107	—	7	11	163	41	—	—	19	7	43	277	—	131	11	—
83	137	—	13	—	7	17	—	—	—	11	—	7	223	19	—	13	—	—	7	53	11	59	17	157	71	7	43	37	13	31
87	17	7	—	67	11	263	71	—	7	—	—	13	—	97	19	7	—	17	103	—	73	—	7	—	13	—	11	—	29	7
89	—	157	97	7	191	19	17	11	59	13	7	31	—	131	61	—	—	7	11	—	—	—	13	17	7	—	47	—	—	11
93	7	17	11	—	—	13	19	7	—	—	29	173	—	11	7	—	—	—	13	59	—	7	—	83	11	19	233	61	7	—
99	11	—	17	—	—	41	7	—	—	113	79	11	13	7	53	47	61	19	83	17	7	29	11	37	—	13	263	7	229	—

	9 90	93	96	9 99	10 02	05	08	11	14	17	20	23	26	29	32	35	38	41	44	47	50	53	56	59	62	65	68	71	74	77
01	7	199	103	—	97	—	—	7	31	—	—	—	37	17	7	29	—	19	11	—	13	7	—	137	61	—	—	—	7	11
07	181	13	—	—	—	11	7	—	28	19	83	263	—	7	13	89	11	—	131	—	7	31	—	—	—	73	29	7	19	37
11	11	47	—	7	23	—	—	—	—	17	7	11	—	—	29	—	—	7	263	—	173	53	11	13	7	43	17	23	37	19
13	—	19	23	11	—	7	73	—	13	37	—	101	7	—	11	17	—	—	193	7	19	13	—	—	—	11	7	43	233	—
17	—	—	7	41	13	—	181	—	37	7	17	—	89	97	—	61	7	13	—	—	11	19	31	7	—	29	223	17	163	—
19	83	11	13	163	7	—	41	—	—	—	—	7	11	101	233	13	17	—	7	23	—	—	—	11	—	7	37	—	13	—
23	—	7	—	—	31	—	—	11	7	—	—	13	41	19	109	7	47	—	11	—	—	—	7	73	13	37	—	—	17	7
29	7	71	67	—	73	11	—	7	—	23	257	—	17	—	7	—	11	31	13	—	127	7	53	—	19	307	317	11	7	17
31	167	17	7	13	113	229	59	23	11	7	—	31	29	—	—	19	7	101	17	11	—	—	73	7	41	—	47	149	53	13
37	97	7	17	37	—	—	11	19	7	—	13	—	197	79	—	7	—	11	181	17	—	—	7	13	23	—	19	—	11	7
41	—	11	37	139	59	7	13	—	19	—	67	29	7	311	17	47	—	223	71	7	23	—	149	11	131	—	7	19	—	—
43	7	41	—	17	11	29	31	7	61	71	—	53	—	113	7	11	—	13	19	—	17	7	89	—	—	—	11	307	7	163
47	13	—	251	89	7	—	—	41	229	—	11	7	—	13	23	17	113	—	7	19	73	11	29	53	181	7	13	109	139	—
49	37	—	11	127	17	—	7	—	—	—	19	13	23	7	223	—	29	—	149	31	7	17	—	101	11	47	59	7	—	19
53	—	73	227	7	29	193	—	13	11	97	7	19	—	—	79	—	17	7	67	11	13	137	—	—	7	127	—	83	—	277
59	17	13	7	19	107	—	11	—	71	7	—	—	251	149	13	29	7	11	—	—	31	—	19	7	59	23	—	13	11	197
61	23	67	—	—	7	227	17	—	241	11	—	7	13	19	31	—	283	—	7	—	11	—	157	17	—	7	—	101	41	—
67	157	—	—	7	—	19	13	11	—	149	7	—	—	—	37	—	—	7	11	13	29	—	—	—	7	61	—	31	—	11
71	7	—	11	—	—	163	19	7	29	—	—	167	83	11	7	13	241	73	—	17	—	7	251	—	11	19	—	—	7	47
73	13	43	7	257	197	11	149	—	17	7	103	23	—	13	61	—	7	—	—	—	179	—	—	7	—	17	13	11	—	—
77	11	—	263	17	149	43	7	23	—	13	—	11	—	7	139	—	109	19	191	29	7	167	11	—	—	197	—	7	31	—
79	—	7	—	11	—	23	281	13	7	17	—	37	—	29	11	7	73	—	—	—	13	—	7	131	—	11	17	19	23	7
83	—	23	83	13	17	7	79	—	—	11	31	43	7	—	179	—	13	—	163	7	11	17	—	—	23	53	7	—	19	13
89	—	19	—	—	7	17	233	11	—	—	13	7	29	181	—	71	—	43	7	—	19	—	17	13	157	7	89	37	47	11
91	197	—	131	—	—	—	7	47	13	137	11	17	103	7	—	—	23	31	—	43	7	11	—	83	—	—	139	7	17	—
97	41	—	13	19	—	7	163	—	11	—	23	—	7	127	53	13	107	29	83	7	—	—	19	—	—	37	7	—	13	17

	9 91	94	9 97	10 00	03	06	09	12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57	60	63	66	69	72	75	78
01	113	—	7	11	19	29	23	17	—	7	—	13	—	—	11	211	7	79	31	—	227	—	—	7	13	11	53	—	193	23
03	—	107	179	—	7	37	11	—	—	13	—	7	31	17	19	313	—	11	7	—	61	109	13	71	—	7	—	23	11	67
07	23	7	—	97	37	13	—	—	7	—	—	—	11	—	—	7	29	—	13	311	—	—	7	11	—	17	—	47	—	7
09	—	—	—	7	11	—	19	—	83	61	7	—	271	239	17	11	13	7	41	163	89	23	37	227	7	19	11	—	—	13
13	7	89	—	103	—	—	—	7	—	17	11	47	13	31	7	—	—	23	—	281	257	7	61	—	41	13	17	29	7	131
19	—	37	—	—	43	239	7	127	11	29	17	23	59	7	—	—	—	89	19	11	7	271	71	—	—	—	31	7	79	137
21	11	7	—	29	13	—	43	—	7	19	—	11	139	71	277	7	17	13	127	37	31	47	7	97	—	—	—	179	19	7
27	7	19	31	23	41	47	—	7	—	11	73	13	43	269	7	173	103	17	—	—	11	7	—	229	13	—	23	—	7	—
31	—	—	19	67	7	103	—	13	—	79	41	7	17	197	191	11	43	—	7	—	13	19	23	—	—	7	11	157	293	17
33	—	17	—	167	—	13	7	11	—	—	109	—	19	7	—	31	37	—	11	79	7	59	—	—	113	29	61	7	191	11
37	—	13	11	7	269	157	—	67	—	—	7	—	71	11	13	37	23	7	—	41	—	—	43	107	7	—	—	13	53	—
39	—	—	17	71	19	7	193	29	59	—	—	89	7	167	23	61	11	—	107	7	47	97	41	19	43	13	7	11	31	—
43	11	277	7	—	—	19	—	137	13	7	23	11	127	—	17	—	7	—	—	59	—	13	11	7	19	47	229	—	41	—
49	—	7	13	—	23	—	29	103	7	11	—	53	37	—	—	7	19	61	—	—	11	—	7	173	—	—	—	23	13	7
51	13	11	23	7	17	251	157	19	173	179	7	—	11	13	181	—	—	7	—	—	71	17	—	11	7	23	13	—	131	29
57	229	271	7	—	—	17	—	13	41	7	11	29	211	257	—	—	7	137	19	23	13	11	17	7	—	—	—	283	59	—
61	17	79	—	13	—	11	7	109	—	37	—	—	—	7	41	23	11	17	—	19	7	163	—	67	31	—	—	7	29	13
63	53	7	67	47	—	43	17	131	7	—	19	79	—	23	13	7	—	41	31	11	103	263	7	17	—	—	—	13	—	7
67	131	17	—	11	167	7	31	—	47	23	13	19	7	—	11	83	—	127	17	7	—	—	—	13	—	11	7	67	263	—
69	7	—	19	—	29	—	11	7	13	—	71	43	—	—	7	—	—	11	53	—	251	7	—	73	17	—	41	—	7	269
73	—	11	17	19	7	—	37	—	—	—	83	7	11	59	167	43	173	13	7	17	—	29	19	11	—	7	23	—	97	—
79	41	31	113	7	—	83	241	—	157	—	7	13	79	—	19	199	—	7	—	—	17	11	139	37	7	107	—	—	179	233
81	—	53	11	41	37	7	—	—	—	13	—	—	7	11	67	—	—	—	23	7	107	313	13	43	11	—	7	71	—	—
87	11	—	—	13	7	107	—	—	29	139	17	7	23	—	—	—	13	—	7	53	293	37	11	—	191	7	83	17	271	13
91	—	7	73	101	—	17	11	199	7	—	—	113	13	—	—	7	—	11	41	—	37	—	7	277	—	13	97	31	11	7
93	281	37	—	7	—	—	23	—	19	11	7	17	—	—	—	97	—	7	—	29	11	31	67	13	7	—	—	19	17	23
97	7	—	23	199	11	101	13	7	283	19	—	—	—	131	7	11	—	—	—	13	59	7	47	17	—	23	11	41	7	—
99	19	29	7	31	13	—	—	11	—	7	—	—	17	—	—	—	7	13	11	19	—	—	241	7	103	—	67	61	—	11

XII b.

	9 92	95	9 98	10 01	04	07	10	13	16	19	22	25	28	31	34	37	40	43	46	49	52	55	58	61	64	67	70	73	76	79
08	13	19	11	—	—	—	7	17	—	181	—	—	223	7	53	—	—	37	29	23	7	—	31	—	11	—	13	7	—	—
09	11	151	—	—	31	7	—	13	17	101	179	11	7	23	—	137	—	—	73	7	13	—	11	—	97	17	7	—	—	29
11	7	191	151	11	—	13	83	7	—	223	43	23	—	97	7	37	47	—	13	—	—	7	19	29	—	11	113	239	7	31
17	47	11	—	53	—	23	7	71	307	—	—	31	11	7	19	17	41	73	233	—	7	—	—	11	—	13	103	7	23	311
21	313	23	173	7	137	47	—	11	13	—	7	157	229	101	—	19	—	7	11	239	43	13	29	—	7	—	—	17	—	11
23	—	—	—	59	233	7	13	—	151	227	11	—	7	—	—	—	17	—	—	7	139	11	23	—	31	19	7	—	281	—
27	67	—	7	223	29	11	—	19	—	7	151	17	31	281	59	13	7	—	23	317	—	—	97	7	—	—	19	11	13	—
29	13	—	—	—	7	263	31	107	11	—	—	7	—	13	293	47	23	17	7	11	—	—	—	—	71	7	13	29	43	37
33	—	7	—	11	67	—	71	-	7	13	—	—	17	151	11	7	—	101	19	—	47	—	7	211	—	11	—	181	37	7
39	7	11	—	13	47	131	23	7	37	—	19	—	11	17	7	227	13	103	—	101	—	7	109	11	163	—	29	—	7	13
41	—	13	7	239	11	—	79	—	—	7	—	41	—	—	13	11	7	151	269	17	19	—	53	7	—	173	11	13	—	—
47	61	7	11	17	—	—	37	—	7	97	59	—	19	11	31	7	—	—	227	—	17	13	7	179	11	—	167	—	—	7
51	—	—	31	—	13	7	—	13	11	269	—	—	7	19	—	17	67	13	—	7	—	59	151	101	—	—	7	—	83	—
53	7	113	13	—	17	53	139	7	—	43	—	11	163	29	7	13	—	241	229	—	—	7	11	19	—	—	—	31	7	41
57	—	29	61	47	7	19	11	79	59	—	293	7	73	43	—	31	17	11	7	103	67	—	37	83	13	7	—	—	11	89
59	—	—	—	37	—	17	7	—	277	11	—	—	—	7	307	19	—	79	—	—	7	283	13	53	29	—	151	7	199	47
63	17	—	37	7	11	13	—	—	—	—	7	—	29	71	157	11	19	7	13	43	—	—	—	—	7	241	11	101	23	107
69	53	17	7	—	—	—	211	167	19	7	31	109	13	11	107	—	7	—	17	37	—	229	23	7	11	13	—	19	67	101
71	37	—	—	109	7	11	53	17	293	107	13	7	—	—	—	41	11	29	7	—	23	193	—	13	17	7	—	11	—	—
77	—	—	—	7	13	179	61	—	17	—	7	67	—	—	11	157	199	7	—	113	—	71	239	89	7	11	—	—	29	19
81	7	—	—	17	89	31	—	7	—	11	23	19	—	13	7	59	29	—	—	61	11	7	113	—	233	—	13	167	7	—
83	101	11	7	—	—	97	271	—	23	7	29	13	11	—	—	67	7	—	—	277	127	19	—	7	13	—	17	73	257	83
87	43	53	59	19	17	—	7	11	61	—	233	—	137	7	239	—	—	47	11	—	7	17	19	—	—	—	173	7	—	11
89	—	7	23	—	317	13	—	53	7	79	11	173	31	19	37	7	—	139	13	67	211	11	7	—	83	23	—	17	113	7
93	31	13	191	—	—	7	43	41	—	29	—	—	7	37	13	271	11	—	—	7	71	23	17	103	109	269	7	11	—	79
99	109	137	283	11	7	—	17	—	13	—	—	7	43	31	11	23	41	—	7	—	29	13	—	17	281	7	—	211	—	—

В.

Таблицы

2-хъ и 3-хъ степеней цѣлыхъ чиселъ

отъ 1 до 999

и 4-хъ, 5-хъ, 6-хъ, 7-хъ, 8-хъ и 9-хъ степеней первыхъ 99 натуральныхъ чиселъ *).

Способъ употребленія.

На первой страницѣ выписаны вполнѣ квадраты и кубы цѣлыхъ чиселъ отъ 1 до 99 включительно; на прочихъ страницахъ недостаетъ справа двухъ цыфръ. Эти невыставленныя цыфры выписываются сообразно десяткамъ и единицамъ даннаго числа изъ первой страницы. Напримѣръ, противъ числа 629 въ графѣ квадратовъ находимъ число 3956, а на 1-ой страницѣ противъ 29 беремъ въ графѣ квадратовъ послѣднія двѣ цыфры 41, которыя приписываемъ справа къ числу 3956; искомый квадратъ числа 629 будетъ равенъ 385641. То же правило примѣняется и при отыскиваніи кубовъ.

Таблицы 4-хъ, 5-хъ, ... 9-хъ степеней первыхъ 99 натуральныхъ чиселъ вслѣдствіе простоты не нуждаются въ объясненіи.

---

*) Эти таблицы перепечатаны изъ книги Н. И. Липина: „Таблицы, формулы и численныя данныя, для сокращенія вычисленій и руководства при соображеніяхъ, относящихся до строительнаго искусства“. С.-П. 1853. Для контроля предварительно перевычислены студентами Бѣлько, Лернеромъ, Хлѣбниковымъ и Шкодой.

Числа. N	Степени. Квадраты. N^2	Степени. Кубы. N^3	Числа. N	Степени. Квадраты. N^2	Степени. Кубы. N^3
00	00	00	50	25 00	1 250 00
1	01	01	1	26 01	1 326 51
2	04	08	2	27 04	1 406 08
3	09	27	3	28 09	1 488 77
4	16	64	4	29 16	1 574 64
5	25	1 25	5	30 25	1 663 75
6	36	2 16	6	31 36	1 756 16
7	49	3 43	7	32 49	1 851 93
8	64	5 12	8	33 64	1 951 12
9	81	7 29	9	34 81	2 053 79
10	1 00	10 00	60	36 00	2 160 00
1	1 21	13 31	1	37 21	2 269 81
2	1 44	17 28	2	38 44	2 383 28
3	1 69	21 97	3	39 69	2 500 47
4	1 96	27 44	4	40 96	2 621 44
5	2 25	33 75	5	42 25	2 746 25
6	2 56	40 96	6	43 56	2 874 96
7	2 89	49 13	7	44 89	3 007 63
8	3 24	58 32	8	46 24	3 144 32
9	3 61	68 59	9	47 61	3 285 09
20	4 00	80 00	70	49 00	3 430 00
1	4 41	92 61	1	50 41	3 579 11
2	4 84	106 48	2	51 84	3 732 48
3	5 29	121 67	3	53 29	3 890 17
4	5 76	138 24	4	54 76	4 052 24
5	6 25	156 25	5	56 25	4 218 75
6	6 76	175 76	6	57 76	4 389 76
7	7 29	196 83	7	59 29	4 565 33
8	7 84	219 52	8	60 84	4 745 52
9	8 41	243 89	9	62 41	4 930 39
30	9 00	270 00	80	64 00	5 120 00
1	9 61	297 91	1	65 61	5 314 41
2	10 24	327 68	2	67 24	5 513 68
3	10 89	359 37	3	68 89	5 717 87
4	11 56	393 04	4	70 56	5 927 04
5	12 25	428 75	5	72 25	6 141 25
6	12 96	466 56	6	73 96	6 360 56
7	13 69	506 53	7	75 69	6 585 03
8	14 44	548 72	8	77 44	6 814 72
9	15 21	593 19	9	79 21	7 049 69
40	16 00	640 00	90	81 00	7 290 00
1	16 81	689 21	1	82 81	7 535 71
2	17 64	740 88	2	84 64	7 786 88
3	18 49	795 07	3	86 49	8 043 57
4	19 36	851 84	4	88 36	8 305 84
5	20 25	911 25	5	90 25	8 573 75
6	21 16	973 36	6	92 16	8 847 36
7	22 09	1 038 23	7	94 09	9 126 73
8	23 04	1 105 92	8	96 04	9 411 92
9	24 01	1 176 49	9	98 01	9 702 99

Числа. N	Степени. Квадр. N^2	Степени. Кубы. N^3	Числа. N	Степени. Квадр. N^2	Степени. Кубы. N^3	Числа. N	Степени. Квадр. N^2	Степени. Кубы. N^3
100	100	10 000	150	225	33 750	200	400	80 000
1	102	10 303	1	228	34 429	1	404	81 206
2	104	10 612	2	231	35 118	2	408	82 424
3	106	10 927	3	234	35 815	3	412	83 654
4	108	11 248	4	237	36 522	4	416	84 896
5	110	11 576	5	240	37 238	5	420	86 151
6	112	11 910	6	243	37 964	6	424	87 418
7	114	12 250	7	246	38 698	7	428	88 697
8	116	12 597	8	249	39 443	8	432	89 989
9	118	12 950	9	252	40 196	9	436	91 293
10	121	13 310	60	256	40 960	10	441	92 610
1	123	13 676	1	259	41 732	1	445	93 939
2	125	14 049	2	262	42 515	2	449	95 281
3	127	14 428	3	265	43 307	3	453	96 635
4	129	14 815	4	268	44 109	4	457	98 003
5	132	15 208	5	272	44 921	5	462	99 383
6	134	15 608	6	275	45 742	6	466	100 776
7	136	16 016	7	278	46 574	7	470	102 183
8	139	16 430	8	282	47 416	8	475	103 602
9	141	16 851	9	285	48 268	9	479	105 034
20	144	17 280	70	289	49 130	20	484	106 480
1	146	17 715	1	292	50 002	1	488	107 938
2	148	18 158	2	295	50 884	2	492	109 410
3	151	18 608	3	299	51 777	3	497	110 895
4	153	19 066	4	302	52 680	4	501	112 394
5	156	19 531	5	306	53 593	5	506	113 906
6	158	20 003	6	309	54 517	6	510	115 431
7	161	20 483	7	313	55 452	7	515	116 970
8	163	20 971	8	316	56 397	8	519	118 523
9	166	21 466	9	320	57 353	9	524	120 089
30	169	21 970	80	324	58 320	30	529	121 670
1	171	22 480	1	327	59 297	1	533	123 263
2	174	22 999	2	331	60 285	2	538	124 871
3	176	23 526	3	334	61 284	3	542	126 493
4	179	24 061	4	338	62 295	4	547	128 129
5	182	24 603	5	342	63 316	5	552	129 778
6	184	25 154	6	345	64 348	6	556	131 442
7	187	25 713	7	349	65 392	7	561	133 120
8	190	26 280	8	353	66 446	8	566	134 812
9	193	26 856	9	357	67 512	9	571	136 519
40	196	27 440	90	361	68 590	40	576	138 240
1	198	28 032	1	364	69 678	1	580	139 975
2	201	28 632	2	368	70 778	2	585	141 724
3	204	29 242	3	372	71 890	3	590	143 489
4	207	29 859	4	376	73 013	4	595	145 267
5	210	30 486	5	380	74 148	5	600	147 061
6	213	31 121	6	384	75 295	6	605	148 869
7	216	31 765	7	388	76 453	7	610	150 692
8	219	32 417	8	392	77 623	8	615	152 529
9	222	33 079	9	396	78 805	9	620	154 382

Числа.	Степени.		Числа.	Степени.		Числа.	Степени.	
	Квадр.	Кубы.		Квадр.	Кубы.		Квадр.	Кубы.
N	N^3	N^2	N	N^3	N^2	N	N^3	N^2
250	625	156 250	300	900	270 000	350	1225	428 750
1	630	158 132	1	906	272 709	1	1232	432 435
2	635	160 030	2	912	275 436	2	1239	436 142
3	640	161 942	3	918	278 181	3	1246	439 869
4	645	163 870	4	924	280 944	4	1253	443 618
5	650	165 813	5	930	283 726	5	1260	447 388
6	655	167 772	6	936	286 526	6	1267	451 180
7	660	169 745	7	942	289 344	7	1274	454 992
8	665	171 735	8	948	292 181	8	1281	458 827
9	670	173 739	9	954	295 036	9	1288	462 682
60	676	175 760	10	961	297 910	60	1296	466 560
1	681	177 795	1	967	300 802	1	1303	470 458
2	686	179 847	2	973	303 713	2	1310	474 379
3	691	181 914	3	979	306 642	3	1317	478 321
4	696	183 997	4	985	309 591	4	1324	482 285
5	702	186 096	5	992	312 558	5	1332	486 271
6	707	188 210	6	998	315 544	6	1339	490 278
7	712	190 341	7	1004	318 550	7	1346	494 308
8	718	192 488	8	1011	321 574	8	1354	498 360
9	723	194 651	9	1017	324 617	9	1361	502 434
70	729	196 830	20	1024	327 680	70	1369	506 530
1	734	199 025	1	1030	330 761	1	1376	510 648
2	739	201 236	2	1036	333 862	2	1383	514 788
3	745	203 464	3	1043	336 982	3	1391	518 951
4	750	205 708	4	1049	340 122	4	1398	523 136
5	756	207 968	5	1056	343 281	5	1406	527 343
6	761	210 245	6	1062	346 459	6	1413	531 573
7	767	212 539	7	1069	349 657	7	1421	535 826
8	772	214 849	8	1075	352 875	8	1428	540 101
9	778	217 176	9	1082	356 112	9	1436	544 399
80	784	219 520	30	1089	359 370	80	1444	548 720
1	789	221 880	1	1095	362 646	1	1451	553 063
2	795	224 257	2	1102	365 943	2	1459	557 429
3	800	226 651	3	1108	369 260	3	1466	561 818
4	806	229 063	4	1115	372 597	4	1474	566 231
5	812	231 491	5	1122	375 953	5	1482	570 666
6	817	233 936	6	1128	379 330	6	1489	575 124
7	823	236 399	7	1135	382 727	7	1497	579 606
8	829	238 878	8	1142	386 144	8	1505	584 110
9	835	241 375	9	1149	389 582	9	1513	588 638
90	841	243 890	40	1156	393 040	90	1521	593 190
1	846	246 421	1	1162	396 518	1	1528	597 764
2	852	248 970	2	1169	400 016	2	1536	602 362
3	858	251 537	3	1176	403 536	3	1544	606 984
4	864	254 121	4	1183	407 075	4	1552	611 629
5	870	256 723	5	1190	410 636	5	1560	616 298
6	876	259 343	6	1197	414 217	6	1568	620 991
7	882	261 980	7	1204	417 819	7	1576	625 707
8	888	264 635	8	1211	421 441	8	1584	630 447
9	894	267 308	9	1218	425 085	9	1592	635 211

Число.	Степени.		Число.	Степени.		Число.	Степени.	
	Квадр.	Кубы.		Квадр.	Кубы.		Квадр.	Кубы.
N	N^2	N^3	N	N^2	N^3	N	N^2	N^3
400	1600	640 000	450	2025	911 250	500	2500	1 250 000
1	1608	644 812	1	2034	917 338	1	2510	1 257 515
2	1616	649 648	2	2043	923 454	2	2520	1 265 060
3	1624	654 508	3	2052	929 596	3	2530	1 272 635
4	1632	659 392	4	2061	935 766	4	2540	1 280 240
5	1640	664 301	5	2070	941 963	5	2550	1 287 876
6	1648	669 234	6	2079	948 188	6	2560	1 295 542
7	1656	674 191	7	2088	954 439	7	2570	1 303 238
8	1664	679 173	8	2097	960 719	8	2580	1 310 965
9	1672	684 179	9	2106	967 025	9	2590	1 318 722
10	1681	689 210	60	2116	973 360	10	2601	1 326 510
1	1689	694 265	1	2125	979 721	1	2611	1 334 328
2	1697	699 345	2	2134	986 111	2	2621	1 342 177
3	1705	704 449	3	2143	992 528	3	2631	1 350 056
4	1713	709 579	4	2152	998 97 3	4	2641	1 357 967
5	1722	714 733	5	2162	1 005 446	5	2652	1 365 908
6	1730	719 912	6	2171	1 011 946	6	2662	1 373 880
7	1738	725 117	7	2180	1 018 475	7	2672	1 381 884
8	1747	730 346	8	2190	1 025 032	8	2683	1 389 918
9	1755	735 600	9	2199	1 031 617	9	2693	1 397 983
20	1764	740 880	70	2209	1 038 230	20	2704	1 406 080
1	1772	746 184	1	2218	1 044 871	1	2714	1 414 207
2	1780	751 514	2	2227	1 051 540	2	2724	1 422 366
3	1789	756 869	3	2237	1 058 238	3	2735	1 430 556
4	1797	762 250	4	2246	1 064 964	4	2745	1 438 778
5	1806	767 656	5	2256	1 071 718	5	2756	1 447 031
6	1814	773 087	6	2265	1 078 501	6	2766	1 455 315
7	1823	778 544	7	2275	1 085 313	7	2777	1 463 631
8	1831	784 027	8	2284	1 092 153	8	2787	1 471 979
9	1840	789 535	9	2294	1 099 022	9	2798	1 480 358
30	1849	795 070	80	2304	1 105 920	30	2809	1 488 770
1	1857	800 629	1	2313	1 112 846	1	2819	1 497 212
2	1866	806 215	2	2323	1 119 801	2	2830	1 505 687
3	1874	811 827	3	2332	1 126 785	3	2840	1 514 194
4	1883	817 465	4	2342	1 133 799	4	2851	1 522 733
5	1892	823 128	5	2352	1 140 841	5	2862	1 531 303
6	1900	828 818	6	2361	1 147 912	6	2872	1 539 906
7	1909	834 534	7	2371	1 155 013	7	2883	1 548 541
8	1918	840 276	8	2381	1 162 142	8	2894	1 557 208
9	1927	846 045	9	2391	1 169 301	9	2905	1 565 908
40	1936	851 840	90	2401	1 176 490	40	2916	1 574 640
1	1944	857 661	1	2410	1 183 707	1	2926	1 583 404
2	1953	863 508	2	2420	1 190 954	2	2937	1 592 200
3	1962	869 383	3	2430	1 198 231	3	2948	1 601 030
4	1971	875 283	4	2440	1 205 537	4	2959	1 609 891
5	1980	881 211	5	2450	1 212 873	5	2970	1 618 786
6	1989	887 165	6	2460	1 220 239	6	2981	1 627 713
7	1998	893 146	7	2470	1 227 634	7	2992	1 636 673
8	2007	899 153	8	2480	1 235 059	8	3003	1 645 665
9	2016	905 188	9	2490	1 242 514	9	3014	1 654 691

Число. N	Степени. Квадр. N^2	Кубы. N^3	Число. N	Степени. Квадр. N^2	Кубы. N^3	Число. N	Степени. Квадр. N^2	Кубы. N^3
550	3025	1 663 750	600	3600	2 160 000	650	4225	2 746 250
1	3036	1 672 841	1	3612	2 170 818	1	4238	2 758 944
2	3047	1 681 966	2	3624	2 181 672	2	4251	2 771 678
3	8058	1 691 123	3	3636	2 192 562	3	4264	2 784 450
4	3069	1 700 314	4	3648	2 203 488	4	4277	2 797 262
5	3080	1 709 538	5	3660	2 214 451	5	4290	2 810 113
6	3091	1 718 796	6	3672	2 225 450	6	4303	2 823 004
7	3102	1 728 086	7	3684	2 236 485	7	4316	2 835 933
8	3113	1 737 411	8	3696	2 247 557	8	4329	2 848 903
9	3124	1 746 768	9	3708	2 258 665	9	4342	2 861 911
60	3136	1 756 160	10	3721	2 269 810	60	4356	2 874 960
1	3147	1 765 584	1	3733	2 280 991	1	4369	2 888 047
2	3158	1 775 043	2	3745	2 292 209	2	4382	2 901 175
3	3169	1 784 535	3	3757	2 303 463	3	4395	2 914 342
4	3180	1 794 061	4	3769	2 314 755	4	4408	2 927 549
5	3192	1 803 621	5	3782	2 326 083	5	4422	2 940 796
6	3203	1 813 214	6	3794	2 337 448	6	4435	2 954 082
7	3214	1 822 842	7	3806	2 348 851	7	4448	2 967 409
8	3226	1 832 504	8	3819	2 360 290	8	4462	2 980 776
9	3237	1 842 200	9	3831	2 371 766	9	4475	2 994 183
70	3249	1 851 930	20	3844	2 383 280	70	4489	3 007 630
1	3260	1 861 694	1	3856	2 394 830	1	4502	3 021 117
2	3271	1 871 492	2	3868	2 406 418	2	4515	3 034 644
3	3283	1 881 325	3	3881	2 418 043	3	4529	3 048 212
4	3294	1 891 192	4	3893	2 429 706	4	4542	3 061 820
5	3306	1 901 093	5	3906	2 441 406	5	4556	3 075 468
6	3317	1 911 029	6	3918	2 453 143	6	4569	3 089 157
7	3329	1 921 000	7	3931	2 464 918	7	4583	3 102 887
8	3340	1 931 005	8	3943	2 476 731	8	4596	3 116 657
9	3352	1 941 045	9	3956	2 488 581	9	4610	3 130 468
80	3364	1 951 120	30	3969	2 500 470	80	4624	3 144 320
1	3375	1 961 229	1	3981	2 512 395	1	4637	3 158 212
2	3387	1 971 373	2	3994	2 524 359	2	4651	3 172 145
3	3398	1 981 552	3	4006	2 536 361	3	4664	3 186 119
4	3410	1 991 767	4	4019	2 548 401	4	4678	3 200 135
5	3422	2 002 016	5	4032	2 560 478	5	4692	3 214 191
6	3433	2 012 300	6	4044	2 572 594	6	4705	3 228 288
7	3445	2 022 620	7	4057	2 584 748	7	4719	3 242 427
8	3457	2 032 974	8	4070	2 596 940	8	4733	3 256 606
9	3469	2 043 364	9	4083	2 609 171	9	4747	3 270 827
90	3481	2 053 790	40	4096	2 621 440	90	4761	3 285 090
1	3492	2 064 250	1	4108	2 633 747	1	4474	3 299 393
2	3504	2 074 746	2	4121	2 646 092	2	4788	3 313 738
3	3516	2 085 278	3	4134	2 658 477	3	4802	3 328 125
4	3528	2 095 845	4	4147	2 670 899	4	4816	3 342 553
5	3540	2 106 448	5	4160	2 683 361	5	4830	3 357 023
6	3552	2 117 087	6	4173	2 695 861	6	4844	3 371 535
7	3564	2 127 761	7	4186	2 708 400	7	4858	3 386 088
8	3576	2 138 471	8	4199	2 720 977	8	4872	3 400 683
9	3588	2 149 217	9	4212	2 733 594	9	4886	3 415 320

Число.	Степени.		Число.	Степени.		Число.	Степени.	
	Квадр.	Кубы.		Квадр.	Кубы.		Квадр.	Кубы.
N	N^2	N^3	N	N^2	N^3	N	N^2	N^3
700	4900	3 430 000	750	5625	4 218 750	800	6400	5 120 000
1	4914	3 444 721	1	5640	4 235 647	1	6416	5 139 224
2	4928	3 459 484	2	5655	4 252 590	2	6432	5 158 496
3	4942	3 474 289	3	5670	4 269 577	3	6448	5 177 816
4	4956	3 489 136	4	5685	4 286 610	4	6464	5 197 184
5	4970	3 504 026	5	5700	4 303 688	5	6480	5 216 601
6	4984	3 518 958	6	5715	4 320 812	6	6496	5 236 066
7	4998	3 533 932	7	5730	4 337 980	7	6512	5 255 579
8	5012	3 548 949	8	5745	4 355 195	8	6528	5 275 141
9	5026	3 564 008	9	5760	4 372 454	9	6544	5 294 751
10	5041	3 579 110	60	5776	4 389 760	10	6561	5 314 410
1	5055	3 594 254	1	5791	4 407 110	1	6577	5 334 117
2	5069	3 609 441	2	5806	4 424 507	2	6593	5 353 873
3	5083	3 624 670	3	5821	4 441 949	3	6609	5 373 677
4	5097	3 639 943	4	5836	4 459 437	4	6625	5 393 531
5	5112	3 655 258	5	5852	4 476 971	5	6642	5 413 433
6	5126	3 670 616	6	5867	4 494 550	6	6658	5 433 384
7	5140	3 686 018	7	5882	4 512 176	7	6674	5 453 385
8	5155	3 701 462	8	5898	4 529 848	8	6691	5 473 434
9	5169	3 716 949	9	5913	4 547 566	9	6707	5 493 532
20	5184	3 732 480	70	5929	4 565 330	20	6724	5 513 680
1	5198	3 748 053	1	5944	4 583 140	1	6740	5 533 876
2	5212	3 763 670	2	5959	4 600 996	2	6756	5 554 122
3	5227	3 779 330	3	5975	4 618 899	3	6773	5 574 417
4	5241	3 795 034	4	5990	4 636 848	4	6789	5 594 762
5	5256	3 810 781	5	6006	4 654 843	5	6806	5 615 156
6	5270	3 826 571	6	6021	4 672 885	6	6822	5 635 599
7	5285	3 842 405	7	6037	4 690 974	7	6839	5 656 092
8	5299	3 858 283	8	6052	4 709 109	8	6855	5 676 635
9	5314	3 874 204	9	6068	4 727 291	9	6872	5 697 227
30	5329	3 890 170	80	6084	4 745 520	30	6889	5 717 870
1	5343	3 906 178	1	6099	4 763 795	1	6905	5 738 561
2	5358	3 922 231	2	6115	4 782 117	2	6922	5 759 303
3	5372	3 938 328	3	6130	4 800 486	3	6938	5 780 095
4	5387	3 954 469	4	6146	4 818 903	4	6955	5 800 937
5	5402	3 970 653	5	6162	4 837 366	5	6972	5 821 828
6	5416	3 986 882	6	6177	4 855 876	6	6988	5 842 770
7	5431	4 003 155	7	6193	4 874 434	7	7005	5 863 762
8	5446	4 019 472	8	6209	4 893 038	8	7022	5 884 804
9	5461	4 035 834	9	6225	4 911 690	9	7039	5 905 897
40	5476	4 052 240	90	6241	4 930 390	40	7056	5 927 040
1	5490	4 068 690	1	6256	4 949 136	1	7072	5 948 233
2	5505	4 085 184	2	6272	4 967 930	2	7089	5 969 476
3	5520	4 101 724	3	6288	4 986 772	3	7106	5 990 771
4	5535	4 118 307	4	6304	5 005 661	4	7123	6 012 115
5	5550	4 134 936	5	6320	5 024 598	5	7140	6 033 511
6	5565	4 151 609	6	6336	5 043 583	6	7157	6 054 957
7	5580	4 168 327	7	6352	5 062 615	7	7174	6 076 454
8	5595	4 185 089	8	6368	5 081 695	8	7191	6 098 001
9	5610	4 201 897	9	6384	5 100 823	9	7208	6 119 600

Число. N	Степени. Квадр. N^2	Степени. Кубы. N^3	Число. N	Степени. Квадр. N^2	Степени. Кубы. N^3	Число. N	Степени. Квадр. N^2	Степени. Кубы. N^3
850	7225	6 141 250	900	8100	7 290 000	950	9025	8 573 750
1	7242	6 162 950	1	8118	7 314 327	1	9044	8 600 853
2	7259	6 184 702	2	8136	7 338 708	2	9063	8 628 014
3	7276	6 206 504	3	8154	7 363 143	3	9082	8 655 231
4	7293	6 228 358	4	8172	7 387 632	4	9101	8 682 506
5	7310	6 250 263	5	8190	7 412 176	5	9120	8 709 838
6	7327	6 272 220	6	8208	7 436 774	6	9139	8 737 228
7	7344	6 294 227	7	8226	7 461 426	7	9158	8 764 674
8	7361	6 316 287	8	8244	7 486 133	8	9177	8 792 179
9	7378	6 338 397	9	8262	7 510 894	9	9196	8 819 740
60	7396	6 360 560	10	8281	7 535 710	60	9216	8 847 360
1	7413	6 382 773	1	8299	7 560 580	1	9235	8 875 036
2	7430	6 405 039	2	8317	7 585 505	2	9254	8 902 771
3	7447	6 427 356	3	8335	7 610 484	3	9273	8 930 563
4	7464	6 449 725	4	8353	7 635 519	4	9292	8 958 413
5	7482	6 472 146	5	8372	7 660 608	5	9312	8 986 321
6	7499	6 494 618	6	8390	7 685 752	6	9331	9 014 286
7	7516	6 517 143	7	8408	7 710 952	7	9350	9 042 310
8	7534	6 539 720	8	8427	7 736 206	8	9370	9 070 392
9	7551	6 562 349	9	8445	7 761 515	9	9389	9 098 532
70	7569	6 585 030	20	8464	7 786 880	70	9409	9 126 730
1	7586	6 607 763	1	8482	7 812 299	1	9428	9 154 986
2	7603	6 630 548	2	8500	7 837 774	2	9447	9 183 300
3	7621	6 653 386	3	8519	7 863 304	3	9467	9 211 673
4	7638	6 676 276	4	8537	7 888 890	4	9486	9 240 104
5	7656	6 699 218	5	8556	7 914 531	5	9506	9 268 593
6	7673	6 722 213	6	8574	7 940 227	6	9525	9 297 141
7	7691	6 745 261	7	8593	7 965 979	7	9545	9 325 748
8	7708	6 768 361	8	8611	7 991 787	8	9564	9 354 413
9	7726	6 791 514	9	8630	8 017 650	9	9584	9 383 137
80	7744	6 814 720	30	8649	8 043 570	80	9604	9 411 920
1	7761	6 837 978	1	8667	8 069 544	1	9623	9 440 761
2	7779	6 861 289	2	8686	8 095 575	2	9643	9 469 661
3	7796	6 884 653	3	8704	8 121 662	3	9662	9 498 620
4	7814	6 908 071	4	8723	8 147 805	4	9682	9 527 639
5	7832	6 931 541	5	8742	8 174 003	5	9702	9 556 716
6	7849	6 955 064	6	8760	8 200 258	6	9721	9 585 852
7	7867	6 978 641	7	8779	8 226 569	7	9741	9 615 048
8	7885	7 002 270	8	8798	8 252 936	8	9761	9 644 302
9	7903	7 025 953	9	8817	8 279 360	9	9781	9 673 616
90	7921	7 049 690	40	8836	8 305 840	90	9801	9 702 990
1	7938	7 073 479	1	8854	8 332 376	1	9820	9 732 422
2	7956	7 097 322	2	8873	8 358 968	2	9840	9 761 914
3	7974	7 121 219	3	8892	8 385 618	3	9860	9 791 466
4	7992	7 145 169	4	8911	8 412 323	4	9880	9 821 077
5	8010	7 169 173	5	8930	8 439 086	5	9900	9 850 748
6	8028	7 193 231	6	8949	8 465 905	6	9920	9 880 479
7	8046	7 217 342	7	8968	8 492 781	7	9940	9 910 269
8	8064	7 241 507	8	8987	8 519 713	8	9960	9 940 119
9	8082	7 265 726	9	9006	8 546 703	9	9980	9 970 029

N.	N^4	N^5	N^6	N^7	N^8	N^9
1	1	1	1	1	1	1
2	16	32	64	128	256	512
3	81	243	729	2187	6561	19683
4	256	1024	4096	16384	65536	262144
5	625	3125	15625	78125	390625	1953125
6	1296	7776	46656	279936	1679616	10077696
7	2401	16807	117649	823543	5764801	40353607
8	4096	32768	262144	2097152	16777216	134217728
9	6561	59049	531441	4782969	43046721	387420489
10	10000	100000	1000000	10000000	100000000	1000000000
11	14641	161051	1771561	19487171	214358881	2357947691
12	20736	248832	2985984	35831808	429981696	5159780352
13	28561	371293	4826809	62748517	815730721	10604499373
14	38416	537824	7529536	105413504	1475789056	20661046784
15	50625	759375	11390625	170859375	2562890625	38443359375
16	65536	1048576	16777216	268435456	4294967296	68719476736
17	83521	1419857	24137569	410338673	6975757441	118587876497
18	104976	1889568	34012224	612220032	11019960576	198359290368
19	130321	2476099	47045881	893871739	16983563041	322687697779
20	160000	3200000	64000000	1280000000	25600000000	512000000000
21	194481	4084101	85766121	1801088541	37822859361	794280046581
22	234256	5153632	113379904	2494357888	54875873536	1207269217792
23	279841	6436343	148035889	3404825447	78310985281	1801152661463
24	331776	7962624	191102976	4586471424	110075314176	2641807540224
25	390625	9765625	244140625	6103515625	152587890625	3814697265625
26	456976	11881376	308915776	8031810176	208827064576	5429503678976
27	531441	14348907	387420489	10460353203	282429536481	7625597484987
28	614656	17210368	481890304	13492928512	377801998336	10578455953408
29	707281	20511149	594823321	17249876309	500246412961	14507145975869
30	810000	24300000	729000000	21870000000	656100000000	19683000000000
31	923521	28629151	887503681	27512614111	852891037441	26439622160671
32	1048576	33554432	1073741824	34359738368	1099511627776	35184372088832
33	1185921	39135393	1291467969	42618442977	1406408618241	46411484401953
34	1336336	45435424	1544804416	52523350144	1785793904896	60716992766464
35	1500625	52521875	1838265625	64339296875	2251875390625	78815638671875
36	1679616	60466176	2176782336	78364164096	2821109907456	101559956668416
37	1874161	69343957	2565726409	94931877133	3512479453921	129961739795077
38	2085136	79235168	3010936384	114415582592	4347792138496	165216101262848
39	2313441	90224199	3518743761	137231006679	5352009260481	208728361158759
40	2560000	102400000	4096000000	163840000000	6553600000000	262144000000000
41	2825761	115856201	4750104241	194754273881	7984925229121	327381934393961
42	3111696	130691232	5489031744	230539333248	9682651996416	406671383849472
43	3418801	147008443	6321363049	271818611107	11688200277601	502592611936843
44	3748096	164916224	7256313856	319277809664	14048223625216	618121839509504
45	4100625	184528125	8303765625	373669453125	16815125390625	756680642578125
46	4477456	205962976	9474296896	435817657216	20047612231936	922190162669056
47	4879681	229345007	10779215329	506623120463	23811286661761	1119130473102767
48	5308416	254803968	12230590464	587068342272	28179280429056	1352605460594688
49	5764801	282475249	13841287201	678223072849	33232930569601	1628413597910449

N.	N^4	N^5	N^6	N^7	N^8	N^9
50	6250000	312500000	15625000000	781250000000	39062500000000	1953125000000000
51	6765201	345025251	17596287801	897410677851	45767944570401	2334165173090451
52	7311616	380204032	19770609664	1028071702528	53459728531456	2779905883635712
53	7890481	418195493	22164361129	1174711139837	62259690411361	3299763591802133
54	8503056	459165024	24794911296	1338925209984	72301961339136	3904305912313344
55	9150625	503284375	27680640625	1522435234375	83733937890625	4605366583984375
56	9834496	550731776	30840979456	1727094849536	96717311574016	5416169448144896
57	10556001	601692057	34296447249	1954897493193	111429157112001	6351461955384057
58	11316496	656356768	38068692544	2207984167552	128063081718016	7427658739644928
59	12117361	714924299	42180533641	2488651484819	146830437604321	8662995818654939
60	12960000	777600000	46656000000	2799360000000	167961600000000	10077696000000000
61	13845841	844596301	51520374361	3142742836021	191707312997281	11694146092834141
62	14776336	916132832	56800235584	3521614606208	218340105584896	13537086546263552
63	15752961	992436543	62523502209	3938980639167	248155780267521	15633814156853823
64	16777216	1073741824	68719476736	4398046511104	281474976710656	18014398509481984
65	17850625	1160290625	75418890625	4902227890625	318644812890625	20711912837890625
66	18974736	1252332576	82653950016	5455160701056	360040606269696	23762680013799936
67	20151121	1350125107	90458382169	6060711605323	406067677556641	27206534396294947
68	21381376	1453933568	98867482624	6722988818432	457163239653376	31087100296429568
69	22667121	1564031349	107918163081	7446353252589	513798374428641	35452087835576229
70	24010000	1680700000	117649000000	8235430000000	576480100000000	40353607000000000
71	25411681	1804229351	128100283921	9095120158391	645753531245761	45848500718449031
72	26873856	1934917632	139314069504	10030613004288	722204136308736	51998697814228992
73	28398241	2073071593	151334226289	11047398519097	806460091894081	58871586708267913
74	29986576	2219006624	164206490176	12151280273024	899194740203776	66540410775079424
75	31640625	2373046875	177978515625	13348388671875	1001129150390625	75084686279296875
76	33362176	2535525376	192699928576	14645194571776	1113034787454976	84590643846578176
77	35153041	2706784157	208422380089	16048523266853	1235736291547681	95151694449171437
78	37015056	2887174368	225199600704	17565568854912	1370114370683136	106868920913284608
79	38950081	3077056399	243087455521	19203908986159	1517108809906561	119851595982618319
80	40960000	3276800000	262144000000	20971520000000	1677721600000000	134217728000000000
81	43046721	3486784401	282429536481	22876792454961	1853020188851841	150094635296999121
82	45212176	3707398432	304006671424	24928547056768	2044140858654976	167619550409708032
83	47458321	3939040643	326940373369	27136050989627	2252292232139041	186940255267540403
84	49787136	4182119424	351298031616	29509034655744	2478758911082496	208215748530929664
85	52200625	4437053125	377149515625	32057708828125	2724905250390625	231616946283203125
86	54700816	4704270176	404567235136	34792782221696	2992179271065856	257327417311663616
87	57289761	4984209207	433626201009	37725479487783	3282116715437121	285544154243029527
88	59969536	5277319168	464404086784	40867559636992	3596345248055296	316478381828866048
89	62742241	5584059449	496981290961	44231334895529	3936588805702081	350356403707485209
90	65610000	5904900000	531441000000	47829690000000	4304672100000000	387420489000000000
91	68574961	6240321451	567869252041	51676101935731	4702525276151521	427929800129788411
92	71639296	6590815232	606355001344	55784660123648	5132188731375616	472161363286556672
93	74805201	6956883693	646990183449	60170087060757	5595818096650401	520411082988487293
94	78074896	7339040224	689869781056	64847759419264	6095689385410816	572994802228616704
95	81450625	7737809375	735091890625	69833729609375	6634204312890625	630249409724609375
96	84934656	8153726976	782757789696	75144747810816	7213895789838336	692533995824480256
97	88529281	8587340257	832972004929	80798284478113	7837433594376961	760231058654565217
98	92236816	9039207968	885842380864	86812553324672	8507630225817856	833747762130149888
99	96059601	9509900499	941480149401	93206534790699	9227446944279201	913517247483640899

C.

Таблицы

первообразныхъ корней для всѣхъ простыхъ чиселъ до 200 и таблицы, въ которыхъ по данному числу находится индексъ и по данному индексу находится число.

Примѣч. Индексы пріискиваются въ таблицахъ означенныхъ буквой I. а числа, въ другихъ таблицахъ, которыя означены буквой N.

Простое число 5.

Первообразные корни: 2, 3.

Основаніе 2.

I.

Num.	1	2	3	4
Ind.	4	1	3	2

N.

Ind.	1	2	3	4
Num.	2	4	3	1

Простое число 7.

Первообразные корни: 3, 5.

Основаніе 3.

I.

Num.	1	2	3	4	5	6
Ind	6	2	1	4	5	3

N.

Ind.	1	2	3	4	5	6
Num.	3	2	6	4	5	1

Простое число 11.

Первообразные корни: 2, 6, 7, 8.

Основаніе 2.

I.

Num.	1	2	3	4	5	6	7	8	9	10
Ind.	10	1	8	2	4	9	7	3	6	5

N.

Ind.	1	2	3	4	5	6	7	8	9	10
Num.	2	4	8	5	10	9	7	3	6	1

Простое число 13.

Первообразные корни: 2. 6. 7. 11.

Основаніе 6.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		12	5	8	10	9	1	7	3	4
1	2	11	6							

N.

I.	0	1	2	3	4	5	6	7	8	9
0		6	10	8	9	2	12	7	3	5
1	4	11	1							

Простое число 17.

Первообразные корни: 3, 5, 6, 7, 10, 11, 12, 14.

Основаніе 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		16	10	11	4	7	5	9	14	6
1	1	13	15	12	3	2	8			

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	15	14	4	6	9	5	16	7
1	2	3	13	11	8	12	1			

Простое число 19.

Первообразные корни: 2. 3. 10. 13. 14. 15.

Основаніе 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		18	17	5	16	2	4	12	15	10
1	1	6	3	13	11	7	14	8	9	

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	5	12	6	3	11	15	17	18
1	9	14	7	13	16	8	4	2	1	

Простое число 23.

Первообразные корни: 5, 7, 10, 11, 14, 15, 17, 19, 20, 21.

Основаніе 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		22	8	20	16	15	6	21	2	18
1	1	3	14	12	7	13	10	17	4	5
2	9	19	11							

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	8	11	18	19	6	14	2	20
1	16	22	13	15	12	5	4	17	9	21
2	3	7	1							

Простое число 29.

Первообразные корни: 2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27.

Основаніе 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		28	11	27	22	18	10	20	5	26
1	1	23	21	2	3	17	16	7	9	15
2	12	19	6	24	4	8	13	25	14	

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	13	14	24	8	22	17	25	18
1	6	2	20	26	28	19	16	15	5	21
2	7	12	4	11	23	27	9	3	1	

Простое число 31.

Первообразные корни: 3, 11, 12, 13, 17, 21, 22, 24.

Основаніе 17.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		30	12	13	24	20	25	4	6	26
1	2	29	7	23	16	3	18	1	8	22
2	14	17	11	21	19	10	5	9	28	27
3	15									

N.

I.	0	1	2	3	4	5	6	7	8	9
0		17	10	15	7	26	8	12	18	27
1	25	22	2	3	20	30	14	21	16	24
2	5	23	19	13	4	6	9	29	28	11
3	1									

Простое число 37.

Первообразные корни: 2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35.

Основаніе 5.

I.

N.	0	1	2	3	4	5	6	9	8	9
0		36	11	34	22	1	9	28	33	32
1	12	6	20	13	3	35	8	5	7	25
2	23	26	17	21	31	2	24	30	14	15
3	10	27	19	4	16	29	18			

N.

I.	0	1	2	3	4	5	6	7	8	9
0		5	25	14	33	17	11	18	16	6
1	30	2	10	13	28	29	34	22	36	32
2	12	23	4	20	26	19	21	31	7	35
3	27	24	9	8	3	15	1			

Простое число 41.

Первообразные корни: 6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35.

Основаніе 6.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		40	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

N.

I.	0	1	2	3	4	5	6	7	8	9
0		6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	1	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7
4	1									

Простое число 43.

Первообратные корни: 3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34.

Основаніе 28.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		42	39	17	36	5	14	7	33	34
1	2	6	11	40	4	22	30	16	31	29
2	41	24	3	20	8	10	37	9	1	25
3	19	32	27	23	13	12	28	35	26	15
4	38	18	21							

N.

I.	0	1	2	3	4	5	6	7	8	9
0		28	10	22	14	5	11	7	24	27
1	25	12	35	34	6	39	17	3	41	30
2	23	42	15	33	21	29	38	32	36	19
3	16	18	31	8	9	37	4	26	40	2
4	13	20	1							

Простое число 47.

Первообразные корни: 5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45.

Основаніе 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		46	30	18	14	17	2	38	44	36
1	1	27	32	3	22	35	28	42	20	29
2	31	10	11	39	16	34	33	8	6	43
3	19	5	12	45	26	9	4	24	13	21
4	15	25	40	37	41	7	23			

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	6	13	36	31	28	45	27	35
1	21	22	32	38	4	40	24	5	3	30
2	18	39	14	46	37	41	34	11	16	19
3	2	20	12	26	25	15	9	43	7	23
4	42	44	17	29	8	33	1			

Простое число 53.

Первообразные корни: 2, 3, 5, 8, 12, 14, 18, 19, 20, 21, 22, 26, 27, 31, 32, 33, 34, 35, 39, 41, 45, 48, 50, 51.

Основаніе 26.

I.

N.	0	1	2	3	4	5	6	7	8	9
0	.	52	25	9	50	31	34	38	23	18
1	4	46	7	28	11	40	48	42	43	41
2	29	47	19	39	32	10	1	27	36	6
3	13	45	21	3	15	17	16	22	14	37
4	2	33	20	30	44	49	12	8	5	24
5	35	51	26							

N.

N.	0	1	2	3	4	5	6	7	8	9
0		26	40	33	10	48	29	12	47	3
1	25	14	46	30	38	34	36	35	9	22
2	42	32	37	8	49	2	52	27	13	20
3	43	5	24	41	6	50	28	39	7	23
4	15	19	17	18	44	31	11	21	16	45
5	4	51	1							

Простое число 59.

Первообразные корни: 2, 6, 8, 10, 11, 13, 14, 18, 23, 24, 30, 31, 32, 33, 34, 37, 38, 39, 40, 42, 43, 44, 47, 50, 52, 54, 55, 56.

Основаніе 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		58	25	32	50	34	57	44	17	6
1	1	45	24	23	11	8	42	14	31	22
2	26	18	12	27	49	10	48	38	36	4
3	33	7	9	19	39	20	56	41	47	55
4	51	2	43	13	37	40	52	53	16	30
5	35	46	15	28	5	21	3	54	29	

N.

N.	0	1	2	3	4	5	6	7	8	9
0		10	41	56	29	54	9	21	15	32
1	25	14	22	43	17	52	48	8	21	33
2	35	55	19	13	12	2	20	23	53	58
3	49	18	3	30	5	50	28	44	27	34
4	45	37	16	42	7	11	51	38	26	24
5	4	40	46	47	57	39	36	6	1	

Простое число 61.

Первообразные корни: 2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55, 59.

Основаніе 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		60	47	42	34	14	29	23	21	24
1	1	45	16	20	10	56	8	49	11	22
2	48	5	32	39	3	28	7	6	57	25
3	43	13	55	27	36	37	58	33	9	2
4	35	18	52	41	19	38	26	40	50	46
5	15	31	54	51	53	59	44	4	12	17
6	30									

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	39	24	57	21	27	26	16	38
1	14	18	58	31	5	50	12	59	41	44
2	13	8	19	7	9	29	46	33	25	6
3	60	51	22	37	4	40	34	35	45	23
4	47	43	3	30	56	11	49	2	20	17
5	48	53	42	54	52	32	15	28	36	55
6	1									

Простое число 67.

Первообразные корни: 2, 7, 11, 12, 13, 18, 20, 28, 31, 32, 34, 41, 44, 46, 48, 50, 51, 57, 61, 63.

Основаніе 12.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		66	29	9	58	39	38	7	21	18
1	2	61	1	23	36	48	50	8	47	26
2	31	16	24	20	30	12	52	27	65	22
3	11	43	13	4	37	46	10	44	55	32
4	60	19	45	63	53	57	49	64	59	14
5	41	17	15	3	56	34	28	35	51	54
6	40	5	6	25	42	62	33			

N.

I.	0	1	2	3	4	5	6	7	8	9
0		12	10	53	33	61	62	7	17	3
1	36	30	25	32	49	52	21	51	9	41
2	23	8	29	13	22	63	19	27	56	2
3	24	20	39	66	55	57	14	34	6	5
4	60	50	64	31	37	42	35	18	15	46
5	16	58	26	44	59	38	54	45	4	48
6	40	11	65	43	47	28	1			

Простое число 71.

Первообразные корни: 7, 11, 13, 21, 22, 28, 31, 33, 35, 42, 44, 47, 52, 53, 55, 56, 59, 61, 62, 63, 65, 67, 68, 69.

Основаніе 62.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		70	58	18	46	14	6	33	34	36
1	2	43	64	27	21	32	22	7	24	38
2	60	51	31	5	52	28	15	54	9	4
3	20	13	10	61	65	47	12	30	26	45
4	48	55	39	44	19	50	63	17	40	66
5	16	25	3	59	42	57	67	56	62	29
6	8	37	1	69	68	41	49	11	53	23
7	35									

N.

I.	0	1	2	3	4	5	6	7	8	9
0		62	10	52	29	23	6	17	60	28
1	32	67	36	31	5	26	50	47	3	44
2	30	14	16	69	18	51	38	13	25	59
3	37	22	15	7	8	70	9	61	19	42
4	48	65	54	11	43	39	4	35	40	66
5	45	21	24	68	27	41	57	55	2	53
6	20	33	58	46	12	34	49	56	64	63
7	1									

Простое число 73.

Первообразные корни: 5, 11, 13, 14, 15, 20, 26, 28, 29, 31, 33, 34, 39, 40, 42, 44, 45, 47, 53, 58, 59, 60, 62, 68.

Основаніе 5.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		72	8	6	16	1	14	33	24	12
1	9	55	22	59	41	7	32	21	20	62
2	17	39	63	46	30	2	67	18	49	35
3	15	11	40	61	29	34	28	64	70	65
4	25	4	47	51	71	13	54	31	38	66
5	10	27	3	53	26	56	57	68	43	5
6	23	58	19	45	48	60	69	50	37	52
7	42	44	36							

N.

I.	0	1	2	3	4	5	6	7	8	9
0		5	25	52	41	59	3	15	2	10
1	50	31	9	45	6	30	4	20	27	62
2	18	17	12	60	8	40	54	51	36	34
3	24	47	16	7	35	29	72	68	48	21
4	32	14	70	58	71	63	23	42	64	28
5	67	43	69	53	46	11	55	56	61	13
6	65	33	19	22	37	39	49	26	57	66
7	38	44	1							

Простое число 79.

Первообразные корни: 3, 6, 7, 28, 29, 30, 34, 35, 37, 39, 43, 47, 48, 53, 54, 59, 60, 63, 66, 68, 70, 74, 75, 77.

Основаніе 29.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		78	50	71	22	34	43	19	72	64
1	6	70	15	74	69	27	44	9	36	10
2	56	12	42	52	65	68	46	57	41	1
3	77	76	16	63	59	53	8	23	60	67
4	28	21	62	47	14	20	24	55	37	38
5	40	2	18	7	29	26	13	3	51	17
6	49	75	48	5	66	30	35	54	31	45
7	25	33	58	4	73	61	32	11	39	

N.

I.	0	1	2	3	4	5	6	7	8	9
0		29	51	57	73	63	10	53	36	17
1	19	77	21	56	44	12	32	59	52	7
2	45	41	4	37	46	70	55	15	40	54
3	65	68	76	71	5	66	18	48	49	78
4	50	28	22	6	16	69	26	43	62	60
5	2	58	23	35	67	47	20	27	72	34
6	38	75	42	33	9	24	64	39	25	14
7	11	3	8	74	13	61	31	30	1	

Простое число 83.

Первообразные корни: 2, 5, 6, 8, 13, 14, 15, 18, 19, 20, 22, 24, 32, 34, 35, 39, 42, 43, 45, 46, 47, 50, 52, 53, 54, 55, 56, 57, 58, 60, 62, 66, 67, 71, 72, 73, 74, 76, 79, 80.

Основаніе 50.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		82	3	52	6	81	55	24	9	22
1	2	72	58	67	27	51	12	4	25	59
2	5	76	75	16	61	80	70	74	39	36
3	54	32	15	42	7	23	28	60	62	37
4	8	38	79	49	78	21	19	69	64	48
5	1	56	73	13	77	71	33	29	39	20
6	57	34	35	46	18	66	45	53	10	68
7	26	17	31	43	63	50	65	14	40	47
8	11	44	41							

N.

I.	0	1	2	3	4	5	6	7	8	9
0		50	10	2	17	20	4	34	40	8
1	68	80	16	53	77	32	23	71	64	46
2	59	45	9	35	7	18	79	14	36	57
3	28	72	31	56	61	62	29	39	41	58
4	78	82	33	73	81	66	63	79	49	43
5	75	15	3	67	30	6	51	60	12	19
6	37	24	38	74	48	76	65	13	69	47
7	26	55	11	52	27	22	21	54	44	42
8	25	5	1							

Простое число 89.

Первообразные корни: 3, 6, 7, 13, 14, 15, 19, 23, 24, 26, 27, 28, 29, 30, 31, 33, 35, 38, 41, 43, 46, 48, 51, 54, 56, 58, 59, 60, 61, 62, 63, 65, 66, 70, 74, 75, 76, 82, 83, 86.

Основаніе 30.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		88	72	87	56	18	71	7	40	86
1	2	4	55	65	79	17	24	82	70	53
2	74	6	76	31	39	36	49	85	63	29
3	1	57	8	3	66	25	54	77	37	64
4	58	67	78	59	60	16	15	34	23	14
5	20	81	33	10	69	22	47	52	13	45
6	73	19	41	5	80	83	75	32	50	30
7	9	26	38	68	61	35	21	11	48	46
8	42	84	51	27	62	12	43	28	44	

N.

I.	0	1	2	3	4	5	6	7	8	9
0		30	10	33	11	63	21	7	32	70
1	53	77	85	58	49	46	45	15	5	61
2	50	76	55	48	16	35	71	83	87	29
3	69	23	67	52	47	75	25	38	72	24
4	8	62	80	86	88	59	79	56	78	26
5	68	82	57	19	36	12	4	31	40	43
6	44	74	84	28	39	13	34	41	73	54
7	18	6	2	60	20	66	22	37	42	14
8	64	51	17	65	81	27	9	3	1	

Простое число 97.

Первообразные корни: 5, 7, 10, 13, 14, 15, 17, 21, 23, 26, 29, 37, 38, 39, 40, 41, 56, 57, 58, 59, 60, 68, 71, 74, 76, 80, 82, 83, 84, 87, 90, 92.

Основаніе 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		96	86	2	76	11	88	53	66	4
1	1	82	78	83	43	13	56	19	90	27
2	87	55	72	79	68	22	73	6	33	47
3	3	26	46	84	9	64	80	41	17	85
4	77	71	45	44	62	15	69	60	58	10
5	12	21	63	14	92	93	23	29	37	65
6	89	32	16	57	36	94	74	51	95	81
7	54	25	70	20	31	24	7	39	75	42
8	67	8	61	91	35	30	34	49	52	18
9	5	40	59	28	50	38	48			

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	3	30	9	90	27	76	81	34
1	49	5	50	15	53	45	62	38	89	17
2	73	51	25	56	75	71	31	19	93	57
3	85	74	61	28	86	84	64	58	95	77
4	91	37	79	14	43	42	32	29	96	87
5	94	67	88	7	70	21	16	63	48	92
6	47	82	44	52	35	59	8	80	24	46
7	72	41	22	26	66	78	4	40	12	23
8	36	69	11	13	33	39	2	20	6	60
9	18	83	54	55	65	68	1			

Простое число 101.

Первообразные корни: 2, 3, 7, 8, 11, 12, 15, 18, 26, 27, 28, 29, 34, 35, 38, 40, 42, 46, 48, 50, 51, 53, 55, 59, 61, 63, 66, 67, 72, 73, 74, 75, 83, 86, 89, 90, 93, 94, 98, 99.

Основаніе 2.

I. N.

N.	0	1	2	3	4	5	6	7	8	9
0		100	1	69	2	24	70	9	3	38
1	25	13	71	66	10	93	4	30	39	96
2	26	78	14	86	72	48	67	7	11	91
3	94	84	5	82	31	33	40	56	97	35
4	27	45	79	42	15	62	87	58	73	18
5	49	99	68	23	8	37	12	65	92	29
6	95	77	85	47	6	90	83	81	32	55
7	34	44	41	61	57	17	98	22	36	64
8	28	76	46	89	80	54	43	60	16	21
9	63	75	88	53	59	20	74	52	19	51
10	50									

I.	0	1	2	3	4	5	6	7	8	9
0		2	4	8	16	32	64	27	54	7
1	14	28	56	11	22	44	88	75	49	98
2	95	89	77	53	5	10	20	40	80	59
3	17	34	68	35	70	39	78	55	9	18
4	36	72	43	86	71	41	82	63	25	50
5	100	99	97	93	85	69	37	74	47	94
6	87	73	45	90	79	57	13	26	52	3
7	6	12	24	48	96	91	81	61	21	42
8	84	67	33	66	31	62	23	46	92	83
9	65	29	58	15	30	60	19	38	76	51
10	1									

Простое число 103.

Первообразные корни: 5, 6, 11, 12, 20, 21, 35, 40, 43, 44, 45, 48, 51, 53, 54, 62, 65, 67, 70, 71, 74, 75, 77, 78, 84, 85, 86, 87, 88, 96, 99, 101.

Основаніе 6.

i.

N.	0	1	2	3	4	5	6	7	8	9
0		102	46	57	92	59	1	32	36	12
1	3	29	47	66	78	14	82	50	58	28
2	49	89	75	90	93	16	10	69	22	76
3	60	99	26	86	96	91	2	81	74	21
4	95	94	33	55	19	71	34	17	37	64
5	62	5	56	11	13	88	68	85	20	70
6	4	84	43	44	72	23	30	53	40	45
7	35	77	48	9	25	73	18	61	67	42
8	39	24	38	100	79	7	101	31	65	27
9	15	98	80	54	63	87	83	52	8	41
10	6	97	51							

N.

I.	0	1	2	3	4	5	6	7	8	9
0		6	36	10	60	51	100	85	98	73
1	26	53	9	54	15	90	25	47	76	44
2	58	39	28	65	81	74	32	89	19	11
3	66	87	7	42	46	70	8	48	82	80
4	68	99	79	62	63	69	2	12	72	20
5	17	102	97	67	93	43	52	3	18	5
6	30	77	50	94	49	88	13	78	56	27
7	59	45	64	75	38	22	29	71	14	84
8	92	37	16	96	61	57	33	95	55	21
9	23	35	4	24	41	40	34	101	91	31
10	83	86	1							

Простое число 107.

Первообразные корни: 2, 5, 6, 7, 8, 15, 17, 18, 20, 21, 22, 24, 26, 28, 31, 32, 38, 43, 45, 46, 50, 51, 54, 55, 58, 59, 60, 63, 65, 66, 67, 68, 70, 71, 72, 73, 74, 77, 78, 80, 82, 84, 88, 91, 93, 94, 95, 96, 97, 98, 103, 104.

Основаніе 63.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		106	95	78	84	13	67	57	73	50
1	2	76	56	58	46	91	62	105	39	96
2	97	29	65	60	45	26	47	22	35	72
3	80	21	51	48	94	70	28	6	85	30
4	86	90	18	93	54	63	49	16	34	8
5	15	77	36	64	11	89	24	68	61	87
6	69	102	10	1	40	71	37	33	83	32
7	59	81	17	41	101	104	74	27	19	88
8	75	100	79	98	7	12	82	44	43	92
9	52	9	38	99	5	3	23	55	103	20
10	4	14	66	31	25	42	53			

N.

I.	0	1	2	3	4	5	6	7	8	9
0		63	10	95	100	94	37	84	49	91
1	62	54	85	5	101	50	47	72	42	78
2	99	31	27	96	56	104	25	77	36	21
3	39	103	69	67	48	28	52	66	92	18
4	64	73	105	88	87	24	14	26	33	46
5	9	32	90	106	44	97	12	7	13	70
6	23	58	16	45	53	22	102	6	57	60
7	35	65	29	8	76	80	11	51	3	82
8	30	71	86	68	4	38	40	59	79	55
9	41	15	89	43	34	2	19	20	83	93
10	81	74	61	98	75	17	1			

Простое число 109.

Первообразные корни: 6, 10, 11, 13, 14, 18, 24, 30, 37, 39, 40, 42, 44, 47, 50, 51, 52, 53, 56, 57, 58, 59, 62, 65, 67, 69, 70, 72, 79, 85, 91, 95, 96, 98, 99, 103.

Основаніе 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		108	93	28	78	16	13	88	63	56
1	1	107	106	7	73	44	48	21	41	3
2	94	8	92	105	91	32	100	84	58	10
3	29	74	33	27	6	104	26	65	96	35
4	79	45	101	66	77	72	90	5	76	68
5	17	49	85	97	69	15	43	31	103	71
6	14	22	59	36	18	23	12	47	99	25
7	89	42	11	80	50	60	81	87	20	83
8	64	4	30	46	86	37	51	38	62	40
9	57	95	75	102	98	19	61	52	53	55
10	2	9	34	67	70	24	82	39	54	

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	100	19	81	47	34	13	21	101
1	29	72	66	6	60	55	5	50	64	95
2	78	17	61	65	105	69	36	33	3	30
3	82	57	25	32	102	39	63	85	87	107
4	89	18	71	56	15	41	83	67	16	51
5	74	86	97	98	108	99	9	90	28	62
6	75	96	88	8	80	37	43	103	49	54
7	104	59	45	14	31	92	48	44	4	40
8	73	76	106	79	27	52	84	77	7	70
9	46	24	22	2	20	91	38	53	94	68
10	26	42	93	58	35	23	12	11	1	

Простое число 113.

Первообразные корни: 3, 5, 6, 10, 12, 17, 19, 20, 21, 23, 24, 27, 29, 33, 34, 37, 38, 39, 43, 45, 46, 47, 54, 55, 58, 59, 66, 67, 68, 70, 74, 75, 76, 79, 80, 84, 86, 89, 90, 92, 93, 94, 96, 101, 103, 107, 108, 110.

Основаніе 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		112	52	79	104	61	19	72	44	46
1	1	22	71	58	12	28	96	59	98	93
2	53	39	74	103	11	10	110	13	64	87
3	80	30	36	101	111	21	38	29	33	25
4	105	34	91	17	14	107	43	97	63	32
5	62	26	50	76	65	83	4	60	27	9
6	20	106	82	6	88	7	41	99	51	70
7	73	35	90	49	81	89	85	94	77	55
8	45	92	86	24	31	8	69	54	66	67
9	47	18	95	109	37	42	3	40	84	68
10	2	15	78	57	102	100	16	75	5	48
11	23	108	56							

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	100	96	56	108	63	65	85	59
1	25	24	14	27	44	101	106	43	91	6
2	60	35	11	110	83	39	51	58	15	37
3	31	84	49	38	41	71	32	94	36	21
4	97	66	95	46	8	80	9	90	109	73
5	52	68	2	20	87	79	112	103	13	17
6	57	5	50	48	28	54	88	89	99	86
7	69	12	7	70	22	107	53	78	102	3
8	30	74	62	55	98	76	82	29	64	75
9	72	42	81	19	77	92	16	47	18	67
10	105	33	104	23	4	40	61	45	111	93
11	26	34	1							

Простое число 127.

Первообразные корни: 3, 6, 7, 12, 14, 23, 29, 39, 43, 45, 46, 48, 53, 55, 56, 57, 58, 65, 67, 78, 83, 85, 86, 91, 92, 93, 96, 97, 101, 106, 109, 110, 112, 114, 116, 118.

Основаніе 109.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		126	18	23	36	111	41	125	54	46
1	3	52	59	20	17	8	72	118	64	42
2	21	22	70	11	77	96	38	69	35	79
3	26	50	90	75	10	110	82	112	60	43
4	39	76	40	121	88	31	29	120	95	124
5	114	15	56	67	87	37	53	65	97	91
6	44	30	68	45	108	5	93	107	28	34
7	2	116	100	24	4	119	78	51	61	32
8	57	92	94	25	58	103	13	102	106	123
9	49	19	47	73	12	27	113	89	16	98
10	6	101	33	14	74	7	85	84	105	1
11	55	9	71	80	83	122	115	66	109	117
12	62	104	48	99	86	81	63			

N

l.	0	1	2	3	4	5	6	7	8	9
0		109	70	10	74	65	100	105	15	111
1	34	23	94	86	103	51	98	14	2	91
2	13	20	21	3	73	83	30	95	68	46
3	61	45	79	102	69	28	4	55	26	40
4	42	6	19	39	60	63	9	92	122	90
5	31	77	11	56	8	110	52	80	84	12
6	38	78	120	126	18	57	117	53	62	27
7	22	112	16	93	104	33	41	24	76	29
8	113	125	36	114	107	106	124	54	44	97
9	32	59	81	66	82	48	25	58	99	123
10	72	101	87	85	121	108	88	67	64	118
11	35	5	37	96	50	116	71	119	17	75
12	47	43	115	89	49	7	1			

Простое число 131.

Первообразные корни: 2, 6, 8, 10, 14, 17, 22, 23, 26, 29, 30, 31, 37, 40, 50, 54, 56, 57, 66, 67, 72, 76, 82, 83, 85, 87, 88, 90, 93, 95, 96, 97, 98, 103, 104, 106, 110, 111, 115, 116, 118, 119, 120, 122, 124, 126, 127, 128.

Основаніе 10.

N.

I.	0	1	2	3	4	5	6	7	8	9
0		130	83	126	36	48	79	38	119	122
1	1	98	32	64	121	44	72	59	75	45
2	84	34	51	89	115	96	17	118	74	73
3	127	67	25	94	12	86	28	23	128	60
4	37	58	117	22	4	40	42	5	68	76
5	49	55	100	78	71	16	27	41	26	46
6	80	104	20	30	108	112	47	43	95	85
7	39	15	111	91	106	92	81	6	13	35
8	120	114	11	3	70	107	105	69	87	52
9	123	102	125	63	88	93	21	77	29	90
10	2	62	8	9	53	82	31	50	24	116
11	99	19	110	10	124	7	109	56	129	97
12	33	66	57	54	103	14	113	101	61	18
13	65									

I.

N.	0	1	2	3	4	5	6	7	8	9
0		10	100	83	44	47	77	115	102	103
1	113	82	34	78	125	71	55	26	129	111
2	62	96	43	37	108	32	58	56	36	98
3	63	106	12	120	21	79	4	40	7	70
4	45	57	46	67	15	19	59	66	5	50
5	107	22	89	104	123	51	117	122	41	17
6	39	128	101	93	13	130	121	31	48	87
7	84	54	16	29	28	18	49	97	53	6
8	60	76	105	2	20	69	35	88	94	23
9	99	73	75	95	33	68	25	119	11	110
10	52	127	91	124	61	86	74	85	64	116
11	112	72	65	126	81	24	109	42	27	8
12	80	14	9	90	114	92	3	30	38	118
13	1									

Простое число 137.

Первообразные корни: 3, 5, 6, 12, 13, 20, 21, 23, 24, 26, 27, 29, 31, 33, 35, 40, 42, 43, 45, 46, 47, 48, 51, 52, 53, 54, 55, 57, 58, 62, 66, 67, 70, 71, 75, 79, 80, 82, 83, 84, 85, 86, 89, 90, 91, 92, 94, 95, 97, 102, 104, 106, 108, 110, 111, 113, 114, 116, 117, 124, 125, 131, 132, 134.

Основаніе 12.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		136	130	13	124	23	7	2	118	26
1	17	90	1	53	132	36	112	86	20	54
2	11	15	84	129	131	46	47	39	126	95
3	30	133	106	103	80	25	14	102	48	66
4	5	51	9	37	78	49	123	111	125	4
5	40	99	41	71	33	113	120	67	89	128
6	24	110	127	28	100	76	97	87	74	6
7	19	29	8	32	96	59	42	92	60	21
8	135	52	45	101	3	109	31	108	72	57
9	43	55	117	10	105	77	119	73	134	116
10	34	82	93	12	35	38	65	98	27	58
11	107	115	114	63	61	16	83	79	122	88
12	18	44	104	64	121	69	22	85	94	50
13	70	75	91	56	81	62	68			

N.

I.	0	1	2	3	4	5	6	7	8	9
0		12	7	84	49	40	69	6	72	42
1	93	20	103	3	36	21	115	10	120	70
2	18	79	126	5	60	35	9	108	63	71
3	30	86	73	54	100	104	15	43	105	27
4	50	52	76	90	121	82	25	26	38	45
5	129	41	81	13	19	91	133	89	109	75
6	78	114	135	113	123	106	39	57	136	125
7	130	53	88	97	68	131	65	95	44	117
8	34	134	101	116	22	127	17	67	119	58
9	11	132	77	102	128	29	74	66	107	51
10	64	83	37	33	122	94	32	110	87	85
11	61	47	16	55	112	111	99	92	8	96
12	56	124	118	46	4	48	28	62	59	23
13	2	24	14	31	98	80	1			

Простое число 139.

Первообразные корни: 2, 3, 12, 15, 17, 18, 19, 21, 22, 26, 32, 40, 50, 53, 56, 58, 61, 68, 70, 72, 73, 85, 88, 90, 92, 93, 98, 101, 102, 104, 108, 109, 110, 111, 114, 115, 119, 123, 126, 128, 130, 132, 134, 135.

Основаніе 92.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		138	119	49	100	22	30	16	81	98
1	3	74	11	26	135	71	62	37	79	83
2	122	65	55	39	130	44	7	9	116	8
3	52	40	43	123	18	38	60	136	64	75
4	103	82	46	23	36	120	20	70	111	32
5	25	86	126	73	128	96	97	132	127	15
6	33	125	21	114	24	48	104	110	137	88
7	19	68	41	35	117	93	45	90	56	102
8	84	58	63	28	27	59	4	57	17	94
9	101	42	1	89	51	105	92	115	13	34
10	6	133	67	129	107	87	54	112	109	121
11	77	47	78	76	113	61	108	124	134	53
12	14	10	106	131	2	66	95	80	5	72
13	29	12	85	99	91	31	118	50	69	

N.

I.	0	1	2	3	4	5	6	7	8	9
0		92	124	10	86	128	100	26	29	27
1	121	12	131	98	120	59	7	88	34	70
2	46	62	5	43	64	50	13	84	83	130
3	6	135	49	60	99	73	44	17	35	23
4	31	72	91	32	25	76	42	111	65	3
5	137	94	30	119	106	22	78	87	81	85
6	36	115	16	82	38	21	125	102	71	138
7	47	15	129	53	11	39	113	110	112	18
8	127	8	41	19	80	132	51	105	69	93
9	77	134	96	75	89	126	55	56	9	133
10	4	90	79	40	66	95	122	104	116	108
11	67	48	107	114	63	97	28	74	136	2
12	45	109	20	33	117	61	52	58	54	103
13	24	123	57	101	118	14	37	68	1	

Простое число 149.

Первообразные корни: 2, 3, 8, 10, 11, 12, 13, 14, 15, 18, 21, 23, 27, 32, 34, 38, 40, 41, 43, 48, 50, 51, 52, 55, 56, 57, 58, 59, 60, 62, 65, 66, 70, 71, 72, 74, 75, 77, 78, 79, 83, 84, 87, 89, 90, 91, 92, 93, 94, 97, 98, 99, 101, 106, 108, 109, 111, 115, 117, 122, 126, 128, 131, 134, 135, 136, 137, 138, 139, 141, 146, 147.

Основаніе 10.

I

N.	0	1	2	3	4	5	6	7	8	9
0		148	117	115	86	32	84	38	55	82
1	1	25	53	133	7	147	24	4	51	60
2	118	5	142	15	22	64	102	49	124	128
3	116	52	141	140	121	70	20	136	29	106
4	87	61	122	77	111	114	132	14	139	76
5	33	119	71	34	18	57	93	27	97	9
6	85	6	21	120	110	17	109	104	90	130
7	39	143	137	72	105	31	146	63	69	113
8	56	16	30	35	91	36	46	95	80	11
9	83	23	101	19	131	92	108	145	45	107
10	2	65	88	58	40	37	3	48	135	13
11	26	103	62	94	144	47	66	67	126	42
12	54	50	123	28	138	96	89	68	79	44
13	134	125	78	98	73	81	59	127	99	75
14	8	129	112	10	106	12	41	43	74	

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	100	106	17	21	61	14	140	59
1	143	89	145	109	47	23	81	65	54	93
2	36	62	24	91	16	11	110	57	123	38
3	82	75	5	50	53	83	85	105	7	70
4	104	146	119	147	129	98	86	115	107	27
5	121	18	31	12	120	8	80	55	103	136
6	19	41	112	77	25	101	116	117	127	78
7	35	52	73	134	148	139	49	43	132	128
8	88	135	9	90	6	60	4	40	102	126
9	68	84	95	56	113	87	125	58	133	138
10	39	92	26	111	67	74	144	99	96	66
11	64	44	142	79	45	3	30	2	20	51
12	63	34	42	122	28	131	118	137	29	141
13	69	94	46	13	130	108	37	72	124	48
14	33	32	22	71	114	97	76	15	1	

Простое число 151.

Первообразные корни: 6, 7, 12, 13, 14, 15, 30, 35, 48, 51, 52, 54, 56, 61, 63, 71, 77, 82, 89, 93, 96, 102, 104, 106, 108, 109, 111, 112, 114, 115, 117, 120, 126, 129, 130, 133, 134, 140, 141, 146.

Основаніе 114.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		150	70	141	140	82	61	37	60	132
1	2	34	131	101	107	73	130	88	52	90
2	72	28	104	115	51	14	21	123	27	54
3	143	58	50	25	8	119	122	76	10	92
4	142	111	98	38	24	64	35	86	121	74
5	84	79	91	69	43	116	97	81	124	30
6	63	59	128	19	120	33	95	93	78	106
7	39	137	42	87	146	5	80	71	12	117
8	62	114	31	3	18	20	108	45	94	53
9	134	138	105	49	6	22	41	118	144	16
10	4	9	149	46	11	110	139	99	113	23
11	36	67	17	85	1	47	44	83	100	125
12	133	68	129	102	48	96	89	126	40	29
13	103	147	15	127	13	55	148	32	26	56
14	109	77	57	135	112	136	7	65	66	145
15	75									

N.

I.	0	1	2	3	4	5	6	7	8	9
0		114	10	83	100	75	94	146	34	101
1	38	104	78	134	25	132	99	112	84	63
2	85	26	95	109	44	33	138	28	21	129
3	59	82	137	65	11	46	110	7	43	70
4	128	96	72	54	116	87	103	115	124	93
5	32	24	18	89	29	135	139	142	31	61
6	8	6	80	60	45	147	148	111	121	53
7	2	77	20	15	49	150	37	141	68	51
8	76	57	5	117	50	113	47	73	17	126
9	19	52	39	67	88	66	125	56	42	107
10	118	13	123	130	22	92	69	14	86	140
11	105	41	144	108	81	23	55	79	97	35
12	64	48	36	27	58	119	127	133	62	122
13	16	12	9	120	90	143	145	71	91	106
14	4	3	40	30	98	149	74	131	136	102
15	1									

Простое число 157.

Первообразные корни: 5, 6, 15, 18, 20, 21, 24, 26, 34, 38, 43, 53, 55, 60, 61, 62, 63, 66, 69, 70, 72, 73, 74, 77, 80, 83, 84, 85, 87, 88, 91, 94, 95, 96, 97, 102, 104, 114, 119, 123, 131, 133, 136, 137, 139, 142, 151, 152.

Основаніе 139.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		156	147	122	138	11	113	57	129	88
1	2	152	104	130	48	133	120	128	79	116
2	149	23	143	81	95	22	121	54	39	15
3	124	58	111	118	119	68	70	28	107	96
4	140	75	14	151	134	99	72	76	86	114
5	13	94	112	25	45	7	30	82	6	27
6	115	155	49	145	102	141	109	12	110	47
7	59	64	61	83	19	144	98	53	87	9
8	131	20	66	97	5	139	142	137	125	32
9	90	31	63	24	67	127	77	37	105	84
10	4	108	85	123	103	34	16	91	36	8
11	154	150	21	56	73	92	153	62	18	29
12	106	148	146	41	40	33	136	46	93	117
13	132	43	100	17	3	65	101	71	38	1
14	50	42	55	126	52	26	74	80	10	51
15	135	35	89	60	44	69	78			

N.

I.	0	1	2	3	4	5	6	7	8	9
0		139	10	134	100	84	58	55	109	79
1	148	5	67	50	42	29	106	133	118	74
2	81	112	25	21	93	53	145	59	37	119
3	56	91	89	125	105	151	108	97	138	28
4	124	123	141	131	154	54	127	69	14	62
5	140	149	144	77	27	142	113	7	31	70
6	153	72	117	92	71	135	82	94	35	155
7	36	137	46	114	146	41	47	96	156	18
8	147	23	57	73	99	102	48	78	9	152
9	90	107	115	128	51	24	39	83	76	45
10	132	136	64	104	12	98	120	38	101	66
11	68	32	52	6	49	60	19	129	33	34
12	16	26	3	103	30	88	143	95	17	8
13	13	80	130	15	44	150	126	87	4	85
14	40	65	86	22	75	63	122	2	121	20
15	111	43	11	116	110	61	1			

Простое число 163.

Первообразные корни: 2, 3, 7, 11, 12, 18, 19, 20, 29, 32, 42, 44, 45, 50, 52, 63, 66, 67, 68, 70, 72, 73, 75, 76, 79, 80, 82, 89, 92, 94, 101, 103, 106, 107, 108, 109, 112, 114, 116, 117, 120, 122, 124, 128, 129, 130, 137, 139, 147, 148, 149, 153, 154, 159.

Основаніе 70.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		162	71	43	142	93	114	161	51	86
1	2	97	23	57	70	136	122	159	157	127
2	73	42	6	153	94	24	128	129	141	145
3	45	39	31	140	68	92	66	75	36	100
4	144	20	113	106	77	17	62	44	3	160
5	95	40	37	18	38	28	50	8	54	27
6	116	30	110	85	102	150	49	155	139	34
7	1	52	137	7	146	67	107	96	9	103
8	53	10	91	134	22	90	15	26	148	65
9	88	56	133	82	115	58	74	130	69	21
10	4	29	111	35	108	135	89	131	109	119
11	99	118	121	14	79	84	125	143	98	158
12	25	32	101	63	19	117	156	147	11	149
13	59	112	120	126	64	60	48	47	105	13
14	72	87	123	154	46	76	78	41	55	151
15	138	104	16	83	5	132	80	33	12	61
16	124	152	81							

N.

I.	0	1	2	3	4	5	6	7	8	9
0		70	10	48	100	154	22	73	57	78
1	81	128	158	139	113	86	152	45	53	124
2	41	99	84	12	25	120	87	59	55	101
3	61	32	121	157	69	103	38	52	54	31
4	51	147	21	3	47	30	144	137	136	66
5	56	8	71	80	58	148	91	13	95	130
6	135	159	46	123	134	89	36	75	34	98
7	14	2	140	20	96	37	145	44	146	114
8	156	162	93	153	115	63	9	141	90	106
9	85	82	35	5	24	50	77	11	118	110
10	39	122	64	79	151	138	43	76	104	108
11	62	102	131	42	6	94	60	125	111	109
12	132	112	16	142	160	116	133	19	26	27
13	97	107	155	92	83	105	15	72	150	68
14	33	28	4	117	40	29	74	127	88	129
15	65	149	161	23	143	67	126	18	119	17
16	49	7	1							

Простое число 167.

Первообразные корни: 5, 10, 13, 15, 17, 20, 23, 26, 30, 34, 35, 37, 39, 40, 41, 43, 45, 46, 51, 52, 53, 55, 59, 60, 67, 68, 69, 70, 71, 73, 74, 78, 79, 80, 82, 83, 86, 90, 91, 92, 95, 101, 102, 103, 104, 105, 106, 109, 110, 111, 113, 117, 118, 119, 120, 123, 125, 129, 131, 134, 135, 136, 138, 139, 140, 142, 143, 145, 146, 148, 149, 151, 153, 155, 156, 158, 159, 160, 161, 163, 164, 165.

Основаніе 10.

I

N.	0	1	2	3	4	5	6	7	8	9
0		166	86	144	6	81	64	96	92	122
1	1	110	150	43	16	59	12	143	42	50
2	87	74	30	51	70	162	129	100	102	32
3	145	152	98	88	63	11	128	127	136	21
4	7	55	160	75	116	37	137	68	156	26
5	82	121	49	31	20	25	22	28	118	23
6	65	34	72	52	18	124	8	85	149	29
7	97	159	48	71	47	140	56	40	107	119
8	93	78	141	163	80	58	161	10	36	24
9	123	139	57	130	154	131	76	14	112	66
10	2	91	41	101	135	155	117	148	106	35
11	111	105	108	103	114	132	38	165	109	73
12	151	54	120	33	158	77	138	90	104	53
13	44	45	94	146	5	15	69	62	115	19
14	17	46	79	153	134	113	157	4	133	125
15	60	95	142	99	126	67	27	84	39	9
16	13	147	164	89	61	3	83			

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	100	165	147	134	4	40	66	159
1	87	35	16	160	97	135	14	140	64	139
2	54	39	56	59	89	55	49	156	57	69
3	22	53	29	123	61	109	88	45	116	158
4	77	102	18	13	130	131	141	74	72	52
5	19	23	63	129	121	41	76	92	85	15
6	150	164	137	34	6	60	99	155	47	136
7	24	73	62	119	21	43	96	125	81	142
8	84	5	50	166	157	67	2	20	33	163
9	127	101	8	80	132	151	7	70	32	153
10	27	103	28	113	128	111	108	78	112	118
11	11	110	98	145	114	138	44	106	58	79
12	122	51	9	90	65	149	154	37	36	26
13	93	95	115	148	144	104	38	46	126	91
14	75	82	152	17	3	30	133	161	107	68
15	12	120	31	143	94	105	48	146	124	71
16	42	86	25	83	162	117	1			

Простое число 173.

Первообразные корни: 2, 3, 5, 7, 8, 11, 12, 17, 18, 19, 20, 26, 27, 28, 30, 32, 39, 42, 44, 45, 46, 48, 50, 53, 58, 59, 61, 62, 63, 65, 66, 68, 69, 70, 71, 72, 74, 75, 76, 79, 82, 86, 87, 91, 94, 97, 98, 99, 101, 102, 103, 104, 105, 107, 108, 110, 111, 112, 114, 115, 120, 123, 125, 127, 128, 129, 131, 134, 141, 143, 145, 146, 147, 153, 154, 155, 156, 161, 162, 165, 166, 168, 170, 171.

Основаніе 91.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		172	13	7	26	163	20	31	39	14
1	4	127	33	142	44	170	52	89	27	85
2	17	38	140	88	46	154	155	21	57	152
3	11	122	65	134	102	22	40	42	98	149
4	30	74	51	60	153	5	101	144	59	62
5	167	96	168	123	34	118	70	92	165	19
6	24	169	135	45	78	133	147	50	115	95
7	35	23	53	94	55	161	111	158	162	71
8	43	28	87	104	64	80	73	159	166	150
9	18	1	114	129	157	76	72	25	75	141
10	8	139	109	121	9	29	136	61	47	164
11	131	49	83	110	105	79	6	156	32	120
12	37	82	10	81	148	145	58	15	91	67
13	146	137	160	116	63	12	128	126	108	16
14	48	151	36	97	66	143	107	69	68	132
15	2	54	124	103	171	113	3	138	84	130
16	56	119	41	90	100	125	117	106	77	112
17	93	99	86							

N.

I.	0	1	2	3	4	5	6	7	8	9
0		91	150	156	10	45	116	3	100	104
1	122	30	135	2	9	127	139	20	90	59
2	6	27	35	71	60	97	4	18	81	105
3	40	7	118	12	54	70	142	120	21	8
4	36	162	37	80	14	63	24	108	140	111
5	67	42	16	72	151	74	160	28	126	48
6	43	107	49	134	84	32	144	129	148	147
7	56	79	96	86	41	98	95	168	64	115
8	85	123	121	112	158	19	172	82	23	17
9	163	128	57	170	73	69	51	143	38	171
10	164	46	34	153	83	114	167	146	138	102
11	113	76	169	155	92	68	133	166	55	161
12	119	103	31	53	152	165	137	11	136	93
13	159	110	149	65	33	62	106	131	157	101
14	22	99	13	145	47	125	130	66	124	39
15	89	141	29	44	25	26	117	94	77	87
16	132	75	78	5	109	58	88	50	52	61
17	15	154	1							

Простое число 179.

Первообразные корни: 2, 6, 7, 8, 10, 11, 18, 21, 23, 24, 26, 28, 30, 32, 33, 34, 35, 37, 38, 40, 41, 44, 50, 53, 54, 55, 58, 62, 63, 69, 71, 72, 73, 78, 79, 84, 86, 90, 91, 92, 94, 96, 97, 98, 99, 102, 103, 104, 105, 109, 111, 112, 113, 114, 115, 118, 119, 120, 122, 123, 127, 128, 130, 131, 132, 133, 134, 136, 137, 140, 143, 148, 150, 152, 154, 157, 159, 160, 162, 163, 164, 165, 166, 167, 170, 174, 175, 176.

Основаніе 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		178	73	52	146	106	125	23	41	104
1	1	27	20	134	96	158	114	14	177	26
2	74	75	100	65	93	34	29	156	169	70
3	53	76	9	79	87	129	72	19	99	8
4	147	101	148	144	173	32	138	136	166	46
5	107	66	102	111	51	133	64	78	143	110
6	126	94	149	127	82	62	152	48	160	117
7	24	35	145	95	92	86	172	50	81	91
8	42	30	174	150	43	120	39	122	68	16
9	105	157	33	128	31	132	61	85	119	131
10	2	170	139	83	175	3	6	56	124	113
11	28	71	137	63	151	171	38	60	5	37
12	21	54	167	153	44	140	22	13	155	18
13	135	77	47	49	121	84	55	59	12	58
14	97	10	108	161	40	176	168	98	165	142
15	159	80	67	118	123	4	154	11	164	163
16	115	88	103	25	69	7	45	109	116	90
17	15	130	112	36	17	57	141	162	89	

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	100	105	155	118	106	165	39	32
1	141	157	138	127	17	170	89	174	129	37
2	12	120	126	7	70	163	19	11	110	26
3	81	94	45	92	25	71	173	119	116	86
4	144	8	80	84	124	166	49	132	67	133
5	77	54	3	30	121	136	107	175	139	137
6	117	96	65	113	56	23	51	152	88	164
7	29	111	36	2	20	21	31	131	57	33
8	151	78	64	103	135	97	75	34	161	178
9	169	79	74	24	61	73	14	140	147	38
10	22	41	52	162	9	90	5	50	142	167
11	59	53	172	109	16	160	168	69	153	98
12	85	134	87	154	108	6	60	63	93	35
13	171	99	95	55	13	130	47	112	46	102
14	125	176	149	58	43	72	4	40	42	62
15	83	114	66	123	156	128	27	91	15	150
16	68	143	177	159	158	148	48	122	146	28
17	101	115	76	44	82	104	145	18	1	

Простое число 181.

Первообразные корни: 2, 10, 18, 21, 23, 24, 28, 41, 47, 50, 53, 54, 57, 58, 63, 66, 69, 76, 77, 78, 83, 84, 85, 90, 91, 96, 97, 98, 103, 104, 105, 112, 115, 118, 123, 124, 127, 128, 131, 134, 140, 153, 157, 158, 160, 163, 171, 179.

Основаніе 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		180	133	68	86	48	21	15	39	136
1	1	146	154	32	148	116	172	55	89	135
2	134	83	99	29	107	96	165	24	101	84
3	69	27	125	34	8	63	42	38	88	100
4	87	59	36	140	52	4	162	109	60	30
5	49	123	118	121	157	14	54	23	37	108
6	22	65	160	151	78	80	167	66	141	97
7	16	57	175	20	171	164	41	161	53	166
8	40	92	12	73	169	103	93	152	5	25
9	137	47	115	95	62	3	13	79	163	102
10	2	130	76	143	71	131	74	81	110	85
11	147	106	7	51	156	77	170	168	61	70
12	155	112	18	127	113	144	104	67	31	28
13	33	139	120	150	19	72	94	142	50	126
14	149	177	10	178	128	132	153	98	124	35
15	117	159	174	11	114	75	6	17	119	9
16	173	44	45	179	145	82	26	58	122	64
17	56	91	46	129	105	111	138	176	158	43
18	90									

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	100	95	45	88	156	112	34	159
1	142	153	82	96	55	7	70	157	122	134
2	73	6	60	57	27	89	166	31	129	23
3	49	128	13	130	33	149	42	58	37	8
4	80	76	36	179	161	162	172	91	5	50
5	138	113	44	78	56	17	170	71	167	41
6	48	118	94	35	169	61	67	127	3	30
7	119	104	135	83	106	155	102	115	64	97
8	65	107	165	21	29	109	4	40	38	18
9	180	171	81	86	136	93	25	69	147	22
10	39	28	99	85	126	174	111	24	59	47
11	108	175	121	124	154	92	15	150	52	158
12	132	53	168	51	148	32	139	123	144	173
13	101	105	145	2	20	19	9	90	176	131
14	43	68	137	103	125	164	11	110	14	140
15	133	63	87	146	12	120	114	54	178	151
16	62	77	46	98	75	26	79	66	117	84
17	116	74	16	160	152	72	177	141	143	163
18	1									

Простое число 191.

Первообразные корни: 19, 21, 22, 28, 29, 33, 35, 42, 44, 47, 53, 56, 57, 58, 61, 62, 63, 71, 73, 74, 76, 83, 87, 88, 89, 91, 93, 94, 95, 99, 101, 105, 106, 110, 111, 112, 113, 114, 116, 119, 123, 124, 126, 127, 131, 132, 137, 140, 141, 143, 145, 146, 148, 151, 157, 164, 165, 167, 168, 171, 173, 174, 175, 176, 178, 179, 181, 182, 183, 187, 188, 189.

Основаніе 157.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		190	102	148	14	90	60	133	116	106
1	2	115	162	156	45	48	28	184	18	93
2	104	91	27	112	74	180	68	64	147	29
3	150	125	130	73	96	33	120	65	5	114
4	16	145	3	174	129	6	24	39	176	76
5	92	142	170	77	166	15	59	51	131	182
6	62	63	37	49	42	56	175	44	8	70
7	135	69	32	189	167	138	107	58	26	66
8	118	22	57	173	105	84	86	177	41	149
9	108	99	126	83	141	183	88	46	178	31
10	4	13	54	136	82	181	179	10	78	152
11	117	23	161	121	153	12	43	72	94	127
12	164	40	165	103	139	80	151	137	144	132
13	158	157	87	36	146	154	110	71	172	75
14	47	187	171	81	134	119	101	34	79	98
15	50	111	19	100	160	25	128	1	168	35
16	30	55	124	52	159	163	85	169	17	122
17	186	9	188	113	89	123	143	140	61	67
18	20	97	11	21	38	155	185	109	53	7
19	95									

N.

I.	0	1	2	3	4	5	6	7	8	9
0		157	10	42	100	38	45	189	68	171
1	107	182	115	101	4	55	40	168	18	152
2	180	183	81	111	46	155	78	22	16	29
3	160	99	72	35	147	159	133	62	184	47
4	121	88	64	116	67	14	97	140	15	63
5	150	57	163	188	102	161	65	82	77	56
6	6	178	60	61	27	37	79	179	26	71
7	69	137	117	33	24	139	49	53	108	148
8	125	143	104	93	85	166	86	132	96	174
9	5	21	50	19	118	190	34	181	149	91
10	153	146	2	123	20	84	9	76	90	187
11	136	151	23	173	39	11	8	110	80	145
12	36	113	169	175	162	31	92	119	156	44
13	32	58	129	7	144	70	103	127	75	124
14	177	94	51	176	128	41	134	28	3	89
15	30	126	109	114	135	185	13	131	130	164
16	154	112	12	165	120	122	54	74	158	167
17	52	142	138	83	43	66	48	87	98	106
18	25	105	59	95	17	186	170	141	172	73
19	1									

Простое число 193.

Первообразные корни: 5, 10, 15, 17, 19, 22, 26, 30, 34, 37, 38, 40, 41, 44, 45, 47, 51, 52, 53, 57, 58, 61, 66, 70, 73, 77, 78, 79, 80, 82, 90, 91, 102, 103, 111, 113, 114, 115, 116, 120, 123, 127, 132, 135, 136, 140, 141, 142, 146, 148, 149, 152, 153, 155, 156, 159, 163, 167, 171, 174, 176, 178, 183, 188.

Основаніе 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		192	182	156	172	11	146	184	162	120
1	1	93	136	15	174	167	152	149	110	59
2	183	148	83	54	126	22	5	84	164	9
3	157	134	142	57	139	3	100	55	49	171
4	173	125	138	72	73	131	44	127	116	176
5	12	113	187	79	74	104	154	23	191	92
6	147	133	124	112	132	26	47	6	129	18
7	185	27	90	41	45	178	39	85	161	109
8	163	48	115	190	128	160	62	165	63	81
9	121	7	34	98	117	70	106	10	166	21
10	2	130	103	25	177	159	69	158	64	32
11	94	19	144	67	13	65	181	135	82	141
12	137	186	123	89	114	33	102	143	122	36
13	16	28	37	51	188	95	119	58	8	170
14	175	91	17	108	80	20	31	140	35	169
15	168	42	29	77	75	145	151	4	99	43
16	153	46	38	61	105	68	180	101	118	30
17	150	179	52	87	155	14	53	56	71	78
18	111	40	189	97	24	66	88	50	107	76
19	60	86	96							

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	100	35	157	26	67	91	138	29
1	97	5	50	114	175	13	130	142	69	111
2	145	99	25	57	184	103	65	71	131	152
3	169	146	109	125	92	148	129	132	162	76
4	181	73	151	159	46	74	161	66	81	38
5	187	133	172	176	23	37	177	33	137	19
6	190	163	86	88	108	115	185	113	165	106
7	95	178	43	44	54	154	189	153	179	53
8	144	89	118	22	27	77	191	173	186	123
9	72	141	59	11	110	135	192	183	93	158
10	36	167	126	102	55	164	96	188	143	79
11	18	180	63	51	124	82	48	94	168	136
12	9	90	128	122	62	41	24	47	84	68
13	101	45	64	61	31	117	12	120	42	34
14	147	119	32	127	112	155	6	60	21	17
15	170	156	16	160	56	174	3	30	107	105
16	85	78	8	80	28	87	98	15	150	149
17	139	39	4	40	14	140	49	104	75	171
18	166	116	2	20	7	70	121	52	134	182
19	83	58	1							

Простое число 197.

Первообразные корни: 2, 3, 5, 8, 11, 12, 13, 17, 18, 21, 27, 30, 31, 32, 35, 38, 44, 45, 46, 48, 50, 52, 56, 57, 58, 66, 67, 71, 72, 73, 74, 75, 78, 79, 80, 82, 86, 89, 91, 94, 95, 98, 99, 102, 103, 106, 108, 111, 115, 117, 118, 119, 122, 123, 124, 125, 126, 130, 131, 139, 140, 141, 145, 147, 149, 151, 152, 153, 159, 162, 165, 166, 167, 170, 176, 179, 180, 184, 185, 186, 189, 192, 194, 195.

Основаніе 73.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		196	61	65	122	137	126	86	183	130
1	2	5	187	153	147	6	48	95	191	182
2	63	151	66	68	52	78	18	195	12	40
3	67	173	109	70	156	27	56	148	47	22
4	124	46	16	54	127	71	129	106	113	172
5	139	160	79	80	60	142	73	51	101	96
6	128	180	38	20	170	94	131	57	21	133
7	88	179	117	1	13	143	108	91	83	59
8	185	64	107	14	77	36	115	105	188	23
9	132	43	190	42	167	123	174	102	37	135
10	4	76	25	69	140	92	141	34	121	90
11	7	17	134	175	112	9	162	87	157	181
12	189	10	45	111	99	19	81	186	35	119
13	155	33	192	72	118	136	82	30	194	3
14	149	171	44	158	178	177	62	41	74	15
15	8	31	169	29	152	114	144	26	120	145
16	50	154	125	58	168	11	75	165	138	110
17	97	116	176	150	166	164	53	161	84	93
18	193	146	104	49	55	89	103	100	32	85
19	184	28	39	24	163	159	98			

N.

I.	0	1	2	3	4	5	6	7	8	9
0		73	10	139	100	11	15	110	150	115
1	121	165	28	74	83	149	42	111	26	125
2	63	68	39	89	193	102	157	35	191	153
3	137	151	188	131	107	128	85	98	62	192
4	29	147	93	91	142	122	41	38	16	183
5	160	57	24	176	43	184	36	67	163	79
6	54	2	146	20	81	3	22	30	23	103
7	33	45	133	56	148	166	101	84	25	52
8	53	126	136	78	178	189	7	117	70	185
9	109	77	105	179	65	17	59	170	196	124
10	187	58	97	186	182	87	47	82	76	32
11	169	123	114	48	155	86	171	72	134	129
12	158	108	4	95	40	162	6	44	60	46
13	9	66	90	69	112	99	135	5	168	50
14	104	106	55	75	156	159	181	14	37	140
15	173	21	154	13	161	130	34	118	143	195
16	51	177	116	194	175	167	174	94	164	152
17	64	141	49	31	96	113	172	145	144	71
18	61	119	19	8	190	80	127	12	88	120
19	92	18	132	180	138	27	1			

Простое число 199.

Первообразные корни: 3, 6, 15, 22, 30, 34, 38, 39, 41, 44, 48, 54, 68, 69, 71, 73, 75, 77, 84, 87, 95, 97, 99, 105, 108, 110, 113, 118, 119, 120, 127, 129, 133, 134, 142, 143, 146, 148, 149, 150, 152, 153, 154, 163, 164, 166, 167, 168, 170, 173, 176, 179, 183, 185, 186, 189, 190, 192, 195, 197.

Основаніе 127.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		198	194	155	190	6	151	32	186	112
1	2	189	147	128	28	161	182	57	108	11
2	196	187	185	74	143	12	124	69	24	158
3	157	76	178	146	53	38	104	121	7	85
4	192	145	183	176	181	118	70	98	139	64
5	8	14	120	136	65	195	20	166	154	129
6	153	126	72	144	174	134	142	39	49	31
7	34	71	100	41	117	167	3	23	81	50
8	188	26	141	51	179	63	172	115	177	92
9	114	160	66	33	94	17	135	109	60	103
10	4	159	10	36	116	193	132	165	61	15
11	191	78	16	73	162	80	150	42	125	89
12	149	180	122	102	68	18	140	1	170	133
13	130	148	138	43	35	75	45	171	27	54
14	30	55	67	119	96	164	37	21	113	107
15	163	40	197	169	19	82	77	84	46	93
16	184	106	22	5	137	152	47	79	175	58
17	59	123	168	25	111	44	173	86	88	97
18	110	9	156	83	62	127	29	48	90	101
19	13	87	131	52	105	91	56	95	99	

N.

I.	0	1	2	3	4	5	6	7	8	9
0		127	10	76	100	163	5	38	50	181
1	102	19	25	190	51	109	112	95	125	154
2	56	147	162	77	28	173	81	138	14	186
3	140	69	7	93	70	134	103	146	35	67
4	151	73	117	133	175	136	158	166	187	68
5	79	83	193	34	139	141	196	17	169	170
6	98	108	184	85	49	54	92	142	124	27
7	46	71	62	113	23	135	31	156	111	167
8	115	78	155	183	157	39	177	191	178	119
9	188	195	89	159	94	197	144	179	47	198
10	72	189	123	99	36	194	161	149	18	97
11	180	174	9	148	90	87	104	74	45	143
12	52	37	122	171	26	118	61	185	13	59
13	130	192	106	129	65	96	53	164	132	48
14	126	82	66	24	63	41	33	12	131	120
15	116	6	165	60	58	3	182	30	29	101
16	91	15	114	150	145	107	57	75	172	153
17	128	137	86	176	64	168	43	88	32	84
18	121	44	16	42	160	22	8	21	80	11
19	4	110	40	105	2	55	20	152	1	

D.

Таблица Коркина

первообразныхъ корней и характеровъ, къ нимъ относящихся, для простыхъ чиселъ, меньшихъ 2000.

p — простое число, g — первообразный корень.

p	$p-1$	g	ХАРАКТЕРЫ
5	2^2	2	$f=2$
7	2.3	3	$z=2$
11	2.5	2	$u=4$
13	$2^2.3$	6	$f=8,\ z=-4$
17	2^4	10	$f''=10,\ f'=-2,\ f=4$
19	2.3^2	10	$z'=5,\ z=11$
23	2.11	10	$u=8$
29	$2^2.7$	10	$f=-12,\ u=-5$
31	$2.3.5$	17	$z=-6,\ u=8$
37	$2^2.3^2$	5	$f=6,\ z'=-4,\ z=10$
41	$2^3.5$	6	$f'=-14,\ f=-9,\ u=10$
43	$2.3.7$	28	$z=6,\ u=11$
47	2.23	10	$u=6$
53	$2^2.13$	26	$f=-23,\ u=10$
59	2.29	10	$u=-18$
61	$2^2.3.5$	10	$f=-11,\ z=13,\ u=-3$
67	$2.3.11$	12	$z=29,\ u=-5$
71	$2.5.7$	62	$u=5,\ v=32$
73	$2^3.3^2$	5	$f'=10,\ f=27,\ z'=2,\ z=8$
79	$2.3.13$	29	$z=-24,\ u=10$
83	2.41	50	$u=10$
89	$2^3.11$	30	$f'=-12,\ f=55,\ u=32$
97	$2^5.3$	10	$f'''=30,\ f''=27,\ f'=50,\ f=-22,\ z=-36$
101	$2^2.5^2$	2	$f=10,\ u'=16,\ u=-6$
103	$2.3.17$	6	$z=46,\ u=-3$
107	2.53	63	$u=10$
109	$2^2.3^3$	10	$f=33,\ z''=-28,\ z'=-43,\ z=-46$
113	$2^4.7$	10	$f''=65,\ f'=44,\ f=15,\ u=-7$
127	$2.3^2.7$	109	$z'=-24,\ z=19,\ u=2$

p	$p=1$	g	ХАРАКТЕРЫ
131	$2.5.13$	10	$u=58,\ v=-18$
137	$2^3.17$	12	$f'=10,\ f=-37,\ u=72$
139	$2.3.23$	92	$z=42,\ u=-39$
149	$2^2.37$	10	$f=-44,\ u=17$
151	$2.3.5^2$	114	$z=32,\ u'=94,\ u=59$
157	$2^2.3.13$	139	$f=28,\ z=-13,\ u=67$
163	2.3^4	70	$z'''=10,\ z''=22,\ z'=53,\ z=58$
167	2.83	10	$u=100$
173	$2^2.43$	91	$f=80,\ u=10$
179	2.89	10	$u=100$
181	$2^2.3^2.5$	10	$f=-19,\ z'=73,\ z=48,\ u=42$
191	$2.5.19$	157	$u=-7,\ v=-84$
193	$2^6.3$	10	$f^{IV}=35,\ f'''=67,\ f''=50,\ f'=-9,$ $f=81,\ z=-85$
197	$2^2.7^2$	73	$f=-14,\ u'=100,\ u=-6$
199	$2.3^2.11$	127	$z'=-37,\ z=92,\ u=-74$
211	$2.3.5.7$	142	$z=-15,\ u=71,\ v=-40$
223	$2.3.37$	10	$z=39,\ u=68$
227	2.113	—10	$u=100$
229	$2^2.3.19$	10	$f=107,\ z=94,\ u=17$
233	$2^3.29$	10	$f'=12,\ f=144,\ u=128$
239	$2.7.17$	—2	$u=-38,\ v=-107$
241	$2^4.3.5$	112	$f''=130,\ f'=30,\ f=-64,\ z=-16,$ $u=91$
251	2.5^3	224	$u''=-24.\ u'=100,\ u=113$
257	2^8	10	$f^{VI}=10,\ f^{V}=100,\ f^{IV}=-23,$ $f'''=15,\ f''=-32,\ f'=-4,\ f=16$
263	2.131	10	$u=100$
269	$2^2.67$	10	$f=-82,\ u=47$
271	$2.3^3.5$	—2	$z''=-60,\ z'=-13,\ z=-29,$ $u=-27$
277	$2^2.3.23$	199	$f=60,\ z=160,\ u=30$
281	$2^3.5.7$	117	$f'=192,\ f=53,\ u=86,\ v=165$
283	$2.3.47$	—10	$z=44,\ u=161$
293	$2^2.73$	204	$f=155,\ u=100$
307	$2.3^2.17$	—10	$z'=53,\ z=-18,\ u=9$
311	$2.5.31$	—10	$u=6,\ v=-51$
313	$2^3.3.13$	10	$f'=5,\ f=25,\ z=-99,\ u=103$
317	$2^2.79$	270	$f=114,\ u=100$
331	$2.3.5.11$	140	$z=-32,\ u=150,\ v=120$
337	$2^4.3.7$	10	$f''=191,\ f'=85,\ f=148,\ z=128,$ $u=175$
347	[illegible]	—10	$u=100$
349	$2^2.[illegible].29$	220	$f=-136,\ z=-123,\ u=-121$
353	$2^5.11$	212	$f''=10,\ f''=100,\ f'=116,\ f=42,\ u=58$
359	2.179	—10	$u=100$
367	$2.3.61$	10	$z=-84,\ u=-75$
373	$2^2.3.31$	291	$f=-104,\ z=-89,\ u=-13$
379	$2.3^3.7$	10	$z''=24,\ z'=180,\ z=-52,\ u=119$

p	$p-1$	g	ХАРАКТЕРЫ
383	2.191	10	$u=100$
389	$2^2.97$	10	$f=115,\ u=-114$
397	$2^2.3^2.11$	28	$f=63,\ z'=-85,\ z=34,\ u=-107$
401	$2^4.5^2$	211	$f''=147,\ f'=-45,\ f=20,\ u'=224,$ $u=-29$
409	$2^3.3.17$	235	$f'=31,\ f=143,\ z=53,\ u=25$
419	$2.11.19$	10	$u=152,\ v=135$
421	$2^2.3.5.7$	238	$f=29,\ z=20,\ u=-67,\ v=75$
431	$2.5.43$	−10	$u=-26,\ v=64$
433	$2^4.3^3$	10	$f''=-151,\ f'=-148,\ f=-179$ $z''=3,\ z'=27,\ z=198$
439	$2.3.73$	−10	$z=-172,\ u=-42$
443	$2.13.17$	−10	$u=188,\ v=59$
449	$2^6.7$	3	$f^{IV}=-58,\ f'''=221,\ f''=-100,$ $f'=122,\ f=67,\ u=-125$
457	$2^3.3\ 19$	380	$f'=207,\ f=-109,\ z=133,\ u=174$
461	$2^2.5.23$	10	$f=48,\ u=-110,\ v=196$
463	$2.3.7.11$	174	$z=21,\ u=-155,\ v=134$
467	2.233	−10	$u=100$
479	2.239	−10	$u=100$
487	2.3^5	10	$z^{IV}=100,\ z'''=189,\ z''=-12,$ $z'=220,\ z=232$
491	$2.5.7^2$	10	$u=-175,\ v'=-109,\ v=153$
499	$2.3.83$	10	$z=139,\ u=4$
503	2.251	10	$u=100$
509	$2^2.127$	10	$f=208,\ u=-180$
521	$2^3.5.13$	439	$f'=-206,\ f=235,\ u=25,\ v=101$
523	$2.3^2.29$	−10	$z'=94,\ z=60,\ u=226$
541	$2^2.3^3.5$	10	$f=52,\ z''=76,\ z'=225,\ z=-130,$ $u=140$
547	$2.3.7.13$	17	$z=40,\ u=9,\ v=-30$
557	$2^2.139$	41	$f=-118,\ u=100$
563	2.281	−10	$u=100$
569	$2^3.71$	420	$f'=76,\ f=86,\ u=-242$
571	$2.3.5.19$	10	$z=109,\ u=106,\ v=-300$
577	$2^6.3^2$	10	$f^{IV}=146,\ f'''=-33,\ f''=-65,$ $f'=186,\ f=-24,\ z'=321,\ z=213$
587	2.293	−10	$u=100$
593	$2^4.37$	10	$f''=-94,\ f'=-59,\ f=-77,\ u=258$
599	$2.13.23$	−10	$u=270,\ v=324$
601	$2^3.3.5^2$	506	$f'=-163,\ f=125,\ z=24,$ $u'=-111,\ u=-178$
607	$2.3.101$	575	$z=210,\ u=100$
613	$2^2.3^2.17$	32	$f=-35,\ z'=160,\ z=-66,\ u=197$
617	$2^3.7.11$	410	$f'=182,\ f=423,\ u=420,\ v=342$
619	$2.3.103$	10	$z=252,\ u=315$
631	$2.3^2.5.7$	−10	$z'=-255,\ z=43,\ u=279,\ v=-204$
641	$2^7.5$	3	$f^{V}=243,\ f^{IV}=77,\ f'''=160,\ f''=-40,$ $f'=318,\ f=-154,\ u=-284$

p	$p-1$	g	ХАРАКТЕРЫ
643	$2 \cdot 3 \cdot 107$	353	$z=177,\ u=100$
647	$2 \cdot 17 \cdot 19$	10	$u=555,\ v=287$
653	$2^2 \cdot 163$	140	$f=504,\ u=100$
659	$2 \cdot 7 \cdot 47$	10	$u=144,\ v=185$
661	$2^2 \cdot 3 \cdot 5 \cdot 11$	284	$f=555,\ z=364,\ u=406,\ v=68$
673	$2^5 \cdot 3 \cdot 7$	198	$f'''=-107,\ f''=8,\ f'=64,\ f=58,$ $z=255,\ u=-23$
677	$2^2 \cdot 13^2$	213	$f=-26,\ u'=100,\ u=-144$
683	$2 \cdot 11 \cdot 31$	−10	$u=-2,\ v=76$
691	$2 \cdot 3 \cdot 5 \cdot 23$	521	$z=253,\ u=320,\ v=20$
701	$2^2 \cdot 5^2 \cdot 7$	10	$f=135,\ u'=-118,\ u=464,\ v=361$
709	$2^2 \cdot 3 \cdot 59$	10	$f=-96,\ z=-228,\ u=385$
719	$2 \cdot 359$	−10	$u=100$
727	$2 \cdot 3 \cdot 11^2$	10	$z=-282,\ u'=375,\ u=181$
733	$2^2 \cdot 3 \cdot 61$	583	$f=380,\ z=-308,\ u=100$
739	$2 \cdot 3^2 \cdot 41$	−9	$z'=317,\ z=-321,\ u=133$
743	$2 \cdot 7 \cdot 53$	10	$u=-151,\ v=-117$
751	$2 \cdot 3 \cdot 5^3$	39	$z=72,\ u''=100,\ u'=171,\ u=460$
757	$2^2 \cdot 3^3 \cdot 7$	2	$f=87,\ z''=228,\ z'=3,\ z=27,\ u=232$
761	$2^3 \cdot 5 \cdot 19$	422	$f'=62,\ f=39,\ u=168,\ v=410$
769	$2^8 \cdot 3$	78	$f^{VI}=79,\ f^{V}=89,\ f^{IV}=231,\ f'''=300,$ $f''=27,\ f'=-40,\ f=62,\ z=408$
773	$2^2 \cdot 193$	302	$f=-317,\ u=100$
787	$2 \cdot 3 \cdot 131$	−10	$z=407,\ u=510$
797	$2^2 \cdot 199$	623	$f=-215,\ u=100$
809	$2^3 \cdot 101$	703	$f'=239,\ f=-318,\ u=100$
811	$2 \cdot 3^4 \cdot 5$	10	$z'''=184,\ z''=213,\ z'=-279,$ $z=130,\ u=212$
821	$2^2 \cdot 5 \cdot 41$	10	$f=-295,\ u=161,\ v=-37$
823	$2 \cdot 3 \cdot 137$	10	$z=-175,\ u=55$
827	$2 \cdot 7 \cdot 59$	−10	$u=270,\ v=440$
829	$2^2 \cdot 3^2 \cdot 23$	598	$f=246,\ z'=-204,\ z=125,\ u=507$
839	$2 \cdot 419$	−10	$u=100$
853	$2^2 \cdot 3 \cdot 71$	394	$f=333,\ z=220,\ u=284$
857	$2^3 \cdot 107$	10	$f'=506,\ f=-207,\ u=98$
859	$2 \cdot 3 \cdot 11 \cdot 13$	2	$z=260,\ u=-66,\ v=-86$
863	$2 \cdot 431$	10	$u=100$
877	$2^2 \cdot 3 \cdot 73$	42	$f=-151,\ z=-283,\ u=220$
881	$2^4 \cdot 5 \cdot 11$	115	$f''=-85,\ f'=177,\ f=494,\ u=268,$ $v=143$
883	$2 \cdot 3^2 \cdot 7^2$	−10	$z'=286,\ z=337,\ u'=126,\ u=707$
887	$2 \cdot 443$	10	$u=100$
907	$2 \cdot 3 \cdot 151$	539	$z=384,\ u=100$
911	$2 \cdot 5 \cdot 7 \cdot 13$	−10	$u=361,\ v=502,\ w=30$
919	$2 \cdot 3^3 \cdot 17$	−10	$z''=515,\ z'=-95,\ z=52,\ u=703$
929	$2^5 \cdot 29$	224	$f'''=269,\ f''=-101,\ f'=-18,$ $f=324,\ u=-361$
937	$2^3 \cdot 3^2 \cdot 13$	10	$f'=67,\ f=-196,\ z'=-241,\ z=322,$ $u=-308$

p	$p-1$	g	ХАРАКТЕРЫ
941	$2^2.5.47$	10	$f=-97,\ u=349,\ v=248$
947	$2.11.43$	—10	$u=185,\ v=-7$
953	$2^3.7.17$	10	$f'=156,\ f=511,\ u=508,\ v=604$
967	$2.3.7.23$	526	$z=142,\ u=97,\ v=187$
971	$2.5.97$	10	$u=-239,\ v=169$
977	$2^4.61$	10	$f''=-403,\ f'=227,\ f=-252,$ $u=-353$
983	2.491	10	$u=100$
991	$2.3^2.5.11$	—10	$z'=-70,\ z=-114,\ u=-166,$ $v=-46$
997	$2^2.3.83$	656	$f=161,\ z=304,\ u=100$
1009	$2^4.3^2.7$	11	$f''=179,\ f'=-247,\ f=469,\ z'=-87,$ $z=374,\ u=-74$
1013	$2^2.11.23$	3	$f=-45,\ u=122,\ v=-427$
1019	2.509	10	$u=100$
1021	$2^2.3.5.17$	10	$f=-374,\ z=-369,\ u=-219,$ $v=81$
1031	$2.5.103$	14	$u=264,\ v=320$
1033	$2^3.3.43$	10	$f'=231,\ f=-355,\ z=195,\ u=336$
1039	$2.3.173$	—10	$z=140,\ u=482$
1049	$2^3.131$	3	$f'=461,\ f=-426,\ u=267$
1051	$2.3.5^2.7$	10	$z=180,\ u'=-454,\ u=-380,\ v=402$
1061	$2^2.5.53$	3	$f=-103,\ u=-196,\ v=-58$
1063	$2.3^2.59$	10	$z'=-282,\ z=343,\ u=99$
1069	$2^2.3.89$	10	$f=-249,\ z=86,\ u=45$
1087	$2.3.181$	10	$z=257,\ u=-40$
1091	$2.5.109$	10	$u=93,\ v=-173$
1093	$2^2.3.7.13$	5	$f=-530,\ z=151,\ u=9,\ v=124$
1097	$2^3.137$	10	$f'=-79,\ f=-341,\ u=-326$
1103	$2.19.29$	10	$u=-354,\ v=-322$
1109	$2^2.277$	10	$f=-354,\ u=19$
1117	$2^2.3^2.31$	2	$f=214,\ z'=529,\ z=-121,\ u=331$
1123	$2.3.11.17$	—10	$z=33,\ u=-384,\ v=36$
1129	$2^3.3.47$	11	$f'=-437,\ f=168,\ z=387,\ u=338$
1151	$2.5^2.23$	—10	$u'=470,\ u=224,\ v=467$
1153	$2^7.3^2$	10	$f^{v}=-359,\ f^{iv}=-255,\ f'''=457,$ $f''=156,\ f'=123,\ f=140,\ z'=-523,$ $z=502$
1163	$2.7.83$	—10	$u=44,\ v=-118$
1171	$2.3^2.5.13$	10	$z'=-388,\ z=750,\ u=-184,\ v=166$
1181	$2^2.5.59$	10	$f=-243,\ u=-9,\ v=-205$
1187	2.593	—10	$u=100$
1193	$2^3.149$	10	$f'=362,\ f=-186,\ u=354$
1201	$2^4.3.5^2$	11	$f''=473,\ f'=343,\ f=-49,\ z=570,$ $u'=96,\ u=-139$
1213	$2^2.3.101$	2	$f=495,\ z=217,\ u=457$
1217	$2^6.19$	10	$f^{iv}=271,\ f'''=421,\ f''=-441,$ $f'=-239,\ f=-78,\ u=-549$
1223	$2.13.47$	10	$u=-554,\ v=-259$

p	$p-1$	g	ХАРАКТЕРЫ
1229	$2^2.307$	10	$f=632,\ u=168$
1231	$2.3.5.41$	3	$z=126,\ u=401,\ v=-231$
1237	$2^2.3.103$	2	$f=-546,\ z=300,\ u=385$
1249	$2^5.3.13$	7	$f'''=577,\ f''=-554,\ f'=-338,$ $f=585,\ z=-94,\ u=994$
1259	$2.17.37$	10	$u=594,\ v=-583$
1277	$2^2.11.29$	2	$f=113,\ u=135,\ v=-313$
1279	$2.3^2.71$	−10	$z'=392,\ z=504,\ n=-641$
1283	2.641	−10	$u=100$
1289	$2^3.7.23$	6	$f'=497,\ f=810,\ u=-204,\ v=-373$
1291	$2.3.5.43$	10	$z=346,\ u=-228,\ v=-299$
1297	$2^4.3^4$	10	$f''=355,\ f'=216,\ f=-36,\ z'''=9,$ $z''=729,\ z'=104,\ z=365$
1301	$2^2.5^2.13$	10	$f=51,\ u'=468,\ u=549,\ v=305$
1303	$2.3.7.31$	10	$z=-96,\ u=98,\ v=140$
1307	2.653	−10	$u=100$
1319	2.659	−10	$u=100$
1321	$2^3.3.5.11$	13	$f'=371,\ f=257,\ z=297,\ u=133,$ $v=-396,$
1327	$2.3.13.17$	10	$z=347,\ u=601,\ v=-506$
1361	$2^4.5.17$	3	$f''=574,\ f'=114\ f=-614,\ u=211,$ $v=260$
1367	2.683	10	$u=100$
1373	$2^2.7^3$	2	$f=668,\ u''=16,\ u'=226,\ u=333$
1381	$2^2.3.5.23$	10	$f=-366,\ z=-355,\ u=670,\ v=20$
1399	$2.3.233$	−10	$z=-391,\ u=-285$
1409	$2^7.11$	3	$f^{v}=-387,\ f^{iv}=415,\ f'''=327$ $f''=-155,\ f'=72,\ f=-452,$ $u=-417$
1423	$2.3^2.79$	3	$z'=-17,\ z=-644,\ u=201$
1427	$2.23.31$	−10	$u=459,\ v=-118$
1429	$2^2.3.7.17$	10	$f=-620,\ z=-665,\ u=-64,$ $v=-324$
1433	$2^3.179$	10	$f'=-507,\ f=542,\ u=961$
1439	2.719	−10	$u=100$
1447	$2.3.241$	10	$z=-705,\ u=123$
1451	$2.5^2.29$	2	$u'=321,\ u=712,\ v=347$
1453	$2^2.3.11^2$	2	$f=497,\ z=-694,\ u'=-263,\ u=131$
1459	2.3^6	3	$z^{v}=9,\ z^{iv}=-730,\ z'''=547,$ $z''=-379,\ z'=-272,\ z=339$
1471	$2.3.5.7^2$	−10	$z=-252,\ u=554,\ v'=-470,$ $v=-208$
1481	$2^3.5.37$	3	$f'=-655,\ f=-465,\ u=-98,$ $v=-264$
1483	$2.3.13.19$	2	$z=-39,\ u=191,\ v=-46$
1487	2.743	10	$u=100$
1489	$2^4.3.31$	14	$f''=-189,\ f'=-15,\ f=225,\ z=483,$ $u=132$
1493	$2^2.373$	2	$f=432,\ u=16$

p	$p-1$	g	ХАРАКТЕРЫ
1499	$2.7.107$	2	$u=-252,\ v=-105$
1511	$2.5.151$	-10	$u=534,\ v=-474$
1523	2.761	-10	$u=100$
1531	$2.3^2.5.17$	10	$z'=276,\ z=-647,\ u=102,\ v=-525$
1543	$2.3.257$	10	$z=681,\ u=136$
1549	$2^2.3^2.43$	10	$f=-88,\ z'=635,\ z=-276,\ u=507$
1553	$2^4.97$	10	$f''=251,\ f'=-672,\ f=-339,$ $u=-388$
1559	$2.19.41$	-10	$u=-531,\ v=-102$
1567	$2.3^3.29$	10	$z''=-382,\ z'=-77,\ z=-536,$ $u=775$
1571	$2.5.157$	10	$u=382,\ v=588$
1579	$2.3.263$	10	$z=-640,\ u=493$
1583	$2.7.113$	10	$u=274,\ v=-688$
1597	$2^2.3.7.19$	11	$f=610,\ z=222,\ u=-447,\ v=-414$
1601	$2^6.5^2$	3	$f^{IV}=-773,\ f'''=356,\ f''=257,$ $f'=408,\ f=-40,\ u'=-182,$ $u=442$
1607	$2.11.73$	10	$u=-605,\ v=82$
1609	$2^3.3.67$	7	$f'=630,\ f=-523,\ z=250,\ u=-468$
1613	$2^2.13.31$	3	$f=127,\ u=775,\ v=-695$
1619	2.809	10	$u=100$
1621	$2^2.3^4.5$	10	$f=166,\ z'''=135,\ z''=-303,$ $z'=-146,\ z=184,\ u=-407$
1627	$2.3.271$	3	$z=-265,\ u=729$
1637	$2^2.409$	2	$f=316,\ u=16$
1657	$2^3.3^2.23$	15	$f'=239,\ f=783,\ z'=-12,\ z=-71,$ $u=-4$
1663	$2.3.277$	10	$z=-319,\ u=537$
1667	$2.7^2.17$	-10	$u'=595,\ u=176,\ v=-544$
1669	$2^2.3\ 139$	2	$f=-220,\ z=248,\ u=758$
1693	$2^2.3^2.47$	2	$f=92,\ z'=356,\ z=-434,\ u=642$
1697	$2^5.53$	10	$f'''=-283,\ f''=330,\ f'=292\ f=414,$ $u=629$
1699	$2.3.283$	3	$z=397,\ u=729$
1709	$2^2.7.61$	10	$f=-390,\ u=223,\ v=305$
1721	$2^3.5.43$	3	$f'=-232,\ f=473,\ u=399,\ =-328$
1723	$2.3.7.41$	3	$z=-42,\ u=555,\ v=-261$
1733	$2^2.433$	2	$f=-410,\ u=16$
1741	$2^2.3.5.29$	10	$f=59,\ z=-357,\ u=-277,\ v=-20$
1747	$2.3^2.97$	2	$z'=472,\ z=371,\ u=94$
1753	$2^3.3.73$	7	$f'=489,\ f=713,\ z=-183,\ u=348$
1759	$2.3.293$	-10	$z=-509,\ u=-871$
1777	$2^4.3.37$	10	$f''=865,\ f'=108,\ f=-775,\ z=629,$ $u=-32$
1783	$2.3^4.11$	10	$z'''=855,\ z''=-709,\ z'=-525$ $z=-194,\ u=367$
1787	$2.19.47$	-10	$u=109,\ v=90$
1789	$2^2.3.149$	10	$f=-724,\ z=-153,\ u=812$

p	$p-1$	g	ХАРАКТЕРЫ
1801	$2^3.3^2.5^2$	11	$f'=524,\ f=824,\ z'=144,\ z=-74$ $u'=256,\ u=350$
1811	$2.5.181$	10	$u=-771,\ v=279$
1823	2.911	10	$u=100$
1831	$2.3.5.61$	7	$z=-673,\ u=481,\ v=-588$
1847	$2.13.71$	10	$u=-459,\ v=921$
1861	$2^2.3.5.31$	10	$f=61,\ z=-455,\ u=758,\ v=-87$
1867	$2.3.311$	-10	$z=834,\ u=-712$
1871	$2.5.11.17$	-10	$u=267,\ v=-323,\ w=3$
1873	$2^4.3^2.13$	10	$f''=-780,\ f'=-325,\ f=737$ $z'=-763,\ z=114,\ u=917$
1877	$2^2.7.67$	2	$f=137,\ u=-747,\ v=55$
1879	$2.3.313$	-2	$z=-489,\ u=64$
1889	$2^5.59$	3	$f'''=-433,\ f''=478,\ f'=-85,$ $f=-331,\ u=-170$
1901	$2^2.5^2.19$	2	$f=218,\ u'=155,\ u=-775,\ v=-668$ $u=100$
1907	2.953	-10	
1913	$2^3.239$	10	$f'=-922,\ f=712,\ u=-162$ $u=-114,\ v=-907$
1931	$2.5.193$	2	
1933	$2^2.3.7.23$	5	$f=-598,\ z=-592,\ u=-121,$ $v=325$
1949	$2^2.487$	10	$f=589,\ u=255$
1951	$2.3.5^2.13$	3	$z=76,\ u'=564,\ u=955,\ v=340$
1973	$2^2.17.29$	2	$f=259,\ u=-25,\ v=224$
1979	$2.23.43$	10	$u=-935,\ v=-928$
1987	$2.3.331$	2	$z=647,\ u=64$
1993	$2^3.3.83$	5	$f'=960,\ f=834,\ z=-313,\ u=-27$ $f=-412,\ u=16$
1997	$2^2.499$	2	
1999	$2.3^3.37$	-10	$z''=920,\ z'=-461,\ z=808,\ u=189$

E.

Таблица разложенія корня квадратнаго изъ цѣлаго числа въ непрерывную дробь.

Согласно обозначенію стр. 139 періодъ непрерывной дроби заключенъ въ скобки, ломанныя же скобки пропущены.

$\sqrt{2}$	1, (2)	$\sqrt{26}$	5, (10)
$\sqrt{3}$	1, (1, 2)	$\sqrt{27}$	5, (5, 10)
$\sqrt{5}$	2, (4)	$\sqrt{28}$	5, (3, 2, 3, 10)
$\sqrt{6}$	2, (2, 4)	$\sqrt{29}$	5, (2, 1, 1, 2, 10)
$\sqrt{7}$	2, (1, 1, 1, 4)	$\sqrt{30}$	5, (2, 10)
$\sqrt{8}$	2, (1, 4)	$\sqrt{31}$	5, (1, 1, 3, 5, 3, 1, 1, 10)
$\sqrt{10}$	3, (6)	$\sqrt{32}$	5, (1, 1, 1, 10)
$\sqrt{11}$	3, (3, 6)	$\sqrt{33}$	5, (1, 2, 1, 10)
$\sqrt{12}$	3, (2, 6)	$\sqrt{34}$	5, (1, 4, 1, 10)
$\sqrt{13}$	3, (1, 1, 1, 1, 6)	$\sqrt{35}$	5, (1, 10)
$\sqrt{14}$	3, (1, 2, 1, 6)	$\sqrt{37}$	6, (12)
$\sqrt{15}$	3, (1, 6)	$\sqrt{38}$	6, (6, 12)
$\sqrt{17}$	4, (8)	$\sqrt{39}$	6, (4, 12)
$\sqrt{18}$	4, (4, 8)	$\sqrt{40}$	6, (3, 12)
$\sqrt{19}$	4, (2, 1, 3, 1, 2, 8)	$\sqrt{41}$	6, (2, 2, 12)
$\sqrt{20}$	4, (2, 8)	$\sqrt{42}$	6, (2, 12)
$\sqrt{21}$	4, (1, 1, 2, 1, 1, 8)	$\sqrt{43}$	6, (1, 1, 3, 1, 5, 1, 3, 1, 1, 12)
$\sqrt{22}$	4, (1, 2, 4, 2, 1, 8)	$\sqrt{44}$	6, (1, 1, 1, 2, 1, 1, 1, 12)
$\sqrt{23}$	4, (1, 3, 1, 8)	$\sqrt{45}$	6, (1, 2, 2, 2, 1, 12)
$\sqrt{24}$	4, (1, 8)	$\sqrt{46}$	6, (1, 3, 1, 1, 2, 6, 2, 1, 1, 3, 1, 12)

$\sqrt{47}$	6, (1, 5, 1, 12)
$\sqrt{48}$	6, (1, 12)
$\sqrt{50}$	7, (14)
$\sqrt{51}$	7, (7, 14)
$\sqrt{52}$	7, (4, 1, 2, 1, 4, 14)
$\sqrt{53}$	7, (3, 1, 1, 3, 14)
$\sqrt{54}$	7, (2, 1, 6, 1, 2, 14)
$\sqrt{55}$	7, (2, 2, 2, 14)
$\sqrt{56}$	7, (2, 14)
$\sqrt{57}$	7, (1, 1, 4, 1, 1, 14)
$\sqrt{58}$	7, (1, 1, 1, 1, 1, 1, 14)
$\sqrt{59}$	7, (1, 2, 7, 2, 1, 14)
$\sqrt{60}$	7, (1, 2, 1, 14)
$\sqrt{61}$	7, (1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14)
$\sqrt{62}$	7, (1, 6, 1, 14)
$\sqrt{63}$	7, (1, 14)
$\sqrt{65}$	8, (16)
$\sqrt{66}$	8, (8, 16)
$\sqrt{67}$	8, (5, 2, 1, 1, 7, 1, 1, 2, 5, 16)
$\sqrt{68}$	8, (4, 16)
$\sqrt{69}$	8, (3, 3, 1, 4, 1, 3, 3, 16)
$\sqrt{70}$	8, (2, 1, 2, 1, 2, 16)
$\sqrt{71}$	8, (2, 2, 1, 7, 1, 2, 2, 16)
$\sqrt{72}$	8, (2, 16)
$\sqrt{73}$	8, (1, 1, 5, 5, 1, 1, 16)
$\sqrt{74}$	8, (1, 1, 1, 1, 16)
$\sqrt{75}$	8, (1, 1, 1, 16)
$\sqrt{76}$	8, (1, 2, 1, 1, 5, 4, 5, 1, 1, 2, 1, 16)
$\sqrt{77}$	8, (1, 3, 2, 3, 1, 16)
$\sqrt{78}$	8, (1, 4, 1, 16)
$\sqrt{79}$	8, (1, 7, 1, 16)
$\sqrt{80}$	8, (1, 16)
$\sqrt{82}$	9, (18)
$\sqrt{83}$	9, (9, 18)
$\sqrt{84}$	9, (6, 18)
$\sqrt{85}$	9, (4, 1, 1, 4, 18)
$\sqrt{86}$	9, (3, 1, 1, 1, 8, 1, 1, 1, 3, 18)
$\sqrt{87}$	9, (3, 18)
$\sqrt{88}$	9, (2, 1, 1, 1, 2, 18)
$\sqrt{89}$	9, (2, 3, 3, 2, 18)
$\sqrt{90}$	9, (2, 18)
$\sqrt{91}$	9, (1, 1, 5, 1, 5, 1, 1, 18)
$\sqrt{92}$	9, (1, 1, 2, 4, 2, 1, 1, 18)
$\sqrt{93}$	9, (1, 1, 1, 4, 6, 4, 1, 1, 1, 18)
$\sqrt{94}$	9, (1, 2, 3, 1, 1, 5, 1, 8, 1, 5, 1, 1, 3, 2, 1, 18)
$\sqrt{95}$	9, (1, 2, 1, 18)
$\sqrt{96}$	9, (1, 3, 1, 18)
$\sqrt{97}$	9, (1, 5, 1, 1, 1, 1, 1, 1, 5, 1, 18)
$\sqrt{98}$	9, (1, 8, 1, 18)
$\sqrt{99}$	9, (1, 18)
$\sqrt{101}$	10, (20)
$\sqrt{102}$	10, (10, 20)
$\sqrt{103}$	10, (6, 1, 2, 1, 1, 9, 1, 1, 2, 1, 6, 20)
$\sqrt{104}$	10, (5, 20)
$\sqrt{105}$	10, (4, 20)
$\sqrt{106}$	10, (3, 2, 1, 1, 1, 1, 2, 3, 20)
$\sqrt{197}$	10, (2, 1, 9, 1, 2, 20)
$\sqrt{108}$	10, (2, 1, 1, 4, 1, 1, 2, 20)
$\sqrt{109}$	10, (2, 3, 1, 2, 4, 1, 6, 6, 1, 4, 2, 1, 3, 2, 20)
$\sqrt{110}$	10, (2, 20)
$\sqrt{111}$	10, (1, 1, 6, 1, 1, 20)
$\sqrt{112}$	10, (1, 1, 2, 1, 1, 20)
$\sqrt{113}$	10, (1, 1, 1, 2, 2, 1, 1, 1, 20)
$\sqrt{114}$	10, (1, 2, 10, 2, 1, 20)
$\sqrt{115}$	10, (1, 2, 1, 1, 1, 1, 1, 2, 1, 20)
$\sqrt{116}$	10, (1, 3, 2, 1, 4, 1, 2, 3, 1, 20)
$\sqrt{117}$	10, (1, 4, 2, 4, 1, 20)
$\sqrt{118}$	10, (1, 6, 3, 2, 10, 2, 3, 6, 1, 20)
$\sqrt{119}$	10, (1, 9, 1, 20)
$\sqrt{120}$	10, (1, 20)

F.

Таблица наименьшихъ рѣшеній Пеллева уравненія $t^2 - Du^2 = 1$.

D	u	t	D	u	t
2	2	3	28	24	127
3	1	2	29	1820	9801
5	4	9	30	2	11
6	2	5	31	273	1520
7	3	8	32	3	17
8	1	3	33	4	23
10	6	19	34	6	35
11	3	10	35	1	6
12	2	7	37	12	73
13	180	649	38	6	37
14	4	15	39	4	25
15	1	4	40	3	19
17	8	33	41	320	2049
18	4	17	42	2	13
19	39	170	43	531	3482
20	2	9	44	30	199
21	12	55	45	24	161
22	42	197	46	3588	24335
23	5	24	47	7	48
24	1	5	48	1	7
26	10	51	50	14	99
27	5	26	51	7	50

D	u	t	D	u	t
52	90	649	76	6630	57799
53	9100	66249	77	40	351
54	66	485	78	6	53
55	12	89	79	9	80
56	2	15	80	1	9
57	20	151	82	18	163
58	2574	19603	83	9	82
59	69	530	84	6	55
60	4	31	85	30996	285769
61	226153980	1766319049	86	1122	10405
62	8	93	87	3	28
63	1	8	88	21	197
65	16	129	89	53000	500001
66	8	65	90	2	19
67	5967	48842	91	165	1574
68	4	33	92	120	1151
69	936	7775	93	1260	12151
70	30	251	94	221064	2143295
71	413	3480	95	4	39
72	2	17	96	5	49
73	267000	2281249	97	6377352	62809633
74	430	3699	98	10	99
75	3	26	99	1	19

$$D = 103 \begin{cases} t = 227528 \\ u = 22419 \end{cases} \qquad D = 109 \begin{cases} t = 158070671986249 \\ u = 15140424455100 \end{cases}$$

$$D = 113 \begin{cases} t = 1204353 \\ u = 113296 \end{cases} \qquad D = 157 \begin{cases} t = 466987287318 49 \\ u = 37269642922 20 \end{cases}$$

G.

Таблица разложенія простыхъ чиселъ вида $4m+1$.

5	$1^2 + 2^2$	229	$2^2 + 15^2$	457	$4^2 + 21^2$
13	$2^2 + 3^2$	233	$8^2 + 13^2$	461	$10^2 + 19^2$
17	$1^2 + 4^2$	241	$4^2 + 15^2$	509	$5^2 + 22^2$
29	$2^2 + 5^2$	257	$1^2 + 16^2$	521	$11^2 + 20^2$
37	$1^2 + 6^2$	269	$10^2 + 13^2$	541	$10^2 + 21^2$
41	$4^2 + 5^2$	277	$9^2 + 14^2$	557	$14^2 + 19^2$
53	$2^2 + 7^2$	281	$5^2 + 16^2$	569	$13^2 + 20^2$
61	$5^2 + 6^2$	293	$2^2 + 17^2$	577	$1^2 + 24^2$
73	$3^2 + 8^2$	313	$12^2 + 13^2$	593	$8^2 + 23^2$
89	$5^2 + 8^2$	317	$11^2 + 14^2$	601	$5^2 + 24^2$
97	$4^2 + 9^2$	337	$9^2 + 16^2$	613	$17^2 + 18^2$
101	$1^2 + 10^2$	349	$5^2 + 18^2$	617	$16^2 + 19^2$
109	$3^2 + 10^2$	353	$8^2 + 17^2$	641	$4^2 + 25^2$
113	$7^2 + 8^2$	373	$7^2 + 18^2$	653	$13^2 + 22^2$
137	$4^2 + 11^2$	389	$10^2 + 17^2$	661	$6^2 + 25^2$
149	$7^2 + 10^2$	397	$6^2 + 19^2$	673	$12^2 + 23^2$
157	$6^2 + 11^2$	401	$1^2 + 20^2$	677	$1^2 + 26^2$
173	$2^2 + 13^2$	409	$3^2 + 20^2$	701	$5^2 + 26^2$
181	$9^2 + 10^2$	421	$14^2 + 15^2$	709	$15^2 + 22^2$
193	$7^2 + 12^2$	433	$12^2 + 17^2$	733	$2^2 + 27^2$
197	$1^2 + 14^2$	449	$7^2 + 20^2$	757	$9^2 + 26^2$

761	$19^2 + 20^2$	1129	$20^2 + 27^2$	1601	$1^2 + 40^2$
769	$12^2 + 25^2$	1153	$8^2 + 33^2$	1609	$3^2 + 40^2$
773	$17^2 + 22^2$	1181	$5^2 + 34^2$	1613	$13^2 + 38^2$
797	$11^2 + 26^2$	1193	$13^2 + 32^2$	1621	$10^2 + 39^2$
809	$5^2 + 28^2$	1201	$24^2 + 25^2$	1637	$26^2 + 31^2$
821	$14^2 + 25^2$	1213	$22^2 + 27^2$	1657	$19^2 + 36^2$
829	$10^2 + 27^2$	1217	$16^2 + 31^2$	1669	$15^2 + 38^2$
853	$18^2 + 23^2$	1229	$2^2 + 35^2$	1693	$18^2 + 37^2$
857	$4^2 + 29^2$	1237	$9^2 + 34^2$	1697	$4^2 + 41^2$
877	$6^2 + 29^2$	1249	$15^2 + 32^2$	1709	$22^2 + 35^2$
881	$16^2 + 25^2$	1277	$11^2 + 34^2$	1721	$11^2 + 40^2$
929	$20^2 + 23^2$	1289	$8^2 + 35^2$	1733	$17^2 + 38^2$
937	$19^2 + 24^2$	1297	$1^2 + 36^2$	1741	$29^2 + 30^2$
941	$10^2 + 29^2$	1301	$25^2 + 26^2$	1753	$27^2 + 32^2$
953	$13^2 + 28^2$	1321	$5^2 + 36^2$	1777	$16^2 + 39^2$
977	$4^2 + 31^2$	1361	$20^2 + 31^2$	1789	$5^2 + 42^2$
997	$6^2 + 31^2$	1373	$2^2 + 37^2$	1801	$24^2 + 35^2$
1009	$15^2 + 28^2$	1381	$15^2 + 34^2$	1861	$30^2 + 21^2$
1013	$22^2 + 23^2$	1409	$25^2 + 28^2$	1873	$28^2 + 33^2$
1021	$11^2 + 30^2$	1429	$23^2 + 30^2$	1877	$14^2 + 41^2$
1033	$3^2 + 32^2$	1433	$8^2 + 37^2$	1889	$17^2 + 40^2$
1049	$5^2 + 32^2$	1453	$3^2 + 38^2$	1901	$26^2 + 35^2$
1061	$10^2 + 31^2$	1481	$16^2 + 35^2$	1913	$8^2 + 43^2$
1069	$13^2 + 30^2$	1489	$20^2 + 33^2$	1933	$13^2 + 42^2$
1093	$2^2 + 33^2$	1493	$7^2 + 38^2$	1949	$10^2 + 43^2$
1097	$16^2 + 29^2$	1549	$18^2 + 35^2$	1973	$23^2 + 38^2$
1109	$22^2 + 25^2$	1553	$23^2 + 32^2$	1993	$12^2 + 43^2$
1117	$21^2 + 26^2$	1597	$21^2 + 34^2$	1997	$29^2 + 34^2$

H.

Таблица Cayley

наименьшихъ нечетныхъ рѣшеній уравненія

$$x^2 - Dy^2 = \pm 4\,, \quad D \equiv 5 \pmod 8$$

D	$\pm$	x	y	D	$\pm$	x	y	D	$\pm$	x	y
5	−	1	1	341	+	277	15	677		imposs.	
13	−	3	1	349		imposs.		685	−	759	29
21	+	5	1	357	+	19	1	693	+	79	3
29	−	5	1	365	−	19	1	701		imposs.	
37		imposs.		373		imposs.		709		imposs.	
45	+	7	1	381		imposs.		717	+	241	9
53	−	7	1	389		imposs.		725	+	27	1
61	−	39	5	397	−	3447	173	733	−	27	1
69	+	25	3	405		imposs.		741	+	245	9
77	+	9	1	413	+	61	3	749	+	12945	473
85	−	9	1	421	−	444939	21685	757		imposs.	
93	+	29	3	429	+	145	7	765	+	83	3
101		imposs.		437	+	21	1	773	−	139	5
109	−	261	25	445	−	21	1	781		imposs.	
117	+	11	1	453	+	149	7	789	+	31825	1133
125	−	11	1	461	−	365	17	797	−	367	13
133	+	173	15	469	+	65	3	805	+	1447	51
141		imposs.		477	+	2599	119	813		imposs.	
149	−	61	5	485		imposs.		821	−	16189	565
157	−	213	17	493	−	111	5	829		imposs.	
165	+	13	1	501	+	28225	1261	837	+	29	1
173	−	13	1	509	−	925	41	845	−	29	1
181	−	1305	97	517	+	10573	465	853	−	27483	941
189		imposs.		525	+	23	1	861	+	1027	35
197		imposs.		533	−	23	1	869	+	49377	1675
205	+	43	3	541	−	1396425	60037	877		imposs.	
213	+	73	5	549	+	1523	65	885		imposs.	
221	+	15	1	557		imposs.		893	+	2301	77
229	−	15	1	565	−	309	13	901		imposs.	
237	+	77	5	573		imposs.		909		imposs.	
245	+	47	3	581	+	6725	279	917	+	1181	39
253	+	1861	117	589	+	4359377	179625	925		imposs.	
261	+	727	45	597	+	9749	399	933		imposs.	
269		imposs		605	+	123	5	941	−	1135	37
277	−	2613	157	613	−	98763	3989	949	−	32685	1061
285	+	17	1	621	+	25	1	957	+	31	1
293	−	17	1	629	−	25	1	965	−	31	1
301	+	22745	1311	637	+	14159	561	973		imposs.	
309	+	5045	287	645	+	127	5	981	+	68123	2175
317	−	89	5	653	−	1661	65	989	+	103245	3283
325		imposs.		661	−	1789539	69605	997		imposs.	
333		imposs.		669	+	305285	11803				

I.

Линейные дѣлители квадратичной формы $x^2 + Dy^2$.

D	
1	$4z \pm$ 1.
2	$8z \pm$ 1, 3.
3	$12z \pm$ 1, 7.
5	$20z \pm$ 1, 3, 7, 9.
6	$24z \pm$ 1, 5, 7, 11.
7	$28z \pm$ 1, 9, 11, 15, 23, 25.
10	$40z \pm$ 1, 7, 9, 11, 13, 19, 23, 37.
11	$44z \pm$ 1, 3, 5, 9, 15, 23, 25, 27, 31, 37.
13	$52z \pm$ 1, 7, 9, 11, 15, 17, 19, 25, 29, 31, 47, 49.
14	$56z \pm$ 1, 3, 5, 9, 13, 15, 19, 23, 25, 27, 39, 45.
15	$60z \pm$ 1, 17, 19, 23, 31, 47, 49, 53.
17	$68z \pm$ 1, 3, 7, 9, 11, 13, 21, 23, 25, 27, 31, 33, 39, 49, 53, 63.
19	$76z \pm$ 1, 5 7, 9, 11, 17, 23, 25, 35, 39, 43, 45, 47, 49, 55, 61, 63, 73.
21	$84z \pm$ 1, 5, 11, 17, 19, 23, 25, 31, 37, 41, 55, 71.
22	$88z \pm$ 1, 9, 13, 15, 19, 21, 23, 25, 29, 31, 35, 43, 47, 49, 51, 61, 71, 81, 83, 85.
23	$92z \pm$ 1, 3, 9, 13, 25, 27, 29, 31, 35, 39, 41, 47, 49, 55, 59, 71, 73, 75, 77, 81, 85, 87.
26	$104z \pm$ 1, 3, 5, 7, 9, 15, 17, 21, 25, 27, 31, 35, 37, 43, 45, 47, 49, 51, 63, 71, 75, 81, 85, 93.
29	$116z \pm$ 1, 3, 5, 9, 11, 13, 15, 19, 25, 27, 31, 33, 39, 43, 45, 47, 49, 53, 55, 57, 65, 75, 79, 81, 93, 95, 99, 109.
30	$120z \pm$ 1, 11, 13, 17, 23, 29, 31, 37, 43, 47, 49, 59, 69, 79, 101, 113.
31	$124z \pm$ 1, 5, 7, 9, 19, 25, 33, 35, 39, 41, 45, 47, 49, 51, 59, 63, 67, 69, 71, 81, 87, 95, 97, 101, 103, 107, 109, 111, 113, 121.
33	$132z \pm$ 1, 7, 17, 19, 23, 25, 29, 37, 41, 43, 47, 49, 59, 65, 71, 79, 97, 101, 119, 127.
34	$136z \pm$ 1, 5, 7, 9, 19, 23, 25, 29, 31, 33, 35, 37, 39, 43, 45, 49, 59, 61, 63, 67, 71, 79, 81, 83, 89, 95, 109, 115, 121, 123, 125, 133.
35	$140z \pm$ 1, 3, 9, 11, 13, 17, 27, 29, 33, 39, 47, 51, 71, 73, 79, 81, 83, 87, 97, 99, 103, 109, 117, 121.
37	$148z \pm$ 1, 9, 15, 19, 21, 23, 25, 31, 33, 35, 39, 41, 43, 49, 51, 53, 55, 59, 65, 73, 77, 79, 81, 85, 87, 91, 101, 103, 119, 121, 131, 135, 137, 141, 143, 145.
38	$152z \pm$ 1, 3, 7, 9, 13, 17, 21, 23, 25, 27, 29, 37, 39, 47, 49, 51, 53, 55, 59, 63, 67, 69, 73, 75, 81, 87, 91, 107, 109, 111, 117, 119, 121, 137, 141, 147.
39	$156z \pm$ 1, 5, 11, 25, 41, 43, 47, 49, 55, 59, 61, 71, 79, 83, 89, 103, 119, 121 125, 127, 133, 137, 139, 149.
41	$164z \pm$ 1, 3, 5, 7, 9, 11, 15, 19, 21, 25, 27, 33, 35, 37, 45, 47, 49, 55, 57, 61, 63, 67, 71, 73, 75, 77, 79, 81, 95, 99, 105, 111, 113, 121, 125, 133, 135, 141, 147, 151.
42	$168z \pm$ 1, 13, 17, 23, 25, 29, 31, 41, 43, 53, 55, 59, 61, 67, 71, 83, 89, 95, 103, 121, 131, 149, 157, 163.
43	$172z \pm$ 1, 9, 11, 13, 15, 17, 21, 23, 25, 31, 35, 41, 47, 49, 53, 57, 59, 67, 79, 81, 83, 87, 95, 97, 99, 101, 103, 107, 109, 111, 117, 121, 127, 133, 135, 139, 143, 145, 153, 165, 167, 169.
46	$184z \pm$ 1, 5, 9, 11, 19, 21, 25, 31, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 61, 67, 71, 73, 81, 83, 87, 91, 95, 99, 105, 107, 109, 119, 121, 125, 127, 149, 151, 155, 157, 167, 169, 171, 177, 181.
47	$188z \pm$ 1, 3, 7, 9, 17, 21, 25, 27, 37, 49, 51, 53, 55, 59, 61, 63, 65, 71, 75, 79, 81, 83, 89, 95, 97, 101, 103, 111, 115, 119, 121, 131, 143, 145, 147, 149, 153, 155, 157, 159, 165, 169, 173, 175, 177, 183.

J.

Линейные дѣлители квадратичной формы $x^2 - Dy^2$.

D	
2	$8z +$ 1, 7.
3	$12z +$ 1, 11.
5	$20z +$ 1, 9, 11, 19.
6	$24z +$ 1, 5, 19, 23.
7	$28z +$ 1, 3, 9, 19, 25, 27.
10	$40z +$ 1, 3, 9, 13, 27, 31, 37, 39.
11	$44z +$ 1, 5, 7, 9, 19, 25, 35, 37, 39, 43.
13	$52z +$ 1, 3, 9, 17, 23, 25, 27, 29, 35, 43, 49, 51.
14	$56z +$ 1, 5, 9, 11, 13, 25, 31, 43, 45, 47, 51, 55.
15	$60z +$ 1, 7, 11, 17, 43, 49, 53, 59.
17	$68z +$ 1, 9, 13, 15, 19, 21, 25, 33, 35, 43, 47, 49, 53, 55, 59, 67.
19	$76z +$ 1, 3, 5, 9, 15, 17, 25, 27, 31, 45, 49, 51, 59, 61, 67, 71, 73, 75.
21	$84z +$ 1, 5, 17, 25, 37, 41, 43, 47, 59, 67, 79, 83.
22	$88z +$ 1, 3, 7, 9, 13, 21, 25, 27, 29, 39, 49, 59, 61, 63, 67, 75, 79, 81, 85, 87.
23	$62z +$ 1, 7, 9, 11, 13, 15, 19, 25, 29, 41, 43, 49, 51, 63, 67, 73, 77, 79, 81, 83, 85, 91.
26	$104z +$ 1, 5, 9, 11, 17, 19, 21, 23, 25, 37, 45, 49, 55, 59, 67, 79, 81, 83, 85, 87, 93, 95, 99, 103.
29	$116z +$ 1, 5, 7, 9, 13, 23, 25, 33, 35, 45, 49, 51, 53, 57, 59, 63, 65, 67, 71, 81, 83, 91, 93, 103, 107, 109, 111, 115.
30	$120z +$ 1, 7, 13, 17, 19, 29, 37, 49, 71, 83, 91, 101, 103, 107, 113, 119.
31	$124z +$ 1, 3, 5, 9, 11, 15, 23, 25, 27, 33, 41, 43, 45, 49, 55, 69, 75, 79, 81, 83, 91, 97, 99, 101, 109, 113, 115, 119, 121, 123.
33	$132z +$ 1, 17, 25, 29, 31, 35, 37, 41, 49, 65, 67, 83, 91, 95, 97, 101, 103, 107, 115, 131.
34	$136z +$ 1, 3, 5, 9, 11, 15, 25, 27, 29, 33, 37, 45, 47, 49, 55, 61, 75, 81, 87, 89, 91, 99, 103, 107, 109, 111, 121, 125, 127, 131, 133, 135.
35	$140z +$ 1, 9, 13, 17, 19, 23, 29, 31, 33, 43, 59, 67, 73, 81, 97, 107, 109, 111, 117, 121, 123, 127, 131, 139.
37	$148z +$ 1, 3, 7, 9, 11, 21, 25, 27, 33, 41, 47, 49, 53, 63, 65, 67, 71, 73, 75, 77, 81, 83, 85, 95, 99, 101, 107, 115, 121, 123 127, 137, 139, 141, 145, 147.
38	$152z +$ 1, 9, 11, 13, 15, 17, 23, 25, 29, 31, 35, 37, 43, 49, 53, 69, 71, 73, 79, 81, 83, 99, 103, 109, 115, 117, 121, 123, 127, 131, 135, 137, 139, 141, 143, 151.
39	$156z +$ 1, 5, 7, 19, 23, 25, 31, 35, 41, 49, 61, 67, 89, 95, 107, 115, 121, 125, 131, 133, 137, 149, 151, 155.
41	$164z +$ 1, 5, 9, 21, 23, 25, 31, 33, 37, 39, 43, 45, 49, 51, 57, 59, 61, 73, 77, 81, 83, 87, 91, 103, 105, 107, 113, 115, 119, 121, 125, 127, 131, 133, 139, 141, 143, 155, 159, 163.
42	$168z +$ 1, 11, 13, 17, 19, 25, 29, 41, 47, 53, 61, 79, 89, 107, 115, 121, 127, 139, 143, 149, 151, 155, 157, 167.
43	$172z +$ 1, 3, 7, 9, 13, 17, 19, 21, 25, 27, 39, 41, 49, 51, 53, 55, 57, 63, 71, 75, 81, 91, 97, 101, 109, 115, 117, 119, 121, 123, 131, 133, 145, 147, 151, 153, 155, 159, 163, 165, 169, 171.
46	$184z +$ 1, 3, 5, 7, 9, 15, 21, 25, 27, 35, 37, 41, 45, 49, 53, 59, 61, 63, 73, 75, 79, 81, 103, 105, 109, 111, 121, 123, 125, 131, 135, 139, 143, 147, 149, 157, 159, 163, 169, 175, 177, 179, 181, 183.
47	$188z +$ 1, 9, 11, 15, 17, 19, 21, 23, 25, 31, 35, 37, 39, 43, 49, 53, 61, 65, 67, 81, 87, 89, 91, 97, 99, 101, 107, 121, 123, 127, 135, 139, 145, 149, 151, 153, 157, 163, 165, 167, 169, 171, 173, 177, 179, 187.

K.

Таблица значеній выраженія $W(p)$

$\frac{2^{p-1}-1}{p} \equiv W(p) \pmod{p}$ (p нечетное простое число).

p	$W(p)$	p	$W(p)$	p	$W(p)$
3	1	131	17	307	$294=2^4 . 19$
5	3	137	53	311	$175=5^2 . 7$
7	2	139	$30=2 . 3 . 5$	313	$120=2^3 . 3 . 5$
11	5	149	$96=2^5 . 3$	317	$175=5^2 . 7$
13	3	151	$56=2^3 . 7$	331	139
17	13	157	$82=2 . 41$	337	$153=3^2 . 17$
19	3	163	67	347	149
23	17	167	47	349	$325=5^2 . 13$
29	1	173	3	353	157
31	$6=2 . 3$	179	$50=2 . 5^2$	359	$58=2 . 29$
37	$26=2 . 13$	181	$148=2^2 . 37$	367	$339=3 . 113$
41	23	191	$50=2 . 5^2$	373	$204=2^2 . 3 . 17$
43	$25=5^2$	197	$175=5^2 . 7$	379	2
47	$44=2^2 . 11$	199	$135=3^3 . 5$	383	$196=2^2 . 7^2$
53	$36=2^2 . 3^2$	211	109	389	$134=2 . 67$
59	$8=2^3$	223	$189=3^3 . 7$	397	$390=2 . 3 . 5 . 13$
61	$36=2^2 . 3^2$	227	$201=3 . 67$	401	$339=3 . 113$
67	$10=2 . 5$	229	$68=2^2 . 17$	409	$156=2^2 . 3 . 13$
71	2	233	7	419	$318=2 . 3 . 53$
73	$56=2^3 . 7$	239	$26=2 . 13$	421	353
79	19	241	$142=2 . 71$	431	$200=2^3 . 5^2$
83	$48=2^4 . 3$	251	$247=13 . 19$	433	197
89	$6=2 . 3$	257	$225=3^2 . 5^2$	439	$39=3 . 13$
97	$57=3 . 19$	263	$128=2^7$	443	$141=3 . 47$
101	$92=2^2 . 23$	269	$260=2^2 . 5 . 13$	449	245
103	59	271	109	457	$255=5 . 3 . 17$
107	13	277	$70=2 . 5 . 7$	461	$417=3 . 139$
109	67	281	$74=2 . 37$	463	$150=2 . 3 . 5^2$
113	83	283	$58=2 . 29$	467	$122=2 . 61$
127	$18=2 . 3^2$	293	$78=2 . 3 . 13$	479	$252=2^2 . 3^2 . 7$

p	$W(p)$	p	$W(p)$	p	$W(p)$
487	$85=5\cdot17$	653	$399=3\cdot7\cdot19$	829	$625=5^4$
491	$35=5\cdot7$	659	$166=2\cdot83$	839	$292=2^2\cdot73$
499	$230=2\cdot5\cdot23$	661	$471=3\cdot157$	853	$642=2\cdot3\cdot107$
503	$57=3\cdot19$	673	$562=2\cdot281$	857	$176=2^4\cdot11$
509	$316=2^2\cdot79$	677	$324=2^2\cdot3^4$	859	277
521	$121=11^2$	683	$497=7\cdot71$	863	$185=5\cdot37$
523	$406=2\cdot7\cdot29$	691	149	877	$384=2^7\cdot3$
541	191	701	$315=3^2\cdot5\cdot7$	881	$294=2\cdot3\cdot7^2$
547	$255=3\cdot5\cdot17$	709	$440=2^3\cdot5\cdot11$	883	$303=3\cdot101$
557	$226=2\cdot113$	719	673	887	$807=3\cdot269$
563	$146=2\cdot73$	727	$530=2\cdot5\cdot53$	907	$898=2\cdot449$
569	$18=2\cdot3^2$	733	$507=3\cdot169$	911	$891=3^4\cdot11$
571	$559=13\cdot43$	739	$38=2\cdot19$	919	311
577	$452=2^2\cdot113$	743	$40=2^3\cdot5$	929	$115=5\cdot23$
587	$303=3\cdot101$	751	$581=7\cdot83$	937	$591=3\cdot197$
593	491	757	$62=2\cdot31$	941	$291=3\cdot97$
599	$148=2^2\cdot37$	761	$582=2\cdot3\cdot97$	947	$892=2^2\cdot223$
601	$315=3^2\cdot5\cdot7$	769	$455=5\cdot7\cdot13$	953	$202=2\cdot101$
607	$324=2^2\cdot3^4$	773	$118=2\cdot59$	967	$825=5^2\cdot3\cdot11$
613	29	787	$304=2^4\cdot19$	971	293
617	$417=3\cdot139$	797	$333=3\cdot2^3\cdot7$	977	$198=2\cdot9\cdot11$
619	$554=2\cdot277$	809	$232=2^3\cdot29$	983	$390=2\cdot5\cdot3\cdot13$
631	$527=17\cdot31$	811	$632=2^3\cdot79$	991	$177=3\cdot59$
641	$402=2\cdot3\cdot67$	821	$723=3\cdot241$	997	$735=3\cdot5\cdot7^2$
643	$104=2^3\cdot13$	823	$46=2\cdot23$		
647	$50=2\cdot5^2$	827	$154=2\cdot11\cdot7$		

L.

Величина періода десятичной дроби равной $\frac{1}{m}$ [1]).

Значеніе m.	Величина періода.	Значеніе m.	Величина періода.	Значеніе m.	Величина періода.	Значеніе m.	Величина періода	Значеніе m.	Величина періода.	Значеніе m	Величина періода.
2	0	199	99	467	233	769	192	1087	1086	1429	1428
3	1	211	30	479	239	773	193	1091	1090	1433	1432
5	0	223	222	487	486	787	393	1093	273	1439	719
7	6	227	113	491	490	797	199	1097	1096	1447	1446
11	2	229	228	499	498	809	202	1103	1102	1451	290
13	6	233	232	503	502	811	810	1109	1108	1453	726
17	16	239	7	509	508	821	820	1117	558	1459	162
19	18	241	30	521	52	823	822	1123	561	1471	735
23	22	251	50	523	261	827	413	1129	564	1481	740
29	28	257	256	541	540	829	276	1151	575	1483	247
31	15	263	262	547	91	839	419	1153	1152	1487	1486
37	3	269	268	557	278	853	213	1163	581	1489	248
41	5	271	5	563	281	857	856	1171	1170	1493	373
43	21	277	69	569	284	859	26	1181	1180	1499	214
47	46	281	28	571	570	863	862	1187	593	1511	755
53	13	283	141	577	576	877	438	1193	1192	1523	761
59	58	293	146	587	293	881	440	1201	200	1531	1530
61	60	307	153	593	592	883	441	1213	1212	1543	1542
67	33	311	155	599	299	887	886	1217	1216	1549	1548
71	35	313	312	601	300	907	151	1223	1222	1553	1552
73	8	317	79	607	202	911	450	1229	1228	1559	779
79	13	331	110	613	51	919	459	1231	41	1567	1566
83	41	337	336	617	88	929	464	1237	206	1571	1570
89	44	347	173	619	618	937	936	1249	208	1579	1578
97	96	349	116	631	315	941	940	1259	1258	1583	1582
101	4	353	32	641	32	947	473	1277	638	1567	266
103	34	359	179	643	107	953	952	1279	639	1601	200
107	53	367	366	647	646	967	322	1283	641	1607	1606
109	108	373	186	653	326	971	970	1289	92	1609	201
113	112	379	378	659	658	977	976	1291	1290	1613	403
127	42	383	382	661	220	983	982	1297	1296	1619	1618
131	130	389	388	673	224	991	495	1301	1300	1621	1620
137	8	397	99	677	338	997	166	1303	1302	1627	271
139	46	401	200	683	341	1009	252	1307	653	1637	409
149	148	409	204	691	230	1013	253	1319	659	1657	552
151	75	419	418	701	700	1019	1018	1321	55	1663	1662
157	78	421	140	709	708	1021	1020	1327	1326	1667	833
163	81	431	215	719	359	1031	103	1361	680	1669	556
167	166	433	432	727	726	1033	1032	1367	1366	1693	423
173	43	439	219	733	61	1039	519	1373	686	1697	1696
179	178	443	221	739	246	1049	524	1381	1380	1699	566
181	180	449	32	743	742	1051	1050	1399	699	1709	1708
191	95	457	152	751	125	1061	212	1409	32	1721	430
193	192	461	460	757	27	1063	1062	1423	158	1723	287
197	98	463	154	761	380	1069	1068	1427	713	1733	866

[1]) Таблица эта перепечатана изъ „Table des diviseurs pour tous les nombres des 1-er, 2-e e 3-e million, ou plus exactement, depuis 1 à 3036000, avec les nombres premiers qui s'y trouvent“ par S.-CH. Burckhardt. Paris. 1817.

M.

Числа Bernoulli.

Нумеръ	Числитель	Знаменатель
1	1	6
2	1	30
3	1	42
4	1	30
5	5	66
6	691	2730
7	7	6
8	3617	510
9	43867	798
10	1 74611	330
11	8 54513	138
12	2363 64091	2730
13	85 53103	6
14	2 37494 61029	870
15	861 58412 76005	14322
16	770 93210 41217	510
17	257 76878 58367	6
18	26315 27155 30534 77373	19 19190
19	2 92999 39138 41559	6
20	2 61082 71849 64491 22051	13530
21	15 20097 64391 80708 02691	1806
22	278 33269 57930 10242 35023	690
23	5964 51111 59391 21632 77961	282
24	560 94033 68997 81768 62491 27547	46410
25	49 50572 05241 07964 82124 77525	66
26	80116 57181 35489 95734 79249 91853	1590
27	29 14996 36348 84862 42141 81238 12691	798
28	2479 39292 93132 26753 68541 57396 63229	870
29	84483 61334 88800 41862 04677 59940 36021	354
30	121 52331 40483 75557 20403 04994 07982 02460 41491	567 86730
31	123 00585 43408 68585 41953 03985 74033 86151	6
32	10 67838 30147 86652 98863 85444 97914 26479 42017	510

ДОБАВЛЕНІЕ:

На страницѣ 246, въ концѣ § 53 необходимо убѣдиться, что $\xi > 0$ и $\eta > 0$.

Мы имѣемъ

$$\xi + \eta\sqrt{D} = (t + u\sqrt{D})(X_n - Y_n\sqrt{D}),$$

откуда

$$\xi = tX_n - uY_nD.$$

но

$$t > u\sqrt{D},\ X_n > Y_n\sqrt{D},$$

слѣдовательно, $\xi > 0$. Еслибы было $\eta < 0$, то есть $\eta = -\zeta$, то

$$\xi + \eta\sqrt{D} = \xi - \zeta\sqrt{D} = \frac{1}{\xi + \zeta\sqrt{D}} < 1.$$

Получается противорѣчіе.

ПОПРАВКИ:

На страницѣ 230: вмѣсто 8-ой строки сверху должно быть

$$(-4,\ 17,\ 6),\ (6,\ 19,\ -1),\ (-1,\ 19,\ 6),\ (6,\ 17,\ -4)$$

На той же страницѣ, въ строкѣ 13 снизу, вмѣсто 3-ей, 4-ой и 5-ой подстановки

$$\begin{pmatrix}0, & -1\\ 1, & -1\end{pmatrix}\ \begin{pmatrix}0, & -1\\ 1, & -1\end{pmatrix}\ \begin{pmatrix}0, & -1\\ 1, & 1\end{pmatrix}$$

должно быть

$$\begin{pmatrix}0, & -1\\ 1, & 3\end{pmatrix},\ \begin{pmatrix}0, & -1\\ 1, & -19\end{pmatrix},\ \begin{pmatrix}0, & -1\\ 1, & -3\end{pmatrix}.$$

На страницѣ 232, 8 строка снизу, послѣдняя подстановка должна быть

$$\begin{pmatrix}0, & -1\\ 1, & -27\end{pmatrix}.$$

На страницѣ 236, 8 строка снизу, вторая подстановка должна быть

$$\begin{pmatrix}0, & -1\\ 1, & 9\end{pmatrix}.$$

На страницѣ 223, въ первой теоремѣ Frobenius'a, напечатано

$$D = p^2 + 1,$$

а должно быть

$$D = p^2 + 4.$$
