А. В. Васильевъ,
заслуженный профессоръ Казанскаго Университета.

ВВЕДЕНІЕ ВЪ АНАЛИЗЪ.

ВЫПУСКЪ I.

Ученіе о цѣломъ положительномъ числѣ.

ИЗДАНІЕ ЧЕТВЕРТОЕ.

Цѣна 1 р. 25 к.

Изданіе книжнаго магазина **М. А. Голубева,**
Воскресенская ул., д. Матвѣевскаго (близъ церкви Воскресенія).

ОГЛАВЛЕНІЕ.

I

Изъ исторіи понятія о цѣломъ положительномъ числѣ.

§ **1.** Для насъ является невозможнымъ прослѣдить по непосредственнымъ источникамъ генезисъ понятія о цѣломъ положительномъ числѣ. Древнѣйшій письменный математическій памятникъ, дошедшій до насъ, папирусъ, написанный Египетскимъ писцомъ Аамесу за 1700 лѣтъ до Р. Х., свидѣтельствуетъ намъ, что и въ это отдаленное время Египтяне были знакомы съ дѣйствіями не только надъ цѣлыми числами, но и надъ дробями. За неимѣніемъ непосредственныхъ свидѣтельствъ, мы должны обратиться къ свидѣтельствамъ косвеннымъ.

Такими косвенными свидѣтельствами являются данныя этнологіи, относящіяся къ современнымъ дикарямъ, данныя, которыя можно почерпнуть, изучая развитіе дѣтей, и наконецъ данныя, извлекаемыя изъ изученія съ одной стороны—народныхъ преданій, съ другой—языка, который является несомнѣнно памятникомъ психологической работы давно отжившихъ поколѣній.

И всѣ эти косвенныя свидѣтельства одинаково освѣщаютъ и подтверждаютъ двѣ истины, имѣющія важное значеніе и для исторіи человѣческаго духа и для психологіи понятія о числѣ.

Многотрудною и продолжительною психологическою работою пріобрѣтало *постепенно* человѣчество понятіе о послѣдовательныхъ цѣлыхъ числахъ, *расширяло,* если позволено такъ выразиться, свой численный кругозоръ; при этомъ понятію о числѣ отвлеченномъ всегда предшествовало и сначала съ нимъ тѣсно сливалось понятіе о числѣ какихъ-нибудь опредѣленныхъ предметовъ, большею частью органовъ человѣка, служившихъ ему пособіемъ при счетѣ.

Мы можемъ даже, съ помощью преимущественно данныхъ лингвистики, видѣть въ дали вѣковъ, намъ предшествующихъ, тѣ этапы, на которыхъ останавливалась по временамъ психологическая работа человѣчества, чтобы, постоянно затѣмъ возобновляясь, привести насъ, наконецъ, къ тому понятію о безконечномъ рядѣ цѣлыхъ положительныхъ чиселъ, который составляетъ предметъ изученія чистой математики и исходя изъ котораго, математика достигла до понятія о комплексномъ числѣ.

§ 2. Съ трудомъ можемъ мы представить себѣ народъ, у котораго не существуетъ особенныхъ названій для чиселъ большихъ **трехъ**, народъ, для котораго всѣ прочія численныя выражаются однимъ словомъ **куча**,—а между тѣмъ многія свидѣтельства путешественниковъ и этнологовъ указываютъ на то, что такіе народы существуютъ.

Какъ ребенокъ, не научившійся считать, не отвѣтитъ числомъ на вопросъ, сколько у него куколъ, но подробно опишетъ всѣ свои куклы,—такъ и эскимосы, по словамъ путешественника Парри, не могутъ правильно сосчитать своихъ дѣтей, если ихъ больше трехъ. Они отличаютъ похожіе предметы не отвлеченными числами: первый, второй, третій и т. д., но названіемъ, индивидуально связаннымъ съ каждымъ пересчитываемымъ предметомъ. Не общее число своихъ собакъ держитъ въ памяти Эскимосъ, но отдѣльныя представленія о бѣлой собакѣ съ черными крапинами, о собакѣ, родившейся въ голодную зиму и т. п. Поэтому пересчитываніе является для дикаря, какъ указываютъ данныя, разбросанныя въ сочиненіяхъ по первобытной культурѣ Леббока, Тайлора и др., операціею тяжелою, трудною, послѣ которой дикарь сейчасъ-же начинаетъ жаловаться на боль въ головѣ.

Эту стадію умственнаго развитія, на которой находятся теперь также Ботокуды Бразиліи и Папуасы Новой Голландіи, проходила несомнѣнно и арійская раса, которая затѣмъ, въ лицѣ высшихъ представителей своего генія, открыла численную закономѣрность и въ движеніи отдаленныхъ небесныхъ свѣтилъ и въ движеніи неизмѣримо-малыхъ молекулъ матеріи.

Что и для арійской расы было время, когда понятіе о числѣ не представлялось съ достаточной отчетливостью, подтверждаютъ прежде всего преданія народовъ, указывающія на тѣхъ благодѣтелей человѣчества, которые научили его числу. У грековъ, напримѣръ, такими изобрѣтателями числа являются то Паламедъ, то Прометей.

Припомнимъ ту поэтическую картину, въ которой передаетъ преданіе объ изобрѣтеніи числа, устами Прометея греческій трагикъ Эсхилъ въ его безсмертной трагедіи „Прикованный Прометей“:

„Послушайте, что смертнымъ сдѣлалъ я...
Число имъ изобрѣлъ
И буквы научилъ соединять,
Имъ память далъ, мать музъ, всего причину“.

Данныя языка, подобно народнымъ преданіямъ, указываютъ намъ на первыя стадіи выработки названій для чиселъ и на первыя стадіи развитія понятія объ отвлеченномъ числѣ.

Существованіе во многихъ языкахъ единственнаго, *двойственнаго* и множественнаго чиселъ указываютъ, повидимому, на ту пройденную ступень развитія, при которой ясно различались понятія объ одномъ предметѣ и о двухъ предметахъ, но начиная съ трехъ такое различіе прекращалось и являлось только одно понятіе о множествѣ, изъ которыхъ еще не дифференцировались другія числительныя.

§ **3**. Но есть данныя, указывающія намъ и на *слѣдующую ступень* развитія, на которой явились *отдѣльныя названія для трехъ и четырехъ*, но вмѣстѣ съ тѣмъ эти числа, являясь крайними предѣлами чиселъ, имѣвшихъ названіе, служили символами множества, громадности. Припомнимъ изреченіе Овидія:

„terque quaterque beati“,

и сопоставимъ съ нимъ изображеніе множества въ египетскихъ іероглифахъ четырьмя чертами или китайское „четыре моря“ вмѣсто всѣхъ морей.

Не лишено значенія и указаніе лингвистики на то, что по грамматическому строю первыя три числительныя во многихъ языкахъ рѣзко отличаются отъ всѣхъ прочихъ числительныхъ; первыя *три числительныя измѣняются по родамъ* (два, двѣ, tres, tria), всѣ прочія не измѣняются. Первыя числительныя принадлежатъ, очевидно, болѣе ранней эпохѣ, чѣмъ та, въ которую вырабатывались названія прочихъ. То обстоятельство, что *корни первыхъ трехъ числительныхъ общи всѣмъ* извѣстнымъ *народамъ арійской* и народамъ семитской расъ, между тѣмъ какъ сходство пропадаетъ для дальнѣйшихъ числительныхъ, показываетъ, что названія прочихъ числительныхъ появились уже въ ту, сравнительно недавнюю эпоху, когда арійскіе и семитскіе народы покинули свою общую родину.

Если названія числительнаго *два* связаны у разныхъ народовъ съ различными органами человѣка или животныхъ (у Китайцевъ два—ny (уши); въ Тибетѣ два—patscha (крыло), у Готтентотовъ два—t'koam (рука), то выработка дальнѣйшихъ названій для чиселъ находится, что признаютъ филологи, въ связи *со счетомъ по пальцамъ.* Имена числительныя во многихъ языкахъ указываютъ намъ, что у первобытнаго человѣка пальцы являются преимущественнымъ орудіемъ счета, т. е. постояннымъ неизмѣннымъ рядомъ значковъ, съ которымъ при пересчитываніи сравнивается всякій другой новый рядъ пересчитываемыхъ предметовъ.

Когда зулусу напр. нужно сказать шесть, онъ говоритъ tatisitupa, что значитъ взять большой палецъ руки; въ Гренландіи, въ долинѣ Ориноко, въ Австраліи шесть равнозначуще съ фразою: одинъ съ другой руки, десять—двѣ руки, одиннадцать—двѣ руки и палецъ, двадцать—человѣкъ. У Эскимосовъ береговъ Гудзонова залива названія числительныхъ для восьми, девяти, десяти несомнѣнно совпадаютъ съ названіями средняго, четвертаго и малаго пальцевъ: то же самое замѣчается у Гуарани Южной Америки и у Малайцевъ. У Таманаковъ съ Ориноко двадцать одинъ—одинъ съ руки другого человѣка; такое выраженіе объясняется, если мы сопоставимъ съ нимъ разсказъ путешественниковъ о томъ, что у нѣкоторыхъ народовъ Южной Африки счетъ чиселъ и теперь производится съ помощью двухъ, трехъ человѣкъ, при чемъ пальцы одного соотвѣтствуютъ единицамъ, пальцы другого—десяткамъ, пальцы третьяго—сотнямъ.

Что касается до языковъ арійской расы, то только корень числительнаго пять (pente) несомнѣнно тожественъ съ корнемъ санскритскаго pankam или персидскаго penjeh (распростертая рука). Но нельзя не упомянуть и о гипотезѣ Потта, объясняющей подобнымъ же образомъ, и слѣдующія числительныя названіями мизинца и прочихъ пальцевъ правой руки. Поттъ сопоставляетъ напримѣръ названіе *мизинца* въ латинскомъ языкѣ (auricularis—чистящій уши) съ тожествомъ въ арійскихъ языкахъ корня числительнаго *шесть* и глагола *скрести.* Подобныя же натянутыя объясненія даетъ Поттъ и для слѣдующихъ числительныхъ.

Но и независимо отъ гипотезы Потта раньше приведенныя лингвистическія данныя несомнѣнно подтверждаютъ ту истину, что названія для первыхъ чиселъ получались отъ конкретныхъ предметовъ, которыми пользовались для счета, что понятіе объ отвлеченномъ цѣломъ числѣ вырабатывалось изъ прикладнаго цѣлаго числа, изъ названій предметовъ служившихъ для счета.

§ 4. На извѣстной стадіи развитія человѣчества расширеніе области ясно представляемыхъ и называемыхъ чиселъ пошло быстрѣе; но мы можемъ все таки указать, основываясь на культурно-историческихъ данныхъ, какъ постепенно расширялась область чиселъ, какъ постепенно то тѣ, то другія все большія и большія числа являлись предѣлами чиселъ, имѣвшихъ свои опредѣленныя названія, и потому символами неопредѣленнаго множества.

Мы находимъ напримѣръ объясненіе, почему число *тринадцать* считалось и до сихъ поръ считается суевѣрными людьми приносящимъ несчастіе, если допустимъ, что число *двѣнадцать* являлось въ извѣстное время символомъ множества, синонимомъ полноты, и слѣдующее за нимъ число являлось лишнимъ и потому нечестивымъ, несчастнымъ.

Въ тюркскихъ легендахъ, въ скиѳскихъ сагахъ синонимомъ неопредѣленнаго множества является или сорокъ или *сорокъ сороковъ*. Вліяніе туранскихъ сказаній на наши были, изученное Стасовымъ, позволяетъ отнести къ туранскому источнику и наше русское *сорокъ сороковъ*, часто употребляемое, какъ символъ несчетнаго множества.

Но еще большій культурно-историческій интересъ связанъ съ числомъ *шестьдесятъ*, которое такъ часто фигурируетъ въ преданіяхъ вавилонскихъ, персидскихъ и греческихъ, являясь въ нихъ всегда синонимомъ большого числа. *Шестьдесятъ* является числомъ вавилонскихъ боговъ, шестьдесятъ локтей—вышина золотаго идола, поставленнаго въ храмѣ Навуходоносора. Позднѣе съ тѣмъже значеніемъ несчетнаго множества являются нѣкоторыя кратныя шестидесяти: 300, 360. Ксерксъ далъ Геллеспонту 300 ударовъ, Киръ раздробилъ рѣку Гиндесъ, въ которой потонула одна изъ его любимыхъ лошадей, на 360 ручьевъ. Въ одной персидской пѣснѣ воспѣваются 360 полезныхъ употребленій пальмы.

Числа, встрѣчающіяся въ вавилонскихъ преданіяхъ, представляютъ культурно-историческій интересъ въ двоякомъ отношеніи. Вавилонъ представляется намъ съ одной стороны родиною гаданій, основанныхъ на числахъ, родиною различныхъ числовыхъ суевѣрій, которыя имѣли обширное вліяніе съ одной стороны на Китай, съ другой на идеи Пиѳагорейской школы, придававшей числамъ особое мистическое значеніе. Это мистическое значеніе, придававшееся числамъ, можетъ служить новымъ указаніемъ на новость и трудность понятія о числѣ на извѣстной ступени человѣческаго развитія ¹).

---

¹) Вопросу о числовой мистикѣ посвящена статья проф. А. В. Васильева: «О числовыхъ суевѣріяхъ». Казань, 1885.

Съ другой стороны число 60, встрѣчающееся въ легендахъ Вавилонскаго происхожденія, впослѣдствіи въ Вавилонѣ-же, при развитіи научныхъ знаній, явилось основаніемъ системы счисленія, слѣды которой сохранились у насъ въ дѣленіи времени и угловъ.

По мѣрѣ развитія десятичной системы счисленія, ея единицы различныхъ разрядовъ являлись символами множества. Въ церковно-славянскомъ языкѣ *тьма*, т. е. неизмѣримое множество, есть синонимъ то тысячи, то десятка тысячъ. Но существовало еще и „великое словенское число“, употреблявшееся, „коли прилучался великій счетъ и перечень“. Этотъ великій счетъ шелъ до единицы 48-го разряда и даже иногда до единицы 49-го разряда. Въ этомъ великомъ счетѣ тьма означаетъ уже тысячу тысячъ, являются и высшія единицы: *легіонъ* т. е. тьма темъ (милліонъ милліоновъ), *леодръ* т. е. легіонъ легіоновъ и наконецъ *воронъ* или леодръ леодровъ.

„И болѣе сего“, говорится въ славянскихъ рукописяхъ, „нѣсть (человѣку) разумѣвати“. Но иногда (въ одной рукописи XVII столѣтія) доходили и до десяти вороновъ или *колоды* и затѣмъ наивно прибавляли: „сего числа нѣсть больше“.

Такимъ образомъ и здѣсь есть *предѣлъ числамъ*, но какъ далеко отстоитъ этотъ предѣлъ отъ тѣхъ первыхъ предѣловъ, на которыя указываютъ данныя лингвистики.

§ **5.** Мы можемъ съ большею вѣроятностью указать ту вѣтвь арійской расы, которая относилась съ особенною любовью къ громаднымъ числамъ и старалась по мѣрѣ возможности расширить предѣлы употребляемыхъ чиселъ, изобрѣтая для нихъ особенныя названія. Эта вѣтвь—**древніе индусы**. Имъ принадлежитъ честь поразительнаго развитія искусства счета, какъ имъ же человѣчество обязано ариѳметикою положенія. Подобно тому, какъ *боги грековъ* сходятъ иногда съ Олимпа и, принимая участіе въ людскихъ битвахъ, *гордятся силою* своихъ *мускуловъ*, учитель Нирваны и закона владыка *Будда* еще въ юномъ возрастѣ отличался *искусствомъ счета*. Я приведу отрывокъ изъ прекраснаго русскаго перевода поэмы Эдвина Арнольда: „Свѣтъ Азіи или Великое Отреченіе“, съ необыкновенною точностью передающей легенду о Буддѣ.

Восьмилѣтній царевичъ, будущій Будда, подвергается испытанію Висвамитрою, „наукъ, искусствъ учителемъ превосходнымъ“.

„И сказалъ Висвамитра:

> Довольно, перейдемъ къ цифрамъ! Повторяй за мной, считай такъ, какъ я буду, пока дойдемъ до лакхи (лакха=100.000): одинъ, два, три, четыре, затѣмъ десятки, и сотни, и тысячи.
>
> И вслѣдъ за нимъ назвалъ отрокъ единицы, десятки, сотни и

не остановился на лакхѣ; нѣтъ онъ шепталъ дальше до тѣхъ чиселъ которыми можно считать все, начиная отъ зеренъ на полѣ и до самой мелкой песчинки. Потомъ онъ перешелъ къ катхѣ, къ счету звѣздъ ночныхъ, къ кати-катхѣ, счету морскихъ капель, и далѣе къ счету песчинокъ Ганга и къ счету, единицами котораго изображается весь песокъ десятка лакхъ рѣкъ такихъ, какъ Гангъ. Затѣмъ пошли еще болѣе громадныя числа..... и, наконецъ, число, при помощи котораго боги вычисляютъ свое прошедшее и будущее [1]).

Lalitavistara (жизнеописаніе Будды) даетъ даже число атомовъ въ іожанѣ (=3200 длинъ лука): оно равно 108,470,495,616,000.

§ 6. „Псаммитъ“ Архимеда. Задача выполненія неопредѣленно далеко простирающагося счета, которую поставили и разрѣшали Индійскіе мудрецы за три столѣтія до начала нашей эры, перешла и къ эллинамъ.

Подъ индійскимъ вліяніемъ, можетъ быть, написано знаменитое сочиненіе Архимеда: „Псаммитъ или исчисленіе песку въ пространствѣ равномъ шару неподвижныхъ звѣздъ“ [2]). Но задача, которая на индійской почвѣ явилась удовлетвореніемъ простого любопытства, имѣетъ въ твореніи греческаго мудреца высокое научное значеніе.

Псаммитъ Архимеда имѣетъ цѣлью доказать, что въ противность мнѣнію тѣхъ, которые думаютъ, что число песчинокъ безконечно и не можетъ быть сосчитано, нетрудно составить понятіе о такихъ числахъ, которыя больше числа песчинокъ, вмѣщающихся въ пространствѣ равномъ величинѣ не только земли, наполненной пескомъ со всѣми своими пропастями и глубиною морскою, даже до вершинъ высочайшихъ горъ, но и цѣлаго міра или шара неподвижныхъ звѣздъ.

Міръ для Архимеда шаръ, котораго центръ въ землѣ, радіусъ-же равенъ разстоянію отъ центра земли до центра солнца; поперечникъ шара неподвижныхъ звѣздъ меньше десять тысячъ разъ взятаго поперечника міра.

Чтобы рѣшить поставленную себѣ задачу, Архимедъ показываетъ, на основаніи предположеній современныхъ ему астрономовъ и собственныхъ наблюденій надъ величиною видимаго поперечника солнца, что поперечникъ міра меньше ста миріадъ миріадъ стадій (миріада=10.000; греческая стадія имѣла въ себѣ 504 фута 4$^{1}/_{2}$ дюйма). Относительно величины песчинокъ онъ дѣлаетъ предполо-

---

[1]) Свѣтъ Азіи—переводъ А. Анненской стр. 8—9.

[2]) Русскій переводъ этого сочиненія изданъ въ 1824 г. Ѳ. Петрушевскимъ.

женіе, что число песчинокъ, содержащихся въ количествѣ песку не больше маковаго зерна, будетъ не больше миріады и что поперечникъ маковаго зерна не меньше сороковой части дюйма (греческій дюймъ былъ немного больше $^3/_4$ нашего). Послѣ этихъ предположеній Архимедъ переходитъ къ изложенію своей номенклатуры чиселъ.

Числа отъ единицы до миріады миріадъ (отъ 1 до 10^8) называются первыми; миріада миріадъ первыхъ чиселъ (10^8) называется единицею вторыхъ чиселъ и вторыя числа идутъ отъ этой единицы до миріады миріадъ этихъ единицъ (отъ 10^8 до 10^{16}). Миріада миріадъ вторыхъ чиселъ называется единицею третьихъ чиселъ и третьи числа идутъ до миріады миріадъ этой единицы (отъ 10^{16} до 10^{24}).

Подобнымъ же образомъ будемъ продолжать называть слѣдующія числа даже до миріады миріадъ чиселъ миріадомиріадныхъ. Всѣ эти числа называются числами перваго періода и послѣднее изъ нихъ (очевидно, равное $\left(10^{8.10^8}\right)$ или единицѣ съ восемьюстами милліоновъ нулей) назовемъ единицею второго періода, и опять миріаду миріадъ первыхъ чиселъ второго періода $\left(10^{8.10^8+8}\right)$ назовемъ единицею вторыхъ чиселъ этого же періода и т. д. Подобнымъ-же образомъ вводятся единицы чиселъ третьяго $\left(10^{2.8.10^8}\right)$, четвертаго $\left(10^{3.8.10^8}\right)$, пятаго періода $\left(10^{4.8.10^8}\right)$ и т. д. даже до миріады миріадъ чиселъ миріадомиріадныхъ періода миріадомиріаднаго $\left(10^{10^8.8.10^8}\right)$.

Послѣднее число изобразится единицею съ восемьюдесятью тысячъ билліоновъ нулей; чтобы написать его, нужно потратить около 2.000.000.000 лѣтъ непрерывной работы днемъ и ночью.

Архимедъ показываетъ, что, для рѣшенія поставленной имъ себѣ задачи объ опредѣленіи числа песчинокъ въ шарѣ міра или даже въ шарѣ неподвижныхъ звѣздъ, нѣтъ никакой необходимости въ столь громадныхъ числахъ. Послѣдовательно вычисляетъ Архимедъ число песчинокъ въ шарѣ, поперечникъ котораго равенъ ста дюймамъ, въ шарахъ съ поперечникомъ въ миріаду дюймовъ, сто стадій, миріаду стадій и т. д. и т. д., постоянно пользуясь свойствомъ геометрической и ариѳметической прогрессіи, въ которомъ можно видѣть начало теоріи логариѳмовъ, и, доходя до шара міра, показываетъ, что число песчинокъ, въ немъ заключающихся, выражается числомъ меньшимъ „тысячи единицъ чиселъ седьмыхъ“ (10^{51}); *число песчинокъ, заключающихся въ шаръ неподвижныхъ звъздъ, меньше тысячи миріадъ чиселъ восьмыхъ* (10^{63}).

Трудно указать въ математической литературѣ сочиненіе, которое превосходило бы Псаммитъ Архимеда по интересу, смѣлости и богатству заложенныхъ въ немъ идей. Оно развивало понятіе о безконечно-большомъ, подобно тому, какъ въ своихъ сочиненіяхъ о квадратурѣ параболы, объ измѣреніи круга Архимедъ касался понятія о безконечно-маломъ, лежащемъ въ основаніи современнаго анализа.

Псаммитъ Архимеда ввелъ въ науку *понятіе о безконечно-продолжающемся рядъ цълыхъ положительныхъ чиселъ.* Многотрудная работа человѣческаго духа была окончена.

Рядъ цѣлыхъ положительныхъ чиселъ, безконечно продолжающихся,—предметъ благоговѣйнаго удивленія для индусовъ и таинственнаго толкованія для мудрецовъ Вавилона и Пиѳагорейцевъ, явился могущественнымъ орудіемъ для познанія природы.

Исходя изъ него чистая математика строитъ понятіе о дробномъ, отрицательномъ, несоизмѣримомъ, комплексномъ числѣ и это обобщенное понятіе о числѣ составляетъ единственный объектъ чистой математики, которая можетъ поэтому быть названа „ариѳметикою“. „*Ариѳметика*“, говоритъ Гауссъ, „*стоитъ въ томъ-же отношеніи къ математикъ* (включая въ нее геометрію и механику), *въ какомъ послъдняя стоитъ къ изученію природы. Математика есть царица естествознанія, и ариѳметика есть царица математики*“.

II

Изъ философіи понятія о цѣломъ положительномъ числѣ.

> Понятія о числѣ, пространствѣ и времени, употребляемыя въ математикѣ, должны быть развиваемы въ чистомъ полѣ философской приготовительной работы, изъ котораго уже потомъ вступаютъ въ отгороженыя области различныхъ наукъ. Развитіе этихъ понятій должно имѣть цѣлью надѣлить ихъ основными свойствами, необходимыми для спеціальнаго изученія.
>
> Л. Кронекеръ.

§ 7. Натуральныя числа или цѣлыя положительныя числа (въ первомъ отдѣлѣ мы будемъ часто называть ихъ просто числами) служатъ для счета и для опредѣленія порядка. Первое научное опредѣленіе числа было дано Евклидомъ (около 300 г. до Р. Х.) въ 7-ой книгѣ его „Началъ“. Опредѣливши *единицу* какъ то, по — чему каждая изъ существующихъ вещей есть единственная, Евклидъ опредѣляетъ число какъ *множество*, *составленное изъ единицъ* (собраніе единицъ). Великимъ шагомъ въ наукѣ было распространеніе понятія о числѣ и введеніе другого научнаго опредѣленія числа, примѣнимаго уже и къ несоизмѣримымъ числамъ. Это опредѣленіе вырабатывалось постепенно ¹) и точно формулировано въ

---

¹) Михаилъ Стифель, который первый говоритъ объ ирраціональныхъ (несоизмѣримыхъ) числахъ, не считаетъ ихъ настоящими числами (sie irrationalis numerus non est verus numerus—Arithmetica integra 1544) подобно тому какъ Евклидъ категорично отличалъ ирраціональныя величины отъ чиселъ (incommensurabiles magnitudines inter se rationem non habent quam numerus ad numerum—7-ое предложеніе 10-й книги Началъ). Декартъ обозначаетъ отношенія отрѣзковъ буквами и оперируетъ съ ними, какъ съ числами, но не формулируетъ точно опредѣленія числа.

первый разъ Ньютономъ (1642—1725) въ его Arithmetica universalis (1707): *Число есть отношеніе одной величины къ другой, принимаемой за единицу* [1].

Таковы два главныя опредѣленія числа, которыя долго ставились въ основаніе математической науки, при чемъ въ XVIII в. и въ XIX в. опредѣленіе Ньютона предпочиталось опредѣленію Евклида, т. е. впереди ставилось общее опредѣленіе вещественнаго числа, а цѣлое положительное число разсматривалось какъ частный случай. Такъ поступали Эйлеръ (1706—1782) (Алгебра) и Лагранжъ (1736—1813) (Leçons élementaires de mathématiqes, denuées en Ecole Normale en 1795).

Такъ поступаетъ и Лобачевскій въ своей Алгебрѣ. Опредѣливши *коликое,* какъ все то, что допускаетъ понятіе о *величинѣ,* онъ прибавляетъ: „*величина* всякаго коликаго познается только черезъ сравненіе съ другимъ, взятымъ за мѣру. Семь аршинъ сукна, напримѣръ, величина одного коликаго—сукна, опредѣленная черезъ сравненіе съ другимъ—аршиномъ, взятымъ здѣсь за мѣру“.

„Когда умалчивается и то, для чего назначается величина, и то, что берется для сравненія, тогда *величина* получаетъ названіе *числа,* а *мѣра единицы.* Въ сказанномъ примѣрѣ семь число, котораго единица—аршинъ..... Число бываетъ цѣлымъ, когда выражается безъ долей“.

Въ послѣднее время, при усилившемся стремленіи обосновать философскую сторону чистой математики, въ основаніе математики ставится не общее понятіе о числѣ вещественномъ, но понятіе о числѣ натуральномъ, какъ указателѣ порядка и численности.

Приведемъ нѣсколько наиболѣе обдуманныхъ объясненій числа, которыя въ общемъ совпадаютъ между собою.

„Естественный исходный пунктъ для развитія понятія о числѣ находится, говоритъ Кронекеръ, въ *порядковыхъ числахъ.* Въ нихъ обладаемъ мы запасомъ извѣстныхъ въ твердой послѣдовательности находящихся обозначеній, которыя мы можемъ приписывать группѣ различныхъ и различаемыхъ нами предметовъ [2]. Совокупность употребляемыхъ при этомъ обозначеній соединяемъ мы въ

---

[1] Numerum non tam multitudinem unitatum (опредѣленіе Евклида!!), quam abstractam quantitatis cujusvis ad aliam ejusdem generis quae pro unitate habetur rationem intelligimus.

[2] Предметы могутъ быть въ извѣстномъ смыслѣ равны между собою и различны только по положенію въ пространствѣ, во времени или въ мысляхъ, какъ напр. двѣ равныя длины или два равныхъ періода времени. (Кронекеръ).

понятіи о „численности предметовъ“, изъ которыхъ состоитъ группа, и выраженіе для этого понятія мы связываемъ съ *послѣднимъ* изъ употребляемыхъ обозначеній, такъ-какъ послѣдовательность ихъ точно опредѣлена. Такъ въ группѣ буквъ (a, b, c, d, e) можно обозначить букву a „первою“, букву b „второю“ и т. д. и наконецъ букву e „пятою“. *Совокупность употребленныхъ при этомъ порядковыхъ чиселъ или „численность“ буквъ* a, b, c, d, e можетъ поэтому быть обозначена, сообразно съ послѣднимъ изъ употребленныхъ порядковыхъ чисель, числомъ „пять“ *).

Можно изъ самихъ порядковыхъ чиселъ составить группу объектовъ. Для той группы, которая состоитъ изъ опредѣленнаго (n—таго) порядковаго числа и изъ всѣхъ предыдущихъ порядковыхъ чиселъ, „численность“ выражается, соотвѣтственно выше данному опредѣленію, количественнымъ числомъ, соотвѣтствующимъ n—тому порядковому числу; эти-то количественныя числа и называются „числами“.

Число m называется „меньшимъ“ чѣмъ другое число n, если порядковое число, соотвѣтствующее m, предшествуетъ соотвѣтствующему n. Такъ называемый естественный рядъ чиселъ 1, 2, 3,... есть ничто иное, какъ рядъ соотвѣтствующихъ порядковыхъ чиселъ.

Когда пересчитываютъ группу объектовъ, т. е. обозначаютъ порядковыми числами по порядку отдѣльные объекты, то этимъ самымъ придаютъ объектамъ извѣстный порядокъ.

Оставляемъ теперь безъ измѣненія порядокъ объектовъ, но установляемъ новую послѣдовательность порядковыхъ чиселъ (переставляя ихъ между собою) и затѣмъ первый объектъ обозначаемъ первымъ порядковымъ числомъ новой послѣдовательности, второй—вторымъ порядковымъ числомъ, и такъ по порядку каждый слѣдующій объектъ слѣдующимъ порядковымъ числомъ; тогда и объекты получаютъ снова особый порядокъ, отличный отъ предъидущаго, но опредѣляемый приписанными имъ порядковыми числами; предметы считаются тогда въ другомъ порядкѣ. [1]).

При этомъ „*совокупность*“ порядковыхъ чиселъ, употребленныхъ для обозначенія, дающая по выше данному опредѣленію понятіе о „численности“ предметовъ, нисколько не измѣняется, и потому *численность* т. е.

---

[1]) Здѣсь намѣренно употребляется перестановка не предметовъ, а ихъ обозначеній порядковыми числами; въ противномъ случаѣ могло-бы возникнуть сомнѣніе въ возможности перестановлять предметы (Кронекеръ).

результатъ счета не зависитъ отъ порядка счета.

„Численность“ предметовъ группы есть поэтому свойство группы какъ таковой, т. е. какъ совокупности предметовъ независимой отъ какого-нибудь опредѣленнаго порядка......

Если мы будемъ называть какія нибудь двѣ системы (a, b, c, d,...), a', b', c',...) *эквивалентными* въ томъ случаѣ, когда можно преобразовать одну систему въ другую, замѣняя по порядку каждый элементъ первой системы элементомъ второй, то *необходимое и достаточное* условіе для эквивалентности двухъ системъ будетъ состоять въ равенствѣ численности ихъ элементовъ и численность элементовъ системы (a, b, c, d,....) можетъ быть характеризована, поэтому, какъ единственная „*инваріанта*“ (неизмѣняющееся всѣхъ между собою эквивалентныхъ системъ [1]).

Тѣ же идеи высказываетъ Гельмгольцъ въ своемъ мемуарѣ „*Счетъ и Измѣреніе*“.

„**Счетъ** есть операція, основывающаяся на томъ, что мы находимся въ состояніи удерживать въ памяти послѣдовательность, въ которой являлись во времени одинъ за другимъ акты нашего сознанія. Мы можемъ поэтому разсматривать числа, какъ рядъ произвольно избранныхъ знаковъ, для которыхъ только одинъ опредѣленный видъ послѣдовательности считается нами естественнымъ или „натуральнымъ“.

Обозначеніе „натуральнаго“ ряда чиселъ связано, правда, съ опредѣленнымъ приложеніемъ счета, именно съ опредѣленіемъ *численности* (Anzahl) данныхъ реальныхъ вещей.

Прикладывая вещь одну за другою къ пересчитываемой кучѣ, мы произносимъ числа одно за другимъ въ ихъ естественномъ порядкѣ.

При этомъ *порядокъ числовыхъ знаковъ не имѣетъ никакого значенія;* какъ слова для обозначенія чиселъ различны въ различ-

---

[1] Съ этими взглядами Кронекера совпадаетъ и теорія Дедекинда, который вводитъ сначала общее понятіе о системѣ элементовъ, т. е. совокупности отдѣльныхъ вещей, различаетъ системы конечныя и безконечныя; одну изъ эквивалентныхъ системъ Кронекера Дедекиндъ называетъ подобнымъ *изображеніемъ* другой. (Теорія изложена въ мемуарѣ: Was sind und was sollen die Zahlen. Braunschw.) Студенческій математическій кружокъ Казанскаго Университета нынѣ издалъ Сборникъ мемуаровъ по основаніямъ ариѳметики, въ который вошли какъ переводъ статьи Дедекинда такъ и мои раньше изданные переводы статей—Гельмгольца, Кронекера и Гильберта.

ныхъ языкахъ, такъ и *послѣдовательность ихъ можетъ быть произвольно опредѣлена*, не только съ тѣмъ, чтобы *неизмѣнно* какая нибудь опредѣленная послѣдовательность считалась нормальною или естественною.

Эта послѣдовательность является дѣйствительно нормою или закономъ, даннымъ нашими предками, выработавшими языкъ. Я оттѣняю это обстоятельство, такъ какъ *кажущаяся „естественность“* ряда чиселъ происходитъ только отъ неполнаго анализа понятія о числѣ.

Математики называютъ этотъ естественный рядъ чиселъ *рядомъ положительныхъ цѣлыхъ чиселъ*.

Рядъ чиселъ врѣзался въ нашу память прочнѣе всякаго другого ряда, что происходитъ безъ сомнѣнія отъ его болѣе частаго повторенія. Мы употребляемъ его поэтому и для того, чтобы укрѣпить въ нашей памяти *воспоминаніе о другихъ послѣдовательностяхъ*, т. е. мы употребляемъ числа какъ *порядковыя числа*“.

§ 8. Итакъ, для счета предметовъ необходимъ рядъ значковъ произвольно избранныхъ, для которыхъ должна быть *строго и неизмѣнно* опредѣлена извѣстная *послѣдовательность*; при счетѣ предметовъ мы сравниваемъ ихъ рядъ съ рядомъ нашихъ значковъ.

Значками нормальнаго ряда могутъ быть матеріальные предметы, взятые въ опредѣленной послѣдовательности, какъ напр:, пальцы руки въ извѣстномъ порядкѣ или камешки calculi=камешки,—calculare=считать) или нарѣзки на деревянной биркѣ; при дальнѣйшемъ развитіи человѣчества такимъ рядомъ значковъ является рядъ *„натуральныхъ чиселъ“*. Рядъ натуральныхъ чиселъ представляетъ приведенную въ строгій порядокъ систему именъ, которая допускаетъ легкое запоминаніе порядка и потому и употребляется для счета.

Тамъ, гдѣ предметовъ немного и они легко различимы—ихъ обозначаютъ собственными именами (друзей, напр., мы не обозначаемъ нумерами); но всѣ предметы, встрѣчающіеся въ большомъ количествѣ и не легко отличаемые, должны быть отмѣчены номерами.

Номера даютъ намъ возможность найти тотъ или другой домъ, ту или другую десятину пашни. Въ малокультурномъ городѣ, какъ напр. Казань, дома на улицѣ отыскиваютъ по внѣшнимъ признакамъ (сѣренькій, на углу, противъ мелочной лавочки) или по фамиліямъ владѣльцевъ; мой другъ—американскій поклонникъ Лобачевскаго—живетъ въ Аустинѣ въ домѣ № 2407.

Такъ какъ во всякомъ нормальномъ рядѣ, служащемъ для счета, преимущественное значеніе имѣетъ строго опредѣленная послѣдовательность, то каждое число опредѣляется своимъ положеніемъ въ разъ на всегда выбранномъ нормальномъ рядѣ. Значекъ *единица* мы приписываемъ тому члену ряда послѣдовательности, съ котораго начинаемъ. *Два* есть число, которое слѣдуетъ непосредственно за единицею; *три* есть число, которое слѣдуетъ непосредственно за двумя, и т. д.

Если какое нибудь число обозначается a, то число, непосредственно слѣдующее за нимъ въ нормальномъ ряду, обозначается $a+1$; $a+b$ обозначаетъ то число нормальнаго ряда, которое получается при счетѣ до b, если при числѣ $a+1$ считать *единица*, при числѣ $a+2$ — *два* и т. д.

Изъ сопоставленія этихъ обозначеній вытекаетъ Грассмановская ариѳметическая аксіома:

$$(a+b)+1=a+(b+1),$$

и, какъ ея слѣдствія, и законы ассоціативности и коммутативности сложенія (см. § 11). Анализъ понятія о нормальномъ рядѣ приводитъ также къ прочимъ аксіомамъ ариѳметики.

Понятіе о родѣ чиселъ и ихъ сложеніи, выведенное изъ разсматриванія ряда чиселъ, какъ нормальнаго ряда значковъ, совпадаетъ съ тѣми понятіями, которыя получаются при опредѣленіи численности предметовъ и соединеніи двухъ или большаго числа группъ предметовъ въ одну; но тотъ-же анализъ указываетъ, что внѣшніе предметы должны удовлетворять извѣстнымъ условіямъ для того, чтобы они могли быть пересчитываемы.

Они не должны пропадать, не должны сливаться одинъ съ другимъ, не могутъ дѣлиться на два или болѣе во время пересчитыванія и къ нимъ не могутъ прибавляться во время этой операціи новые предметы. Выполняются ли эти условія для опредѣленнаго класса объектовъ—можетъ быть естественно рѣшено только посредствомъ опыта. Поэтому только опытъ можетъ указать на возможность примѣненія къ данному ряду предметовъ ариѳметическихъ аксіомъ и, слѣдовательно, сами эти аксіомы, подобно аксіомамъ геометріи, не могутъ имѣть того трансцедентальнаго, независимаго отъ опыта значенія, какое имъ приписывалъ Кантъ.

Зависимое отъ опыта происхожденіе понятія о цѣломъ числѣ и связанныхъ съ нимъ аксіомъ подтверждается вмѣстѣ съ тѣмъ и вышеприведенными данными изъ исторіи числа.

Мы видѣли, съ какимъ трудомъ и какою постепенностью расширялся численный кругозоръ и какую важную роль играли при этомъ органы человѣка, сначала двѣ руки или два уха, потомъ пальцы, представлявшіе такимъ образомъ матеріальные значки, употреблявшіеся при счетѣ, которые только постепенно замѣнялись рядомъ отвлеченныхъ цѣлыхъ чиселъ.

§ **9**. Взгляды Гельмгольца и Кронекера, изложенные нами, къ которымъ примыкаютъ также и взгляды извѣстнаго философа Маха 1), не совпадаютъ ни со взглядами эмпирической школы, ни со взглядами послѣдователей Канта.

Они отличаются отъ взглядовъ эмпирической школы, которые особенно обстоятельно изложены въ „Логикѣ“ Джона-Стюарта Милля. По мнѣнію Милля—„всѣ вещи обладаютъ количествомъ, всѣ состоятъ изъ частей, которыя могутъ быть перечисляемы, и въ этомъ смыслѣ онѣ обладаютъ всѣми тѣми свойствами, которыя называются *числовыми свойствами*. Поэтому истины ариѳметики имѣютъ *въ дѣйствительности своимъ предметомъ физическіе факты*, подобные другимъ фактамъ естествознанія, которые мы можемъ воспринимать при помощи нашихъ органовъ чувствъ; онѣ имѣютъ опытный характеръ, потомучто суть обобщенія изъ опыта и наблюденія“.

Изложенная нами теорія, напротивъ, разсматриваетъ числа, какъ продуктъ нашего ума 2), ибо числа—рядъ знаковъ, необходимыхъ для того, чтобы отмѣчать акты нашего сознанія;—и опредѣливъ такимъ образомъ числа, мы не можемъ говорить о числовыхъ свойствахъ вещей и о происхожденіи понятія о числѣ исключительно изъ внѣшняго опыта и наблюденія надъ физическими вещами.

Впрочемъ, въ цитированной статьѣ Махъ смотритъ на предложенія ариѳметики, какъ *на опытныя* предложенія, хотя и почерпнутыя изъ внутренняго опыта.

Но изложенная точка зрѣнія не менѣе отличается и отъ Кантовскаго апріоризма, *который принималъ истины ариѳметики за данныя a priori положенія независимыя отъ опыта и даже отъ* всѣхъ *впечатлѣній* внѣшнихъ чувствъ, а потому и *обладаю-*

---

1) См. его Principien der Wärmelehre (статья Namen und Zahlen). Также научно-популярныя статьи объ экономической природѣ физическаго изслѣдованія.

2) Кронекеръ приводитъ цитату изъ письма Гаусса къ Бесселю, въ которомъ Гауссъ противополагаетъ истины геометріи и истины ариѳметики: «Наше знаніе истинъ геометріи совершенно лишено того полнаго убѣжденія въ ихъ необходимости (а слѣдовательно абсолютной истинѣ), которое принадлежитъ ученію о величинахъ: мы должны скромно сознаться, что если *число есть только продуктъ нашего духа*, то пространство и помимо нашего духа имѣетъ реальность, которой мы не можемъ-a priori предписывать законы».

щія всеобщностью и необходимостью. Такой необходимой всеобщности въ примѣненіи къ объективному міру,—какъ было указано въ предыдущемъ §, истины ариѳметики не имѣютъ: предметы должны имѣть особыя эмпирическія качества для того, чтобы могли быть пересчитываемы [1]).

Положенія ариѳметики не вносятся въ познаніе внѣшняго міра; они составляютъ *только методъ употребленія* выработанной продолжительною психическою работою человѣчества *системы знаковъ*, съ помощью которой мы замѣняемъ изученіе отношеній между вещественными предметами мысленными операціями надъ этими знаками, достигая этимъ „экономіи мысли“.

Какіе бы перечисляемые предметы мы ни подставляли вмѣсто натуральныхъ цѣлыхъ чиселъ, положенія ариѳметики остаются одни и тѣ же, т. е. могутъ быть выводимы одинъ разъ и примѣняемы въ безконечномъ множествѣ различныхъ случаевъ.

Мы и переходимъ теперь къ выводу необходимыхъ для обоснованія ариѳметики аксіомъ и законовъ сложенія и умноженія.

III.

Аксіомы и законы операцій въ ученіи о цѣлыхъ числахъ.

§ 10. Рядомъ натуральныхъ или цѣлыхъ положительныхъ чиселъ, мы будемъ называть рядъ знаковъ, опредѣляемый слѣдующими свойствами:

I. Рядъ *начинается* нѣкоторымъ числомъ, и это первое число ряда называется единицею и обозначается 1.

II. *За каждымъ числомъ ряда слѣдуетъ одно, и только одно, число и каждому числу ряда* (кромѣ числа 1) *предшествуетъ одно—и только одно—число.* (Первое обобщеніе понятія о числѣ будетъ состоять во введеніи числа, предшествующаго 1 и обозначаемаго 0; но пока мы не вводимъ его, такъ какъ введеніе его не является необходимымъ при пересчитываніи [2]). Число *слѣдующее*

---

[1]) Желающихъ ближе познакомиться съ эмпирическою и апріорною теоріею понятія о числѣ отсылаемъ къ сочиненію проф. Челпанова: «Проблема воспріятія пространства». Часть 2, Кіевъ 1904, стр. 227—254; а также къ его статьѣ: «Обзоръ новѣйшей литературы по теоріи понятія» (Кіев. Унив. Изв. 1900 г.).

[2]) При изображеніи чиселъ мы можемъ, какъ показываютъ церковно-славянскій, латинскій и греческій способы писанія, обойтись безъ нуля.

за какимъ-нибудь числомъ a обозначимъ (временно) $a+$ и будемъ называть числомъ „высшимъ“ a и всѣхъ чиселъ предшествующихъ a. (Для обозначенія того, что b выше a, будемъ употреблять значокъ $>$: $b>a$).

Число, предшествующее a, будетъ обозначаться $a-$ и будетъ называться низшимъ, чѣмъ a и всѣ числа, слѣдующія за a (b ниже a обозначается $b<a$).

Изъ опредѣленія понятій высшій, низшій слѣдуетъ, что: 1° если $a>b$, то $b<a$, и 2° если $a>b$, $b>c$, то $a>c$ и если $a<b$, $b<c$, то $a<c$. Если два числа a и b различны, то изъ того, что каждому числу предшествуетъ только одно число и за каждымъ числомъ слѣдуетъ только одно число,—вытекаетъ, что если за двумя числами a и b слѣдуетъ одно и то же число, то a и b тождественны, и если числамъ a и b предшествуетъ одно число, то a и b тождественны.

III. *Ни одно число не повторяется въ нашемъ ряду.*

Изъ этого положенія вытекаютъ слѣдующія слѣдствія:

1. Каждое число равно себѣ, и только самому себѣ (число, стоящее въ нашемъ ряду на одномъ мѣстѣ, не можетъ равняться числу, стоящему на другомъ мѣстѣ).

Для нашего ряда чиселъ понятія о равенствѣ и тождествѣ совпадаютъ. Отношеніе равенства или тождества двухъ чиселъ будетъ обозначаться: $a=b$, и если $a=b$, то и $b=a$ (симметричность).

Поэтому изъ $a=b$, $b=c$ слѣдуетъ непосредственно: $a=c$, ибо оба вышеприведенныя равенства выражаютъ, что оба числа a и c тождественны (транзитивность).

Это слѣдствіе совпадаетъ съ 1-ою аксіомою ученія о равенствѣ величинъ: если двѣ величины равны порознь третьей, то онѣ равны между собою. [1]).

---

[1]) Приведемъ рядъ аксіомъ ученія о величинахъ въ томъ видѣ какъ они формулированы были Евклидомъ въ его «Началахъ»:

1) Величины, равныя одной и той-же величинѣ, равны между собою.

2) Если къ величинамъ равнымъ придадимъ величины равныя, то суммы получимъ равныя.

3) Если отъ величинъ равныхъ отнимемъ величины равныя, то остатки получимъ равные.

4) Если къ величинамъ неравнымъ придадимъ величины равныя, то суммы получимъ неравныя.

Такимъ образомъ подтверждается примѣнимость 1-й аксіомы къ числамъ.

2. Если a, b суть какія-нибудь два числа, стоящія на разныхъ мѣстахъ, то они различны, и обратно—т. к. въ нашемъ ряду знаковъ на каждомъ мѣстѣ можетъ стоять одно—и только одно—число, то если a и b суть два *различныя* числа, то *одно* опредѣленное изъ нихъ *выше другого*: или $a>b$ или $a<b$.

Обозначенія (временныя). Въ виду того, что десятеричная система счисленія основывается на введеніи операцій (сложенія, умноженія и возвышенія въ степень) надъ числами, мы вводимъ временно слѣдующія обозначенія: $1+=2$, $2+=3$.... $8+=9$, $9+=X$, $X+=XI$, ... $X9+=XX$, ... $XXXX9+=L$, $LXXXX9+=C$, ... и т. д. Съ помощью этихъ обозначеній мы можемъ тогда письменно передавать другимъ результаты нашего пересчитыванія.

§ 11. Сложеніе натуральныхъ чиселъ.

Числа натуральнаго ряда, опредѣленнаго свойствами перечисленными въ предъидущемъ параграфѣ, могутъ быть сами принимаемы за объекты счета, могутъ быть сами пересчитываемы. Начнемъ пересчитывать числа нашего ряда, начиная съ числа $a+$. Если число $a+$ я считаю первымъ (разъ); число $(a+)+$ (т. е. слѣдующее за $a+$) вторымъ (два) и т. д., и если такимъ образомъ последовательно считая числа ряда, я дойду до числа c, отсчитавши b, то число c называется *суммою* числа a и числа b, и это отношеніе между тремя числами обозначается:

$$c=a+b.$$

Напр. считая при числахъ 8, 9, 10, 11 послѣдовательно разъ, два, три, четыре, я пишу

$$11=7+4.$$

Операція этого дальнѣйшаго отсчитыванія называется сложеніемъ съ числомъ a числа b. Порядокъ чиселъ имѣетъ значеніе,

---

5) Если отъ величинъ неравныхъ отнимемъ величины равныя, то остатки получимъ неравные.

6) Величины двойныя одной и той же величины равны между собою.

7) Половины одной и той же величины равны между собою.

8) Цѣлое болѣе своей части.

такъ какъ въ нашей операціи числа a и b играютъ неодинаковую роль.

Послѣ введенія этого новаго обозначенія, очевидно, что число $a+$ можетъ быть обозначено и $a+1$, число $(a+)+$ знакомъ $a+2$ и т. д.

Изъ даннаго опредѣленія операціи сложенія вытекаетъ, что 1^0 если $a=b$, то $a+c=b+c$ и 2^0 если $a>b$, $c=d$, то $a+c>b+d$ или если $a<b$, $c=d$, то $a+c<b+d$. Такимъ образомъ и аксіомы: равное приданное къ равному, дастъ равное, равное, приданное къ неравному дастъ неравное (аксіомы 2-я и 4-ая выше даннаго ряда) сохраняютъ свою примѣнимость къ нашему „натуральному" ряду.

3) Изъ опредѣленія сложенія вытекаетъ также, что если число c выше чѣмъ другое число a, то я могу представить всегда число c, какъ сумму a и нѣкотораго другого числа b. Дѣйствительно, начиная считать съ числа $a+1$, я всегда дойду до числа c и то число b, которое будетъ послѣднимъ, мною употребленнымъ для счета, и будетъ искомымъ числомъ.

Наконецъ, изъ опредѣленія операціи сложенія вытекаетъ слѣдующее свойство этой операціи, которое я буду называть *Грассмановскою аксіомою сложенія*:

IV. $(a+b)+1=a+(b+1)$

Объясненіе. Дѣйствительно, если я, пересчитывая по порядку числа $a+1$, $a+2$, ... $a+b$, говорю при этомъ пересчитываніи 1, 2, ... b, то при слѣдующемъ за $a+b$ числѣ т. е. числѣ $(a+b)+1$ я долженъ сказать $b+1$, т. е. это слѣдующее за $a+b$ число есть, по данному опредѣленію сложенія, сумма чиселъ a и $b+1$.

Грассмановская аксіома есть, очевидно, *только описаніе* нашей *операціи отсчитыванія* ряда чиселъ и можетъ быть также разсматриваема, какъ опредѣленіе операціи сложенія.

Слѣдствіемъ Грассмановской аксіомы являются частныя числовыя формулы, подобныя формулѣ $5+4=9$, природа которыхъ такъ интересовала всегда философовъ¹). На основаніи Грассмановской аксіомы имѣемъ:

---

¹) Лейбницъ доказывалъ ихъ почти такъ-же точно, какъ онѣ доказаны въ текстѣ на основаніи Грассмановской аксіомы. Кантъ напротивъ считалъ ихъ синтетическими апріорными сужденіями, и изученіе вопроса о томъ, какъ возможны подобныя синтетическія апріорныя сужденія и чѣмъ обусловливается ихъ объективное значеніе—есть *основной вопросъ* Кантовской «Критики чистаго разума».

$$5+4=5+(3+1)=(5+3)+1.$$

Подобнымъ-же образомъ: $5+3=(5+2)+1$,

$$5+2=(5+1)+1$$

Но $5+1=6$, слѣдовательно $5+2$ есть число слѣдующее за 6 т. е. 7, $5+3$ есть 8, $5+4$ есть 9.

Провѣрка частныхъ числовыхъ формулъ требуетъ, такимъ образомъ, примѣненія Грассмановской аксіомы *конечное* число разъ. Мы переходимъ теперь къ выводу общихъ законовъ, приложимыхъ ко всѣмъ числамъ нашего безконечнаго ряда. Очевидно, что къ этой цѣли насъ не можетъ привести конечное число сужденій (силлогизмовъ). Общая теорема примѣнимая ко всѣмъ числамъ, выражающая свойства безконечнаго ряда чиселъ (а выводъ такихъ общихъ теоремъ и составляетъ цѣль науки), требуетъ для своего доказательства безконечнаго множества силлогизмовъ. Но это безконечное множество силлогизмовъ замѣняется въ математикѣ особеннымъ методомъ доказательства, извѣстнымъ подъ названіемъ *способа* полной или **математической индукціи** или способа перехода отъ n къ $n+1$ или способа разсужденія par récurrence (иногда способъ Бернулли). Методъ основывается на слѣдующемъ предложеніи:

Чтобы доказать, что нѣкоторая теорема вѣрна для всякаго цѣлаго числа n, достаточно доказать: 1⁰ *что эта теорема вѣрна для $n=1$,* 2⁰ *что если она вѣрна для нѣкотораго числа n, то она вѣрна и для слѣдующаго числа $n+1$.*

Напр. $1+2+\ldots+n=\frac{n\ (n+1)}{2}$ вѣрно для $n=1$; допустивъ вѣрность равенства для n и прилагая къ обѣимъ частямъ по $n+1$, получаемъ:

$$1+2+\ldots\ +n+(n+1)=\frac{n\ (n+1)}{2}+n+1=\frac{(n+1)\ (n+2)}{2}$$

т. е. теорема вѣрна для $n+1$; потому вѣрность теоремы для $n=1$ влечетъ за собою вѣрность для $n=2$, вѣрность для $n=2$ влечетъ за собою вѣрность $n=3$ и т. д.

Предлагаю читателю для уясненія этого важнѣйшаго математическаго пріема доказать на основаніи его слѣдующія равенства:

a) $$1^2+2^2\ldots+n^2=\frac{n\ (n+1)\ (2n+1)}{6}$$

b) $$1^3+2^3+\dots+n^3=(1+2+3+\dots+n)^2$$

c) $$1+3+6+10+\dots+\frac{n\,(n+1)}{2}=\frac{n\,(n+1)\,(n+2)}{1.2.3.}$$

d) $$1+4+10+20+35+\dots+\frac{n(n+1)(n+2)}{1.2.3.}=\frac{n(n+1)(n+2)(n+3)}{1.2.3.4.}$$

e) Составимъ рядъ чиселъ 0, 1, 1, 2, 3, 5, 8, 13, 21,... котораго первыя числа суть 0, 1, а каждое слѣдующее получается складывая два предыдущія. Если мы обозначимъ числа этого ряда послѣдовательно u_0, u_1, u_2, u_3, u_4,... ($u_0=0$, $u_1=1$, $u_2=1$. $u_3=2$ и т. д.) то рядъ, извѣстный подъ названіемъ ряда Фибоначчи или Ламе, имѣетъ слѣдующія свойства:

1. $u_{n+1}=u_0+u_1+u_2+\dots+u_{n-1}+1$.

2. $u_0+u_2+u_4+u_6+\dots+u_{2n}-(u_1+u_3+u_5+\dots+u_{2n-1})=u_{\overline{2n-1}}\,1$

3. $u^2_n=u_{n-1}u_{n+1}\pm 1$.

4. $u_{n+p-1}=u_{n-1}.u_{p-1}+u_nu_p$.

Пуанкаре въ своей статьѣ: „О природѣ математическаго разсужденія“ [1]) справедливо видитъ въ методѣ перехода отъ n къ $n+1$ образцовый методъ математическаго доказательства (le raisonnement mathématique par excellence). Въ немъ на самомъ порогѣ математической науки мы встрѣчаемся съ идеей математической безконечности, и методъ перехода отъ n къ $n+1$ есть то орудіе, которое позволяетъ замѣнить безконечное множество силлогизмовъ одною формулою, позволяетъ намъ переходить отъ конечнаго къ безконечному. „Этотъ методъ, недоступный ни аналитическому доказательству, ни опыту, есть истинный типъ синтетическаго апріорнаго сужденія“. (Пуанкаре) [2]).

§ 12. Законы сложенія. Изъ Грассмановской аксіомы выводятся законы сложенія.

---

[1]) Изв. Каз. Физико-Мат. Общ. т. IX. Смотри также его «Гипотеза и Наука», 1903.

[2]) Дедекиндъ (Was sind und was sollen die Zahlen) и Шредеръ въ своей «Algebra der Logik» смотрятъ на принципъ полной индукціи какъ на теорему, которая можетъ быть доказана́ логически. Пеано (и за нимъ Штольцъ) видятъ въ немъ свойство ряда цѣлыхъ чиселъ и принимаютъ его за аксіому.

IV_1 $\quad a+(b+c)=(a+b)+c$ (законъ ассоціативности)

IV_2 $\quad a+b=b+a$ (законъ коммутативности)

1. *Ассоціативность.* Предположимъ, что формула вѣрна для $c=\gamma$, докажемъ, что она будетъ вѣрна для $c=\gamma+1$. По предположенію

$$a+(b+\gamma)=(a+b)+\gamma.$$

Такъ какъ за каждымъ числомъ слѣдуетъ одно и только одно число, то

$$[a+(b+\gamma)]+1=[(a+b)+\gamma]+1.$$

Но по IV (стр. 20).

$$[a+(b+\gamma)]+1=a+((b+\gamma)+1)=a+(b+(\gamma+1)).$$

По той же аксіомѣ IV

$((a+b)+\gamma)+1=(a+b)+(\gamma+1)$; итакъ по аксіомѣ 1 ученія о величинахъ, которой примѣнимость къ ученію о числахъ мы выяснили,

$$a+(b+(\gamma+1))=(a+b)+(\gamma+1),$$ что и тр. док.

2. ***Коммутативность.*** Чтобы показать справедливость этого закона докажемъ сначала, что $a+1=1+a$; для $a=1$ формула есть тождество. Покажемъ поэтому, что если формула вѣрна для $a=\alpha$, то она вѣрна и для $a=\alpha+1$;

дѣйствительно,

$$(\alpha+1)+1=(1+\alpha)+1=(\text{на основаніи IV})\ 1+(\alpha+1).$$

Итакъ, формула $a+b=b+a$ вѣрна для $b=1$; покажемъ поэтому, что если формула вѣрна для $b=\beta$, то она вѣрна и для $b=\beta+1$.

Дѣйствительно, $a+(\beta+1)=(a+\beta)+1=(\beta+a)+1=1+(\beta+a)$ $=(1+\beta)+a$ (на основаніи закона ассоціативности) $=(\beta+1)+a$ что и тр. док.

3. Въ ученіи о числахъ имѣютъ значеніе не только равенства, но и **неравенства.**

Доказанная коммутативность сложенія даетъ возможность обобщить вышеприведенныя неравенства и доказать слѣдующія два положенія: 1) если $a>b$, $c>d$, то $a+c>b+d$

2) если $a<b$, $c<d$, то $a+c<b+d$

Дѣйствительно, если $a>b$, $c>d$, то $a+c>b+c$, $c+b>d+b$ или по закону коммутативности $b+c>b+d$; слѣдовательно $a+c>b+d$.

Подобнымъ же образомъ докажется второе неравенство.

4. Введеніе нуля. Письменное изображеніе чиселъ (см. дальше) привело индусовъ къ введенію особаго знака, который ставился для указанія отсутствія въ числѣ какого-либо разряда (единицъ, десятковъ, сотенъ и т. д.). *Первое* обобщеніе понятія о числѣ заключается въ томъ, что этотъ знакъ разсматривается также какъ *число*, предшествующее 1. Тогда это число O должно имѣть слѣдующія свойства: 1^0 оно меньше всѣхъ чиселъ, $2'$ $O+a=a$ (убѣдимся въ этомъ, считая отъ O, какъ прежде считали отъ *1*).

Мы допускаемъ законъ коммутативности и въ томъ случаѣ. если одно изъ чиселъ есть O (это первое примѣненіе такъ называемаго *принципа постоянства формальныхъ законовъ*) и потому имѣемъ $O+a=a$ (въ частности $O+O=O$).

Число O называется модулемъ операцій *сложенія и вычитанія*. [Въ общемъ ученіи о формахъ (Formenlehre) модулемъ операціи соединенія двухъ чиселъ въ одно θ (a, n) называется такое число n, при которомъ $\theta(a, n)=a$].

§. 13. Умноженіе чиселъ и его законы.

Назовемъ повторенное сложеніе (т. е. сложеніе равныхъ чиселъ, взятыхъ въ числѣ b) *умноженіемъ* числа a на число b и будемъ обозначать результатъ этой операціи знакомъ $a\times b$ или $a.b$, *строго соблюдая порядокъ чиселъ*:

$$(1)\qquad a+a+\ldots\ldots+a=a\times b$$

Изъ этого опредѣленія умноженія и свойствъ сложенія вытекаютъ слѣдующія положенія: 1^0 если $a=a'$, $b=b'$, то $ab=a'b'$ [въ частномъ случаѣ если $b=2$ имѣемъ приложимость къ цѣлымъ числамъ аксіомы Евклида: величины двойныя одной и той же величины равны между собою]. 2^0 если $a>a'$, $b=b'$, то $ab>a'b'$.

Изъ опредѣленія 1, вытекаютъ также слѣдующія два равенства:

2) $a\times 1=a$ (равенство это показываетъ, что число 1 есть модуль умноженія) и

$$3)\qquad a\times b=\Big[\,a\times(b-1)\,\Big]+a \text{ или } a.(b+1)=ab+a.$$

Равенство (3) позволяетъ послѣдовательно переходить отъ $a+2$ къ $a+3$, отъ $a+3$ къ $a+4$ и т. д., т. е. выводить справедливость новыхъ числовыхъ формулъ, какъ напр.

$$5\times 3=XV \text{ или } X.X=C.$$

Изъ равенствъ (2) и (3) выводятся слѣдующіе законы дѣйствія умноженія, позволяющіе сократить время необходимое для вывода числовыхъ формулъ, въ которыя входитъ знакъ умноженія.

1. Законы дистрибутивности (*распредѣлительные*).

$$(a+b)\,c=a.c+b\,c. \qquad a(b+c)=ab+ac. \tag*{(4) ... (5)}$$

Формула 4, очевидно, справедлива для $c=1$, докажемъ, что если она справедлива для $c=\gamma$, то она справедлива для $c=\gamma+1$.

Дѣйствительно, $(a+b)\ (\gamma+1)=$(по 3) $(a+b)\gamma+(a+b)=$(по предположенію и по закону ассоціативности сложенія) $a\gamma+b\gamma+a+b$ $=$(по коммутативности и ассоціативности сложенія) $(a\gamma+a)+(b\gamma+b)$ $=$(по 3) $a\ (\gamma+1)+b(\gamma+1)$, что и тр. док.

Формула 5 также справедлива для $c=1$, совпадая тогда съ формулой 3; докажемъ, что если она справедлива для $c=\gamma$, то она справедлива и для $c=\gamma+1$. Дѣйствительно, имѣемъ по предположенію для $c=\gamma$, по опредѣленію (3) и по свойствамъ сложенія:

$$a(b+(\gamma+1))=a((b+\gamma)+1)=a(b+\gamma)+a=ab+a\gamma+a=$$
$$=ab+a(\gamma+1), \text{ что и тр. док.}$$

2. Законъ ассоціативности (*соединительный*):

$$(ab)\ c=a\ (bc). \tag{5}$$

Формула (6) для $c=1$ есть тождество; докажемъ, что если она вѣрна для $c=\gamma$, то вѣрна и для $c=\gamma+1$. Дѣйствительно, $(a.b)\ (\gamma+1)=(ab.)\gamma+ab=a(b.\gamma)+ab=$(по формулѣ 5)

$$a(b\gamma+b)=a(b(\gamma+1)).$$

3. Законъ коммутативности (*перемѣстительный*).

$$ab=ba \tag{7}$$

Докажемъ, что формула (7) вѣрна для $b=1$, т. е. $a.1=1.a$ Эта формула для $a=1$ есть тождество, допустивъ, что она вѣрна для $a=\alpha$, покажемъ, что она вѣрна и для $a=\alpha+1$. Дѣйствительно $(\alpha+1).1=$(по ф. 4)$\alpha.\ 1+1=1.\alpha+1=$(по форм. 5)$=1(\alpha+1)$.

Теперь покажемъ, что если формула (7) вѣрна для $b=\beta$, то она будетъ вѣрна и для $b=\beta+1$. Дѣйствительно $a(\beta+1)=$(по 5) $a\beta+a=\beta a+a=$(по 4)$=(\beta+1)a$.

4. Изъ неравенства $a>b$ слѣдуетъ неравенство $ac>bc$. Чтобы доказать это, примѣнимъ тотъ же пріемъ математической индукціи. Если неравенство справедливо для $c=\gamma$, т. е. $a\gamma>b\gamma$, то $a(\gamma+1)=a\gamma+a>b\gamma+a>b\gamma+b$, а на основаніи (5), $b\gamma+b=b(\gamma+1)$; итакъ $a(\gamma+1)>b(\gamma+1)$, что и тр. док.

Какъ обобщеніе имѣемъ, если $a>b$, $c>d$, то $ac>bd$. Доказывается, какъ соотвѣтствующее неравенство въ случаѣ сложенія.

5. ***Модуль умноженія.*** Равенство $a\times1=a$ показываетъ, какъ это уже и было указано, что модуль умноженія есть 1.

Сопоставимъ теперь найденные законы операцій сложенія и умноженія:

Сложеніе		*Умноженіе*
$a+b=b+a$		$ab=ba$
$a+(b+c)=(a+b)+c$		$a(bc)=(ab)c$
	$a(b+c)=ab+ac$	
	$(a+b)c=ac+cb$	
$a+0=0+a=a$		$a.\ 1=1.\ a=a.$

§ **14.** Выясненіе важности законовъ ассоціативности, коммутативности и дистрибутивности операцій сложенія и умноженія есть заслуга преимущественно англійской школы математиковъ (Peacock, Морганъ, Грегори, Гамильтонъ, Буль и др.) [1]. Къ выясненію понятій элементарной математики они были приведены, создавая болѣе общія теоріи (символическое исчисленіе, теорію кватерніоновъ (Гамильтонъ), математическую логику (Буль)).

На континентѣ къ теоріи законовъ операцій пришелъ независимо отъ англійской школы знаменитый Г. Грассманъ, который въ своей „Ausdehungslehre“ 1844 г. далъ общую теорію операцій (Formenlehre), которая заключаетъ въ себѣ математику (Grössenlehre) только какъ часть, а въ своей „Lehrbuch der Arithmetik, Berlin 1861“ излагалъ ее въ формѣ удобной для преподаванія,

---

(1) Впрочемъ Servois еще въ 1814 г. ввелъ термины коммутативности и дистрибутивности.

Вышеприведенные выводы законовъ изъ основной аксіомы Грассмана и даны въ Ариѳметикѣ. Идеи Грассмана популяризованы были Ганкелемъ въ его „Theorie der complexen Zahlensysteme“ 1867 г.

Лобачевскій въ своей Алгебрѣ 1834 г., опредѣливъ сложеніе какъ присчитаніе къ единицамъ перваго числа единицъ второго, считаетъ нужнымъ опредѣлить сложеніе, когда одно изъ чиселъ есть нуль, [придать нуль къ цѣлому числу, значитъ ничего къ нему не присчитывать; придать же къ нулю цѣлое число, все равно, что пересчитать прямо единицы цѣлаго числа] и затѣмъ показываетъ слѣдующее общее положеніе, заключающее въ себѣ какъ частный случай законъ коммутативности:

Все равно къ числу a придать сперва b, потомъ c, или сперва c, потомъ b. Приведемъ его доказательство, замѣчательное по своей строгости. „Предложеніе само по себѣ ясно, когда $b=c$. Если же b и c неравны, то случай $b>c$ тотъ же, что и $b<c$. Итакъ пусть $b>c$. Число b можно произвести, придавая къ c какое-нибудь число d, такъ что $b=c+d$, потому что въ этомъ и состоитъ неравенство чиселъ. Придать же число b не иначе можно, какъ присчитывая единицы числа c, потомъ единицы въ d (свойство ассоціативности такимъ образомъ принимается Лобачевскимъ за очевидное), слѣдовательно

$$a+b+c=a+c+d+c$$

$$a+c+b=a+c+c+d.$$

Здѣсь вмѣсто $a+c$ можно ставить число A, сумму a съ c, остается доказывать

$A+d+c=A+c+d$, такое же уравненіе, какъ и

$a+b+c=a+c+b$, но только мѣсто b заступило $d<b$.

Продолжая такимъ образомъ, всякій разъ будемъ большее изъ двухъ придаваемыхъ уменьшать по крайней мѣрѣ единицею; а такъ какъ они цѣлыя, то наконецъ одно изъ нихъ сдѣлается нулемъ. Это предполагаетъ впереди равенство ихъ, а слѣдовательно тождественное уравненіе.

Въ особенности замѣтимъ случай $a=0$. Тогда $b+c=c+b$. Это значитъ, что *въ суммѣ двухъ чиселъ все равно, которое къ которому ни придавать*. Вотъ почему, не различая, которое къ которому придается, о двухъ числахъ говорятъ, что они складываются; также о многихъ числахъ, потому что и здѣсь различіе не нужно“.

Кромѣ этого доказательства коммутативности сложенія, въ изложеніи основаній алгебры Лобачевскаго заслуживаетъ еще вниманіе слѣдующее доказательство предложенія: *разность двухъ чиселъ можетъ быть только одно число.* „Въ цѣлыхъ, когда продолжаемъ считать отъ вычитаемаго, пока дойдемъ до уменьшаемаго, число присчитанныхъ единицъ изобразитъ разность, а какъ *всякое цѣлое число въ продолженіи счета можетъ быть упомянуто только одинъ разъ, то и разность двухъ чиселъ можетъ быть только одна*".

Въ послѣднее время вопросъ объ аксіомахъ ариѳметики былъ предметомъ обширной литературы и многихъ глубокихъ изысканій.

Важнѣйшія изъ сочиненій, разсматривающихъ вопросъ съ *математической*[1] точки зрѣнія суть слѣдующія:

1. *Schröder*. Lehrbuch der Arithmetik und Algebra. Leipz. 1873. Подробный анализъ понятія о числѣ и выводъ законовъ операцій двумя путями. 1° по Грассману (in recurrenter Behandlung) и 2° исходя изъ выставленной Шредеромъ съ особенною опредѣленностію единственной аксіомы ученія о цѣлыхъ числахъ —аксіомы о независимости числа отъ порядка счета (см. § 15).

2. *Dedekind*, Was sind und was sollen die Zahlen. 1888. 2-е изданіе. 1893. Braunschw.

3. *Peano*. Arithmetices principia nova methodo exposita. Torino. 1889. Подобно Гельмгольцу и Кронекеру Дедекиндъ и Пеано исходятъ также изъ *порядковыхъ* чиселъ. Для Пеано вся ариѳметика цѣлыхъ чиселъ сводится къ тремъ первоначальнымъ (не опредѣленнымъ) идеямъ; *0*, идея цѣлаго числа и идея *слѣдующаго*

---

[1] Изъ сочиненій, разсматривающихъ вопросъ съ *философской* точки зрѣнія, упомянемъ *Frege*. Die Grundlagen der Arithmenk Eine logisch mathematische Untersuchung über den Begriff der Zahl. Breslau. 1884. *Husserl*, Philosophie der Arithmetik 1891. *Couturat*, De l'infini mathématique Paris. 1896 и соотвѣтствующія главы логикъ Милля, Вундта и Зигварта. Нельзя не указать на то, что большинство этихъ авторовъ (Husserl, Зигвартъ и Кутюра) являются противниками изложенной нами теоріи цѣлыхъ чиселъ, основанной на идеѣ порядка, Аргументы Зингварта, а также и другія сочиненія по философіи ариѳметики, изложены въ вышеупомянутой статьѣ Челпанова «Обзоръ новѣйшей литературы по теоріи познанія». Изъ учебниковъ составленныхъ по идеямъ Генриха Грассмана кромѣ вышеупомянутаго его учебника укажемъ выше на учебникъ, составленный его братомъ: Die Zahlenlehre oder Arithmetik streng wissenchaftlich in strenger Formeentwickelung von Robert Grassmann. Stetin 1891 и учебникъ Шредера (см. въ текстѣ).

за другими и къ слѣдующимъ пяти независимымъ между собою предложеніямъ: (1) 0 есть число; (2) если a есть число, то *слѣдующее* за a есть также число; (3) если два числа имѣютъ одно слѣдующее число, то они тождественны, (4) 0 не слѣдуетъ ни за какимъ числомъ; (5) принципъ математической индукціи.

Дедекиндъ исходитъ изъ понятія о системахъ вещей (элементовъ системы) и изъ понятія объ изображеніи (Abbildung) системы. Система S *изображается* системою S', если каждому элементу S соотвѣтствуетъ одинъ и только одинъ элементъ S', (этотъ элементъ x' есть изображеніе элемента x системы S), но нѣсколькимъ элементамъ S можетъ соотвѣтствовать одинъ элементъ S' (такъ, если S есть система, состоящая изъ людей разсматриваемыхъ какъ *сыновья*, S' есть система *отцовъ*). Если же и обратно каждому элементу S' соотвѣтствуетъ одинъ и только одинъ элементъ S', то двѣ системы будутъ *подобны* (такъ, системы *отцовъ* и *сыновей-первенцевъ* суть системы подобныя). Система можетъ заключать въ себѣ свое *изображеніе* (такъ, система *отцовъ* заключаетъ въ себѣ свое *изображеніе*, т. к. каждый отецъ есть въ тоже время и сынъ, другого элемента той-же системы). Пусть x есть элементъ системы S, x' его *изображеніе*, заключающееся также въ S, а именно x'' изображеніе x', x''' изображенія x'' и т. д. всѣ эти изображенія заключаются въ S.

Система x, x', x'',...., составляющая *часть* системы S, называется цѣпью (такъ, напр., возьмемъ въ системѣ всѣхъ отцовъ лицо A, его отца A'. его дѣла A'', его прадѣда A'' и т. д. и т. д.; A', A', A''.... составляютъ *цѣпь*). Представимъ теперь систему элементовъ N, характеризуемую слѣдующими 4 свойствами:

1°. Изображеніе N заключается въ N.

2°. Изображеніе N подобно системѣ N.

3°. Система N есть *цѣпь* одного изъ своихъ элементовъ A, но

4°. Этотъ элементъ A не заключается въ N'.

(Всѣ эти свойства принадлежатъ, какъ легко видѣть, приведенной выше въ примѣръ, системѣ A, A', A''.....,; система содержитъ въ себѣ свое подобное изображеніе A'. A'',....; она есть цѣпь. начинающаяся съ A, но этотъ элементъ A не содержится въ изображеніи системы. Система *сыновей первенцевъ* будетъ также система, имѣющая указанныя свойства). Такія системы называются *однократно безконечными.* Система цѣлыхъ положительныхъ чиселъ есть частный случай такой однократно безконечной системы; тотъ первый элементъ, съ котораго начинается система, обозначается 1, изображеніе 1 ($1'$) асть 2, $2'=3$, $3'=4$,... Система цѣлыхъ чиселъ есть въ то же время *абстракція*, получающаяся, если мы, разсматривая однократно безконечныя системы, оставимъ безъ вниманія свойство элементовъ и обратимъ наше вниманіе только на ихъ взаимное отношеніе. Эта система цѣлыхъ чиселъ и можетъ поэтому послужить къ опредѣленію порядка, занимаемаго какимъ-либо элементомъ въ какой-либо однократно-безконечной системѣ. Свойства системы цѣлыхъ чиселъ выходятъ изъ общихъ свойствъ подобныхъ системъ, цѣпей и однократно-безконечныхъ системъ [1]). Ариѳметика становится частью логики, т. к. понятіе о числѣ выводится вполнѣ независимо отъ представленій о пространствѣ и времени, какъ непосредственный результатъ „чистыхъ законовъ мысли“.

Теоріи Дедекинда и Пеано подвергнуты критической обработкѣ въ замѣчательномъ трудѣ по философіи чистой математики, появившемся въ 1903 г.: *Russel.* Principles of Mathematics. Теорія Пеано положена въ основаніе ученія о числахъ въ сочиненіи Stolz-Gmeiner, Theoretische Arithmetik, Leipz.

4. Гильбертъ. *Понятіе о числѣ* [2]). Въ этой небольшой работѣ авторъ, слѣдуя идеямъ, положеннымъ имъ въ основаніе его классической работы. „Основанія Геометріи“ (получившей премію Лобачевскаго по конкурсу 1903 г.), даетъ классификацію аксіомъ ариѳметики, подобную данной имъ классификаціи аксіомъ геометріи.

I. Аксіомы сочетанія. Для цѣлыхъ положительныхъ чиселъ эти аксіомы будутъ:

I. 1. Изъ числа a и изъ числа b образуется посредствомъ сложенія опредѣленное число c, это обозначается

$$a+b=c \text{ или } c=a+b$$

I. 2. Если a и b суть данныя числа, то существуетъ (если $a>b$; см. аксіому III. 1) всегда одно и только одно число x и также одно и только одно число y, такъ что $a+x=b$ и соотвѣтственно $y+a=b$.

I. 3. Существуетъ опредѣленное число—оно обозначается 0—такъ что для каждаго a мы имѣемъ одновременно

$$a+0=a \text{ и } 0+a=a.$$

I. 4. Изъ числа a и числа b образуется также посредствомъ „*Умноженія*“ опредѣленное число c; употребляя обозначенія:

$$ab=c \text{ или } c=ab.$$

(¹) Такъ напр. число m называется числомъ меньшимъ числа n, если цѣпь числа n заключается въ изображеніи цѣпи числа m.

(²) Извѣстія Каз. Физико-Матем. Общ. Т. XI.

I. 5. Существуетъ опредѣленное число—обозначаемъ его 1—такъ-что для каждаго a одновременно:

$$a.1=a \text{ и } 1.a=a.$$

II. Аксіомы счета (Законы коммутативности, ассоціативности и дистрибутивности операцій сложенія и умноженія)

III. Аксіомы порядка.

III. 1. Если a, b суть какія нибудь два различныя числа, то всегда одно опредѣленное изъ нихъ больше ($>$), чѣмъ другое; это послѣднее называется тогда меньшимъ; это обозначается:

$$a>b \text{ и } b<a$$

III. 2. Если $a>b$ и $b>c$, то и $a>c$.

III. 3. Если $a>b$, то всегда и $a+c>b+c$ и $c+a>c+b$.

III. 4. Если $a>b$ и $c>0$, то всегда и $ac>bc$ и $ca>cb$.

IV. Архимедова аксіома. Если $a>0$ и $b>0$ суть два произвольныя числа, то всегда возможно сложить a послѣдовательно столько разъ, что соотвѣтствующая сумма будетъ имѣть свойство:

$$a+a+a+\ldots+a>b.$$

Аксіомы не независимы между собою; такъ существованіе 0 (аксіома I. 3) есть слѣдствіе I. 1, I. 2 и II. 1. $(a+(b+c))=((a+b)+c)$; оно основывается такимъ образомъ существенно на ассоціативномъ законѣ сложенія. Подобнымъ же образомъ существованіе 1 есть слѣдствіе закона ассоціативности умноженія. Коммутативность сложенія (аксіома II. 2) есть слѣдствіе аксіомы I, ассоціативнаго закона сложенія и обоихъ дистрибутивныхъ законовъ. Дѣйствительно, имѣемъ съ одной стороны

$$(a+b)(1+1)=(a+b).1+(a+b).1=a+b+a+b,$$

съ другой стороны

$$(a+b)(1+1)=a(1+1)+b(1+1)=a+a+b+b, \text{ откуда } b+a=a+b.$$

Эти примѣры приводятъ къ задачѣ:
развить логическую зависимость аксіомъ между собою (¹).

(¹) Въ своемъ сообщеніи на Международномъ Парижскомъ конгрессѣ Гильбертъ ставитъ какъ одну изъ тѣхъ задачъ математики, отъ рѣшенія (или доказательства невозможности рѣшенія) которыхъ будетъ зависѣть будущее движенія математической науки,—задачу доказательства непротиворѣчивости ариѳметическихъ аксіомъ.

§ 15. Въ предыдущемъ изложеніи въ основаніе ариѳметики или ученія о цѣлыхъ числахъ былъ положенъ рядъ порядковыхъ чиселъ т. е. законовъ, служащихъ для указанія порядка. Свойства чиселъ, равно какъ и законы операцій надъ ними, выводятся изъ такого опредѣленія ихъ какъ указателей порядка. Но опредѣленный такимъ образомъ рядъ можетъ послужить и для другой цѣли, *для опредѣленія численности* элементовъ какой-либо группы конечныхъ вещей или абстрактныхъ понятій или иначе объектовъ какого-либо множества, состоящаго изъ раздѣльныхъ и различимыхъ вещей (припомнимъ Эвклидово опредѣленіе натуральнаго числа).

Если для того, чтобы каждому элементу группы соотвѣтствовало число ряда, понадобится полный численный рядъ отъ 1 до n, то n называется *численностью* группы или множества. Представимъ себѣ теперь нѣсколько группъ, имѣющихъ одинаковую численность. Эти множества будутъ, очевидно, имѣть то свойство, что будетъ возможно каждому элементу одного (того или другого) множества поставить въ соотвѣтствіе одинъ—и только одинъ—элементъ другого множества.

Это свойство множествъ, которое мы постоянно замѣчаемъ во внѣшнемъ мірѣ, мы можемъ принять за основную базу ученія о цѣлыхъ положительныхъ числахъ. Назовемъ множества, имѣющія указанное свойство, вмѣстѣ съ Г. Канторомъ множествами эквивалентными (Дедекиндъ называетъ ихъ, какъ мы видѣли, подобными),

Такъ группа цвѣтовъ радуги и группа основныхъ тоновъ октавы, группа названій дней недѣли и группа мудрецовъ древней Греціи—суть группы между собою эквивалентныя.

Численностью множества (иначе *кардинальнымъ* числомъ, иначе *мощностью* множества) можно назвать ту общею **идею**, которая выводится, разсматривая эквивалентныя группы и *отвлекаясь* какъ *отъ природы* элементовъ, такъ *и отъ порядка*, въ которомъ они расположены.

Вслѣдствіе этого опредѣленія, кардинальное число, не завися отъ порядка, въ которомъ расположены предметы, не можетъ зависѣть и отъ того порядка, въ которомъ они пересчитываются.

Такимъ образомъ, слѣдствіемъ опредѣленія является основная аксіома ученія о цѣлыхъ положительныхъ числахъ: *число всякой конечной группы раздѣльныхъ вещей не зависитъ отъ порядка ихъ пересчитыванія.*

Легко видѣть, что законы коммутативности и ассоціативности сложенія и умноженія, равно какъ и законъ дистрибутивности, являются слѣдствіемъ этой основной аксіомы. Чтобы показать, напр., что $ab=(\overset{1}{a}+\overset{2}{a}+\ .\ .\ .\ .\ \overset{b}{a})=ba=(\overset{1}{b}+\overset{2}{b}+\ .\ .\ .\ .\ \overset{a}{b})$, представимъ себѣ группу предметовъ въ числѣ $N=ab$ и расположимъ ее въ b горизонтальныхъ строкахъ такъ, чтобы каждая строка заключала a предметовъ; пересчитывая предметы въ одномъ вертикальномъ столбцѣ, получимъ b предметовъ, а такъ-какъ число вертикальныхъ столбцовъ есть a, то въ результатѣ новаго пріема пересчитыванія найдемъ $N=ba$, что и тр. д.

Такимъ образомъ показывается примѣнимость и другихъ законовъ сочетанія.

Замѣтимъ, что понятіе объ эквивалентности множествъ, данное нами, можетъ быть распространено и на множества, заключающія въ себѣ *безконечное* число вещей, напр., на ряды, состоящіе изъ безконечнаго множества цѣлыхъ чиселъ. Такъ напр., ряды
1, 2, 3, 4,....
2, 4, 6, 8,.... суть очевидно множества эквивалентныя, т. к. каждому элементу одного множества можно поставить въ соотвѣтствіе одинъ, и только одинъ, элементъ—другого множества. Мы называемъ эти ряды имѣющими одну и ту-же *мощность* (Mächtigkeit), такъ что мощность есть распространеніе понятія о числѣ. Подобнымъ-же образомъ рядъ паръ цѣлыхъ чиселъ [составленный по слѣдующему правилу: пары распредѣляются по порядку возрастанія суммы чиселъ пары, при одинаковой-же суммѣ по порядку возрастанія перваго числа пары]:

[0,1], [1,0], [0,2], [1,1], [2,0], [0,3], [1,2], [2,1], [3,0] . . . . .
есть рядъ эквивалентный съ рядомъ 1, 2, 3, 4, 5,.....

Безконечныя множества отличаются отъ конечныхъ тѣмъ, что для нихъ, очевидно, не имѣетъ примѣненія аксіома: *цѣлое болѣе своей части*. Дедекиндъ принимаетъ за опредѣленіе безконечнаго множества именно это свойство: *множество есть множество безконечное, если его часть можетъ быть эквивалентна цѣлому.*

§ 16. Операціи третьей и четвертой ступеней.

Если мы назовемъ сложеніе операціею *первой* ступени, а умноженіе—операціею *второй* ступени, то между ними существуетъ соотношеніе, по которому умноженіе есть повторенное сложеніе, т. е. сложеніе, въ которомъ одно и то же число a берется слагаемымъ b разъ: $ab=\overset{1}{a}+\overset{2}{a}+\ .\ .\ +\overset{b}{a}$. Поэтому, если мы захотимъ составить операцію *третьей* ступени, которая относилась-бы къ умноженію подобно тому, какъ умноженіе относится къ сложенію, то мы должны взять одно и то же число a множителемъ b разъ. Новая операція соединенія двухъ чиселъ a и b называется *возвышеніемъ въ степень* и обозначается a^b; a—называется *основаніемъ*, b—*показателемъ* степени. a^b—*степенью*.

$$a^b = \overset{1}{a} \cdot \overset{2}{a} \cdot \overset{3}{a} \ldots \overset{b}{a}$$

Изъ этого опредѣленія возвышенія въ степень получимъ, примѣняя законы умноженія, слѣдующіе законы возвышенія въ степень:

$$\text{(I)} \qquad a^p \cdot a^q = a^{p+q}; \quad a^p \cdot b^p = (ab)^p \qquad \text{(II)}$$

$$\text{(III)} \qquad (a^p)^q = a^{pq}.$$

Вторыя и третьи степени, имѣющія такое важное значеніе въ геометріи, разсматривались уже греческими геометрами. Въ ариѳметическихъ изслѣдованіяхъ Діофанта разсматривались уже степени до 6-ой. Въ 14 и 16 столѣтіяхъ находимъ начала теоріи дѣйствій надъ степенями и корнями у Орезма, Ризе, Рудольфа и въ особенности у Михаила Стифеля. Но особенное значеніе получило ученіе о степеняхъ послѣ изобрѣтенія логариѳмовъ.

Отъ операціи третьей ступени можно перейти къ операціи *четвертой* ступени—*возвышенію въ сверхъ-степень* (гиперпотенцированію), опредѣляя b (ую) сверхъ-степень отъ числа a слѣдующимъ образомъ:

$$a^{(b)} = a^{a^{\cdot^{\cdot^{\cdot^{a^a}}}}}$$

(b) показываетъ, сколько разъ повторяется a.

Эта операція и по своей трудности и по отсутствію примѣненій разсматривалась до сихъ поръ еще очень мало. Кажется, первый, кто заинтересовался ею, былъ математикъ и философъ—позитивистъ маркизъ Кондорсе. Послѣ него Эйлеръ изслѣдовалъ быстроту возрастанія „сверхъ-степени“, которая поразительна:

$$2^{(1)} = 2,\ 2^{(2)} = 4,\ 2^{(3)} = 2^{2^2} = 16,\ 2^{(4)} = 65536,$$

а $2(^5)$—заключаетъ въ себѣ уже 19729 цифръ;

$$3(^3) = 1594.323 \times 59040, \text{ и т. д.}$$

Между тѣмъ для $a=1$, $a(^m)=1$, какъ бы велико—ни было m. Точно также для $a=\sqrt{2}$, $a(^m)$, какъ-бы велико ни было m, очевидно, меньше, чѣмъ

$a^{a^{\cdot^{\cdot^{\cdot^{a^2}}}}}= 2$. Эйлеръ и поставилъ интересную задачу: опредѣлить, при какомъ a, очевидно заключающемся между $\sqrt{2} =1,4121..$ и 2, сверхъ—степень начинаетъ быстро возрастать (ubi ista enormis augmentatio incipiat), и находитъ число $e^{\frac{1}{e}} = 1,44467.....$ (e есть такъ называемое Неперово число 2,71828...)[1]).

Сверхъ-степень $a(^{m})$ есть частное значеніе для $x= 1$ отъ функціи $a^{a^{\cdot^{\cdot^{\cdot^{a^x}}}}}$, которая при $a = e$ играетъ въ настоящее время весьма важную роль въ ученіи о сходимости положительныхъ строкъ.

§ 17. Обратныя операціи первыхъ трехъ ступеней.

Каждое положеніе можетъ быть обращено въ одинъ или нѣсколько вопросовъ. Гауссъ отпечаталъ свои знаменитыя „Disquisitiones“ въ 1801 г. Это положеніе можетъ послужить къ постановкѣ нѣсколькихъ вопросовъ: когда напечатаны „Disquisitiones“, какая знаменитая книга была напечатана въ 1801 г. и т. д. Подобно этому, если два числа a и b, соединенныя знакомъ $+$, даютъ третье число c, то мы можемъ сдѣлать изъ этого положенія два вопроса:

1) **Къ какому числу** нужно придать извѣстное число b для того, чтобы получить другое извѣстное число c?

2) **Какое число** нужно придать къ извѣстному числу a для того, чтобы получить другое извѣстное число c?

Оба вопроса по своему логическому смыслу различны. Если года A больше годовъ B на m лѣтъ, то два обратные вопроса: 1) сколько лѣтъ B и 2) на сколько лѣтъ A старше B очевидно различны по своему смыслу. *Но математическая операція*, съ помощью которой рѣшаются оба вопроса, *одна и та-же* и называется *вычитаніемъ*. *Причина* этого въ *коммутативности сложенія*, которая дозволяетъ видоизмѣнять по произволу порядокъ слагаемыхъ.

---

[1]) De formulis exponentialibus replicatis (Acta Acad. Petropol 1768).

Въ послѣднее время многіе результаты Эйлера были найдены снова Лемере, статьи котораго «о четвертомъ натуральномъ алгориѳмѣ» печатались въ Nouv Ann. за 1898 и 1899 г.

$$\left.\begin{array}{l}\sqrt[n]{a}\cdot\sqrt[n]{b}=\sqrt[n]{ab},\quad \sqrt[n]{a}:\sqrt[n]{b}=\sqrt[n]{a:b}\\ \sqrt[p]{a^q}=\left(\sqrt[p]{a}\right)^q,\ \sqrt[p]{\sqrt[q]{a}}=\sqrt[pq]{a}=\sqrt[q]{\sqrt[p]{a}},\ \sqrt[np]{a^{nq}}=\sqrt[p]{a^q}\end{array}\right\}\ \text{(III)}$$

$$\left.\begin{array}{r}Log_b\,(p.q)=Log_b\,p+Log_b\,q\\ Log_b\,(p:q)=Loq_b\,p-Log_b\,q\\ Log_b p^m=m.Log_b p,\ Log_b a=\dfrac{Log_c\,a}{Log_c\,b}.\end{array}\right\}\ \text{(IV)}$$

Доказательства всѣхъ этихъ формулъ, имѣющихъ *для насъ* смыслъ, пока символами выражаются *цѣлыя* числа, основываются также на опредѣленіи обратныхъ дѣйствій, на законахъ соотвѣтствующаго прямого дѣйствія и на аксіомахъ.

§ **19. Алгебра есть послѣдовательное комбинированіе основныхъ законовъ.** Повторное примѣненіе и комбинированіе данныхъ въ предыдущихъ §§ законовъ 7 алгебраическихъ операцій даетъ всю ту цѣпь формулъ, которая составляетъ алгебру (пока алгебру цѣлыхъ чиселъ).

Алгебра имѣетъ цѣлью раскрыть или вывести всѣ слѣдствія, вытекающія изъ аксіомъ и законовъ сложенія и умноженія. Доказать формулу алгебры—значитъ комбинировать аксіомы и законы. „Доказательство въ формальныхъ наукахъ, какова алгебра“, говоритъ Грассманъ, „не выходитъ изъ предѣловъ мышленія и состоитъ только въ комбинаціи мыслительныхъ актовъ“.

Примѣры. 1. Предлагаемъ читателю прослѣдить доказательство формулы бинома Ньютона и убѣдиться въ томъ, что эта формула есть только послѣдовательное примѣненіе законовъ сложенія и умноженія и способа математической индукціи. Напр.:

$$(a+b)^2=(a+b)(a+b)=a(a+b)+b(a+b)=a^2+ab+ba+b^2=$$
$$=a^2+2ab+b^2$$

2. Обозначая знакомъ $a^{(m)}=a(a-1)....(a-m+1)$ имѣемъ формулу Вандермонда, обобщающую формулу Ньютона:

$$(a+b)^{(m)}=a^{(m)}+\frac{m}{1}a^{(m-1)}b+\frac{m(m-1)}{1.2}a^{(m-2)}b^{(2)}....+b^{(m)}.$$

3. Лобачевскій въ Алгебрѣ (стр. 359 и слѣд.) даетъ формулу для вычисленія произведенія

$(x+\varphi(1)).(x+\varphi(2)).....(x+\varphi(n))$, гдѣ φ (n) есть многочленъ отъ n.

Если къ законамъ сложенія и умноженія присоединить законъ вычитанія, то получатся новыя формулы, въ примѣръ которыхъ приведу основныя формулы исчисленія конечныхъ разностей.

Имѣя рядъ чиселъ u_0, u_1, $u_2.....u_n$,.... обозначимъ знакомъ Δu_i разность $u_{i+1}-u_i$; пусть также

$$=\Delta u_{i+1}-\Delta u_i, \qquad \Delta^3 u_i=\Delta^2 u_{i+1}-\Delta^2 n_i \text{ и т. д.}$$

По способу математической индукціи легко доказываются слѣдующія двѣ формулы.

$$1) \qquad u_n=u_0+\frac{n}{1}\Delta u_0+\frac{n(n-1)}{1.2}\Delta^2 u_0+....\frac{n}{1}\Delta^{n-1}u_0+\Delta^n u_0$$

$$2) \qquad \Delta^n u_0=u^n-\frac{n}{1}u_{n-1}+\frac{n(n-1)}{1.2}u_{n-2}-....+(-1)^n u_0.$$

(Коэффиціенты обѣихъ формулъ суть коэффиціенты формулы бинома Ньютона).

4. Вывести изъ формулы (2) формулу

$$1.2.....n=(n+1)^n-\frac{n}{1}n^n+\frac{(n-1)}{1.2}(n-1)^n.....+(-1)^n.1^n.$$

5. Изъ тожествъ, доказываемыхъ на основаніи законовъ сложенія, умноженія, возвышенія въ степень и вычитанія, приведемъ въ примѣръ тожество:

$$(a^2+b^3+c^2+d^2)\,(a'^2+b'^2+c'^2+d'^2)-(aa'+bb'+cc'+dd')^2=$$
$$=(ab'-a'b+cd'-c'd)^2+(ac'-a'c+b'd-bd')^2+(ad'-a'd+bc'-b'c)^2;$$

изъ котораго легко получить тожество Эйлера-Лагранжа, имѣющее важное значеніе въ геометріи:

$$(a^2+b^2+c^2)(a'^2+b'^2+c'^2)-(aa'+bb'+cc')^2=$$
$$=(ab'-ba')^2+(bc'-b'c)^2+ca'-ac')^2.$$

Къ тѣмъ-же тожествамъ относятся формулы, выражающія черезъ x_1, x_2,...x_n коэффиціенты p многочлена $x^n-p_1x^{n-1}+$ $+p.x^{n-}{}_1-...\pm p_n$, равнаго произведенію $(x-x_1)(x-x_2)......(x-x_n)$, и формулы Ньютона, дающія выраженіе суммы степеней чиселъ x_1, x_2, ... x_n посредствомъ p_1,p_2, . . p_n. Тѣмъ же путемъ выводится выраженіе такъ называемой знакоперемѣнной функціи.

$$\begin{array}{l} (\alpha-\beta)\ (\alpha-\gamma)\ (\alpha-\delta)\ldots\ldots(\alpha-\varkappa)\ (\alpha-\lambda) \\ \qquad(\beta-\gamma)\ \ldots\ldots\ (\beta-\lambda) \\ \qquad\ldots\ldots\ldots\ldots\ldots\ldots \\ \qquad\qquad\qquad\qquad(\varkappa-\lambda) \end{array}$$

расположенное по степенямъ α, β, ... λ.

Еще болѣе интересныя и разнообразныя формулы получаются, если къ операціямъ сложенія, вычитанія, умноженія, возвышенія въ цѣлую положительную степень мы присоединимъ операціи дѣленія.

Сюда относятся напр. формулы Безу, выражающія въ видѣ цѣлаго многочлена $\frac{x^n-a^n}{x-a}$ и $\frac{x^{2m+1}+a^{2m+1}}{x+a}$. Сюда-же относится теорія такъ называемыхъ возвратныхъ рядовъ, въ которой частное отъ дѣленія двухъ цѣлыхъ многочленовъ $\frac{x^m+p'x^{m-1}+\ldots p_m}{x^n+q'x^{n-1}+\ldots q_n}$ приравнивается $A_0+A_1x+A_2x^2+\ldots+A_nx^n+\ldots$ Для того, чтобы равенство было возможно, необходимо, чтобы начиная съ нѣкотораго A_i существовало соотношеніе:

$$A_i+A_{i-1}\,q_1+A_{i-2}\,q_2+\ldots+A_{i-n}\,q_n=0,$$

дающее возможность опредѣлить A_i посредствомъ A_{i-1}, $A_{i-2}..A_{i-n}$

Примѣняя этотъ пріемъ къ разложенію дробей $\frac{1}{1-x}$, $\frac{1}{(1-x)^2}$, $\frac{1}{(1-x)^3}$...

находимъ

$$\frac{1}{1-x}=1+x+x^2+x^3+\ldots\ldots$$

$$\frac{1}{(1-x)^2}=1+2x+3x^2+4x^3+\ldots\ldots$$

$$\frac{1}{(1-x)^3}=1+3x+6x^2+10x^3+\ldots\ldots$$

(Коэффиціенты 1, 3, 6, 10,.....суть, такъ называемыя, треугольныя числа)

$$\frac{1}{(1-x)^4}=1+4x+10x^2+20x^3+\ldots\ldots$$

(Коэффиціенты—пирамидальныя числа).

Разложеніе раціональныхъ функцій въ ряды имѣетъ важное значеніе въ такъ называемомъ вопросѣ **о разбіеніи** чиселъ (*на слагаемыя*). Такъ, напримѣръ,

$$\frac{1}{(1-x)(1-x^2)(1-x^3)(1-x^4)\ldots\ldots}=$$
$$=1+x+2x^2+3x^3+5x^4+7x^5+11x^6+\ldots\ldots$$

Коэффиціентъ каждаго числа строки показываетъ, сколькими способами соотвѣтствующій показатель можетъ быть составленъ— путемъ сложенія цѣлыхъ чиселъ равныхъ или неравныхъ. Такъ число 6 можетъ быть 10-ю способами составлено сложеніемъ цѣлыхъ чиселъ.

Наконецъ, комбинированіе аксіомъ и законовъ *семи* операцій даетъ еще болѣе разнообразную систему формулъ, неявно заключающуюся въ этихъ законахъ, и, слѣдовательно, въ основныхъ аксіомахъ и законахъ сложенія и умноженія, т. к. законы прочихъ дѣйствій суть законы производные.

§ 20. Алгебра логики. Указанная въ предыдущемъ § **возможность развить всю цѣпь формулъ алгебры изъ основныхъ аксіомъ и изъ законовъ** сложенія и умноженія не составляетъ особенности ученія о цѣлыхъ положительныхъ числахъ, единственныхъ, введенныхъ нами до сихъ поръ. Главная цѣль „курса введенія въ анализъ“ заключается въ томъ, чтобы показать возможность послѣдовательнаго **обобщенія** понятія о числѣ (введенія чиселъ отрицательныхъ, дробныхъ, несоизмѣримыхъ, комплексныхъ). При всѣхъ этихъ обобщеніяхъ законы операцій надъ числами остаются безъ измѣненія; остается, поэтому, безъ измѣненія вся система формулъ алгебры, дедуктивнымъ путемъ получаемая изъ аксіомъ и законовъ операцій. Во всѣхъ формулахъ предыдущаго § буквы могутъ обозначать, поэтому, не только цѣлыя положительныя числа, **но и** отрицательныя, дробныя, несоизмѣримыя, комплексныя.

Дедуктивный характеръ ученія о числахъ не составляетъ особенности только этого ученія. Алгебра чиселъ можетъ быть разсматриваема, какъ частный случай другой болѣе общей науки, которой придавались разныя названія: операціоннаго исчисленія (англійская школа), ученія о формахъ (Г. Грассманъ) и, наконецъ, всеобщей алгебры (подъ этимъ названіемъ издана въ прошломъ году книга Уайтхеда (Whitehead)).

Такъ мы можемъ изучить систему формулъ, которая является слѣдствіемъ основныхъ законовъ сложенія и умноженія (§ 11—13), если къ нимъ кромѣ того присоединимъ два новые закона:

(α) $a+ab=a$ (въ частности $a+a=a$)
(β) $a\,.\,a=a$

Какъ въ алгебрѣ чиселъ, такъ и здѣсь вводимъ модули сложенія (0) и умноженія (i), такъ что $a+0=a$, $a\,.\,i=a$.

Выведемъ нѣсколько слѣдствій изъ этихъ основныхъ законовъ, напримѣръ, докажемъ, что

$$(x+y)\times(x+z)=x+yz.$$

Дѣйствительно, $(x+y)(x+z)=xx+xy+xz+yz=$

$x+xy+xz+yz=x+x(x+y)+yz$; но $x+x(y+z)=x$.

Итакъ, $(x+y)\times(x+z)=x+yz$

Съ другой стороны, $xy+xz=x\times(y+z)$.

Сопоставленіе этихъ двухъ формулъ указываетъ на интересную особенность новаго исчисленія, на дуализмъ всѣхъ его формулъ. Изъ каждой формулы можетъ быть получена другая, замѣняя знакъ $(+)$ знакомъ умноженія $(\times)$ и обратно знакъ $(\times)$ знакомъ $(+)$. Въ нашей алгебрѣ этотъ дуализмъ отсутствуетъ, такъ-какъ закону дистрибутивности $x(y+z)=yx+xz$ не соотвѣтствуетъ закона $x+yz=(x+y)\times(x+z)$, который имѣетъ мѣсто въ новой алгебрѣ и является слѣдствіемъ закона (поглощенія) $a+ab=a$.

Алгебра, основанная на новыхъ законахъ, имѣетъ **реальную** приложимость къ изученію областей плоскости (или пространства; для большей наглядности, мы ограничимся областями плоскости).

Пусть A, B, C.... суть **части плоскости**, ограниченныя какими-либо контурами; пусть $A+B$ означаетъ область **объемлющую** и область A и область B, $A\times B$—**общую часть** областей A и B, если онѣ таковую имѣютъ, i—**всю плоскость**, 0—**несуществующую** область. (Поэтому, если A и B не имѣютъ общей части, то $A\times B=0$). Легко убѣдиться въ томъ, что всѣ законы, выше данные для новой алгебры, имѣютъ мѣсто для соединенія областей знаками сложенія и умноженія. Напр., часть общая областямъ A и B совпадаетъ съ частью общею областямъ B и A, т. е. $A\times B=B\times A$; если къ области A прибавить часть, общую [1] ей и области B, то получимъ ту-же самую область A, т. е. $A+A\times B=A$.

Эйлеръ въ своихъ „Lettres à princesse allemande" (ранѣе его Людовикъ Вивесъ, логикъ 15 вѣка) примѣнили графическое изображеніе понятій областями плоскости къ формальной или дедуктивной логикѣ. Области соотвѣтствуютъ понятіямъ (классамъ); **область объемлющая нѣсколько** другихъ **областей**, соотвѣтствуетъ **понятію** (классу), объемлющему **нѣсколько** другихъ **понятій** (понятіе: Европеецъ—объемлетъ понятія: Русскій, Англичанинъ, Французъ...);

---

[1] Если мы условились обозначать $A\times B$; $Ai=A$, т. к. *A лежитъ вся на плоскости i*, и A есть *общая* часть у A и i.

область общая двумъ областямъ соотвѣтствуетъ понятію, соединяющему въ себѣ **признаки двухъ понятій** (понятіе бѣлая лошадь соединяетъ въ себѣ признаки понятія бѣлаго и понятія лошади). Отсюда ясно, что вышеизложенная алгебра можетъ быть названа **алгеброю логики.**

Первый, кто обратилъ вниманіе на аналогію между элементарными законами алгебры и законами умственныхъ операцій надъ понятіями или классами, былъ знаменитый **Лейбницъ**, который предвидѣлъ возможность **замѣны логическихъ разсужденій рядомъ преобразованій формулъ**, подобныхъ тѣмъ, которыми пользуется алгебра для рѣшенія уравненій. Лейбницъ, Ламберъ и Сегнеръ положили начало этому логическому исчисленію; но наиболѣе разработанную систему, представляющую весьма большой интересъ для математики, далъ Буль. [1]) Математическая логика, созданная Булемъ, разработывалась въ направленіи, имъ данномъ, въ особенности Шредеромъ (большое 3-томное сочиненіе Algebra der Logik. Leipz.), Венномъ, Макъ—Фарланомъ и у насъ въ Россіи П. С. Порѣцкимъ, нѣсколько сочиненій котораго напечатаны въ „Извѣстіяхъ Физ.-Мат. Общ. при Императорскомъ Каз. Унив“.

Большія услуги въ разработкѣ математической логики оказаны также итальянскою школою профессора Пеано. Результатомъ трудовъ этой школы является изданіе „Formulaire de Mathématiques“, которое преслѣдуетъ цѣль—всѣ предложенія и доказательства представить символически, при помощи особыхъ знаковъ. Новѣйшая математическая логика разсматриваетъ отдѣльно:

a) логику предложеній, *b*) логику классовъ и *c*) логику отношеній. Для знакомства съ ними можно рекомендовать сочиненіе Россэля: Philosophy of Mathematics. Cambr. 1903.

IV

Техника ариѳметики.

§ **21**. Если требуется сложить или перемножить два числа, то мы можемъ всегда произвести эти операціи путемъ послѣдовательнаго присчитыванія по единицѣ (см. § 11—13); но понятно, какъ утомителенъ и продолжителенъ этотъ пріемъ въ случаѣ двухъ сколько-нибудь значительныхъ чиселъ. Однимъ изъ первыхъ и

---

[1]) Сочиненія Буля относятся къ *1847* (The mathematical analysis of logic, being an essay toward a calculus of deductive reasonning) и *1854* (Investigation of the laws of thought).

важнѣйшихъ слѣдствій пользованія вышеприведенными законами операцій является громадная экономія труда, получающаяся отъ облегченія всѣхъ операцій надъ числами. На этихъ-же законахъ и на введеніи операцій сложенія, умноженія и возвышенія въ степень основаны способы передачи чиселъ отъ одного мыслящаго субъекта другому (словесные и письменные).

Способы эти основаны на введеніи системъ счисленія. Общій пріемъ, которымъ пользуются при этомъ, заключается въ слѣдующемъ: нѣкоторое *собраніе единицъ* (a) составляетъ *единицу второго порядка*; такое-же точно *собраніе единицъ второго порядка—единицу третьяго порядка* и т. д. Если основаніемъ подобной группировки или, какъ говорятъ, *основаніемъ системы счисленія* принято число a, то всякое число N выразится въ видѣ цѣлаго многочлена, расположеннаго по степенямъ a: $N=p_0a^n+pa^{n-1}+...+p_n$, гдѣ числа $p_0, p_1, p_2.. ... p_n$ суть числа цѣлыя меньшія p (въ томъ числѣ и число 0). При такомъ способѣ изображать числа, всякое число потребуетъ для письменнаге изображенія только знаки для обозначенія чиселъ отъ нуля до (a—1).

Такъ въ бинарной (діадической) ариѳметикѣ, которая интересовала Лейбница и которая и теперь употребляется во многихъ теоретическихъ вопросахъ, всѣ числа могутъ быть изображены двумя знаками 0 и 1. Въ системѣ двѣнадцатеричной, которая имѣла бы нѣкоторыя преимущества предъ десятеричной (признаки дѣлимости на 2, 3, 4, 6, 12 были бы также просты, какъ въ десятеричной признаки дѣлимости на 2, 5 и 10), нужно было бы 12 знаковъ; кромѣ нашихъ 0, 1,......, 9 нужны были бы особые знаки для обозначенія числа 10 и числа 11. Извѣстный натуралистъ Бюффонъ въ своей „Моральной ариѳметикѣ“ защищалъ мысль о переходѣ отъ десятеричной системы къ двѣнадцатеричной.

Позже О. Контъ остроумно указалъ на то, что природа какъ-бы подсказывала намъ именно эту систему счисленія: число суставовъ на 4 пальцахъ есть именно 12, пятый палецъ игралъ бы только роль счетчика.

Этнографія съ одной стороны, исторія человѣчества съ другой стороны даютъ намъ указаніе на пользованіе разными числами, какъ основаніями системы счисленія. Повидимому, наиболѣе распространенными системами счисленія были, кромѣ десятеричной системы, съ основаніями 5 и 20, такъ же связанныя со счисленіемъ по пальцамъ рукъ и ногъ, какъ и наша десятеричная.

Многочисленныя данныя по этому поводу собраны въ сочиненіи Потта: „Die quinäre und vigesimale Zählmethode“ (Halle 1847). Такъ, напр., Майи въ Юкатанѣ имѣютъ особыя слова для обозначенія 20, 400, 8000, 160.000. Ацтеки въ Мексикѣ имѣли особыя слова для обозначенія 20, 400, 8000. Какъ основаніе системы счисленія, *двадцать* оставило свои слѣды во многихъ языкахъ, какъ, напр., во французскомъ quatre—vingt, въ англійскомъ score.

Болѣе сомнительны приводимые нѣкоторыми авторами примѣры употребленія другихъ чиселъ кромѣ 5, 10, 20. Ал. Гумбольдтъ приводитъ извѣстіе, что Боппъ нашелъ систему, имѣющую основаніемъ шестнадцать, на страницахъ санскритской рукописи. Гунфальви нашелъ семеричную систему у цыганъ, упоминается 12-ричная система, 18-ричная система (у Осетинъ); наконецъ, 11-ричная (у Новозеландцевъ); всѣ эти свѣдѣнія, однако, требуютъ еще подтвержденій. Но въ нашей обыденной жизни при измѣреніи времени, въ геометріи и астрономіи при измѣреніи дуги круга, мы пользуемся дѣленіемъ часа на 60 минутъ, минуты на 60 секундъ, дѣленіемъ круга на 360 градусовъ и градуса на 60 минутъ, что является остаткомъ шестидесятиричной системы счисленія, употреблявшейся въ древне-вавилонской (сумерійской) культурѣ. Удастся-ли десятеричной системѣ вытѣснить этотъ остатокъ вавилонской культуры? Какъ извѣстно, въ настоящее время вопросъ о введеніи десятеричной системы дѣленія круга поставленъ на очередь.

Счетъ по пальцамъ, удобный при пересчитываніи небольшого числа предметовъ (впрочемъ въ Китаѣ, въ средневѣковой Европѣ по пальцамъ считали очень большія числа; по имени ученаго Рабды Смирнскаго это искусство называлось рабдологіею), конечно, неудобенъ для счета большихъ чиселъ; въ этомъ случаѣ пользовались другими пособіями: камешками (отсюда calculare—считать отъ calculus—камешекъ), шнуркомъ съ узлами (древній Китай, Перу, гдѣ особенные чиновники хранили эти *квинпо*), шнурками съ подвижными косточками, четками христіанскихъ или буддійскихъ монаховъ. Наши русскіе *счеты* представляютъ повидимому видоизмѣненіе Китайскаго *сюанпанъ* и представляютъ, такимъ образомъ, одно изъ заимствованій изъ китайской культуры. Въ древней Греціи роль счетовъ выполнялъ такъ называемый *абакусъ*, ящикъ съ возвышенными краями, наполнявшійся пескомъ, и на которомъ черты отдѣляли единицы, десятки, сотни. Знаки, которые употреблялись при счетѣ на абакусѣ, имѣютъ сходство съ нашими цифрами, и вопросъ о ихъ происхожденіи есть одинъ изъ интересныхъ и темныхъ вопросовъ исторіи ариѳметики.

§ 22. Болѣе ясною представляется для насъ исторія нашего способа письменнаго представленія чиселъ, который носитъ иногда названіе ариѳметики положенія. Изслѣдованія по этому поводу принадлежатъ знаменитому Александру Гумбольдту и изложены имъ въ статьѣ: „О различныхъ системахъ числовыхъ знаковъ, употреблявшихся у разныхъ народовъ“ (журналъ Крелле. Т. 4). Эти изслѣдованія даютъ возможность прослѣдить постепенное развитіе этого способа изображенія чиселъ и введенія нуля на Остъ-Индскомъ полуостровѣ.

Отъ индусовъ онъ перешелъ къ арабамъ вѣроятно съ астрономическими таблицами, привезенными въ Багдадъ однимъ индійскимъ посланникомъ въ 773 г. по Р. Х. Во всякомъ случаѣ система была уже у арабовъ въ полномъ употребленіи въ 9-омъ вѣкѣ. Въ Европу она перешла въ 12-мъ столѣтіи и долго носила названіе *algorithmus*. Это слово есть испорченное Alkhovarizmi— указаніе на мѣсто рожденія арабскаго ученаго *Мохаммеда Ибнъ-Муза* (818—883), по сочиненію котораго европейскіе средневѣковые ученые главнымъ образомъ познакомились съ новою методою. Распространенію ея въ особенности содѣйствовали *Леонардъ Пизанскій*, иначе *Фибоначчи*. Его книга: Liber Abaci, изданная въ 1202 г. передавала европейцамъ всѣ знанія арабовъ по алгебрѣ и ариѳметикѣ и доставляла имъ возможность производить просто и скоро операціи надъ числами. Но рутина, какъ всегда, держалась еще долго. Въ 1299 г., т. е. черезъ 100 лѣтъ послѣ появленія книги Леонарда, флорентинское правительство запрещало купцамъ употреблять арабскія цифры въ ихъ торговыхъ книгахъ и предписывало имъ писать числа цѣликомъ или употреблять римскія цифры. Но вскорѣ громадная экономія труда счета, получающаяся при употребленіи новой системы, стала слишкомъ очевидною.

ТЕОРІЯ ЧИСЕЛЪ.

V.

§ **I. Предметъ теоріи чиселъ.** Техника дѣйствій надъ цѣлыми числами зависитъ отъ способовъ ихъ изображенія и измѣняется вмѣстѣ съ ними; но цѣлыя числа имѣютъ кромѣ того свойства, *независимыя отъ способа изображенія, свойства принадлежащія числамъ, какъ указателямъ порядка и множественности.* Такъ, число 6 можетъ быть 11 способами представлено какъ сумма чиселъ равныхъ или неравныхъ, число 6 есть сумма чиселъ 1, 3, 3, на которыя это число дѣлится безъ остатка; оба эти свойства принадлежатъ числу 6, будемъ-ли мы писать его по десятичной системѣ или по двоичной, буквами или арабскими цифрами.

Древніе греки отличали *логистику*—правила производства операцій надъ числами—отъ *ариѳметики*, науки о теоретическихъ свойствахъ чиселъ. Въ настоящее время терминъ *логистика* не употребляется; *ариѳметикою* называется или *техника операцій* надъ числами цѣлыми (отвлеченными и именованными) и дробными или *общее ученіе о числахъ*; наука о свойствахъ цѣлыхъ чиселъ называется *теорію чиселъ* или *высшею ариѳметикою* Arithmetica sublimior) или наконецъ *ариѳмологіею* (Н. В. Бугаевъ). Какъ указатели порядка, цѣлыя числа, естественно, являются во всѣхъ тѣхъ вопросахъ, гдѣ идея порядка имѣетъ важное значеніе; къ такимъ вопросамъ, напр., относится въ геометріи вопросъ о звѣздчатыхъ многоугольникахъ [1]) (о N вершинахъ), число которыхъ, включая сюда и обыкновенный, равно *половинѣ числа чиселъ меньшихъ N и взаимно простыхъ съ N* (см. § 21 стр. 68).

Въ тѣсной связи съ теоріей чиселъ находится, поэтому, *комбинаторика или синтактика—ученіе о перемѣщеніяхъ и сочетаніяхъ*. Изученіе перемѣщеній и сочетаній доставляетъ намъ рядъ теоремъ, относящихся къ теоріи чиселъ. Таковы, напр., теоремы:

1) *Произведеніе $m(m-1)(m-2)\ldots\ldots(m-n+1)$ всегда цѣликомъ дѣлится на произведеніе $1.2.3\ldots\ldots n$.*

2) *Произведеніе $1.2.3..N$ дѣлится на $1.2\ldots a.1.2\ldots b\ldots\ 1.2\ldots k$, при условіи, если $N=a+b+c+\ldots\ldots+k$.*

Приведемъ, наконекъ, слѣдующее доказательство одной изъ важнѣйшихъ теоремъ теоріи чиселъ—теоремы Фермата (см. § 34. стр. 92).

Сосчитаемъ, сколько можно составить p—цифровыхъ чиселъ изъ 0, 1, 2,......$(a-1)$—цифръ a-ричной системы.

Таковы будутъ прежде всего числа $\overset{1}{0}\ \overset{2}{0}\ \overset{3}{0}\ \overset{4}{0}\ldots\ldots\overset{p}{0}$, 1 1 1...... 1, 2 2 2......2, $(a-1)\ (a-1)\ldots\ldots(a-1)$, не мѣняющіяся отъ круговыхъ перемѣщеній [2]).

---

[1]) Если мы на кругѣ возьмемъ N равно отстоящихъ другъ отъ друга точекъ 1, 2, 3,........N, то мы получаемъ обыкновенный правильный многоугольникъ, изучаемый въ элементарной геометріи, соединяя послѣдовательно точки 1 съ 2, 2 съ 3, съ 4,......$N-1$ съ N, N съ 1.

Если же будемъ соединять точки *въ опредѣленномъ направленіи*, но пропуская каждый разъ m точекъ (т. е. соединяя точки: 1 съ $m+2$ и т. д.) мы получимъ или звѣздчатый многоугольникъ или фигуру *изъ комбинацій многоугольниковъ меньшаго числа сторонъ*, смотря по тому, будетъ ли $m+1$ число взаимно простое съ N или же нѣтъ.

[2]) Круговымъ перемѣщеніемъ n—элементовъ называется такое, при которомъ всѣ элементы сохраняютъ свой относительный порядокъ, и одне перемѣщеніе отли-

Изъ каждаго же другого числа, путемъ круговыхъ перемѣщеній, можно составить p новыхъ чеселъ, и всѣ эти числа при p абсолютно-простомъ будутъ между собою различны, такъ что общее число чиселъ $k = a + Np = a +$ кратное p. Что касается до общаго числа чиселъ, то нетрудно видѣть, что оно равняется a^p [1]). Такимъ образомъ, мы имѣемъ равенство: $a^x = a + Np$, или $a(a^{p-1} - 1) = Np =$ кратное отъ p,—составляющее знаменитую теорему Фермата.

Подобно „комбинаторикѣ", и „теорія чиселъ" является пособіемъ при рѣшеніи задачъ „теоріи вѣроятностей".

Первый вопросъ, касающійся „теоріи вѣроятностей", былъ вопросъ, обращенный къ знаменитому Галилею: почему при паденіи 3-хъ кубическихъ костей, на граняхъ которыхъ стоятъ цифры 1, 2, 3, 4, 5, 6 выходятъ чаще сумма 10, чѣмъ 9 и сумма 11 чаще чѣмъ 12? Вопросъ этотъ рѣшается въ теоріи разбіенія чиселъ.

§ **2.** Какъ указатели множественности группъ *изъ отдѣльныхъ и различимыхъ между собою* предметовъ, цѣлыя числа имѣютъ примѣненіе вообще къ изученію *дискретныхъ* или *раздѣльныхъ* величинъ, въ отличіе отъ величинъ непрерывныхъ.

Если изученіе кривой линіи, состоящей изъ непрерывнаго ряда точекъ требуетъ обобщеннаго понятія о числѣ, то изученіе группъ точекъ, находящихся одна отъ другой на конечномъ разстояніи, находится въ самой тѣсной связи съ теоріей цѣлыхъ чиселъ.

Примѣръ такихъ группъ представляютъ такъ называемые *квинкунксы.* Если мы возьмемъ двѣ системы равно-отстоящихъ параллельныхъ линій, при чемъ разстояніе между линіями одной системы можетъ не равняться разстоянію между линіями другой, и линіи одной системы пересѣкаютъ линіи другой подъ какимъ-нибудь угломъ, то всѣ точки пересѣченія линій этихъ системъ образуютъ правильно расположенную систему точекъ, называемую **квинкунксомъ**. Изученіе квинкункса имѣетъ большія *приложенія*

чается отъ другого только начальнымъ элементомъ. Такъ напримѣръ, перемѣщенія буквъ *a b c d*: *a b c d*, *b c d a*, *c d a b*, *d a b c* суть всѣ возможныя круговыя перемѣщенія изъ 4-хъ буквъ *a*, *b*, *c*, *d*.

[1]) Пояснимъ это конкретнымъ примѣромъ: пусть даны 2 ящика и въ каждомъ по три (№ 0-й, № 1-й, № 2-й) шаровъ. Мы вынимаемъ изъ каждаго ящика заразъ по одному шару. Спрашивается, сколькими различными способами можно вынуть шары? Нетрудно убѣдиться, что число комбинацій будетъ равно $3^2 = 9$ комбинаціи будутъ 10, 00, 01, 02, 22, 21, 12, 20, 11). Здѣсь число ящиковъ соотвѣтствуетъ числу цифръ—p, а число нумеровъ=порядку системы (троичная).

въ ботаникѣ и ткацкомъ дѣлѣ [1]). Подобную же систему правильно расположенныхъ точекъ можно получить въ пространствѣ, разсматривая три системы плоскостей, взаимно между собой параллельныхъ: такая система, называемая „пространственною рѣшеткою“ (Raumgitter), изучается въ кристаллографіи.

Можно указать и въ химіи нѣкоторые вопросы, въ которыхъ пріемы теоріи чиселъ должны быть примѣнимы. Таковы атомистическая структурная теорія Кекуле—Бутлерова и періодическая система химическихъ элементовъ Д. И. Менделѣева.

Не подлежитъ вообще сомнѣнію, что при дальнѣйшемъ развитіи философіи природы явится все большая и большая необходимость въ приложеніи методовъ и теоремъ теоріи чиселъ, какъ ученія о дискретныхъ или раздѣльныхъ величинахъ. Но въ теоріи чиселъ и въ ея будущихъ примѣненіяхъ останется характеристическою чертою постоянство и неизмѣнность законовъ этой науки. Въ этомъ отношеніи она ничѣмъ не отличается отъ другихъ вѣтвей математической науки, и поэтому нельзя не смотрѣть, какъ на увлеченіе, легко оправдываемое продолжительною работою въ этой области, на идеи Н. В. Бугаева, который проводилъ мысль о недостаточности для объясненія міровыхъ явленій современнаго научно-философскаго міровоззрѣнія и необходимости дополнить его иною точкою зрѣнія, *ариѳмологическою*, не уничтожающею индивидуальности наблюдаемыхъ элементовъ и *свободы* ихъ дѣйствій. Переходъ отъ дискретности (раздѣльности) къ индивидуальности, обладающей свободою, является логическимъ скачкомъ, и новое возрожденіе на русской почвѣ Лейбницевской монадологіи едва-ли будетъ имѣть то значеніе, которое ему придаютъ нѣкоторые ученики Н. В. Бугаева. Методы и законы теоріи чиселъ своеобразны и отличаются отъ методовъ и законовъ другихъ математическихъ доктринъ; но они такъ же строги и опредѣленны, какъ другіе математическіе законы, и поэтому едва-ли можно на нихъ основать доказательство существованія свободы воли.

VI.

Составленіе чиселъ при помощи сложенія и умноженія.

§ **3.** Простѣйшіе изъ вопросовъ *теоріи чиселъ* суть тѣ, въ которыхъ разсматривается составленіе бо́льшихъ чиселъ посред-

---

[1]) См. Извѣстія С-ПБ. Технологическаго Института. 1893 г. Котурницкій Квинкунксъ и его примѣненія.

ствомъ меньшихъ. Числа могутъ быть составлены изъ меньшихъ или посредствомъ сложенія, или посредствомъ умноженія. Вопросъ о составленіи чиселъ путемъ сложенія есть упомянутый выше вопросъ *о разбіеніи* чиселъ (de partitione numerorum). Нѣкоторые изъ частныхъ вопросовъ рѣшаются элементарными соображеніями. Напр. предлагаю доказать теорему: *каждое число, если оно не есть 2,* можетъ быть представлено, какъ *сумма* нѣсколькихъ *послѣдовательныхъ чиселъ.* Большой интересъ представляетъ пріемъ, данный Эйлеромъ и состоящій въ примѣненіи безконечныхъ произведеній для рѣшенія вопросовъ, касающихся разбіенія чиселъ, который мы приложимъ къ доказательству слѣдующей теоремы.

§ 4. **Теорема**. *Каждое положительное число можетъ быть столько разъ составлено изъ различныхъ слагаемыхъ, сколько разъ оно можетъ быть составлено изъ равныхъ или различныхъ, но непремѣнно нечетныхъ, слагаемыхъ.*

Доказательство этой теоремы основывается на слѣдующемъ тождествѣ:

$$\Big[(1+x)\ (1+x^2)\ (1+x^3)\ldots\ldots\Big]\times\Big[(1-x^3)\ (1-x)\ (1-x^5)\ldots\ldots\Big]=1.$$

или иначе $PP_1=1$, если $P=\prod\limits_{m=1}^{m=\infty}(1+x^m), P_1=\prod\limits_{k=1}^{k=\infty}(1-x^{2k-1})$

Другими словами, имѣемъ

$$\Big(1+x\Big)\Big(1+x^2\Big)\ldots\Big(1+x^m\Big)\ldots=\frac{1}{(1-x)}\cdot\frac{1}{(1-x^3)}\cdots\frac{1}{(1-x^{2k-1})}\cdots$$

Но (см. стр. 40) $\frac{1}{(1-x)}=1+x+x^2+x^3+\ldots\ldots=\Sigma x^{\mu}$,

$$\frac{1}{(1-x^3)}=1+x^3+x^{2.3}+x^{3.3}+\ldots\ldots=\Sigma x^{3\nu},\quad \frac{1}{1-x^5}=\Sigma x^{5\pi}\ldots\ldots$$

Итакъ: $(1+x)\ (1+x^2)\ \ldots\ldots\ (1+x^m)=\Sigma x.^{\mu}\ \Sigma x.^{3\nu}\ \Sigma x.^{5\pi}\ldots\ldots$

Производя умноженіе въ первой части равенства, мы увидимъ, что коэфиціентъ при всякой степени x^N будетъ равенъ числу способовъ, которыми можно число N составить изъ чиселъ 1, 2, 3, 4, 5, 6, 7 .... взявъ каждое изъ нихъ слагаемымъ только по одному разу. Развертывая вторую часть, видимъ, что въ ней коеффиціентъ при x^N будетъ равняться числу способовъ, которыми можно число N составить изъ *нечетныхъ* чиселъ: 1, 3, 5, 7, ..., взявъ каждое число *слагаемымъ* по одному или по нѣсколько разъ.

Такъ какъ коэффиціенты при одинаковыхъ степеняхъ въ обѣихъ частяхъ равенства должны быть равны, то теорема, очевидно, доказана.

Мы видѣли при доказательствѣ этой теоремы, что *число способовъ разбіенія* чиселъ выражается коэффиціентомъ безконечнаго произведенія.

Если слагаемыя не должны превышать извѣстнаго предѣла, то число способовъ разбіенія выражается съ помощью коэффиціентовъ конечныхъ многочленовъ. Такъ, коеффиціентъ при t^N въ степени полинома $(t^1+t^2...+t^6)^i$ выражаетъ собою число способовъ, которыми число N можетъ быть составлено изъ i чиселъ, каждое изъ коихъ есть одно изъ чиселъ 1, 2, 3, 4, 5, 6. Точно также коэффиціентъ при x^N въ произведеніи

$$(1+x).(1+x^2). . . . (1+x^m),$$

есть число способовъ, которыми число N можетъ быть составлено изъ различныхъ чиселъ ряда 1, 2, 3, 4, 5....m, при чемъ въ сумму можетъ входить *какое угодно число слагаемыхъ*. Эти результаты имѣютъ приложеніе въ теоріи вѣроятностей, при рѣшеніи вопроса объ опредѣленіи вѣроятности того, что при бросаніи разъ кубической кости, на граняхъ которой выставлены цифры 1, 2, 3, 4, 5, 6, выпадетъ непремѣнно число N, а также при опредѣленіи вѣроятности того, что при вниманіи изъ урны, въ которой лежатъ шары № 1, № 2,... № m, сумма нумеровъ на вынутыхъ шарахъ будетъ N.

§ 5. **Простыя числа**. Какъ ни интересны вопросы о составленіи чиселъ посредствомъ сложенія, гораздо большее значеніе имѣетъ составленіе чиселъ посредствомъ перемноженія двухъ или нѣсколькихъ предшествующихъ. При изученіи этого вопроса выступаетъ различіе глубокой важности между числами *простыми* и *сложными*, которое имѣетъ существенное значеніе во всѣхъ вопросахъ высшей математики, связанныхъ съ теоріей порядка. Укажу для примѣра на рѣшеніе такъ называемаго уравненія дѣленія круга $\frac{x^p-1}{x-1}=0$. Къ рѣшенію этого уравненія сводится въ Анализѣ ученіе о правильныхъ многоугольникахъ).

Если каждое цѣлое число можетъ быть получено путемъ сложенія двухъ предшествующихъ, то не каждое можетъ быть получено чрезъ умноженіе двухъ предшествующихъ. Числа 4, 6—выражаются произведеніемъ двухъ предыдущихъ, но числа 5, 7. 11 не могутъ быть представлены подобнымъ образомъ. Числа, которыя не могутъ быть выражены чрезъ произведеніе двухъ предшествующихъ, называются *простыми* или *первообразными*. Прочія числа называются *сложными*. Съ установленіемъ различія между простыми и сложными числами возникаетъ рядъ интересныхъ вопросовъ, рѣшеніе которыхъ до сихъ поръ не достигнуто. Тайна простыхъ чиселъ пока не раскрыта наукою. Отъ этого остаются не доказанными такія теоремы, какъ напр. теоремы Гольдбаха, практически провѣренныя на большомъ количествѣ чиселъ и поэтому обладающія очень большою эмпирическою достовѣрностію.

Теорема Гольдбаха читается такъ: *Всякое нечетное число есть сумма двухъ абсолютно простыхъ чиселъ*[1]). Другая такая же теорема, которой точность *эмпирически* подтверждается, утверждаетъ, что: „какъ бы мы далеко ни продолжили рядъ натуральныхъ чиселъ, всегда найдемъ два такихъ абсолютно простыхъ числа N_1 и N_2 что $N_2 - N_1 \equiv 2$ или $N_1 = N_2 + 2$“.

Напримѣръ: $N_1 = 3029867$ и $N_2 = 3029869$.

Вопросъ о простыхъ числахъ занималъ еще греческихъ геометровъ. Въ IX-ой книгѣ „*Началъ*“ Эвклида доказанъ одинъ изъ самыхъ замѣчательныхъ результатовъ теоріи чиселъ:

§ **6. Число простыхъ чиселъ безконечно**, т. е., какъ бы мы далеко ни продолжили рядъ натуральныхъ чиселъ, всегда между *послѣдующими* найдутся простыя числа. Предположимъ, что послѣднее абсолютно простое число есть p. Взявъ произведеніе всѣхъ простыхъ чиселъ до p включительно и прибавивъ къ этому произведенію единицу, мы получимъ число: $[1.\ 2.\ 3.\ 5.\ 7.\ 11.....p]+1$, большее p. Если это число простое, то теорема доказана; если же сложное, то оно должно дѣлиться на простое число или меньшее p или большее p. Но на число меньшее p эта сумма дѣлиться не можетъ, такъ какъ одно изъ слагаемыхъ ея равно единицѣ, слѣдовательно, и въ этомъ случаѣ необходимо допустить существованіе простого числа, большаго p[2]).

Примѣчаніе. Тотъ способъ, къ которому мы прибѣгли для доказательства положенія Эвклида и которымъ впослѣдствіи намъ придется много разъ пользоваться, носитъ названіе способа *доказательства отъ противнаго* (апагогическій способъ) и состоитъ, очевидно, въ томъ, что мы, допустивъ существованіе положенія, обратнаго доказываемому, выводимъ изъ этого допущенія нелѣпое заключеніе и тѣмъ доказываемъ его несостоятельность.

---

[1]) Знаменитый созданіемъ теоріи трансфинитныхъ чиселъ—*Канторъ* провѣрилъ эту теорему *на всѣхъ* числахъ до 1000 и высказалъ убѣжденіе, что число разложеній растетъ до безконечности вмѣстѣ съ числами.

[2]) Идея этого доказательства можетъ быть примѣнена къ доказательству слѣдующихъ теоремъ:

Существуетъ безконечное множество простыхъ чиселъ вида $4k+1$, $6k+1$ $4k-1$, $6k-1$, $8k+5$ и т. д.

Доказательство Эйлера. Въ упомянутомъ уже выше сочиненіи: „Introductio in Analysin infinitorum“ Эйлеръ далъ слѣдующее тожество, изъ котораго вытекаетъ доказательство безконечности числа абсолютно простыхъ чиселъ:

$$\frac{1}{\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)\ldots\left(1-\frac{1}{n}\right)}=$$

$$=1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\ldots$$

Справедливость этого разложенія легко доказывается если замѣтимъ что, доля 1 на $1-x$ и полагая $x={}^1/_2,\ {}^1/_3,\ldots$, получимъ:

$$\frac{1}{1-x}=\frac{1}{1-\frac{1}{2}}=1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\ldots\ldots+\frac{1}{2a}+\ldots$$

$$\frac{1}{1-x}=\frac{1}{1-\frac{1}{3}}=1+\frac{1}{3}+\frac{1}{3^3}+\ldots\ldots+\frac{1}{3^b}+\ldots$$

и примемъ за доказанную теорему (см. стр. 70): всякое число можетъ быть однимъ и только однимъ способомъ разложено на произведеніе простыхъ множителей. Съ другой стороны безконечная строка, стоящая во второй части (гармоническая строка), есть строка расходящаяся, т. е. сумма

$1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{n}+\ldots$ может быть сдѣлана болѣе сколь угодно большого числа, если мы возьмемъ n достаточно великимъ [1]. Это доказывается слѣдующимъ образомъ Возьмемъ $n=2^m$, тогда члены суммы $1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{2^m}$ могутъ быть разбиты на группы

$$\left(1+\frac{1}{2}\right)+\left(\frac{1}{3}+\frac{1}{4}\right)+\left(\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}\right)+\left(\frac{1}{9}+\ldots\frac{1}{16}\right)+$$

$$+\left(\frac{1}{17}+\ldots\frac{1}{32}\right)+\ldots+\left(\frac{1}{2^{m-1}+1}+\ldots+\frac{1}{2^m}\right);$$

Всѣ эти теоремы заключаются въ теоремѣ, высказанной Лежандромъ и доказанной вполнѣ строго Леженомъ-Дирихле: Всякая ариѳметическая прогрессія, въ которой первый членъ и разность суть взаимно-простыя числа, заключаетъ въ себѣ безконечное множество простыхъ чиселъ.

[1] Возрастаніе суммы однако идетъ медленно. Эйлеръ вычислилъ сумму 1000 членовъ и нашелъ ее равною 7,485 и сумму милліона членовъ—14,393 (Institutiones Calc. Diff. pars 2. § 144).

сумма членовъ каждой группы очевидно болѣе $\frac{1}{2}$ и потому вся сумма болѣе $1+\frac{1}{2}+(m-1)\frac{1}{2}$, т. е. болѣе $1+\frac{m}{2}$ — числа, которое очевидно можетъ быть сдѣлано болѣе всякаго сколь угодно большого *n*.

Отсюда слѣдуетъ, что въ первой части число множителей не можетъ быть конечнымъ т. е. число абсолютно простыхъ чиселъ безконечно велико.

Тожество Эйлера можетъ быть обобщено: $\Pi\frac{1}{\left(1-\frac{1}{p^s}\right)}=\Sigma\frac{1}{p^s}$.

Строка, стоящая во второй части, зависитъ отъ s и есть функціи отъ s; эта функція отъ s (для значеній s не только вещественныхъ, но и комплексныхъ) было изучена Риманомъ и эта Римановская функція $\zeta(s)$ очевидно находится въ тѣснѣйшей связы съ *закономъ простыхъ чиселъ*.

Нѣсколько позже Эвклида Эратосѳенъ, знаменитый греческій математикъ, географъ и астрономъ, указалъ очень несложный способъ нахожденія простыхъ чиселъ. Возьмемъ рядъ натуральныхъ чиселъ: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14. 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61....

Зачеркивая въ этомъ ряду послѣдовательно кратныя двухъ, трехъ, пяти и т. д., для чего только надо механически выбрасывать числа черезъ одно, два, четыре и т. д., мы будемъ постепенно получать числа абсолютно простыя: 1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61.....

Способъ этотъ носитъ названіе **„рѣшета Эратосѳена“**, т. к. числа какъ бы просѣиваются: сложныя выбрасываются, а простыя остаются.

§ 7. Разложеніе сложнаго числа на простые множители и рѣшеніе вопроса о томъ, есть ли данное число простое.

Первый и простѣйшій способъ узнать, есть-ли данное число N простое или сложное, заключается въ томъ, чтобы дѣлить его на простыя числа меньшія $\sqrt{N}$.

Но тождества алгебры и теоремы теоріи чиселъ даютъ возможность рѣшать эти вопросы относительно чиселъ иногда гораздо проще и скорѣе. Такъ тождество $x^4+4y^4=(x^2+2xy+2y^2)(x^2-2xy+$ $+2y^2)$ показываетъ, что $p^4+4=(p^2+2p+2)(p^2-2p+2)$ и поэтому всякое число вида p^4+4, исключая 5, есть число сложное.

Такъ, простое тождество Aurifeuill'я

$$2^{4\mu+2}+1=(2^{2\mu+1}+2^{\mu+1}+1)(2^{2\mu+1}-2^{\mu+1}+1)$$

показываетъ, что всѣ числа вида $2^{4n+2}+1$ суть числа сложныя; таковы $2^6+1=5.13$, $2^{10}+1=5\,.\,4401$, $2^{14}+1=16385$ и т. д. (Предлагаемъ выяснить, случайно-ли, что всѣ эти числа содержатъ множитель 5?).

Изъ теоремъ теоріи чиселъ, ведущихъ къ той же цѣли, упомянемъ слѣдующія:

Методъ Фермата основывается на томъ, что каждое нечетное абсолютно простое число только единственнымъ способомъ можетъ быть разложено на разность двухъ квадратовъ цѣлыхъ чиселъ. Если простое число $p=x^2-y^2$, то x и y суть числа взаимно простыя между собою и единственное рѣшеніе есть

$$p=\left(\frac{p+1}{2}\right)^2-\left(\frac{p-1}{2}\right)^2$$

Но если $p=p_1p_2$, то возможно и другое рѣшеніе того-же уравненія: можно положить $p_1=x+y$, $p_2=x-y$, откуда $x=\frac{p_1+p_2}{2}$, $y=\frac{p_1-p_2}{2}$. На основаніи этого будемъ придавать къ p всѣ квадраты; если сумма будетъ квадратомъ только тогда, когда она будетъ равна $\left(\frac{p+1}{2}\right)^2$, то число есть абсолютно простое. Такъ прибавляя къ 17 квадратныя числа 1, 4, 9... 64, мы получимъ квадратъ только 17+64; но прибавивъ 1 къ 15 мы уже получимъ квадратъ.

Эйлеръ посвятилъ большое число мемуаровъ разсматриваемому вопросу. Одинъ изъ методовъ Эйлера основывается на слѣдующей теоремѣ теоріи бинарныхъ квадратичныхъ формъ. Если A и B обозначаютъ два цѣлыя положительныя числа, то для абсолютно простого числа p не существуетъ двухъ различныхъ разложеній:

$$(*)\qquad p=Aa^2+Bb^2,\ p=A\alpha^2+B\beta^2$$

Дѣйствительно, если бы таковыя разложенія существовали, то умноживъ первое изъ равенствъ (*) на β^2, а второе на b^2, и вычтя изъ перваго произведенія второе, получимъ:

$p(\beta^2-b^2)=A(a^2\beta^2-b^2\alpha^2)$; т. е. одно изъ чиселъ $a\beta\pm b\alpha$ было бы кратнымъ p; но

$$p^2=(Aa^2+Bb^2)\ (A\alpha^2+B\beta^2) = (Aa\alpha\pm Bb\beta)^2+AB(a\beta\pm b\alpha)^2.$$

Если $AB>1$, то квадратъ, умножающій AB, долженъ равняться нулю, ибо иначе второй членъ былъ бы больше перваго; слѣдовательно

$$\frac{a^2}{\alpha^2}=\frac{b^2}{\beta^2}=\frac{Aa^2+Bb^2}{A\alpha^2+B\beta^2}=1,\text{ откуда } a=\pm\alpha,\ b=\pm\beta\cdot$$

Для $AB=1$, [1] можно предположить $a\beta\pm b\alpha=\pm p$, но тогда другой квадратъ былъ-бы равенъ нулю, и потому $a=\pm\beta$, $b=\pm\alpha$.

Какъ приложеніе этой теоремы докажемъ снова теорему (Софіи Жерменъ), что числа вида p^4+4 суть числа сложныя. Дѣйствительно

$$p^4+4=(p^2)^2+2^2=(p^2-2)^2+(2p)^2.$$

Прилагаю ту же методу къ числу $1.000.009=1000^2+3^2$ Эйлеръ показалъ, что оно есть число сложное.

Другой методъ Эйлера основанъ на теоріи степенныхъ вычетовъ, дающей форму дѣлителей чиселъ вида $a^n\pm1$. Число 2^n+1 можетъ быть абсолютно простымъ, только если $n=2^m$, а 2^n-1, только если n есть простое число. Такъ онъ доказалъ, что всякій абсолютно простой нечетный множитель чиселъ вида $a^{2^n}+1$ имѣетъ форму $2^{n+1}k+1$. Понятно, какъ послѣ доказательства этой теоремы упрощается розысканіе абсолютно-простыхъ множителей чиселъ вида $a^{2^n}+1$. Ферматъ утверждалъ, что числа вида $2^{2^n}+1$ суть числа абсолютно-простыя: утвержденіе это справедливо для $n=1$, 2, 3, 4. Посмотримъ теперь, основываясь на теоремѣ Эйлера, справедливо-ли оно для числа $2^{2^5}+1=4\ 296\ 961\ 297$; простые дѣлители числа должны имѣть форму $64\ k+1$ и поэтому мы можемъ ограничиться испытаніемъ только слѣдующихъ чиселъ

193, 257, 449, 577, 641,...

Это послѣднее число дѣлить $2^{2^5}+1$ и даетъ въ частномъ 6700417. Посмотримъ, будетъ-ли это число простымъ или сложнымъ. Для этого нужно испытать его на всѣ простыя числа вида $64k+1$ отъ 641 до 2588, т. е. на числа

641, 769, 1153, 1217, 1409, 1601, 2113, 2581.

---

[1] Такія числа A и B Эйлеръ называлъ *numeri idonei.*

Ни одно изъ этихъ дѣленій не удается. Слѣдовательно, число 6 700 417 есть абсолютно простое.

Въ недавнее время числами вида $2^{2^n}+1$ занимался талантливый русскій человѣкъ священникъ Іоаннъ Михеевичъ Первушинъ, который въ 1877 г. сообщилъ СПБ. Акад. Наукъ найденные имъ результаты, что число $2^{2^{12}}+1$ и $2^{2^{23}}+1$ суть числа сложныя, а именно—число $2^{2^{13}}+1$ дѣлится на $7.2^{14}+1$, число $2^{2^{23}}+1$ дѣлится на число $5.2^{25}+1$ (эти результаты были провѣрены академикомъ Буняковскимъ и Золотаревымъ). Изъ этихъ чиселъ послѣднее заключаетъ въ себѣ до двухъ съ половиною милліоновъ цифръ. Зельгофъ показалъ, что число $2^{2^{36}}+1$ (имѣющее до 20 милліардовъ цифръ) есть также число сложное.

Изслѣдованіе относительно чиселъ вида $a^n \pm 1$ привели Эйлера къ результату, что число $2^{31}-1=2\ 147\ 483\ 647$ есть число абсолютно простое, что даетъ восьмое совершенное число. Бъ 1883 году Свящ. Первушинъ нашелъ, что число $2^{61}-1$ есть часло абсолютно простое (этотъ результатъ, подтверждаемый Seelhoff и Houdelot интересенъ, т. к. даетъ девятое совершенное число).

Методы Гаусса основаны на теоріи квадратичныхъ бинарныхъ формъ. Пользуясь ими, Pepin показалъ, что число $\frac{31^7-1}{31-1}$ есть абсолютно простое.

§ 8. Таблица простыхъ чиселъ (и дѣлителей).

Первыя таблицы простыхъ чиселъ и дѣлителей принадлежатъ Ф. Шутену (Franc. Schooten. Liste des nombres premiers jusqu'a 10.000. 1657) и Неллю (Pell. Liste des diviseurs autres que 2 et 5 des nombres jusqu'a 100.000. 1668). Марци (Marci) въ 1772 г. издалъ таблицу простыхъ чиселъ до 400.000. Затѣмъ въ XIX вѣкѣ были изданы: 1^0 таблицы Чернака (Chernac) подъ названіемъ Cribrum arithmecicum, заключающія въ себѣ числа до 1.020.000.

2^0 таблицы Бургардта (Burckhardt), изданныя отъ 1814 до 1817 и заключающія въ себѣ числа до 3.036.000.

3. Таблицы Дазе, составленныя этимъ феноменальнымъ счетчикомъ по иниціативѣ Гаусса и заключающія числа отъ 6.000.000 до 9.000.000.

(Factoren Tafeln изд. въ 1862 (седьмой милліонъ), 1863 (восьмой) и 1865 (девятый милліонъ). Что касается до таблицъ для четвертаго, пятаго и шестого милліона, то они, по словамъ одного письма Гаусоа отъ 1850 г., были составлены, но не опубликованныя, находятся въ рукописи въ Берлинской библіотекѣ. На этотъ пробѣлъ обратилъ вниманіе, образованный Британскою ассоціаціею для содѣйствія успѣхамъ науки, комитетъ математическихъ таблицъ, состоявшій изъ Кэли, Стокса, В. Томсона, Смита Глэшера и по порученію этого комитета Глэшеръ (James Glaisher) приступилъ къ составленію и изданію таблицъ простыхъ чиселъ и дѣлителей для четвертаго, пятаго и шестого милліоновъ. Таблицы эти сыли имъ изданы послѣдовательно въ 1879, 1880 и 1883 т. е. къ 1883 г. мы уже имѣли полныя таблицы простыхъ чиселъ и дѣлителей въ первыхъ девяти милліонахъ.

Эти таблицы доставляютъ возможность судить о распредѣленіи простыхъ чиселъ въ ряду всѣхъ натуральныхъ чиселъ. Но Мейссель далъ пріемъ опредѣленія дѣйствительнаго числа простыхъ чиселъ далеко за предѣлами этихъ таблицъ. Его формула сводитъ опредѣленіе числовой функціи $\varphi\ (m)$ — (число простыхъ чиселъ менѣе m) на опредѣленіе той же функціи для чиселъ значительно меньшихъ и на опредѣленіе функціи $\Phi\ (m,\ n)$, дающей число тѣхъ чиселъ, которыя въ интервалѣ отъ 1 до m не дѣлятся на простыя числа.

$$p_1=2,\ p_2=3,\ p_3=5,\ .....$$

Вотъ эта формула:

$$\varphi(m)=\Phi(m,n)+n(\mu+1)+\frac{\mu(\mu-1)}{1.2}-1-\sum_{s-1}^{s-\mu}\varphi\left(\frac{m}{p_n+3}\right)$$

числа μ и n опредѣляются равенствами

$$\varphi\left(\sqrt{m}\right)=n+\mu,\quad \varphi\left(\sqrt[3]{m}\right)=n$$

Такъ для $m=20.000,\ n+\mu=\varphi\left(\sqrt{20.000}\right)=34$

$$n=\varphi\ \left(\sqrt[3]{20.000}\right)=9,\ \mu=25$$

$$\varphi(m)=\Phi(m,\ n)-1+9.26+\frac{25.24}{2}-\left[\varphi\ \left(\frac{20000}{p_{10}}\right)+\varphi\left(\frac{20000}{p_{11}}\right)+\right.$$
$$\left.\quad .\ .\ .\ .+\varphi\left(\frac{20000}{p_{34}}\right)\right]$$

$$p_{10}=29,\ .\ .\ .\ p_{34}=139.$$

Остается опредѣленіе числа чиселъ, не дѣлящихся въ интервалѣ 1, ... 20000 на 2, 3, 5 .... $p_9=23$. Оно равно, какъ это доказывается въ теоріи чиселъ.

$$20000\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\,.\,.\left(1-\frac{1}{p_n}\right)$$

Такимъ путемъ Meissel опредѣлилъ, что въ 1 милл. ихъ—78498, въ 1 сотнѣ милл.—5761460 и въ милліардѣ—5847478.

§ **9**. Приведемъ теперь наиболѣе интересныя данныя, которыя могутъ быть выведены изъ таблицъ простыхъ чиселъ.

Число простыхъ чиселъ для полныхъ милліоновъ.

	Число простыхъ чис.	Разности.
Первый милліонъ	78499	
Второй »	70433	—8006
Третій »	67885	—2548
Четвертый »	66329	—1556
Пятый »	63369	— 960
Шестой »	64336	—1033
Седьмой »	63799	— 537
Восьмой »	63158	— 611
Девятый »	62760	— 398

Эта таблица указываетъ на постепенно уменьшающееся число, уменьшающуюся *плотность* простыхъ чиселъ. Но эта правильность, съ которой число простыхъ чиселъ уменьшается отъ одного милліона къ слѣдующему, уже нарушается, если мы будемъ разсматривать меньшіе интервалы. Такъ для интерваловъ въ полмилліона число простыхъ чиселъ не уменьшается постоянно при переходѣ отъ одного полумилліона къ слѣдующему: въ интервалѣ между 8.500.000 и 9.000.000 число простыхъ чиселъ равно 31 396, между тѣмъ какъ въ предыдущемъ полумилліонѣ (8.000.000—8.500.000) ихъ на 32 числа меньше (31364). Еще большая неправильность обнаруживается, если мы будемъ разсматривать меньшіе интервалы напр., въ сотню тысячъ натуральныхъ чиселъ; уже во второмъ милліонѣ находится сотня тысячъ (1.100.000—1.200.000), въ которой число простыхъ чиселъ на 9 больше чѣмъ въ предыдущей.

Въ общемъ въ 9 милліонахъ такихъ сотенъ тысячъ, въ которыхъ число простыхъ чиселъ больше чѣмъ въ предъидущей, равно 34. Иногда число простыхъ чиселъ значительно превышаетъ число чиселъ въ предшествующей сотнѣ тысячъ: напримѣръ между 7.800.000 и 7.900.000 число простыхъ чиселъ равно 6364, между тѣмъ какъ въ предыдущей сотнѣ тысячъ ихъ 6245.

Еще большая неправильность обнаруживается, если мы будемъ разсматривать сотни. Во введеніи къ таблицамъ простыхъ чиселъ въ шестомъ милліонѣ Глэшера мы находимъ интересныя таблицы, которыя для каждой сотни тысячъ (и для каждаго десятка тысячъ) указываютъ число сотенъ, заключающихъ въ себѣ опредѣленное число абсолютно простыхъ. Такъ, напр., между 0 и 100.000 мы имѣемъ слѣдующую таблицу, въ которой вторая строка даетъ *число* тѣхъ *сотенъ* разсматриваемаго интервалла, въ которыхъ число простыхъ чиселъ равно соотвѣтствующему числу первой строки:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	21	26
0	0	0	3	6	8	39	106	149	185	177	124	104	46	17	14	8	2	1	1

Подобная-же таблица для интервалла между 8.900.000 и 9.000.000 будетъ имѣть слѣдующій видъ:

0	1	2	3	4	5	6	7	8	9	10	11	12
1	4	13	53	117	177	196	175	130	72	47	11	4

Общій характеръ этого *явленія* (распредѣленія простыхъ чиселъ между сотнями натуральныхъ чиселъ), изучаемаго нами эмпирически, сходенъ съ характеромъ всѣхъ случайныхъ явленій. Представимъ себѣ, что предъ нами 1000 ящиковъ, а мы имѣемъ 6270 шаровъ и стараемся, бросая, распредѣлить ихъ равномѣрно между ящиками. Мы найдемъ, что наибольшее число ящиковъ будетъ содержать 6, 7, 5, 8, 4 шаровъ, наименьшее число будетъ содержать или слишкомъ мало (0, 1, 2) или слишкомъ много 11, 12. Именно это мы и видимъ въ послѣдней таблицѣ.

Приведемъ въ заключеніе таблицу, въ которой сопоставлены результаты частныхъ таблицъ и даны во второй строкѣ числа сотенъ (во всемъ интервallѣ отъ 0 до 9.000.000), число простыхъ чиселъ, въ которыхъ указано въ первой строкѣ.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
24	2 3	1138	3601	7864	13063	16813	16901	13334	8877	4795	2162	830	272	62	20	9

Мы видимъ такимъ образомъ изъ этой таблицы, что въ 9 милліонахъ существуютъ 24 сотни, не содержащихъ ни одного абсолютно простого числа. Наименьшая изъ такихъ сотенъ начинается числомъ 1,671.800.

Наиболѣе длинные промежутки, не содержащіе ни одного простого числа, суть промежутки въ 153 и въ 151 число (4.652.353—4.652.507 и 8.421.251.—8.421.403).

Съ другой стороны, на всемъ протяженіи 9 милліоновъ встрѣчаются пары двухъ смежныхъ нечетныхъ чиселъ, состоящія изъ абсолютно простыхъ чиселъ. Такъ напр. 5.971.847 и 5.971.849. Такихъ паръ въ интерваллѣ между 0 и 100.000—1225, въ интерваллѣ между 8.000.000 и 8.100.000—518.

§ 10. Законъ распредѣленія простыхъ чиселъ. Вопросъ о распредѣленіи простыхъ чиселъ—есть вопросъ объ опредѣленіи числа простыхъ чиселъ меньшихъ N. Если бы мы знали для всякаго N (θ (N), то число простыхъ чиселъ въ интерваллѣ между N и N_1 развилось бы θ (N_1)—θ (N).

Вопросъ объ опредѣленіи θ (N) занималъ многихъ математиковъ и привлекалъ ихъ своею трудностью. Эйлеръ въ своемъ мемуарѣ: „De numeris primis valde magnis“ (Commentationes. r. I) сравниваетъ вопросъ о законахъ простыхъ чиселъ (законъ ихъ распредѣленія и законъ зависимости отъ мѣста) съ вопросомъ о квадратурѣ круга и говоритъ, что, подобно вопросу о квадратурѣ круга, вопросъ о простыхъ числахъ, не имѣя практической важности, долженъ въ случаѣ удачнаго разрѣшенія дать математикѣ новые могущественные методы (summa subsidia); за это ручается трудность вопроса, отбившая всѣ усилія математиковъ. Не найдя закона выраженія θ (N), математики занялись рѣшеніемъ вопроса о нахожденіемъ *асимптотическихъ* формулъ.

Ассимптотическою формулою для θ (n) мы назовемъ выраженіе f (n) въ томъ случаѣ, если въ предѣлѣ или разность $f(n)-\theta(n)$ обращается въ 0, или отношеніе $\frac{f(n)}{\theta(n)}$ обращается въ 1.

Такихъ асимптотическихъ формулъ дано нѣсколько.

Лежандръ далъ формулу1) $\frac{n}{logn-1{,}08366}\Bigg\lceil$ (Такъ напримѣръ до 1.000 000 истинное число простыхъ чиселъ (по таблицамъ) равняется 78499. Если мы вычислимъ $\frac{1.001.000}{log 1.001-1{,}08.466}$ то получимъ

---

1) l g n берется по основанію e=2.17828... (Неперов. логариѳм. См. G. Papelier. Начала Анализа, b. 1, § 106. Изд. Н. Іовлева).

78543.] Во второмъ томѣ сочиненій Гаусса помѣщено его письмо къ Энке отъ 24 дек. 1839, въ которомъ онъ говоритъ, что изслѣдованія о частности простыхъ чиселъ, начатыя еще въ 1792 или 1793, скоро привели его къ убѣжденію, что средняя плотность приблизительно обратно пропорціональна логарифму или, иначе, количество простыхъ чиселъ убываетъ пропорціонально возрастанію логариѳмовъ, т. е. если обозначить (i) число абсолютно-простыхъ чиселъ въ i—ой сотнѣ, то имѣемъ:

$$(1):(2):\ldots\ldots:(102)\ldots\ldots=\frac{1}{log(101+\theta.100)}:\frac{1}{log(200+\theta 100)},$$

гдѣ θ, θ, есть правильныя дроби, т. е. число $200+\theta_1$. 100 есть нѣкоторое среднее чиело между 200 и 300.

Исходя изъ этихъ соображеній Гауссъ пришелъ къ убѣжденію, что число простыхъ чиселъ до N представляется функціею извѣстною подъ названіемъ логариѳма-интервала. Къ этому же заключенію пришелъ Чебышевъ. Риманнъ далъ еще болѣе точную формулу, для которой формула Гаусса—Чебышева

$$\theta N=\int_2^N\frac{dx}{log\,x}=lix$$

является только первымъ членомъ.

§ 11. Вопросъ о томъ, насколько формулы, дающія число простыхъ чиселъ, соотвѣтствуютъ дѣйствительному распредѣленію простыхъ чиселъ, съ большею подробностью разсмотрѣнъ во введеніи къ таблицамъ 6-го милліона Глешера, гдѣ результаты изслѣдованія представлены графически. Приведемъ въ слѣдующей таблицѣ нѣкоторые результаты, относящіеся къ послѣднему полумилліону, до сихъ поръ изученному:

	Риманнъ.	Чебыщевъ.	Лежандръ
8.600.000	— 73	+163	+319
8 700.000	— 95	+142	+503
8.800.000	—139	+100	+264
8.900.000	—108	+131	+301
9.000.000	—132	+108	+282

[т. е. число простыхъ чиселъ до 8.600.000, вычисленное по формулѣ Риманна, на 73 *меньше* настоящаго; вычисленіе-же по формуламъ Чебышева и Лежандра дастъ на 163 и на 319 чиселъ больше настоящаго].

Графическое изображеніе даетъ тотъ общій результатъ, что формула Риманна даетъ наименьшія отклоненія и колеблется по ту и по другую сторону *настоящаго* числа; формулы Чебышева lix и Лежандра даютъ числа постоянно большія, при чемъ формула Чебышева, сначала дающая худшіе результаты чѣмъ формула Лежандра, при большихъ числахъ даетъ результаты значительно лучшіе.

§ **12. Формулы для простыхъ чиселъ.** Другой вопросъ, который занималъ многихъ математиковъ, есть вопросъ о формулахъ для простыхъ чиселъ (lex quam numeri primi progrediunfur, какъ говоритъ Эйлеръ). Идеальнымъ рѣшеніемъ этого вопроса было-бы нахожденіе формулы $p=\theta(n)$ [θ обозначаетъ совокупность дѣйствій, которыя нужно произвести надъ n, чтобы получить p], дающей **всѣ** простыя числа (p) въ зависимости отъ мѣста (n), ими занимаемаго въ ряду простыхъ чиселъ, т. е. дающей для $n=1$, $p=2$; для $n=2$, $n=3$; для $n=3$, $p=4$ и т. д.

Такая формула не найдена и, если требуется выразить θ съ помощью знаковъ аналитическихъ операцій, едва ли можетъ быть найдена. Также безуспѣшно искали формулу, которая давала бы хотя не всѣ, но *только* простыя числа. Еще М. Стифель былъ занятъ этимъ вопросомъ и думалъ, что такая формула имѣетъ видъ $2^{2n+1}-1$, но уже $2^9-1=511$ есть число сложное. Мы видѣли уже, что и утвержденіе Фермата, будто числа вида $2^{2^n}+1$ суть абсолютно простыя, не вѣрно. Эйлеръ, показавшій невѣрность утвержденія Фермата, далъ нѣсколько интересныхъ формулъ, дающихъ подъ рядъ весьма большое число простыхъ чиселъ. Таковы формулы

$$x^2+x+41,\quad x^2+x+17,\quad x^2+29.$$

Но онъ-же показалъ, что (см. § 32 стр. 87) каждая такая формула (цѣлый полиномъ расположенный по степенямъ x) непремѣнно даетъ и сложныя числа.

Кромѣ простыхъ чиселъ, въ ряду чиселъ натуральныхъ находятся такія *сложныя* числа, которыя допускаютъ дѣлителей отличныхъ отъ 1 и самого себя. По опредѣленію, такое сложное число A всегда можетъ быть представлено разложеннымъ на простые множители.

Мы докажемъ, что разложеніе цѣлаго числа на простые множители единственно,—теорема основная во всей теоріи чиселъ. Изученіе свойствъ всякаго сложнаго числа существенно связано съ разложеніемъ на простые множители, для него единственно характеристичнымъ. Перейдемъ къ доказательству этой теоремы.

VII.

Единственность разложенія сложнаго числа на простые множители.

§ 12. Основное свойство цѣлыхъ чиселъ. Положимъ, что мы имѣемъ два цѣлыхъ положительныхъ числа—A и B, при чемъ $A>B$. Всегда можно въ такомъ случаѣ найти два цѣлыхъ положительныхъ числа q и r такъ, что

$$A=Bq+r, \tag{1}$$

гдѣ $r<B$. Эти числа найдутся дѣленіемъ A на B (тогда q—частное r—остатокъ меньшій B).

Въ возможности найти для всякихъ двухъ чиселъ A и B въ ряду цѣлыхъ положительныхъ чиселъ *числа* q и r состоитъ *основное свойство* цѣлыхъ положительныхъ чиселъ.

§ 14. Алгориѳмъ нахожденія общаго наибольшаго дѣлителя. Изъ формулы (1) непосредственно вытекаетъ важное слѣдствіе. Если при $A>B$ получается $A=B.q+r$, то, такъ какъ $B>r$, выходитъ:

$$B=r.q'+r', \quad \text{гдѣ } r>r'. \tag{2}$$

Въ свою очередь $$r=r'q''+r'', \tag{3}$$

и т. д. такъ что получаемъ $A>B>r>r'>r''>...$

Эту операцію можно продолжать, пока не дойдемъ до нуля, т. е. пока не получимъ:

$$r_{n-2}=r_{n-1}q_n+r_n \tag{4}$$

$$r_{n-1}=r_nq_{n+1}+r_{n+1}, \tag{5}$$

гдѣ $r_{n+1}=0$, а $r_n=1$ или числу отличному отъ 1.

1°. Разсмотримъ тотъ случай, когда $r_n=1$, и докажемъ, что A и B при этомъ условіи суть числа *взаимно простыя, т. е. не имѣющія общаго дѣлителя.*

Въ самомъ дѣлѣ, если A и B имѣютъ общимъ дѣлителемъ какое-нибудь число d, то, раздѣливъ обѣ части уравненія (1) на это число, получимъ равенство:

$$\frac{A}{d}=\frac{B}{d}q+\frac{r}{d}$$

$\frac{A}{d}$ и $\frac{B}{d}$, согласно нашему допущенію, суть числа цѣлыя, слѣдовательно, и $\frac{r}{d}$ должно быть цѣлымъ числомъ, т. е. d—есть дѣлитель числа r.

Тогда изъ уравненія (2), повторяя ту же операцію, найдемъ:

$$\frac{B}{d}=\frac{r}{d}\,q'+\frac{r'}{d};$$

и разсуждая какъ раньше, мы заключаемъ, что d есть дѣлитель и числа r': изъ равенства (3) найдемъ, что d также дѣлитель r'', r''', r^{iv} r^{v}... и т. д. Наконецъ, изъ выраженія (4), которое при дѣленіи на d принимаетъ видъ:

$$\frac{r_{n-2}}{d}=\frac{r_{n-1}}{d}q_n+\frac{r_n}{d},$$

вытекаетъ, что d должно быть дѣлителемъ r_n, что невозможно ($r_n=1$).

Итакъ, общій дѣлитель чиселъ A и B можетъ равняться только 1, другими словами—A и B суть числа взаимно простыя.

2°. Теперь разсмотримъ тотъ случай, когда r_n не равно единицѣ. Уравненіе (5) обратится тогда въ

$$r_{n-1}=r_nq_{n+1}$$

и показываетъ, что r_{n-1} дѣлится на r_n. Предпослѣднее выраженіе (4), полученное при послѣдовательномъ дѣленіи,

$$r_{n-2}=r_{n-1}q_n+r_n, \tag{4}$$

обратится, по раздѣленіи его на r_n. въ такое:

$$\frac{r_{n-2}}{r_n}=\frac{r_{n-1}}{r_n}q_n+\frac{r_n}{r_n},$$

откуда видимъ, что r_n дѣлитъ на-цѣло число r_{n-2}.

Подобнымъ же образомъ, если раздѣлимъ слѣдующее высшее выраженіе на r_n, то получимъ

$$\frac{r_{n-3}}{r_n}=\frac{r_{n-2}}{r_n}q_{n-1}+\frac{r_{n-1}}{r_n};$$

слѣдовательно r_n есть также дѣлитель r_{n-3}, такъ какъ правая часть равна цѣлому числу.

Продолжая такимъ образомъ далѣе, заключаемъ въ концѣ концовъ, что r_n есть дѣлитель чиселъ A и B. Значитъ, если последній остатокъ, изъ всѣхъ полученныхъ нами при послѣдовательномъ дѣленіи, $r_{n+1}=0$,—то предыдущій остатокъ r_n есть общій дѣлитель данныхъ чиселъ.

3°. Можно затѣмъ доказать, что этотъ общій дѣлитель есть притомъ и наибольшій.

Воспользуемся опять способомъ *доказательства отъ противнаго*, т. е. допустимъ, что есть какое-то число $\delta > r_n$, которое есть также общій дѣлитель чиселъ A и B.

Дѣлимъ уравненіе (1) на δ: $$\frac{A}{\delta}=\frac{B}{\delta}q+\frac{r}{\delta} \qquad (7)$$

Такъ какъ мы предположили, что δ—общій дѣлитель A и B, то изъ полученнаго уравненія (6) должны заключить, что δ есть дѣлитель r. Взявши уравненія (2), (3) и т. д. и разсуждая относительно нихъ такимъ же точно образомъ, послѣдовательно найдемъ, что δ есть дѣлитель чиселъ: r', r'', r'''... r_n. Но r_n не можетъ дѣлиться на δ—число большее его. Слѣдовательно, наше предположеніе, что r_n не есть общій наибольшій дѣлитель чиселъ A и B, приводитъ къ нелѣпому результату.

Этотъ *рядъ операцій*, которыя мы производили, отыскивая общаго наибольшаго дѣлителя, и называется *алгориѳмомъ нахожденія общаго наибольшаго дѣлителя.*

Изъ основнаго свойства цѣлыхъ положительныхъ чиселъ вытекаетъ конечность алгориѳма для нахожденія общаго наибольшаго дѣлителя, т. е. возможность послѣ конечнаго числа дѣйствій достигнуть до числа $r_{n+1}=0$.

Дѣйствительно, рядъ чиселъ

$$A>B>r>r'>\ldots>r_n$$

есть рядъ убывающій и конечный.

§ 15 Теорема Эвклида. На основаніи предыдущихъ выводовъ доказывается теорема Эвклида, которую можно формулировать такъ. *Произведеніе двухъ чиселъ A и C, взаимно простыхъ съ третьимъ —B, даетъ число, взаимно простое съ тѣмъ же третьимъ числомъ B.* Другими словами, если число A—взаимно простое съ числомъ B, и C—также взаимно простое съ B, то и произведеніе AC—взаимно простое съ числомъ B.

Исходя изъ положенія теоремы, что числа A и B—взаимно простыя, мы, примѣняя алгориѳмъ для нахожденія общаго наибольшаго дѣлителя, получаемъ слѣдующій рядъ равенствъ:

$$\text{I.}\left\{\begin{array}{l} A=Bq+r,\ B=rq'+r',\ r=r'.q''+r'' \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ r_{n-3}=r_{n-2}q_{n-1}+r_{n-1};\ r_{n-2}=r_{n-1}q_n+r_n. \\ r_{n-1}=r_nq_{n+1}+r_{n+1}, \\ (r_{n+1}=0), \end{array}\right.$$

гдѣ предпослѣдній остатокъ $r_n=1$.

Умножая всѣ члены группы равенствъ (1) на C, находимъ:

$$\text{II.}\left\{\begin{array}{l} AC=BC.q+rC,\ BC=Cr.q'+Cr',\ Cr=Cr'q''+Cr'' \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ Cr_{n-3}=Cr_{n-2}q_{n-1}+Cr_{n-1} \\ Cr_{n-2}=Cr_{n-1}q_n+C. \end{array}\right.$$

Теперь предположимъ, что произведеніе AC имѣетъ общаго дѣлителя съ B—какое нибудь число δ. И если подобное допущеніе приведетъ насъ къ нелѣпому результату, то это укажетъ на невозможность этого предположенія, обратнаго заключенію теоремы.

Раздѣлимъ всѣ равенства (II) группы на δ. Тогда изъ перваго полученнаго выраженія:

$$\frac{AC}{\delta}=\frac{BC}{\delta}.q+\frac{Cr}{\delta},$$

основываясь на предыдущемъ допущеніи, мы должны заключить, что $\frac{Cr}{\delta}$ есть цѣлое число. Изъ второго равенства—

$$\frac{BC}{\delta}=\frac{Cr}{\delta}.q'+\frac{Cr'}{\delta}$$

гдѣ $\frac{BC}{\delta}$ и $\frac{Cr}{\delta}$ суть цѣлыя числа, находимъ, что $\frac{Cr'}{\delta}$ — цѣлое число.

Переходя далѣе отъ равенства къ равенству, мы получаемъ, что $\frac{Cr''}{\delta}$, $\frac{Cr'''}{\delta}$, ... , $\frac{Cr_{n-3}}{\delta}$, $\frac{Cr_{n-2}}{\delta}$, $\frac{Cr_{n-1}}{\delta}$—числа цѣлыя; и, наконецъ, изъ послѣдняго равенства (II) заключаемъ, что $\frac{C}{\delta}$ есть цѣлое число, т. е. C, *какъ и* B, дѣлится безъ остатка на δ, имѣетъ общаго дѣлителя съ B, что противорѣчитъ условію теоремы. Слѣдовательно, предположеніе, что произведеніе AC не взаимно простое съ B,— ошибочно, и теорему Эвклида можно считать строго доказанной.

§ 16. Слѣдствія теоремы Эвклида. Теперь распространимъ эту терему. Положимъ, что мы имѣемъ рядъ чиселъ:

$$A,\ C,\ E,\ K,\ P' \ .\ .\ .\ .\ ,$$

взаимно простыхъ съ нѣкоторымъ числомъ B. Въ такомъ случаѣ только что доказанная теорема приводитъ къ заключенію, что и произведеніе чиселъ даннаго ряда--взаимно простое съ B. Дѣйствительно, взявъ два изъ данныхъ чиселъ A и C, мы по предыдущему доказываемъ, что ихъ произведеніе—AC—взаимно простое съ B. Присоединивъ къ этому произведенію третье число — E, мы опять доказываемъ, что новое произведеніе $AC.E$ также взаимно простое съ B, такъ какъ AC представляетъ также нѣкоторое число. Перебравъ такимъ образомъ всѣ числа даннаго ряда, мы приходимъ къ вышеуказанному положенію.

Затѣмъ беремъ еще рядъ чиселъ, подобныхъ B по отношенію къ первому ряду, т. е. такихъ, что каждое изъ нихъ—взаимно простое съ числами перваго ряда. Если мы будемъ примѣнять къ нимъ тѣ же операціи, какъ и къ числу B, то докажемъ, что произведеніе чиселъ перваго ряда—взаимно простое съ произведеніемъ чиселъ второго ряда.

Отсюда, какъ слѣдствіе, можно вывести лемму: „какія угодно степени двухъ взаимно простыхъ чиселъ суть числа взаимно простыя“. Въ самомъ дѣлѣ, ничто не можетъ воспрепятствовать намъ предположить, что всѣ числа перваго ряда равны другъ другу, т. е.

$$A = C = E = K = I = \dots$$

точно также, что всѣ числа второго ряда равны:

$$B = D = F = L = N = \ .\ .\ .\ .$$

Тогда произведенія чиселъ можно представить въ такомъ видѣ:

$$A.A.A.A. \ .\ .\ . = A^m, \qquad B.B.B.B.\ . = B^n,$$

Очевидно, что A^m и B^n суть числа взаимно простыя.

§ 17. Ирраціональныя числа. Результатомъ этой леммы является необходимость допустить существованіе т. н. ирраціональныхъ чиселъ. Въ самомъ дѣлѣ, предположимъ, что намъ дано выраженіе: $\sqrt[n]{D}$, гдѣ D не представляетъ полной n ой степени, т. е. $\sqrt[n]{D}$ не можетъ быть представленъ никакимъ цѣлымъ числомъ. Теперь предположимъ, что онъ выражается нѣкоторою несократимою дробью $\frac{A}{B}$, такъ что $\sqrt[n]{D}=\frac{A}{B}$. Возвышая это равенство въ n-тую степень, найдемъ—

$$D=\frac{A^n}{B^n},$$

гдѣ A^n и B^n суть числа взаимно простыя по доказанному, т. е. $\frac{A^n}{B^n}$—*несократимая дробь, а D—число цѣлое.* Слѣдовательно, допуская, что корень изъ числа, не представляющаго полной данной степени, выражается нѣкоторою дробью, мы впали въ ошибку и потому должны ввести т. н. ирраціальныя числа для выраженія корней въ этомъ случаѣ.

Къ этому же выводу мы придемъ, разсматривая *восьмое* алгебраическое дѣйствіе—дѣйствіе рѣшенія уравненій. Въ самомъ дѣлѣ, положимъ, что намъ дано приведенное уравненіе:

$$p^n=px^{n-1}+qx^{n-2}+\ldots+tx+u=0,$$

гдѣ коэффиціенты: $p, q, \ldots t, u$—числа цѣлыя. Въ такомъ случаѣ, если корни этого уравненія не цѣлыя числа, то они (корни) не могутъ быть дробными, т. е. будутъ выражаться числами или ирраціональными или мнимыми. Допустимъ обратное, т. е. предположимъ, что какой-нибудь корень уравненія равенъ несократимой дроби $\frac{A}{B}$.

Подставляя этотъ корень въ уравненіе, получимъ тождество:

$$\frac{A^n}{B^n}+p.\frac{A^{n-1}}{B^{n-1}}+q.\frac{A^{n-2}}{B^{n-2}}+\ldots+t.\frac{A}{B}+u=0.$$

Умножая его на B^{n-1} и перенося всѣ члены, кромѣ перваго, во вторую часть, найдемъ, что

$$\frac{A^n}{B}=-p.A^{n-1}-q\,A^{n-2}B-\ldots-t.A.B^{n-2}-uB^{n-1}.$$

Каждый изъ членовъ второй части—число цѣлое, значитъ и $\frac{A^n}{B}$ должно быть цѣлымъ числомъ, а это противорѣчитъ нашему предположенію, что A и B=числа взаимно простыя. Другими словами, наше предположеніе приводитъ къ нелѣпому результату и потому его должно считать неправильнымъ и допустить существованіе ирраціональныхъ чиселъ.

§ **18**. На основаніи предыдущихъ выводовъ можно доказать двѣ чрезвычайно важныя теоремы. 1) *Если произведеніе AC и нѣ-*

которое число B имѣютъ общаго дѣлителя δ, при чемъ A взаимно простое съ B, то C должно имѣть общаго дѣлителя δ съ B.

Дѣйствительно, такъ какъ A и B взаимно простыя, то мы, по предыдущему, имѣемъ рядъ равенствъ:

$$A=B.q+r,\ \ B=Aq_1+r, \ldots\ r_{n-2}=r_{n-1}.q_n+r_n, \text{ гдѣ } r_n=1.$$

Умножая эти равенства на C и дѣля затѣмъ мысленно на δ, мы придемъ въ концѣ концовъ къ тому заключенію, что C должно дѣлиться на δ, т. е. имѣетъ съ B общаго дѣлителя δ.

2) *Другая теорема говоритъ, что если число A дѣлится порознь на два взаимно простыхъ числа B и D, то оно должно дѣлиться и на ихъ произведеніе BD.*

Если A дѣлится на B, то $A=Bq$.

Но такъ какъ A дѣлится и на D, то произведеніе Bq должно дѣлиться на D, т. е. на основаніи теоремы (1), q дѣлится на D, или $q=D.q_1$, т. к. B и D взаимно простыя. Подставляя значеніе q въ выраженіе A, придемъ прямо къ результату.

§ **19. Теорема о разложеніи числа на множителей.** Вышеприведенныхъ теоремъ (§§ 13—18) совершенно достаточно для доказательства того, что **всякое сложное число только единственнымъ способомъ можетъ быть разложено на простыхъ множителей.** Мы будемъ опять пользоваться способомъ обратнаго доказательства, т. е. предположимъ, что данное число—N можно представить разложеннымъ двояко: или

1) $N=a^{\alpha}.b\beta c\gamma.\ .\ .\ .l^{\lambda}$, или—2) $A=a_1{}^{\alpha'}.b_1\beta' c_1\gamma'.\ .\ .\ .l_1{}^{\lambda'}$.

На основаніи второго разложенія N цѣликомъ дѣлится на a_1; а если вмѣсто N мы возьмемъ его выраженіе изъ перваго разложенія, то получимъ, что произведеніе: $a^{\alpha}.\ b\beta.\ c\gamma\ldots l\lambda$—безъ остатка дѣлится на a_1, что возможно только тогда, когда одинъ изъ сомножителей его напр. $a=a_1$. Прилагая подобное разсужденіе къ b_1, c_1, ...l_1, мы найдемъ, въ концѣ концовъ, что $b=b_1$, $c=c_1$, ...$l=l_1$. Слѣдовательно, каждый изъ множителей перваго разложенія встрѣчается среди множителей второго и наоборотъ, и эти два разложенія могутъ отличаться другъ отъ друга развѣ только показателями. Но мы сейчасъ докажемъ, что и степени множителей равны. Въ самомъ дѣлѣ

$$\frac{a^{\alpha}\cdot b\beta\cdot c^{\gamma}\cdot\ \cdot\ \cdot l^{\lambda}}{a_1{}^{\alpha'}.b_1\beta'.c_1\gamma'\ldots l_1{}^{\lambda'}}=1.$$

Умножая это равенство на $b_1^{\beta'}.c_1^{\gamma'}\ldots l^{\lambda'}_1$, мы найдемъ ($a=a_1$)

$$\frac{a^{\alpha}b^{\beta}c^{\gamma}\cdots l^{\lambda}.}{a^{\alpha'}}=b_1^{\beta'}\,c_1^{\gamma'}\ldots l_1^{\lambda'},$$

гдѣ вторая часть цѣлое число; а потому $a^{\alpha}\cdot b^{\beta}\cdots l^{\gamma}$ дѣлится на $a^{\alpha'}$, т. е. $a^{\alpha'}$ дѣлится на $a^{\alpha'}$, что возможно при условіи $\alpha<\alpha'$. Точно такимъ же способомъ мы убѣждаемся, что

$$\beta>\beta',\ \gamma>\gamma',\ \ldots\lambda>\lambda'.$$

Но, вслѣдствіе равенства числителя и знаменателя, мы можемъ взятое нами равенство написать въ видѣ:

$$\frac{a_1^{\alpha'}.b_1^{\beta'}.c_1^{\gamma'}\ldots l_1^{\lambda'}}{a^{\alpha'}b^{\beta}c^{\gamma}\ldots l^{\lambda}}=\frac{a^{\alpha'}\cdot b^{\beta'}\cdots l^{\lambda'}}{a^{\alpha}b^{\beta}\cdots l^{\lambda}}=1.$$

А отсюда, примѣняя разсужденіе, подобное предыдущему, получимъ: $\alpha'>\alpha$, $\beta'>\beta$, $\gamma'>\gamma$, $\ldots\lambda'>\lambda$. И такъ какъ послѣднія неравенства должны быть совмѣщены съ первыми, полученными нами, то $\alpha'=\alpha$, $\beta'=\beta$, $\gamma'=\gamma$, $\ldots\lambda'=\lambda$.

Итакъ, *разложеніе на простыхъ множителей возможно только единственнымъ способомъ.*

§ **20 О дѣлителяхъ даннаго числа.** Рѣшимъ теперь такого рода вопросъ: какова форма всѣхъ дѣлителей даннаго числа N? Положимъ, что

$$N=a^{\alpha}\cdot b^{\beta}\cdot\ldots k^{\mu},$$

и докажемъ прежде всего, что въ составъ дѣлителя не входитъ ни одного множителя, отличнаго отъ множителей самого числа N.

Допустимъ, что такой множитель въ дѣлителѣ есть,—какое нибудь число l^q, т. е.

$$d=a^{\alpha'}.b^{\beta'}.c^{\gamma'}\ldots k^{\mu'}.l^q.$$

Тогда при дѣленіи числа N на d, мы получимъ:

$$\frac{N}{d}=\frac{a^{\alpha}\,b^{\beta}\,c^{\gamma}\ldots k^{\mu}.}{a^{\alpha'}b^{\beta'}c^{\gamma'}k'\ldots l^{q}}.$$

Умножаемъ обѣ части равенства на $a^{\alpha'}.\ b^{\beta'}.c^{\gamma'}.k^{\mu}$.

$$\frac{N}{d}a^{\alpha'}.b^{\beta'}c^{\gamma}\ldots k^{\mu'}=\frac{a^{\alpha}.b^{\beta}.c^{\gamma}\ldots k^{\mu}}{l^{q}.}$$

Первая часть этого уравненія—число цѣлое, слѣдовательно—$a^{\alpha}b^{\beta}.c^{\gamma}.k^{\mu}=N$ должно дѣлиться на l^q; другими словами, наше допущеніе, что дѣлитель даннаго числа можетъ имѣть множителей, не входящихъ въ составъ самого числа, привело насъ къ нелѣпому результату, и потому каждый изъ дѣлителей числа N можетъ быть представленъ въ видѣ:

$$d = a^{\alpha'}.b^{\beta'}.c^{\gamma'}...k^{\mu'}$$

гдѣ α', β',, γ', ...μ', очевидно, не могутъ быть болѣе соотвѣтвѣтствующихъ имъ показателей въ числѣ N, такъ что α' можетъ имѣть всѣ значенія, начиная съ 0 и кончая α—всего $(\alpha+1)$ значеній, β'—отъ 0 до β—всего $(\beta+1)$ значеній, γ'—$(\gamma+1)$,... μ'—$(\mu+1)$ значеній. Однимъ словомъ, $\alpha' \leqq \alpha$, $\beta' \leq \beta$, $\gamma' < \gamma$,... $\mu' \leq \mu$.

§ 21. **Число дѣлителей даннаго числа.** Мы подошли къ двумъ чрезвычайно интереснымъ задачамъ: во первыхъ, нельзя-ли, пользуясь предыдущими положеніями, вывести формулу, дающую **число** всевозможныхъ **дѣлителей** даннаго числа? и во-вторыхъ, какъ опредѣлить **сумму дѣлителей** даннаго числа?

Первая изъ этихъ задачъ рѣшается очень просто.

Изъ предыдущаго § намъ извѣстно, что общій видъ дѣлителей даннаго числа N будетъ такой:

$$d = a^{\alpha'}.b^{\beta'}.c^{\gamma'}.k^{\mu'},$$

гдѣ α', β', γ'...μ' могутъ имѣть соотвѣтственно $(\alpha+1)$, $(\beta+1)$, $(\gamma+1)$,...$(\mu+1)$ значеній. Чтобы опредѣлить число дѣлителей N, мы рѣшимъ слѣдующій посторонній примѣръ и примѣнимъ рѣшеніе его къ числамъ.

Положимъ, что у насъ есть $(\alpha+1)$ бѣлыхъ шаровъ; на каждомъ проставленъ соотвѣтствующій номеръ—0, 1, 2, 3,..., $a-1$, a; затѣмъ, $(\beta+1)$ зеленыхъ шаровъ, то же перенумерованныхъ $(\gamma+1)$—синихъ и т. д., наконецъ, $(\mu+1)$ черныхъ шаровъ.

Намъ задается вопросъ: сколькими различными способами можно составить группы, по μ шаровъ въ каждой [1], чтобы въ каждой былъ одинъ шаръ опредѣленнаго цвѣта? Представимъ, что у насъ есть только бѣлые и зеленые шары. Очевидно, комбинацій между ними можетъ быть только $(\alpha+1)$. $(\beta+1)$ Къ этой комбинаціи присоединяемъ слѣдующую группу синихъ шаровъ; тогда число комбинацій изъ трехъ цвѣтовъ будетъ равно: $(\alpha+1)$. $(\beta+1)$ $(\gamma+1)$.

Продолжая подобный пріемъ, мы получимъ въ концѣ концовъ общее число комбинацій: $(\alpha+1)$ $(\beta+1)$...$(\mu+1)$.

---

[1] μ—очевидно—число цвѣтовъ шаровъ.

Поступая точно такимъ же образомъ съ числами, мы найдемъ, что число всѣхъ дѣлителей числа N т. е. $[\rho(N)]$ равно произведенію

$$\rho(N)=(\alpha+1)\ (\beta+1)\ (\gamma+1)\ldots\ (\mu+1).$$

§ 22. **Сумма дѣлителей даннаго числа.** Вторая задача—опредѣленіе суммы дѣлителей даннаго числа—рѣшается слѣдующимъ образомъ. Если число N представляется подъ видомъ:

$$N=a^\alpha.b^\beta.c^\gamma\ldots k^\mu.$$

то очевидно, что сумма дѣлителей перваго множителя—a^α будетъ равна: $(1+a+a^2+a^3+\ldots\ldots+a^{\alpha-1}+a^\alpha)$; сумма дѣлителей числа b^β будетъ $(1+b+b^2+b^3+\ldots\ldots+b^{\beta-1}+b^\beta)$, числа c^γ: $(1+c+c^2+c^3+\ldots+c^{\gamma-1}+c^\gamma)$ и т. д., наконецъ, сумма дѣлителей послѣдняго множителя k^μ будетъ: $(1+k+k^2+\ldots+k^{\mu-1}+k^\mu)$. Перемноживъ эти полиномы, мы получимъ сумму дѣлителей всего числа N, потому что въ это произведеніе войдутъ всевозможныя комбинаціи его дѣлителей, начиная съ 1 и кончая произведеніемъ всѣхъ множителей, т. е. самымъ числомъ N.

$$\Sigma d(N)=(1+a+a^2+\ldots+a^\alpha).(1+b+b^2+b^\beta)\ldots\ldots$$
$$\ldots\ldots(1+k+k^2+\ldots\ldots+k^\mu)\ ^{*})$$

Перемножить эти полиномы весьма легко, принявъ въ соображеніе, что каждый изъ нихъ представляетъ изъ себя геометрическую прогрессію. Суммируя эти прогрессіи по правиламъ алгебры, найдемъ, что:

$$\Sigma d(N)=\left(\frac{a^{\alpha+1}-1}{a-1}\right).\left(\frac{b^{\beta+1}-1}{b-1}\right).\left(\frac{c^{\gamma+1}-1}{c-1}\right)\ldots\ldots\left(\frac{k^{\mu+1}-1}{k-1}\right).\quad (A)$$

Числовая функція суммы дѣлителей, т. е. $\Sigma d(N)$ обозначается также $\int(N)$.

§ 23. **Числа совершенныя и дружественныя.** При помощи формулы, дающей сумму дѣлителей, можно показать, что числа вида

---

*) Рѣшить предыдущую задачу, т. е. опредѣлить *число* дѣлителей, можно исходя непосредственно изъ этой формулы. Въ самомъ дѣлѣ, такъ какъ въ нее входятъ всѣ дѣлители числа N, то число всѣхъ членовъ этой формулы и дастъ число дѣлителей. Въ первой скобкѣ число членовъ, очевидно, равно $(\alpha+1)$, во второй—$(\beta+1)$, въ третьей—$(\gamma+1)$ и т. д., въ послѣдней—$(\mu+1)$. Слѣдовательно, число дѣлителей выразится произведеніемъ: $(\alpha+1)\ (\beta+1)\ (\gamma+1)\ldots.(\mu+1)$.

(1) 2^{p-1} $(2^p—1)$ суть числа *совершенныя*, если $2^p—1$ есть число простое. Дѣйствительно, въ этомъ случаѣ (по формулѣ А):

$$(1)\ \Sigma d(N) = \frac{2^p—1}{2—1} . \frac{(2^p—1)^2\ \ 1}{2^p-1—1} = \frac{2^p—1}{1} . \frac{2^p—1+1}{1} = \mathrm{N} = 2^p(2^p—1).$$

Для того, чтобы число $(2^p—1)$ было простое, необходимо чтобы p было простое, ибо число $2^{pq}—1$, очевидно, дѣлится и на $2^p—1$ и на $2^q—1$.; но это необходимое условіе не есть достаточное напр. $\Sigma d(2^{11}—1) = 23+89$.

Извѣстныя въ настоящее время совершенныя числа соотвѣтствуютъ слѣдующимъ значеніямъ p:

$p=2$, 3, 5, 7, 13, 17, 19, 31, 61, т. е. суть:
6, 28, 496, 8128, *3350336*, *8589869056*, . . .

(*Задача*. Доказать, что всѣ четныя совершенныя числа заключаются въ формулѣ (1), данной еще Эвклидомъ въ 9-ой книгѣ его „Началъ“).

До сихъ поръ не найдено *ни одного нечетнаго совершеннаго* числа; но и не дано доказательства, что такихъ чиселъ не существуетъ.

Въ тѣсной связи съ вопросомъ о совершенныхъ числахъ находится другой вопросъ, касающійся чиселъ *дружественныхъ* *), т. е. такихъ, что сумма дѣлителей одного числа равна другому, и наоборотъ. Возьмемъ два числа: A и B. Пусть $A=2^n.p.q$, а $\mathrm{B}=2^n r$, гдѣ p, q и r суть абсолютно-простыя числа. При условіи, что $p=3.2^n—1$, $q=3.2^{n-1}—1$ и $r=9.^{2n-1}—1$, числа A и B будутъ дружественными. Въ самомъ дѣлѣ, положимъ, что $n=2$. Тогда: $p=11$, $q=5$ и $r=71$, $A=2^2.11.5=220$, а $B=2^2.71=284$,

$$\Sigma d(220)=284=B, \text{ а } \Sigma d(284)=220=A.$$

Въ трехъ мемуарахъ Эйлера, посвященныхъ вопросу о дружественныхъ числахъ, дано 65 паръ дружественныхъ чиселъ. Важнѣйшій изъ этихъ мемуаровъ находится въ 1-мъ томѣ вышеупомянутыхъ Commentationes p. 102. Вторая пара состоитъ изъ числа 2^4. 23. 47 и 2^4. 1151; отмѣтимъ еще пары 2^3. 19. 41 и 2^5. 199; также 3^2. 7. 13. 5. 17 и 3^2. 7. 13. 107. Въ Эйлеровскій каталогъ не входитъ пара 1210 и 1284.

---

*) Открытіе дружественныхъ чиселъ приписываютъ Пиѳагору. Извѣстно преданіе, какъ Пиѳагоръ на вопросъ: «Что такое дружба?»—отвѣтилъ: «Это два числа 220 и 284».

§ 24. Формула Эйлера.

Euler далъ интересное свойство суммы дѣлителей числа N:

$$\int(N)=\int(N-1)+\int(N-2)-\int(N-5)-\int(N-7)+$$
$$+\int(N-12)+\int(N-15)-\int(N-22)\ldots\ldots$$

гдѣ 1, 2, 5, 7, 12, 15, 22 и т. д.—т. н. пятиугольныя числа *), Возьмемъ, напр., число 20. По формулѣ Эйлера

$$\Sigma d(20)=\int(19)+\int(18)-\int(15)-\int(13)+\int(8)-\int(5)=$$
$$+20+39-24-14+15+6=42.$$

Дѣйствительно, дѣлители 20-ти суть: 1, 2, 4, 5, 10, 20, сумма которыхъ равна 42.

Формула Эйлера представляетъ простѣйшій примѣръ изъ ряда формулъ теоріи чиселъ, получаемыхъ съ помощью такъ называемой теоріи эллиптическихъ функцій.

§ 25. О числовыхъ функціяхъ. *Перемѣннымъ* числомъ въ анализѣ называется такое число, которое не имѣетъ опредѣленнаго значенія, но можетъ принимать ихъ безконечное множество. Наоборотъ, если число въ продолженіе вычисленій или изслѣдованія имѣетъ опредѣленную величину, то оно называется *постояннымъ*.

---

*) Если мы представимъ себѣ шары равнаго діаметра и зададимся составить изъ нихъ какія-нибудь фигуры: правильные 3-угольники, 4-угольники, 5-угольники и т. д., то мы невольно придемъ къ вопросу: сколько надо шаровъ, чтобы получить желаемую фигуру? Если мы будемъ брать ариѳметическія прогрессіи съ разностями: для 3-угольниковъ=1, для 4-уг.=2, для 5-угольниковъ=3 и вообще, для $(d+2)$—угольниковъ$=d$, и тогда, суммируя послѣдовательно два, три, четыре и т. д. члена этихъ прогрессій, мы будемъ получать желаемыя числа шаровъ. Такъ, напр., 3-угольныя числа (изъ прогрессіи ÷ 1. 2. 3. 4....) будутъ: 1, 3, 6, 10 и т. д.; 4-угольныя (÷ 1. 3. 5. 7....)—1, 4, 9, 16 и т. д.; 5-угольныя (÷ 1. 4. 7. 10. 13. 16....)—1, 5, 12, 22, 35 и т. д. Для болѣе быстраго полученія фигурныхъ чиселъ выведены ихъ общія формулы: такъ общій видъ 3-угольныхъ чиселъ есть $\frac{n(n+1)}{2}$, 4-угольныхъ — n^2, пятиугольныхъ $\frac{3n^2+n}{1}$ и т. п. Обобщенными пятиугольными числами называются числа вида $\frac{3n^2+n}{2}$.

Перемѣнныя числа обозначаются большею частью буквами x, y, z, и ξ, η, ζ... и другими, напр. N, а постоянныя—a, b, c,.., α, β, γ. и т. д.

Такъ, въ уравненіи $ax+by+c=0$ x, y—перемѣнныя, a, b, c—постоянныя.

Перемѣнныя, въ свою очередь, раздѣляются: 1) на *независимыя перемѣнныя*, могущія принимать какія угодно значенія и 2) на *функціи*, значеніе которыхъ зависитъ отъ одной или нѣсколькихъ независимыхъ перемѣнныхъ. Функціи обозначаются знаками: $f(x)$, $F(x)$ Φ (x), ρ (x), и т. д. Напр. значеніе многочлена $f(x)=5x^2+4x-1$ всецѣло зависитъ отъ одного независимаго перемѣннаго x, а значеніе $F(x, y)=3x+5y-5xy$ зависитъ уже отъ того, какое значеніе мы придадимъ перемѣннымъ x,y, т. е. это функція отъ двухъ перемѣнныхъ и т. д.

Площадь круга есть функція отъ *одного* незав. пер.—радіуса, а площадь прямоугольника зависитъ отъ 2-хъ независ. перем.—высоты и основанія и т. д.; $sin\ x$, $cos\ x$, $lg\ x$ и т. д.—суть также функціи отъ одного независимаго перемѣннаго x. Независимое перемѣнное x функціи называется иногда *аргументомъ ея*.

Функціи раздѣляются прежде всего на *аналитическія и числовыя* [1]).

Въ *анализѣ* изучаются функціи, которыхъ аргументъ принимаетъ какія угодно вещественныя (или комплексныя) значенія и значенія которыхъ суть какія угодно вещественныя (или комплексныя) числа.

Функціи ρ (N) и $\int$ (N) представляютъ простѣйшіе примѣры *числовыхъ функцій*, т. е. функцій опредѣленныхъ только для цѣлыхъ значеній перемѣнной и имѣющихъ только цѣлыя значенія.

Кромѣ числовыхъ функцій въ теоріи чиселъ имѣютъ важное значеніе функціи *полуаналитическія*, аргументъ которыхъ какое угодно число, но сами функціи имѣютъ только *цѣлыя* значенія. Важнѣйшая изъ полуаналитическихъ функцій есть функція $E)x)$, *означающая наибольшее цѣлое число*, *заключающееся въ* x. Она встрѣчается, напримѣръ, въ рѣшеніи вопроса—опредѣлить наи-

---

[1]) Аналитическія функціи раздѣляются 1) на алгебраическія, и 2) трансцендентныя напр. $sinx$, $cosx$, $lg\ x$ и т. д. Алгебраическія функціи въ свою очередь раздѣляются на цѣлыя, (x не входитъ въ знаменатели), дробныя, раціональныя (x нѣтъ подъ корнемъ), ирраціональныя и пр.

большую степень абсолютно простого числа p, входящую въ произведеніе $1.\ 2.\dots n$. Степень эта, какъ легко видѣть, равняется

$$E\left[\frac{n}{p}\right]+E\left[\frac{n}{p^2}\right]+E\left[\frac{n}{p^3}\right]+\dots$$

Такъ наибольшая степень 2, входящая въ произведеніе 1.2.3. . .12 равна

$$E(6)+E(3)+E\left[\frac{12}{8}\right]=6+3+1=10.$$

Интересно слѣдующее свойство числовой функціи $E\ (x)$:

$$E(x)+E\left[x+\frac{1}{n}\right]+E\left[x+\frac{2}{n}\right]+\dots+E\left[x+\frac{n-1}{n}\right]=E(nx).$$

Переходимъ теперь къ числовой функціи $\varphi\,(\mathrm{N})$, выражающей число чиселъ, меньшихъ съ N и взаимно простыхъ съ N.

§ 26. Число чиселъ меньшихъ N и взаимно простыхъ съ N.

Задача объ опредѣленіи числа чиселъ меньшихъ N и взаимно простыхъ съ N сводится на опредѣленіе того, *сколько въ ряду* (1): *1, 2, 3, . . .N чиселъ, не имѣющихъ дѣлителей общихъ съ N?*

Вопросъ этотъ мы разрѣшимъ тогда, когда произведемъ рядъ слѣдующихъ дѣйствій: выбросимъ изъ ряда (1):

1) всѣ числа, дѣлящіяся на a,

2) изъ оставшихся—всѣ числа дѣлящіяся на b,

3) изъ оставшихся послѣ двухъ первыхъ операцій—числа, дѣлящіяся на c, и т. д., наконецъ—числа дѣлящіяся на l, и

4) опредѣлимъ, сколько чиселъ останется послѣ послѣдней операціи.

Теперь выполняемъ сказанное:

1) Не трудно видѣть, что въ ряду (1) чиселъ, дѣлящихся на a будетъ $\frac{\mathrm{N}}{a}$. (Число N можетъ быть представлено подъ видомъ $\frac{\mathrm{N}}{a}a$, гдѣ $\frac{\mathrm{N}}{a}$ будетъ цѣлое число, т. к. N дѣлится на a).

Слѣдовательно, послѣ того, какъ изъ (1) ряда выбросимъ всѣ числа, дѣлящіяся на a,—получимъ:

$$\mathrm{N}-\frac{\mathrm{N}}{a}=\mathrm{N}\left(-\frac{1}{a}\right) \qquad (2).$$

чиселъ не дѣлящихся на *a*.

2) Изъ выраженія (1) выбрасываемъ числа кратныя *b*. Но всѣ кратныя *b*, не превышающія N, могутъ быть представлены подъ видомъ $1.b$, $2.b$, $3.b$, $4.b \ldots\ldots \frac{\mathrm{N}}{b}b$; изъ нихъ придется выбросить только тѣ, которыя не дѣлятся на *a* (кратныя *a* уже выброшены, а для того, чтобы какое нибудь изъ кратныхъ *b*, напр. *rb*, не дѣлилось на *a*, достаточно чтобы *r* на него не дѣлилось. т. к. *a* и *b* числа абсолютно простыя; поэтому, очевидно, число кратныхъ *b*, на *a* дѣлящихся, равняется числу чиселъ ряда,

$$1,\ 2,\ 3,\ 4,\ 5 \ldots\ldots \frac{N}{b},$$

не дѣлящихся на *a*; т. е. равно $\frac{N}{b}\left(1-\frac{1}{a}\right)$. Вычитая это число

изъ $N\left(1-\frac{1}{a}\right)$, получаемъ:

$$N\left(1-\frac{1}{a}\right)-\frac{N}{b}\left(1-\frac{1}{a}\right)=N\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right) \qquad (3)$$

чиселъ, не дѣлящихся ни на *a*, ни на *b*. Прилагая тѣ же разсужденія къ отысканію числа чиселъ, не дѣлящихся на *c*, получимъ (4) рядъ чиселъ, уже не дѣлящихся ни на *a*, ни на *b*, ни на c; и число чиселъ въ нихъ будетъ:

$$\mathrm{N}\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right) \qquad (4)$$

Отсюда по способу математической индукціи доказываемъ, что формула опредѣляющая въ ряду (1) число чиселъ, не дѣлящихся на *a*, *b*, c... .*l* должна представиться подъ слѣдующимъ видомъ:

$$N\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\ldots\left(1-\frac{1}{l}\right) \qquad (5)$$

Обозначая число чиселъ меньшихъ *N* и взаимно простыхъ съ *N* черезъ $\varphi(N)$, получимъ:

$$\varphi(N)=N\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\ldots\ldots\left(1-\frac{1}{l}\right) \qquad (6)$$

или $\varphi(N)=(a^{\alpha}.b^{\beta}.c^{\gamma}..\,l^{\lambda})\dfrac{a-1}{a}\ \dfrac{b-1}{b}\ \dfrac{c-1}{c}\cdot\cdots\dfrac{l-1}{l}$

или $\varphi(N)=(a^{\alpha-1}.b^{\beta}b^{1}.c^{\gamma-1}....l^{\lambda-1}).(a-1)(b-1)(c-1)....(l-1)$ (7)

Возьмемъ напр., число $12=2^{2}3$; тогда $\varphi(12)=2.3^{0}.1.2=4$. Дѣйствительно, 12 взаимно простое съ 1, 5, 7, 11.
Изъ формулы (7) вытекаетъ равенство

$\varphi(\mathrm{N})=\varphi(a^{\alpha}).\varphi(b^{\beta}).\varphi(c^{\gamma})\,...\varphi(l^{\lambda})$, потому что
$a^{\alpha-1}(a-1)=\varphi(a^{\alpha})$. $b^{\beta-1}(b-1)=\varphi(b^{\beta})$; $c^{\gamma-1}(c-1)=\varphi(l^{\gamma})$.

§ **27. Теорема Гаусса.** Пользуясь формулой $\varphi(\mathrm{N})$ можно доказать теорему Гаусса, по которой если d есть дѣлитель числа N, то $\Sigma\varphi(d)=N$.

Замѣтивъ, что общій видъ дѣлителей числа $N=a^{\alpha}.b^{\beta}.c^{\gamma}....l^{\lambda}$ есть $d=a^{\alpha'}..b^{\beta'}..c^{\gamma'}...l^{\lambda'}$, гдѣ $\alpha'=(0,1,2,...\alpha)$, $\beta'=(0,1,2,..\,\beta)$,... $\lambda'==(0,1,2,..\,.\lambda)$, по предыдущему найдемъ, что

$$\varphi(d)=\varphi(a^{\alpha'})\varphi(b^{\beta'})\,...\varphi(l^{\lambda'}).$$

Припомнимъ, что

$$\Sigma d=(1+a+a^{2}+..+a^{\alpha})(1+b+b^{2}+..+b^{\beta})..(1+l+l^{2}+..+l^{\lambda})$$

заключаетъ въ себѣ всѣхъ дѣлителей числа N, находимъ P равно

$$P=[1+\varphi(a)+\varphi(a^{2})+....+\varphi(a^{\alpha})][1+\varphi(b)+\varphi(b^{2})+....+\varphi(b^{\beta})]....$$
$$.....[1+\varphi(l)+(l^{2})+....+\varphi(l^{\gamma})],$$

гдѣ первыя скобки содержатъ въ себѣ ничто иное, какъ $\Sigma\varphi(a^{\alpha'})$, такъ какъ a по вышеуказанному имѣетъ всѣ значенія отъ 0 до a; вторыя скобки представляютъ $\Sigma\varphi(b^{\beta'})$, такъ что $P=\Sigma\varphi(d)$.

Но, съ другой стороны, полиномъ, содержащійся *въ первыхъ скобкахъ*, можетъ быть представленъ такъ—

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

Точно также полиномъ во вторыхъ скобкахъ$=b^{\beta}$ и т. д. Такъ что $P=\Sigma\varphi(d)$ *равняется* $a^{\alpha}\,b^{\beta}.c^{\gamma}....l^{\lambda}$, *т. е.*$=N$.

§ **28.** Теорема Гаусса представляетъ собою одинъ изъ изящнѣйшихъ результатовъ теоріи числовыхъ функцій. Приведемъ нѣкоторыя понятія этой теоріи.

Интеграломъ числовой функціи $f(n)$ по всѣмъ числамъ называется функція $F(n)$, опредѣляемая равенствомъ

$$f(1)+f(2)+f(3)+\ .\ .\ .\ +f(n)=F(n).$$

Интеграломъ по дѣлителямъ функцій $f(n)$ мы будемъ называть функцію $\Phi(n)$, опредѣляемую равенствомъ

$$\Sigma f(d)=f(1)+f(d)+f(d')+.\ .+f(n)=\Phi(n),$$

гдѣ 1, d, d', . . . n суть всѣ дѣлители числа n.
Функція $f(n)$ *будетъ числовая производная функціи* $\Phi(n)$.

Введемъ числовую функцію $\mu(n)$, которая обладаетъ слѣдующими свойствами: $\mu(n)=0$, если n содержитъ кратные простые множители, т. е. дѣлится на какой-нибудь квадратъ; $\mu(n)=+1$, если n содержитъ простые множители только въ первой степени и притомъ въ четномъ числѣ; $\mu(n)=-1$, если n содержитъ простые множители только въ первой степени, но въ нечетномъ числѣ.

Напр. $\mu(12)=0$, $\mu(14)=+1$, $\mu(13)=-1$.

Тогда между числовыми функціями $f(n)$ и $\Phi(n)$ существуетъ слѣдующее соотношеніе:

$$(fn)=\Sigma\mu\left(\frac{n}{d}\right)\Phi(d) \qquad \text{(I)}$$

Изъ теоремы Гаусса $\Sigma\varphi(d)=n$ слѣдуетъ поэтому соотношеніе, которое не трудно доказать:

$$\varphi(n)=\Sigma\mu\left(\frac{n}{d}\right)d=\Sigma d-\Sigma d'$$

при чемъ первая сумма относится къ тѣмъ дѣлителямъ, для которыхъ $\frac{n}{d}$ содержитъ нечетное число простыхъ множителей, а Σd къ тѣмъ, для которыхъ $\frac{n}{d}$ содержитъ нечетное число таковыхъ.

Напр. $\varphi(12)=2-4-6+12=4$.

Нетрудно видѣть, что эта новая формула для числовой функціи $\varphi(n)$ легко выводится изъ выраженія, даннаго въ § 26.

Нетрудно также доказать, что между тремя числовыми функціями $f(n)$. $F(n)$ и $\Phi(n)$ существуютъ слѣдующія соотношенія:

$$\sum_{n=1}^{n=\infty} f(n)x^n \times \sum_{n=1}^{n=\infty} x^n = \sum_{n=1}^{n=\infty} F\,(n)\;x^n \qquad \text{(II)}$$

$$\sum_{n=1}^{n=\infty} \frac{f(n)}{n^s} \times \sum_{n=1}^{n=\infty} \frac{1}{n^s} = \sum_{n=1}^{n=\infty} \frac{\Phi(n)}{n^s} \qquad \text{(III)}$$

Вводя Риманнову функцію $\zeta(s)=\sum_{n=1}^{n=\infty}\frac{1}{n^s}$ и полагая $f(n)=$ $=\varphi\ (n)$, имѣемъ изъ формулы (III) и теоремы Гаусса

$$\Sigma\frac{\varphi\ (n)}{n^s}=\frac{\zeta(s-1)}{\zeta(s)}$$

Полагая $f(n)=\mu(n)$, легко докажемъ, что $\Phi(n)$ для всякаго числа n, отличнаго отъ 1, равна 0. Пусть $n=a^\alpha\ b^\beta\ c^\gamma\ k^\mu\ l^\lambda$; тогда дѣлители n, не заключающіе квадратовъ, будутъ 1, $(a,\ b,\ c,\ldots k,\ l)$ $(ab,\ ac,\ \ldots\ kl)$; $(abc\ \ldots\ kl)$. . . . . , и число ихъ будетъ равно

$1+r+\frac{r(r-1)}{1.\ 2.}+\frac{r(r-1)\ (r-2)}{1.\ 2.\ 3.}+\ldots$, если черезъ r обозначимъ число простыхъ множителей $a,\ b,\ c,\ \ldots,\ k,\ l$, входящихъ въ составъ n. Сумма же значенія функціи μ будетъ

$$1-\frac{r}{1}+\frac{r(r-1)}{1.\ 2.}-\frac{r(r-1)\ (r-1)}{1.\ 2.\ 3.}+.\ .\pm\ 1=0.$$

Формула (III) даетъ, слѣдовательно, при $f\ (n)=\mu\ (n)$,

$$\zeta(s)\ \sum_{n=1}^{n=\infty}\frac{\mu(n)}{n^s}=1,\ \text{откуда}$$

$$\sum_{=1}^{n=\infty}\frac{\mu(n)}{n^s}=\frac{1}{\zeta(s)}$$

§ **29. Указатель р — аго порядка.** Обобщеніемъ функціи $\varphi(n)$ является слѣдующая числовая функція $\varphi_p(n)$, называемая указателемъ p—аго порядка. Такъ называютъ **число группъ изъ p чиселъ не превышающихъ** n, имѣющихъ то свойство, что ихъ **общій наибольшій дѣлитель есть число взаимно простое съ** p (въ группу могутъ входить и одинаковыя числа, но группы, отличающіяся **порядкомъ чиселъ**, считаются различными). Такъ, напр., при $n=3$ можно составить слѣдующія группы изъ двухъ чиселъ, имѣющія указанное свойство: 1, 1; 1, 3; 2, 1; 2, 2; 2, 3; 3, 1; 3, 2; число ихъ равно $8=3^2-1$. Изъ трехъ чиселъ можно составить слѣдующія группы: 1, 1, 1; 1, 1, 2; 1, 1, 3; . . . . и т. д. въ числѣ равномъ $26=3^3-1$, такъ что изъ всѣхъ возможныхъ группъ только одна 3, 3, 3 не удовлетворяетъ нашему условію.

Функціи $\varphi_p(n)=n\left[1-\frac{1}{a^p}\right]\left[1-\frac{1}{б^p}\right]\ldots\left[1-\frac{1}{l^p}\right]$.

Она удовлетворяетъ теоремѣ аналогичной теоремѣ Гаусса:

$$\Sigma\varphi_p(d)=n^p.$$

VIII. СРАВНЕНІЯ.

§ 30. Сравнимость чиселъ по модулю. Положимъ, мы имѣемъ два числа a и $б$, изъ которыхъ $a>б$; несомнѣнно $a=бq+r$, гдѣ r, какъ остатокъ, меньше $б$ и можетъ принимать какія угодно значенія отъ 0 до $б-1$ включительно. Если $r=0$, то это показываетъ, что a нацѣло дѣлится на $б$,—если $r=1$, то отъ дѣленія a на $б$ въ остаткѣ получается 1, и т. д. до $r=б-1$. На основаніи этихъ остатковъ, получаемыхъ при дѣленіи на постоянное число (модуль), числа раздѣляютъ *на классы.*

Числа, которыя при дѣленіи на постоянное число даютъ всегда одинъ и тотъ же остатокъ, Гауссъ назвалъ *равноостаточными* или *сравнимыми по модулю* и ввелъ знакъ ($\equiv$) для обозначенія сравненія. Положимъ, что имѣемъ два числа a и a', которыя при дѣленіи на число $б$ даютъ остатокъ r, т. е. (I) $a=бq+r$ и (II) $a'=бq_1+r$. На основаніи только что сказаннаго мы пишемъ: $a\equiv a'$ (*мод* $б$), и это читается такъ: a сравнимо съ a' по модулю $б$. Сравнимыя цѣлыя числа a и a' могутъ быть какими угодно: положительными, *отрицательными* и нулями, но **модуль** предполагается **положительнымъ**. Если мы вычтемъ (II) изъ (I), то получимъ $a-a'=б(q-q_1)$ или $\frac{a-a'}{б}=q-q_1$, т. е. цѣлому числу. Изъ этого слѣдуетъ

Теорема: *Разность сравнимыхъ чиселъ безъ остатка дѣлится на модуль.* Эта теорема позволяетъ ввести новое опредѣленіе равноостаточныхъ чиселъ: тѣ числа сравнимы или равноостаточны, разность которыхъ безъ остатка дѣлится на модуль. Какъ слѣдствіе, изъ этого второго опредѣленія вытекаетъ первое опредѣленіе, данное нами сравнимымъ числамъ. Въ самомъ дѣлѣ $\frac{a-a'}{б}=\vartheta$ (ϑ число цѣлое, $б$—модуль); $a-a'=\vartheta б$; $a=\vartheta б+a'$

но $a'=bd_1+r$ (II); слѣдовательно $a=\vartheta b+bd_1+r=b.\ (\vartheta+q_1)+r$; т. е. остатки получаются равными. Такимъ образомъ, оба приведенныя опредѣленія совпадаютъ.

Всѣ числа, сравнимыя между собою по модулю b, составляютъ одинъ *классъ*; поэтому всѣ числа по отношенію къ модулю b раздѣляются на b классовъ.

Общій видъ всѣхъ чиселъ, принадлежащихъ къ одному и тому же классу съ a по модулю b, есть

$$x=a+b\mathrm{N} \tag{*}$$

Если будемъ придавать числу N различныя отрицательныя и положительныя значенія, мы найдемъ безконечное множество чиселъ, сравнимыхъ съ a по модулю p; изъ всѣхъ этихъ чиселъ особенно замѣчательны два числа, которыя могутъ быть названы *представителями класса*: 1) число **положительное, наименьшее изъ** всѣхъ положительныхъ чиселъ, **сравнимыхъ** съ a по модулю b, называемое *наименьшимъ положительнымъ* **вычетомъ** числа a по модулю p; 2) число отрицательное, численная величина котораго менѣе численной величины всѣхъ отрицательныхъ чиселъ, сравнимыхъ съ a по модулю b; это число называется *наименьшимъ отрицательнымъ вычетомъ* числа a по модулю b. Для опредѣленія наименьшаго положительнаго и наименьшаго отрицательнаго числа a изъ сравнимыхъ по модулю b, мы обратимся къ формулѣ (*), которую можемъ написать такъ:

$$(1)\qquad x=a-b\mathrm{N};\ \text{или}\ x=b\left(\frac{a}{b}-\mathrm{N}\right)\qquad(2)$$

Изъ формулы (2) видно, что наименьшая численная величина x зависитъ отъ числа N, ближе всѣхъ остальныхъ подходящаго къ $\frac{a}{b}$. Въ то же самое время не трудно видѣть, что x будетъ имѣть положительное значеніе, когда $\mathrm{N}<\frac{a}{b}$, и отрицательное, когда $\mathrm{N}>\frac{a}{b}$.

Зная это, мы можемъ опредѣлить, напримѣръ, наименьшій положительный вычетъ числа 23 по модулю 7. По формулѣ (1) имѣемъ $x=23-7\mathrm{N}$, по формулѣ же (2) пишемъ, что $x=7\left(\frac{23}{7}-\mathrm{N}\right)$, гдѣ за N мы должны взять число цѣлое, полученное отъ дѣленія 23 на 7, т. е. 3. (Остатками мы, очевидно, вправѣ пренебречь). Подставляя 3 въ формулу (1) вмѣсто N, получимъ $x=2$, т. е. 2 будетъ наименьшимъ положительнымъ вычетомъ 23 по модулю 7.

Для опредѣленія наименьшаго *отрицательнаго* вычета мы должны въ формулѣ (2) принять за N непремѣнно такое число, которое было бы *больше* $\frac{a}{b}$ и всего ближе подходило къ $\frac{a}{b}$. Поэтому, желая найти наименьшій отрицательный вычетъ числа 23 по модулю 7, поступаемъ такимъ образомъ:

$$x=23-7N \text{ или } x=7\left(\frac{23}{7}-N\right)$$

Частное отъ дѣленія $\frac{23}{7}=3+\frac{2}{7}$. Въ данномъ случаѣ дробь $\frac{2}{7}$ замѣняемъ 1, получаемъ $N=4$; тогда $x=-5$. Слѣдовательно -5 есть наименьшій отрицательный вычетъ числа 23 по модулю 7.

Тотъ изъ двухъ вычетовъ, наименьшій положительный или наименьшій отрицательный, котораго *абсолютная величина* меньше, называется *абсолютнымъ наименьшимъ вычетомъ.*

Если абсолютныя величины равны (что можетъ случиться, если b есть число четное и $a=\frac{b}{2}+bN$), то каждый изъ нихъ будетъ абсолютнымъ.

§ 31. Свойства сравненій, аналогичныя свойствамъ равенствъ.

Изъ опредѣленія сравненій вытекаютъ ихъ свойства, аналогичныя основнымъ свойствамъ равенствъ.

1°. **Первое свойство.** Какъ въ равенствахъ всякое число равно самому себѣ, такъ и въ сравненіяхъ:

Всякое число a сравнимо съ самимъ собою по модулю k, т. е. $a\equiv a$ (*мод k*) и если $a\equiv a$ (*мод k*), то и $-a\equiv -a$ (*мод k*).

2°. **Второе свойство.** Аксіомѣ равенствъ „два числа, порознь равныя третьему, равны“ соотвѣтствуетъ въ теоріи сравненій теорема:

Два числа, сравнимыя съ третьимъ по какому либо модулю, сравнимы между собою по тому же модулю.

Пусть $a\equiv b$ (*мод k*), $c\equiv b$ (*мод k*);

требуется доказать, что $a \equiv c\ (\textit{мод}\ k)$?

Выраженіе $a \equiv b (\textit{мод}\ k)$ значитъ, что $\frac{a-b}{k} =$ цѣлому числу, также и $\frac{c-b}{k} =$ цѣлому числу. Взявши разность двухъ послѣднихъ равенствъ имѣемъ:

$$\left(\frac{a-b}{k}\right)-\left(\frac{c-b}{k}\right)=\text{цѣлому числу},$$

или:

$$\frac{a-c}{k}=\text{цѣлому числу},$$

а это по предыдущему значитъ, что $a \equiv c\ (\textit{мод}\ k)$.

3°. Третье свойство. *Прибавляя къ обѣимъ частямъ сравненія по одному и тому же числу, сравненія не нарушаемъ,* т. е. если

$$a \equiv b\ (\textit{мод}\ k),\ \text{то и}\ a+c \equiv b+c\ (\textit{мод}\ k)$$

Дѣйствительно, $\frac{(a+c)-(b+c)}{k} \equiv \frac{a-b}{k} =$ цѣлому числу,

а это равносильно тому, что $a+c \equiv b+c\ (\textit{мод}\ k)$, т. е. отъ прибавленія къ обѣимъ частямъ по c данное сравненіе не нарушилось. Тоже самое можно сказать и относительно отниманія отъ обѣихъ частей сравненія равныхъ чиселъ.

4°. Четвертое свойство. *Во всякомъ сравненіи*, совершенно такъ, какъ и въ уравненіи, *члены могутъ быть переносимы изъ одной части въ другую.*

$a \equiv b+c\ (\textit{мод}\ k)$ значитъ ничто иное, какъ $\frac{a-(b+c)}{k} =$ цѣлому числу, или $\frac{a-b-c}{k} =$ цѣлому числу, а это въ свою очередь можетъ быть представлено подъ видомъ $\frac{(a-c)-b}{k} =$ цѣлому числу, откуда видно, что $a-c \equiv b\ (\textit{мод}\ k)$.

5°. Пятое свойство. *Два сравненія съ однимъ и тѣмъ-же модулемъ могутъ быть почленно складываемы и вычитаемы.* Положимъ, что даны сравненія:

$$a \equiv b\ (\textit{мод}\ k)\ \text{и}\ a_1 \equiv b_1\ (\textit{мод}\ k).$$

На основаніи вышесказаннаго заключаемъ, что: $\frac{a-b}{k}=$цѣл. числу, $\frac{a_1-b_1}{k}$ цѣл. числу. По сложеніи послѣднихъ равенствъ имѣемъ: $\frac{a-b+a_1-b_1}{k}=$ цѣлому числу или $a+a_1\equiv b+b_1$ $(\text{мод } k)$; вычитая изъ перваго равенства второе, получимъ: $a-a_1\equiv b-b_1$ $(\text{мод } k)$.

Послѣднее свойство относилось только къ одной парѣ сравненій, конечно оно будетъ справедливо и для нѣсколькихъ сравненій. Положимъ, мы имѣемъ n сравненій.

$$a=b\ (\text{мод } k),\ a_1\equiv b_1\ (\text{мод } k),\ \dots,\ a_{n-1}\equiv b_{n-1}\ (\text{мод } k).$$

Отъ сложенія перваго сравненія со вторымъ получаемъ новое сравненіе $a+a_1\equiv(b+b_1)$ $(\text{мод } k)$. Если придадимъ къ нему третье сравненіе, то получимъ $a+a_1+a_2\equiv b+b_1+b_2$ $(\text{мод } k)$ — сумму трехъ сравненій. Продолжая подобную операцію, мы въ концѣ концовъ дойдемъ до суммы всѣхъ n сравненій.

$$a+a_1+a_2+\dots a_{n-1}\equiv b+b_1+b_2+\dots b_{n-1}\ (\text{мод } k).$$

Допустимъ теперь, что въ этомъ сравненіи $a=a_1=a_2=\dots=a_{n-1}$ и $b=b_1=b_2=\dots=b_{n-1}$.

Тогда очевидно $na\equiv nb$ $(\text{мод } k)$, гдѣ n—какъ число всѣхъ сравненій, должно быть цѣлымъ и *положительнымъ*. Но такъ какъ въ сравненіи мы можемъ перемѣнить знакъ у обоихъ членовъ сравненія (св. I), то n можетъ быть и отрицательнымъ.

6. Шестое свойство. *Два или нѣсколько сравненій могутъ быть почленно перемножены.* Пусть даны сравненія:

$$a\equiv b\ (\text{мод } k),\ a_1\equiv b_1\ (\text{мод } k).$$

Требуется доказать, что $aa_1\equiv bb_1$ $(\text{мод } k)$. Дѣйствительно, такъ какъ по предыдущему $aa_1\equiv ba_1$ $(\text{мод } k)$ и $a_1b\equiv b_1b$ $(\text{мод } k)$, то:

$$aa_1\equiv bb_1\ (\text{мод } k).$$

Изъ этихъ свойствъ очень легко выводится слѣдующая важная теорема:

7. Седьмое свойство. *Оба члена сравненія* (какъ и равенства) *могутъ быть возвышены въ одну и ту же степень.* Само собою разумѣется, что тутъ можетъ итти дѣло только о цѣлой и положительной степени.

Положимъ, что мы имѣемъ n сравненій

$a \equiv b$ (*мод* k), $a_1 \equiv b_1$ (*мод* k). . . . . , $a_{n-1} \equiv b_{u-1}$ (*мод* k).

Перемноживъ эти сравненія, получимъ:

$$aa_1 \; . \; . \; . \; . \; a_{n-1} \equiv bb_1 \; . \; . \; . \; . \; b_{n-1} \text{ (мод } k).$$

Если же $a = a_1 = \; . \; . \; . \; = a_{n-1}$ и $b = b_1 = \; . \; . \; . \; = b_{n-1}$,

то $$a^n \equiv b^n \text{ (мод } k).$$

Свойства эти имѣютъ примѣненіе при нахожденіи остатковъ отъ дѣленія большихъ чиселъ на сравнительно небольшія. Попробуемъ, напр., отыскать остатокъ отъ дѣленія 10^6 на 7. Разсуждаемъ такъ: $10 \equiv 3$ (*мод* 7); $10^6 \equiv 3^6$ (*мод* 7); но $3^2 \equiv 2$ (*мод* 7); $3^6 \equiv 2^3$ (*мод* 7), а $2^3 \equiv 1$ (*мод* 7), значитъ $10^6 \equiv 1$ (*мод* 7), т. е. отъ дѣленія 10^6 получается остатокъ $= 1$.

Предлагаемъ найти остатокъ отъ дѣленія 2^{32} на 641 и остатокъ отъ дѣленія $2^{64}+1$ на 274177.

§ **32.** Всѣ вышеизложенныя свойства позволяютъ намъ доказать слѣдующую, весьма важную въ теоріи сравненій теорему.

Значенія цѣлыхъ, съ цѣлыми коэффиціентами функцій (многочленовъ) отъ двухъ чиселъ, сравнимыхъ по какому нибудь модулю, сравнимы по тому же модулю, т. е. если $A \equiv B$ (*мод* k); то $f(A) \equiv f(B)$ (*мод* k).

Пусть данъ какой либо полиномъ, расположенный по степенямъ буквы x: $f(x) = ax^m + bx^{m-1} + cx^{m-2} \; . \; . \; .$, гдѣ $a, b, c \ldots m$ числа цѣлыя (знаки членовъ полинома не имѣютъ значенія и могутъ быть какіе угодно).

На основаніи раньше выведенныхъ свойствъ, мы можемъ написать:

$$A^m \equiv B^m (\text{мод } k), \; A^{m-1} \equiv B^{m-1} \text{ (мод } k),$$
$$A^{m-2} \equiv B^{m-2} \text{ (мод } k) \; . \; . \; . \; . \; . \; . \; A \equiv B \text{ (мод } k).$$

Умножая члены перваго сравненія на a, второго на b, третьяго на c и т. д., получимъ слѣдующій рядъ сравненій:

$$aA^m \equiv aB^m \text{ (мод } k), \; bA^{m-1} \equiv bB^{m-1} \text{ (мод } k) \ldots\ldots$$

На основаніи третьяго свойства, мы можемъ эти сравненія написать такъ:

$$aA^m + bA^{m-1} + cA^{m-2} + \ldots \equiv aB^m + bB^{m-1} + cB^{m-2} + \ldots \text{ (мод } k),$$
$$\text{или } f(A) \equiv f(B) \text{ (мод } k).$$

Теорема эта имѣетъ важное значеніе. Напримѣръ, получая въ большомъ количествѣ простыя числа изъ формулы: $41-x+x^2$, мы можемъ индуктивно заключить, что при всякихъ значеніяхъ x формула будетъ давать только простыя числа. Вышедоказанная теорема позволяетъ намъ показать противное, т. е., что нѣтъ такого многочлена, который бы давалъ при всѣхъ значеніяхъ главной буквы простыя числа.

Положимъ, мы имѣемъ $f(x)=Ax^m+Bx^{m-1}+..$, и если при $x=m$, $f(m)$ равняется простому числу p, то при $x=m+p$, всегда получается число сложное.

Дѣйствительно $m+p\equiv m$ (*мод* p): по доказанной теоремѣ $f(m+p)\equiv f(m)$ (*мод* p); но $f(m)\equiv p$ (*мод* p), значитъ $f(m+p)\equiv p$ (*мод* p), такъ какъ $p\equiv 0$ (*мод* p), $f(m+p)\equiv 0$ (*мод* p): другими словами $\frac{f(m+p)}{p}=$цѣл. числу, или $f(m+p)$, дѣлясь нацѣло на p, представляетъ уже число сложное.

Напримѣръ, пусть $f(x=3)=47$; тогда $f(47+3)$ будетъ числомъ сложнымъ, потому что $\frac{f(47+3)}{47}$—число цѣлое.

§ 33. Особыя свойства сравненій.

До сихъ поръ мы исключительно разсматривали свойства сравненій, вполнѣ аналогичныя со свойствами равенствъ: теперь перейдемъ къ изученію свойствъ сравненій, отличныхъ отъ свойствъ уравненій.

Изъ четырехъ основныхъ операцій у насъ не разсматривалась только послѣдняя—операція дѣленія. Здѣсь то и обнаруживается разница съ аналогичнымъ дѣйствіемъ въ равенствахъ. Оказывается, *члены сравненія могутъ быть сокращены на ихъ общаго множителя въ томъ только случаѣ, когда послѣдній есть число, взаимно простое съ модулемъ.*

Чтобы это свойство лучше врѣзалось въ память, возьмемъ два примѣра:

1) $8\equiv 14$ (*мод* 6) и 2) $6\equiv 27$ (*мод* 7).

Въ первомъ общій множитель 2 входитъ и въ составъ модуля, во второмъ—множитель 3 взаимно простой съ модулемъ. Если мы попробуемъ сократить члены перваго сравненія, то сейчасъ же замѣтимъ, что у насъ получается нелѣпый результатъ, тогда какъ второе сравненіе свободно можно сократить.

Теперь докажемъ эту теорему въ общемъ случаѣ. Пусть

$$ad \equiv bd \ (мод\ k)$$

гдѣ a—число простое съ k; въ такомъ случаѣ, такъ какъ $\frac{da-db}{k}=\frac{d(a-b)}{k}=$цѣл. числу, и т. к. d есть число взаимно простое съ k, то$\frac{a-b}{k}=$ цѣлому числу или

$$a \equiv b \ (мод\ k)$$

Во всѣхъ предыдущихъ теоремахъ модуль оставался неизмѣннымъ; теперь разсмотримъ тѣ теоремы, когда и модуль подвергается измѣненію.

1) *Если члены сравненія и модуль имѣютъ общаго множителя, то можно сократить на него не только члены сравненія, но и модуль.*

Такъ, если въ сравненіи $a \equiv b$ (мод p) $a=a_1 d$, $b=b_1 d$ $p=p_1 d$, т. е. если существуетъ сравненіе: $a_1 d \equiv b_1 d$ (мод $p_1 d$), то

$$a_1 \equiv b_1 \ (мод\ p_1).$$

Дѣйствительно, $a \equiv b$ (мод p) означаетъ, какъ было сказано раньше, что$\frac{a-b}{p}=$цѣл. числу. Вставляя въ это равенство значенія a, b, p, находимъ:

$$\frac{a_1 d-b_1 d}{p_1 d}=\frac{d(a_1-b_1)}{p_1 d}=\frac{a_1-b_1}{p_1}=\text{цѣлому числу,}$$

или, что-то-же: $a_1 \equiv b_1$ (Мод p_1)

Во взятомъ нами выше сравненіи: $8 \equiv 14$ (мод 6), члены его отдѣльно отъ модуля сокращать нельзя, но вмѣстѣ съ модулемъ, по доказанной теоремѣ, вполнѣ возможно. Дѣйствительно, сокративъ все на 2, мы получимъ правильное сравненіе:

$$4 \equiv 7 \ (мод\ 3).$$

2. *Если одинъ изъ членовъ сравненія $a \equiv b$ (мод. p) и модуль имѣютъ общаго множителя, то и другой членъ есть*

кратное общаго множителя, т. е. если $b=b_1d$ и $p=p_1d$, то a должно быть кратнымъ d.

Мы имѣемъ $\frac{a-b}{p}$ = цѣл. числу; вставляя на мѣсто b и p ихъ значенія, получаемъ:

$$\frac{a-b_1d}{p_1d}=\text{цѣл. числу } \theta.$$

Отсюда $a=b_1d+p_1d\theta=d(b_1+p_1\theta)$, т. е. a кратное d, такъ какъ

$$b_1+p_1\theta=\text{числу цѣлому}.$$

Итакъ, въ сравненіи $a\equiv b_1d$ (*мод* $p_1.\ d$) необходимо, чтобы a дѣлилось на d, въ противномъ случаѣ сравненіе существовать не можетъ.

3) *Два числа, сравнимыя по двумъ или нѣсколькимъ модулямъ, взаимно простымъ между собою, сравнимы и по произведеніямъ этихъ модулей* *).

Пусть $a\equiv b$ (*мод* k), $a\equiv b$ (*мод* k_1)

Требуется доказать, что $a\equiv b$ (*мод* kk_1)? Такъ какъ

(I) $\frac{a-b}{k}$ = цѣл. числу θ и (II) $\frac{a-b}{k_1}$ = цѣл. числу θ_1, то

$a-b=k\theta$; подставивъ значеніе $a-b$ во II-ое равенство, будемъ имѣть $\frac{k\theta}{k^1}=\theta_1$, гдѣ по условію k и k_1 числа простыя, почему $\frac{\theta}{k_1}=p$ (цѣл. числу), а $\theta=k_1p$; вставляя въ равенство $a-b=k\theta$ значеніе θ, получимъ $a-b=kk_1p$ или $\frac{a-b}{kk_1}=p$. Слѣдовательно,

$$a\equiv b\ (\text{мод } kk_1),$$

Теорему эту можно распространить на тотъ случай, когда число сравненій велико, какъ угодно. Въ самомъ дѣлѣ, рядомъ операцій, подобныхъ предыдущей, не трудно доказать, что если

---

*) Теорему эту примѣняютъ при нахожденіи признаковъ дѣлимости сложнаго числа: $\frac{A}{N}$ = цѣл. числу, $\frac{A}{N_1}$ — цѣл. числу; $\frac{A}{NN}$ — цѣл. числу.

$$a \equiv b \ (мод\ k), \quad a \equiv b \ (мод\ k_1), \quad a \equiv b \ ((мод\ k_2).$$

. . . .

$$a \equiv b \ (мод\ k_n),$$

то $$a \equiv b \ (мод\ kk_1\ k_2 \ldots\ k_n)$$

Возьмемъ частный примѣръ:

$37 \equiv 7$ (*мод* 2), $37 \equiv 7$ (*мод* 3), $37 \equiv 7$ (*мод* 5).

Очевидно, что $37 \equiv 7$ (*мод* $30 \equiv 2.3.5$)

4) *Сравненіе не нарушается, если модуль замѣнить его дѣлителемъ*, т. е. если

$$a \equiv b \ (мод\ k), \text{ гдѣ } k \equiv dd,$$

то $$a \equiv b \ (мод\ d)$$

Дѣйствительно: $\frac{a-b}{k} = \frac{a-b}{dd_1}$ = цѣл. числу; умноживъ последнее выраженіе на d_1, получимъ $\frac{a-b}{d}$ = цѣл. числу, иначе говоря, $a \equiv b$ (*мод* d).

§ 34. Теорема Фермата.

Свойства сравненій, выведенныя въ предыдущихъ §§, даютъ возможность доказать одну изъ важнѣйшихъ теоремъ въ теоріи чиселъ, высказанную въ первый разъ Ферматомъ. Эта теорема была помѣщена имъ безъ доказательствъ въ его комментаріи къ „Ариеметическимъ вопросамъ“ Діофанта (греческ. матем., жившаго въ IV вѣкѣ по Р. Хр.).

Вотъ эта теорема. *Если a не дѣлится на обсолютно простое число p, то*

$$a^{p-1} \equiv 1 \ (мод\ p).$$

Такъ какъ p число абсолютно простое, то числа взаимно простыя съ p и меньшія p суть: 1,2,3,4,5,.... $p-1$, всего $(p-1)$ чиселъ.

Будемъ теперь множить a на 1, 2,.... $p-1$, а произведенія дѣлить на p; отъ дѣленія мы будемъ получать различные остатки:

$a.\ 1$	дѣленное	на p,	даетъ	остатокъ	r_1
$a.\ 2$	—	„	—	„	r_2
$a.\ 3$	—	„	—	„	r_3
. . . . .	. . .	. . .	. . .	. . .	.
as	—	„	—	„	r_s
. . . . .	. . .	. . .	. . .	. . .	.
at	—	„	—	„	r_t
. . . . .	. . .	. . .	. . .	. . .	.
$a(p-2)$	—	„	—	„	r_{p-2}
$a(p-1)$	—	„	—	„	r_{-p1}

Очевидно, что эти числа и ихъ остатки сравнимы по модулю p, т. е.

$$a.1\equiv r_1\ (мод\ p),\qquad a.2\equiv r_2\ (мод\ p),\qquad a.3\equiv r_3\ (мод\ p),$$

$$\ldots\ldots\ as\equiv_s(мод\ p),\qquad at\equiv r_t\ (мод\ p)\ \ldots\ldots$$

$$a(p-2)\equiv r_{p-2}\ (мод\ p),\ a(p-1)\equiv r_{p-1}\ (мод\ p)$$

1^0. Легко видѣть, что ни одинъ изъ полученныхъ остатковъ не можетъ равняться 0; въ самомъ дѣлѣ, если бы какой нибудь остатокъ $r_s=0$, то мы видѣли бы сравненіе: $as\equiv 0$ (*мод* p) или $\frac{as}{p}$=цѣл. числу, чего быть не можетъ, потому что произведеніе as простое съ числомъ p.

Далѣе, никакіе два остатка не могутъ быть равны: если мы предположимъ, что $r_s=r_t$, то (см. § 31 второе свойство) $at\equiv as$ (*мод* p), другими словами $\frac{a(t-s)}{p}$=цѣлому числу; но этого быть не можетъ на томъ основаніи, что и a и $t-s$ числа взаимно простыя съ p. Кромѣ того очевидно, что всѣ эти остатки должны быть меньше p. Все сказанное даетъ намъ возможность заключить, что r_1, r_2... r_s, r_t,... r_{p-1} *суть числа 1, 2, 3...* $p-1$, *но только взятыя въ другомъ порядкѣ.*

Перемножая почленно вышеозначенныя сравненія, получаемъ:

$$a^{p-1}.\ 1.2.3\ldots.\ s.t..,(p-1)\equiv r_1\ r_2\ldots r_{p-1}\ (мод\ p)$$

а по сокращеніи на 1.2.3... $p-1$ имѣемъ;

$$a^{p-1}\equiv 1\ (мод\ p)$$

Такъ, напримѣръ: $10^6\equiv 1$ (*мод* 7), $10^{10}\equiv 1$ (*мод* 11).

§ **35. Второе доказательство теоремы Фермата.** Въ виду особой важности теоремы Фермата, мы считаемъ не лишнимъ дать еще два доказательства ея. Возьмемъ $(x+1)^p$, гдѣ p—число абсолютно простое, и возведемъ въ степень по формулѣ Ньютона. Тогда мы получимъ полиномъ:

$$(x+1)^p=x^p+\frac{p}{1}x^{p-1}+\frac{p(p-1)}{1.2}x^{p-2}+..+\frac{p(p-1).(p-i+1)}{1.2.3...i}x^{p-i}+...\frac{p}{1}x+1$$

въ которомъ коэффиціенты при всѣхъ членахъ, кромѣ перваго и послѣдняго, суть не только цѣлыя числа, но и *кратныя* p. Чтобы доказать послѣднее положеніе, разсмотримъ коэффиціентъ общаго члена формулы:

$$\frac{p(p-1)...(p-i+1)}{1.2.3...i}$$

Такъ какъ коэффиціентъ долженъ быть числомъ цѣлымъ, а p—взаимно простое съ числомъ $1.2.3...i$, то произведеніе $(p-1)\ (p-2...(p-i+1)$ должно дѣлиться на $1.2.3...i$, т. е.

$$\frac{(p-1)(p-2)...(p-i+1)}{1.2\ 3...i}=\text{цѣлому числу } \vartheta.$$

Каждый коэффиціентъ, кромѣ двухъ крайнихъ, представится тогда въ видѣ $p\vartheta$., т. е. кратнаго отъ p.

Перенося въ лѣвую часть разложенія бинома первый и послѣдній члены полинома изъ правой, оставивъ, слѣдовательно, во второй части только члены, кратные p, найдемъ, что

$$(x+1)^p-x^p-1=\text{числу, кратному отъ } p,$$

или
$$(x+1)^p-x^p-1\equiv0\ (\textit{мод}\ p).$$

Такъ какъ x есть какое угодно цѣлое число, то мы можемъ придавать ему послѣдовательно значенія: 0,1,2...., $a-3$, $a-2$, $a-1$; тогда мы получимъ слѣдующій рядъ сравненій:

$$\left.\begin{array}{l}1^p-0^p-1\equiv0\\2^p-1^p-1\equiv0\\3^p-2^p-1\equiv0\\ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\\ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\\(a-2)^p-(a-3)^p-1\equiv0\\(a-1)^p-(a-2)^p-1\equiv0\\a^p-(a-1)^p-1\equiv0\end{array}\right\}\ (\textit{мод}\ p)$$

Складывая эти сравненія, замѣчаемъ, что первый членъ каждаго сравненія уничтожается со вторымъ членомъ слѣдующаго. Во всѣхъ этихъ сравненіяхъ въ лѣвой части *останутся только* a^p *и 1, повторенная столько разъ, сколько сравненій, т. е. a разъ*; такъ что окончательно сумма сравненій выразится:

$$a^p - a \equiv 0\ (мод\ p)\ \text{или}\ a(p^{-1} - 1) \equiv 0\ (мод\ p).$$

т. е. $$\frac{a(a^{p-1} - 1)}{p} = \text{цѣл. числу};$$

но a взаимно простое съ p, поэтому

$\dfrac{a^{p-1} - 1}{p}$ = цѣл. числу, что равносильно $a^{p-1} \equiv 1$ (*мод* p).

§ 36. Третье доказательство теоремы Фермата основано **на томъ же принципѣ, какъ и второе.**

Беремъ полиномъ Ньютона:

$$(a + b + c + .. + i)^p = a^p + b^p + c^p + .. + i^p + \Sigma\frac{1.2.3...p a^{\alpha}\cdot b^{\beta}\cdots i^{\lambda}}{\alpha!\beta!...\lambda!}$$

гдѣ α, β.... λ **придаются** различныя значенія отъ 0 до p—1, **при чемъ ихъ сумма** всегда $= p$ ($1.2...\alpha = \alpha!$ полагается равнымъ 1, если $a = 0$). **Легко видѣть, что если** p **абсолютно** простое, то Σ **должна быть цѣлымъ числомъ кратнымъ** p, **такъ какъ всѣ числа, составляющія** Σ, **цѣлыя и кратныя** p.

Такимъ образомъ, перенося всѣ члены съ коэффиціентами не дѣлящимся на p, **въ одну часть, а въ другой оставляя члены кратные** p, **получимъ:**

$(a + b + ... + i)^p - a^p - b^p - . . - i^p =$ кратн. p.

Если предположимъ, что $a = b = c = ... = i$, **и число ихъ** k, то

$$k^p - k = \text{кратн. отъ р};\ \frac{k(k^{p-1} - 1)}{p} = \text{цѣл. числу}.$$

Если k **число взаимно** простое съ p, то $k^{p-1} \equiv 1$ (*мод* p.)

§ 37. **Теорема Эйлера**. Теперь переходимъ къ доказательству теоремы Эйлера:

Если a взаимно простое съ N—модулемъ (при чемъ N—какое угодно число), то $a^{\varphi(N)}\equiv 1$ (*мод* N);

Доказательство этой теоремы очень сходно съ доказательствомъ теоремы Фермата, составляющей ея частный случай.

Обозначивъ черезъ N_1, N_2, N_3......N_n, всѣ числа, простыя съ N и $<N$ такъ что $n=\varphi(N)$ составляемъ произведенія:

aN_1, aN_2, aN_3,.......aN_n; далѣе, дѣлимъ эти произведенія на модуль N; они будутъ сравнимы съ получающимися остатками.

Обозначая соотвѣтствующіе остатки черезъ r_1, r_2, r_3.......r_n, имѣемъ рядъ сравненій:

$$aN_1\equiv r_1\ (\textit{мод}\ N),\ aN_2\equiv r_2\ (\textit{мод}\ N),\ aN_3\equiv r_3\ (\textit{мод}\ N),$$

. . . .

$$aN_s\equiv r_s\ (\textit{мод}\ N),\ aN_t\equiv r_t\ (\textit{мод}\ N),\ aN_n\equiv r_n\ (\textit{мод}\ N),$$

откуда: $a_n . N_1 . N_2 .. N_s ... N_n\equiv r_1\ r_2 ... r_s\ r_n$ (*мод* N). (1)

Въ полученномъ сравненіи не трудно замѣтить, 1) что остатки—$r_1, r_2\ r_3 ... r_n$ всѣ $<N$; 2) ни одинъ изъ нихъ не можетъ равняться нулю, такъ какъ тогда напр. aN_s дѣлилось бы на N нацѣло, а это противно условію, что a—взаимно простое съ N; 3) остатки должны также быть взаимно простые съ модулемъ: еслибы какой-нибудь остатокъ r_s и модуль N имѣли общаго дѣлителя, то такой же дѣлитель долженъ бы входить и въ число aN_s, ибо въ обратномъ случаѣ не могло бы существовать самое сравненіе: $aN_s\equiv r_s$ (*мод* N). Наконецъ, легко доказать, 4) что въ ряду остатковъ $r_1, r_2, r_3,....r_n$; нѣтъ равныхъ между собою. Дѣйствительно, положимъ, что $r_s=r_t$; въ такомъ случаѣ $aN_s\equiv aN_t$ (*мод* N); слѣдовательно

$$\frac{a(N_s--N_t)}{N}=\text{цѣлому числу},$$

но a взаимно простое съ N, а N_t и N_s каждое меньше N, поэтому и разность ихъ будетъ обязательно $<N$. Значитъ $\frac{a(N_s-N_t)}{N}$ не можетъ быть цѣлымъ числомъ, а это указываетъ на то, что равныхъ остатковъ въ ряду r_1, r_2, r_3,....r_n нѣтъ.

Изъ всего вышеизложеннаго необходимо заключить, что числа ряда: r_1, r_2, r_3,...r_n суть ничто иное, какъ числа N_1, N_2,

$N_3,....N_n$, только расположенные въ другомъ порядкѣ; а отсюда

$$r_1 . r_2 . r_3 .... r_n = N_1 . N_2 . N_3 .... N_n .$$

Это равенство показываетъ, что обѣ части сравненія (1) имѣютъ общаго множителя, который, несомнѣнно, простой относительно N: на основаніи этого мы имѣемъ право сократить на него сравненіе (1); тогда получимъ

$$a^n \equiv 1 \ (\textit{мод}\ N);\ \text{но}\ n = \varphi\ (N);\ \text{значитъ}\ a^{\varphi(N)} \equiv 1\ (\textit{мод}\ \mathrm{N}).$$

Теорема Фермата вытекаетъ изъ теоремы Эйлера, какъ частный случай. Если $a^{\varphi(N)} \equiv 1$ (*мод* N),
то при N, равномъ абсолютно простому числу p, $\varphi(\mathrm{N}) = p - 1$ (т. е. число чиселъ меньшихъ и взаимно простыхъ съ p будетъ $p-1$); иначе говоря, $a^{p-1} \equiv 1$ (*мод* p).

Если $\mathrm{N} = \mathrm{p}^{\alpha}$, то $\varphi\ (\mathrm{N}) = \mathrm{p}^{\alpha-1}(p-1)$, и формула Эйлера приметъ видъ: $a^{(p-1)p^{\alpha-1}} \equiv 1$ (*мод* p), такъ, напр., если $p^{\alpha} = 2^3$, то $\varphi\ (\mathrm{N}) = 2^2.1 = 4$, и $a^4 \equiv 1$ (*мод* 3); такъ что $3^4 \equiv 1$ (*мод* 8), $5^4 \equiv 1$ (*мод* 8).

§ 38. Теорема Вильсона и Варинга.

Произведеніе всѣхъ натуральныхъ чиселъ, меньшихъ абсолютно-простого числа p, сложенное съ 1, дѣлится на p безъ остатка, т. е.:

$$[1.2.3:..(p-1)] + 1 \equiv 0 (\textit{мод}\ p).$$

Если a—число, взаимно простое съ p, то рядъ произведеній

$$a.1,\ a.2,\ a.3, ... a.(p-1)$$

при дѣленіи на p, дастъ рядъ остатковъ: r_1, r_2, r_3,....., r_{p-1}.

Несомнѣнно, среди этихъ остатковъ мы найдемъ такой, который равенъ единицѣ; иначе говоря, всегда можно найти такое произведеніе $a\alpha$ (гдѣ α называется числомъ *сопряженнымъ* съ a). которое при дѣленіи на p даетъ остатокъ, равный единицѣ. Въ произведеніи $a\alpha$, α можетъ равняться a и можетъ быть не равно a. Если $\alpha = a$, то

$$a\alpha = a^2 \text{ и } a^2 \equiv 1\ (\textit{мод}\ p),$$

т. е. $$\frac{(a-1)(a+\ )}{p} = \text{цѣлому числу}.$$

Такъ какъ p—число простое, то произведеніе $(a-1)\ (a+1)$ только въ томъ случаѣ дѣлится на p, когда какой нибудь изъ его множителей дѣлится на p; $a-1$ дѣлится на p, если $a=1$; $\frac{a+1}{p}$ равняется цѣлому числу тогда только, когда $a=p-1$.

Поэтому только числа 1 и $p-1$ имѣютъ то свойство, что они, будучи умножены на самихъ себя, даютъ, при дѣленіи на p, остатокъ $=1$.

Во всякомъ другомъ случаѣ α—сопряженное число, отличное отъ a. Выбрасывая изъ ряда $1.2.3....p-1$ единицу и $p-1$, получимъ $2, 3,...p-3$, $p-2$. Очевидно, если изъ этого ряда мы возьмемъ какое нибудь число b, то найдемъ число β, сопряженное съ нимъ въ томъ же самомъ ряду. Числа $2, 3,...p-2$ могутъ быть поэтому раздѣлены на пары такъ, что числа одной пары суть сопряженныя, т. е.

$$\left.\begin{array}{ll} & b\beta\equiv 1 \\ & c\gamma\equiv 1 \\ & \ldots. \\ & l\lambda\equiv 1 \\ \text{откуда} & b\beta c\gamma...l\lambda\equiv 1 \end{array}\right\} (\textit{мод } p).$$

$$\text{но} \quad b\beta c\gamma..l\lambda=2.3.....p-2;$$

слѣдовательно, $2.3.\ 4....p-2\equiv 1$ (*мод* p).

Умноживъ обѣ части сравненія на $1.(p-1)$, получимъ:

$$1.2.3.4.....(p-2)\ (p-1)\equiv p-1\ (\textit{мод } p);$$

$$\text{но} \quad p-1\equiv -1\ (\textit{мод } p),$$

$$\text{значитъ,} \quad 1.2.3...(p-2)\ (p-1)\equiv -1\ (\textit{мод } p)$$

$$\text{или:} \quad [1.2.3....(p-1)]+1\equiv 0\ (\textit{мод } p)$$

§ 39. О рѣшеніи сравненій съ одною неизвѣстною.

Вышеизложенныя свойства сравненій позволяютъ намъ рѣшать сравненія аналогично рѣшенію уравненій.

Теорія чиселъ занимается между прочимъ рѣшеніемъ сравненій вида

$$f(x)=x^m+Ax^{m-1}+Bx^{m-2}+\ldots\ldots+Lx+M\equiv 0\ (\textit{мод } N),$$

гдѣ лѣвая часть представляетъ многочленъ съ коэффиціентами $A,B....\ L,M$ цѣлыми (положительными или отрицательными—безразлично).

Рѣшить сравненіе*) $f(x)\equiv 0$ (*мод* N), значитъ подыскать для x та-

---

*) Рѣшеніе этого сравненія тожественно съ рѣшеніемъ неопредѣленнаго уравненія $f(x)-Ny=0$ въ цѣлыхъ числахъ.

кое цѣлое число, которое удовлетворяло бы данному сравненію, т. е. обращало бы его въ тождество.

Подобно уравненіямъ, сравненія различаются по степенямъ неизвѣстной величины (x). Существуютъ *сравненія первой степени*, второй и т. д. (рѣшеніе сравненій второй степени составляетъ предметъ т. н. теоріи квадратичныхъ вычетовъ).

Прежде чѣмъ приступить къ изученію теоріи рѣшенія сравненій докажемъ общую теорему, которая лежитъ въ основаніи этой теоріи.

Если сравненію $f(x)\equiv 0$ (мод p) удовлетворяетъ $x=a$, то ему удовлетворяютъ и всѣ числа, сравнимыя съ a по модулю p, т. е. составляющія одинъ классъ.

Изъ сравненія $x\equiv a$ (*мод* p) вытекаетъ *, что $f(x)\equiv f(a)$ (*мод* p). По положенію же a удовлетворяетъ сравненію, значитъ:

$$f(a)\equiv 0 \quad (\textit{мод}\ p)$$

или:

$$f(x)\equiv 0 \quad (\textit{мод}\ p).$$

Такимъ образомъ, найдя одно число, удовлетворяющее данному сравненію, тотчасъ же находимъ, что всѣ числа, принадлежащія къ одному и тому же классу, удовлетворяютъ сравненію

Такъ, напримѣръ, въ сравненіи.

$$2x^2+7x+3\equiv 0 \quad (\textit{мод}\ 11)$$

$x=5$, и этому же сравненію удовлетворяютъ слѣдующія числа:

$$x=5,\ 16,\ 27, \ldots\ldots -6, -17, -28 \ldots\ldots$$

Слѣдовательно, рѣшить сравненіе—значитъ найти цѣлые классы чиселъ, обращающихъ данное сравненіе въ тождество, при чемъ каждый классъ составитъ одно рѣшеніе. Этимъ обстоятельствомъ вносится существенное различіе сравненій отъ уравненій.

§ 40. О сравненіи первой степени. Общій видъ сравненій первой степени есть:

$$ax\equiv b \quad (\textit{мод}\ N)$$

гдѣ a, b числа положительныя или отрицательныя; N число положительное. При рѣшеніи сравненій этого вида могутъ представиться два случая: 1) когда a и N числа относительно другъ друга простыя; 2) когда они имѣютъ общаго дѣлителя.

Въ первомъ случаѣ сравненіе $ax\equiv b$ (*мод* N) можетъ имѣть только одно рѣшеніе. Въ самомъ дѣлѣ, положимъ, что оно удовлетворяется при $x=\alpha$ и $x=\beta$, при чемъ α не$\equiv\beta$ (*мод* N).

Если $x=\alpha$, то $\qquad a.\alpha\equiv b$ (*мод* N);

а если $x=\beta$, то $\qquad a.\beta\equiv b$ (*мод* N)

---

*) См. § 32.

Вычтя изъ перваго сравненія второе получимъ:

$$a(\alpha-\beta)\equiv 0 \text{ (мод N)},$$

т. е. $a(\alpha-\beta)$ должно цѣликомъ дѣлиться на N. Но этого быть не можетъ, такъ какъ a и $(\alpha-\beta)$—взаимно простыя съ N. Слѣдовательно, въ этомъ случаѣ существуетъ только одно рѣшеніе сравненія.

Теоретически говоря, можно найти рѣшеніе, примѣняя теоремы Фермата и Эйлера. Пусть дано сравненіе: $ax\equiv b$ (мод p), гдѣ p—абсолютно простой модуль. Теорема Фермата даетъ намъ, что $a^{p-1}\equiv 1$ (мод p).

Умножая обѣ части этого сравненія на b и разлагая a^{p-1} на множителя—$a.a^{p-2}$, получимъ:

$$a.b.a^{p-2}\equiv b \text{ (мод } p).$$

Сопоставляя это сравненіе съ даннымъ, заключаемъ, что

$$x=b.a^{p-2}$$

Если, напр., дано сравненіе: $7x\equiv 3$ (мод 5), то $x=3.7^3=1029$; дѣйствительно, $7.1029-30\equiv$ (мод 5).

Аналогично съ этимъ, при модулѣ сложномъ—N можно воспользоваться теоремой Эйлера. Если дано сравненіе: $ax\equiv b$ (мод N) то, по теоремѣ Эйлера: $a^{\varphi(N)}\equiv 1$ (мод N).

Практическаго значенія этотъ способъ очевидно не имѣетъ.

Умножая, по предыдущему, обѣ части этого сравненія на b и разлагая $a^{\varphi(N)}$ на a и $a^{\varphi(N)-1}$, получимъ:

$$a.ba^{\varphi(N)-1}\equiv b \text{ (мод } N).$$

откуда — $x=b.a^{\varphi(N)-1}$

Такъ сравненію: $3x\equiv 11$ (мод 8) удовлетворяютъ $x=11.3^3=297$.

Разсмотримъ теперь вторoй случай, когда a и N имѣютъ общаго дѣлителя δ. Тутъ можетъ быть два подслучая: или 1) b не дѣлится на δ или 2) b дѣлится на δ.

Въ первомъ подслучаѣ сравненіе въ цѣлыхъ числахъ рѣшено быть не можетъ. Дѣйствительно, если бы можно было найти цѣлое число x, которое удовлетворяетъ данному сравненію, тогда существовало бы сравненіе:

$$ax_1-b\equiv 0 \text{ (мод N), или } \frac{ax_1}{\delta}-\frac{b}{\delta}\equiv 0 \text{ (мод N)},$$

$\frac{ax_1}{\delta}-\frac{b}{\delta}=$цѣлому числу, кратному N, чего быть не можетъ, такъ какъ $\frac{ax_1}{\delta}$ цѣлое число, а $\frac{b}{\delta}$ — несократимая дробь.

Если же b дѣлится на δ (2-й подслучай), то рѣшеніе даннаго сравненія

$$ax\equiv b\ (\textit{мод}\ \mathrm{N}), \qquad (1).$$

сводится къ рѣшенію сравненія: $\frac{a}{\delta}x\equiv\frac{b}{\delta}\left(\textit{мод}\frac{\mathrm{N}}{\delta}\right)$. (2).

Чтобы доказать это, покажемъ сначала, что если какое-нибудь значеніе $x=x_1$ удовлетворяетъ сравненію (1), то оно удовлетворяетъ и (2).

Итакъ, пусть $ax_1\equiv b\ (\textit{мод}\ \mathrm{N})$;

тогда $\frac{ax_1-b}{N}$=цѣлому числу.

Раздѣливъ числителя и знаменателя этого выраженія на δ, получимъ:

$$\frac{\frac{ax_1}{\delta}-\frac{b}{\delta}}{\frac{N}{\delta}}=\text{цѣлому числу, т. е. }\frac{ax_1}{\delta}\equiv\frac{b}{\delta}\left(\textit{мод}\frac{\mathrm{N}}{\delta}\right).$$

Другими словами, x_1 удовлетворяетъ сравненію (2). Теперь обратно, если какое-нибудь x_2 удовлетворяетъ сравненію (2), т. е. если

$$\frac{ax_2}{\delta}\equiv\frac{b}{\delta}\left(\textit{мод}\frac{\mathrm{N}}{\delta}\right),\ \text{то}\ \frac{\frac{ax_7}{\delta}-\frac{b}{\delta}}{\frac{\mathrm{N}}{\delta}}=\frac{ax_2-b}{N}=\text{цѣл. числу,}$$

или $ax_2\equiv b\ (\textit{мод}\ \mathrm{N})$

Такимъ образомъ, рѣшенія сравненія (1) тождественны съ рѣшеніями сравненія (2); но это послѣднее подходитъ подъ 1-й случай, такъ какъ въ немъ $\frac{a}{\delta}$ и $\frac{\mathrm{N}}{\delta}$ уже взаимно простыя, а поэтому всѣ числа, удовлетворяющія (2) сравненію будутъ по отношенію къ нему составлять одно рѣшеніе, но по отношенію къ (1) сравненію они составляютъ уже различныя рѣшенія, число которыхъ равно δ, т. е. общему дѣлителю членовъ сравненія и модуля.

Дѣйствительно, всѣ рѣшенія (2), слѣдовательно и (1) сравненій, представляются подъ видомъ:

$$x \equiv \alpha \left(\textit{мод}\frac{N}{\delta}\right), \text{ или: } x=\alpha+\frac{N}{\delta}q;$$

гдѣ q—цѣлое число, а α не<0 и$<\frac{N}{\delta}$

Придавая q значенія $0,1,2,\ldots\delta-1\ldots$, мы будемъ получать числа:

$$\alpha,\ \alpha+\frac{N}{\delta},\ \alpha+2\frac{N}{\delta},\ldots\alpha+\frac{N}{\delta}(\delta-1),\ \alpha+\frac{N}{\delta}.\delta,\ \alpha+\frac{N}{\delta}(\delta+1),\ldots$$

изъ которыхъ первыя δ $\left(\text{отъ } \alpha \text{ до } \alpha+\frac{N}{\delta}(\delta-1)\right)$, очевидно, не сравнимы между собою по модулю N, а каждое изъ слѣдующихъ $\left(\text{начиная съ } \alpha+\frac{N}{\delta}.\ \delta\right)$ непремѣнно найдетъ среди первыхъ число одного съ собою класса. Такимъ образомъ, данное сравненіе имѣетъ δ рѣшеній:

$$x\equiv\alpha\ (\textit{мод}\ N),\ x\equiv\left[\alpha+\frac{N}{\delta}\right](\textit{мод}\ N),\ x\equiv\left[\alpha+2\frac{N}{\delta}\right](\textit{мод}\ N),\ldots$$

$$\ldots\ldots x\equiv\left[\alpha+\frac{N}{\delta}(\delta-1)\right]\ (\textit{мод}\ N)$$

Рѣшеніе сравненія (1): $ax\equiv b$ $(\textit{мод}\ N)$, гдѣ a и N взаимно простыя, тождественно съ рѣшеніемъ въ цѣлыхъ числахъ неопредѣленнаго уравненія:

$$ax-Ny=b.$$

§ **41.** Не останавливаясь на способахъ рѣшенія неопредѣленныхъ уравненій (они изложены въ элементарной алгебрѣ) мы обратимся къ нѣкоторымъ частнымъ результатамъ теоріи рѣшенія сравненій 1-й степени, которые будутъ имѣть большое значеніе въ теоріи рѣшенія сравненій, высшихъ степеней, теоріи степенныхъ вычетовъ.

1. *Если даны два взаимно простыхъ числа—m и n, то всегда можно найти другія два положительныхъ числа x и y, при чемъ $x<m$, а $y<n$ такъ, что*

$$mx-ny=1.$$

Эта весьма важная теорема вытекаетъ непосредственно изъ сравненія: $mx\equiv1$ $(\textit{мод}\ n)$,
которое всегда имѣетъ рѣшеніе, такъ какъ m и n суть числа взаимно простыя.

Въ болѣе общемъ видѣ эта теорема выразится такъ:

2. *Если даны два числа M и H, имѣющія общаго дѣлителя δ, то всегда можно найти цѣлыя положительныя числа x и y такъ что $Mx-Hy=\delta$.*

Если M и H—кратныя отъ δ, то $\frac{M}{\delta}=m$ и $\frac{H}{\delta}=n$.

По предыдущему $mx-ny=1$.

Умноживъ это равенство на δ, получимъ:

$$\delta.mx-\delta\ ny=\delta,\text{ или } Mx-Hy=\delta.$$

3. Теперь предположимъ, что намъ дано число a такое, что

$$a^M\equiv1\ (\text{мод } p)\text{ и } a^H\equiv1\ (\text{мод } p).$$

Въ такомъ случаѣ можно написать сравненіе:

$$a^\delta\equiv1\ (\text{мод } p),$$

гдѣ δ—общій наибольшій дѣлитель чиселъ M и H.

Въ самомъ дѣлѣ, возведя первое сравненіе въ степень x, а второе—въ y, получимъ:

$$a^{Mx}\equiv1\ (\text{мод } p),\qquad a^{Hy}\equiv1\ (\text{мод } p),$$

откуда $a^{Mx}\equiv a^{Hy}\ (\text{мод } p)$, $\quad a^{Mx}-a^{Hy}\equiv0\ (\text{мод } p)$;

$$a^{Hy}\ (a^{Mx-Hy}-1)\equiv0\ (\text{мод } p),\qquad a^{Mx-Hy}\equiv1\ (\text{мод } p).$$

Но $Mx-Hy\equiv\delta$; слѣдовательно, $a^\delta\equiv0\ (\text{мод } р)$.

IX.

Теорія степенныхъ вычетовъ.

§ 42. Степенные вычеты. Возьмемъ степени числа a: a, a^2, a^3,...a^{p-2},a^{p-1},... и будемъ дѣлить ихъ на p, тогда получимъ рядъ различныхъ остатковъ,

$$r_1,\ r_2,\ r_3,\ r_4....r_{p-2},\ r_{p-1},...$$

которые называются *степенными вычетами* числа a по модулю p. Въ ряду этихъ остатковъ будетъ остатокъ равный 1; такъ $a^{p-1}\equiv1$ ($\text{мод } p$); кромѣ этой степени дадутъ остатки 1 еще $a^{2(p-1)}$, $a^{3(p-1}$,....$a^{n(p-1)}$ (a^0 .несомнѣнно дастъ 1, но эту степень мы пока въ разсчетъ не принимаемъ).

Въ ряду степеней 10^0, 10^1, 10^2,....10^{10} при дѣленіи на 10 получится остатокъ равный 1 отъ степени 10^{10}, ибо $10^{10}\equiv1$ ($\text{мод }11$), но несомнѣнно, что $10^2\equiv1$ ($\text{мод }11$). Это показываетъ, что для нѣкоторыхъ чиселъ есть степень $<p-1$, которая даетъ при дѣленіи на p остатокъ, равный 1. Условимся обозначать наименьшую степень, дающую остатокъ 1 (опять таки исключая a^0) буквою s и будемъ говорить въ этомъ случаѣ, что *a принадлежитъ къ числу s по модулю p*. Докажемъ слѣдующую теорему.

Если a^s есть первая степень дающая при дѣленіи на p остатокъ 1, то $p-1$ дѣлится нацѣло на s.

Имѣемъ $a^s\equiv1$ (*мод* p) и $a^{p-1}\equiv1$ (*мод* p).
Если же δ есть общій дѣлитель чиселъ s и $p-1$, то на основаніи теоремы § 41 мы получимъ:

$$a^{\delta}\equiv1 \text{ (мод } p)$$

Не трудно видѣть, что δ есть ничто иное, какъ само s. Дѣйствительно, относительно δ можетъ быть только два предположенія: или оно меньше s или равно s. Первое предположеніе уничтожается само собою, ибо s по условію есть первая степень, дающая остатокъ 1; слѣдовательно $\delta=s$, или s есть дѣлитель $p-1$, а это требовалось доказать. Имѣя рядъ степеней a^0, a^1,. a^2,... a^s,.. .a^{p-1}, при дѣленіи на p получимъ остатки 1. r,....r_s,.... r_{p-1} и, взявъ s-тую степень a, будемъ имѣть $a^s\equiv1$ (*мод* p); но $a^{s+1}\equiv a$ (*мод* p) и $a\equiv r_1$ (*мод* p). Слѣдовательно, $a^{s+1}\equiv r_1$ (*мод* p): также и $a^{s+2}\equiv r_2$ (*мод* p), $a^{s+3}\equiv r_3$ (*мод* p). ..$a^{2s}\equiv1$ (*мод* p), $a^{2s+1}\equiv r_1$ (*мод* p) и т. д., т. е. остатки будутъ повторяться періодически. Всѣхъ же различныхъ остатковъ будетъ s, потому что для a^{s+1} остатокъ тотъ же, что и для a.

Въ ряду натуральныхъ чиселъ есть такія, у которыхъ $s=p-1$, другими словами ни одна степень $<p-1$ при дѣленіи на p не даетъ остатка равнаго числу 1. Числа эти называются ***первообразными корнями*** (g) числа p. Напримѣръ, 10 есть первообразный корень чиселъ 7, 17, 19, 23, 29, т. е. $10^6\equiv1$ (*мод.* 7) $10^{16}\equiv1$ (*мод* 17),.... $10^{28}\equiv1$ (*мод* 29).

На теоріи степенныхъ вычетовъ основывается нахожденіе признаковъ дѣлимости чиселъ на абсолютно простое число, разложеніе дробей въ періодическія (и въ томъ и въ другомъ случаѣ система счисленія роли не играетъ).

§ 43. Приложеніе теоріи степенныхъ вычетовъ къ нахожденію признаковъ дѣлимости. Переходимъ къ общей постановкѣ вопроса о нахожденіи признаковъ дѣлимости. Задача эта есть частная задача болѣе общей: какой остатокъ получится отъ дѣленія N на простое число p? Намъ уже извѣстно, что всякое число N можетъ быть изображено подъ видомъ полинома, расположеннаго по степенямъ основанія α.

т. е. $$N=a_1\ \alpha^n+a_1\alpha^{n-1}+a_2\alpha^{n-2}+\ldots+a_n$$

гдѣ a_0, a_1,... не должны превышать α—1.

Въ данной задачѣ можетъ быть два случая:

1) основаніе системы счисленія α есть дѣлитель числа p; въ этомъ случаѣ признакъ дѣлимости на p опредѣляется очень просто: нужно посмотрѣть на послѣднее число a_n и узнать, дѣлится ли оно на p;

2) α не дѣлится на p. Разсмотримъ остатки отъ дѣленія различныхъ степеней основанія α на число p и для общности положимъ, что наименьшая степень, дающая остатокъ$=1$, есть α^s (гдѣ =дѣлителю r—1); получимъ рядъ сравненій:

$$\alpha\equiv r_1\ (мод\ p),\qquad \alpha^2\equiv r_2\ (мод\ p),\ \ldots$$

$$\alpha^s\equiv 1\ (мод\ p),\qquad \alpha^{s+1}\equiv r_1\ (мод\ p),\qquad \alpha^{s+2}\equiv r_2\ (мод\ p),\ \ldots$$

$$\alpha^{2s}\equiv 1\ (мод\ p),\ \ldots$$

Присоединимъ сюда еще сравненіе:

$$a_n\equiv a_n\ (мод\ p).$$

Умножая каждое изъ этихъ сравненій па соотвѣтствующіе коэффиціенты a_0, a_1, a_2.... и складывая ихъ, получимъ въ лѣвой части сравненія самое число N, а въ правой $a_0+a_1.r_1+a_2r_2+\ldots$ $\ldots+a_{n-1}r_{n-1}+a_n$. Такимъ образомъ у насъ получается сравненіе которое позволяетъ для опредѣленія признака дѣлимости числа N разсматривать не это число, а гораздо меньшее, стоящее во второй части сравненія. Для практическаго примѣненія оказывается возможнымъ ввести способъ болѣе изящный и болѣе простой. Если бы мы хотѣли узнать по первому способу признакъ дѣлимости какого нибудь числа на 7, то очевидно мы должны были бы дѣлить его на группы по 6 цифръ въ каждой, что для дальнѣйшаго вычисленія было бы весьма затруднительно; потому для упрощенія доказывается теорема, что *если* s *четное, то* $\alpha^{\frac{s}{2}}\equiv-1$ (*мод* p) Въ самомъ дѣлѣ,

$$\alpha^s\equiv 1\ (мод\ p),\quad \frac{\alpha^s-1}{p}=\frac{(\alpha^{\frac{s}{2}}+1)\ (\alpha^{\frac{s}{2}}-1)}{p};$$

но $a^{\frac{s}{2}}-1$ не можетъ дѣлиться на p (по опредѣленію числа s), поэтому

$$a^{\frac{s}{2}} \equiv -1 \ (мод\ p), \qquad a^{\frac{s}{2}} \equiv -r_1 \ (мод\ p)$$

Слѣдовательно, число разобьется на группы по $\frac{s}{2}$ цифръ въ каждой, остатки же будутъ имѣть видъ:

$$1,\ r_1,\ r_2, \ldots r_{\frac{s}{2}-1}\ -1, -r_1, -r_2, \ldots 1,\ r_1,\ \text{и т. д.}$$

Такъ напр. для простого числа 91, $s=6$. Послѣдовательные остатки отъ дѣленія степеней 10 на 91 суть 1, 10, 9, —1, —10, —9. Поэтому получаемъ очень изящный признакъ дѣлимости. Если дано, напр., число 234156588101345, то нужно раздѣлить число на грани, по три цифры въ каждой грани, взять произведеніе первой слѣва цифры на 9 и прибавить къ этому произведенію число, состоящее изъ двухъ другихъ цифръ, затѣмъ, составивъ такимъ образомъ числа для всѣхъ граней, изъ суммы чиселъ для нечетныхъ граней вычесть сумму чиселъ для четныхъ. Для написаннаго числа будемъ имѣть:

для первой грани число 72, для второй—10, для третьей 133, для четвертой—65, для пятой 52.

Алгебрическая сумма $72-10+133-65+52=182=2{,}91$. Слѣдовательно, число дѣлится на 91.

Предлагаю въ видѣ упражненія: 1) найти признаки дѣлимости для числа, написаннаго по десятеричной системѣ, на числа: 13, 37, 73, и 101; 2) признаки дѣлимости на всѣ простыя числа меньшія 20 для числа, написаннаго по бинарной или троичной системѣ.

X.

Теорія индексовъ.

§ 44. Понятіе объ индексѣ. На теоріи степенныхъ вычетовъ основано также чрезвычайно важное ученіе объ указателяхъ или индексахъ, съ помощью которыхъ значительно облегчается рѣшеніе сравненій какъ первой, такъ и высшихъ степеней.

Если g есть первообразный корень числа p, то, какъ мы раньше видѣли, рядъ степеней g: $g^0, g^1, g^2, g^3 \ldots g^s, \ldots g^{p-2}, g^{p-1}, g^p, \ldots$ при дѣленіи на p даетъ рядъ остатковъ:

$$1,\ r_1,\ r_2,\ r_3, \ldots r_s, \ldots r_{p-2},\ 1,\ r_1, \ldots$$

которые періодически повторяются. Числа 1, r_1, r_2,...r_{p-2} составляющіе періодъ, будучи всѣ меньше p и неравны между собою, очевидно совпадаютъ съ числами 1, 2, 3,...p—1, расположенными въ другомъ порядкѣ.

Положимъ, что намъ дано какое-либо число L, не дѣлящееся на p; тогда остатокъ отъ дѣленія L на p непремѣнно найдется въ ряду: 1, 2, 3...p—1,—какое нибудь r_k, а въ ряду: g^0, g^1, g^2, g^{p-2} —этому числу L будетъ соотвѣтствовать какая нибудь степень g_k. Иначе говоря,

$$L\equiv r_k \ (\text{мод } p); \qquad g^k\equiv r_k \ (\text{мод } p).$$

Слѣдовательно,

$$L\equiv g^k \ (\text{мод } p).$$

Вотъ этотъ то показатель степени, k, въ которую надо возвысить основаніе—g, чтобы получить число, сравнимое съ даннымъ—L по модулю p, и называется *указателемъ*, *индексомъ*, (*Ind*) числа L. Это принято выражать слѣдующимъ обозначеніемъ:

$$k=Ind_g\ L \ (\text{мод } p) \ ^{*)}.$$

Для всѣхъ чиселъ одного и того же класса по модулю p индексъ имѣетъ одно и то-же значеніе и является „инваріантою“.

§ 45. Прежде чѣмъ перейти къ вопросу о нахожденіи *Ind* даннаго числа и, наоборотъ, числа по данному *Ind*, мы познакомимся съ главнѣйшими свойствами индексовъ и предварительно докажемъ двѣ теоремы, которыми намъ не разъ придется пользоваться.

1. *Двѣ степени первообразнаго корня* (g), *показатели которыхъ отличаются другъ отъ друга на число кратное* (p—1), *сравнимы между собою по модулю* p;

и 2. *Если двѣ степени первообразнаго корня* (g) *сравнимы между собою по модулю* p, *то показатели ихъ сравнимы по модулю* p—1.

Пусть даны двѣ степени: g^s и g^t, причемъ $t=\lambda\ (p-1)+s$, т. е. t отличается отъ s на число $\lambda\ (p-1)$—кратное отъ (p—1). Въ такомъ случаѣ непремѣнно будетъ существовать сравненіе:

$$g^s\equiv g^t \ (\text{мод } p).$$

Дѣйствительно, изъ теоремы Фермата слѣдуетъ, что:

$$g^{\lambda(p-1)}\equiv 1 \ (\text{мод } p)$$

Умножая обѣ части этого сравненія на g^s, получимъ:

---

*) Какъ можно видѣть изъ этого перваго понятія объ индексѣ, оно аналогично понятію о лагориемѣ въ алгебрѣ; эта аналогія сдѣлается, еще яснѣе, когда мы разсмотримъ далѣе свойства *Ind* и сравнимъ ихъ со свойствами *log*.

$$g^{\lambda(p-1)+s} \equiv g^s \ (мод\ p),$$

или:

$$g^t \equiv g^s \ (мод\ p),$$

что и требовалось доказать.

Положимъ теперь, что наоборотъ—дано сравненіе:

$$g^s \equiv g^t \ (мод\ p).$$

Перенеся g^t въ первую часть и взявъ его за скобки, получимъ:

$$g^t(g^{s-t} - 1) \equiv 0 \ (мод\ p),$$

или, раздѣливъ это сравненіе на g^t и перенеся 1 во вторую часть;

$$g^{s-t} \equiv 1 \ (мод\ p).$$

Съ другой стороны, такъ какъ g есть первообразный корень, то

$$g^{\lambda(p-1)} \equiv 1 \ (мод\ p).$$

Сопоставляя оба эти сравненія, мы должны заключить, что

$$s-t=\lambda\ (p-1);$$

другими словами, $s-t$ безъ остатка дѣлится на $p-1$,

т. е.

$$s \equiv t \ (мод\ p-1),$$

и вторая теорема является строго доказанной.

§ 46. Индексъ произведенія. При помощи этихъ теоремъ нетрудно вывести основныя свойства индексовъ.

Пусть индексъ нѣкотораго числа A будетъ m, а индексъ другого числа B положимъ $=n$, индексъ произведенія $A.B$ обозначимъ чрезъ l. Спрашивается, въ какомъ отношеніи между собою находятся m, n и l? Изъ того, что $Ind\ A=m$ и $Ind\ B=n$; слѣдуетъ, что

$$A \equiv g^m \ (мод\ p) \text{ и } B \equiv g^n \ (мод\ p).$$

Перемноживъ эти сравненія, мы получимъ:

$$AB \equiv g^{m+n} \ (мод\ p).$$

Съ другой стороны, если $Ind\ AB=l$, то значитъ

$$AB \equiv g^l \ (мод\ p).$$

Изъ этихъ двухъ сравненій вытекаетъ, что

$$g^{m+n} \equiv g^{l} \ (мод\ p),$$

откуда, на основаніи предыдущихъ теоремъ,

$$m+n \equiv l \ (мод\ p-1),$$

или $$Ind\ A.B \equiv [Ind\ A + Ind\ B] \ (мод\ p-1)$$

т. е. индексъ произведенія двухъ чиселъ сравнимъ съ суммою индексовъ обоихъ чиселъ.

Отъ случая двухъ множителей легко можно перейти въ какому угодно ихъ числу. Положимъ, что мы имѣемъ рядъ чиселъ: A, B, C,....R, индексы которыхъ по модулю p будутъ соотвѣтственно l, m, n,....r. Тогда, слѣдовательно, существуютъ сравненія:

$$A \equiv g^{l} \ (мод\ p),\quad B \equiv g^{m} \ (мод\ p),\quad C \equiv g^{n} \ (мод\ p), .. R \equiv g^{r} \ (мод\ p),$$

Перемноживъ ихъ, мы получимъ:

$$ABC\ldots .R \equiv r^{l+m+n+\ldots+r} \ (мод\ p).$$

Обозначивъ $Ind\ ABC\ldots.R$ чрезъ s, найдемъ, что—

$$g^{s} = g^{l+m+-+\ldots+r} \ (мод\ p);$$

а отсюда, по предыдущему; $s \equiv l+m+n+\ldots.+r \ (мод\ p-1)$,

или $$Ind ABC\ldots R \equiv Ind A + Ind B + Ind C + \ldots + Ind R \ (мод\ p-1)$$

Итакъ, *индексъ произведенія сравнимъ съ суммой индексовъ производителей по модулю p -1* *).

§ 47. Индексъ степени. Доказавъ эту общую теорему, мы разсмотримъ частный случай ея—именно предположимъ, что числа $A, B, C, \ldots R$ равны, при чемъ число ихъ пусть равно k. Тогда сравненіе

$$Ind\ ABC\ldots R = Ind\ A + Ind\ B + Ind C + \ldots + Ind\ R \ (мод\ p-1)—$$

---

*) Это общее положеніе можно доказать нѣсколько другимъ способомъ. Взявъ произведеніе первыхъ двухъ чиселъ даннаго ряда: A и B, мы заключаемъ, что $Ind\ AB \equiv [Ind\ А + Ind\ Б]$ (*мод* $p-1$). Разсматривая затѣмъ произведеніе AB и третье число—C, мы найдемъ: $Ind\ AB.C \equiv [Ind AB + Ind C]$ (*мод* $p-1$) или: $Ind\ ABC \equiv Ind\ AB + Ind\ C$ (*мод* $p-1$). Продолжая эту операцію точно также и надъ дальнѣйшими числами, мы получимъ въ концѣ концовъ: $Ind ABC\ldots R \equiv [Ind A + Ind B + Ind C + \ldots + Ind R]$ (*мод* $p-1$).

приметъ видъ. $\mathit{Ind}\ A^k \equiv k.\ \mathit{Ind}\ A\ (\text{мод}\ p-1)$,

т. е. *индексъ степени сравнимъ по модулю p—1 съ индексомъ основанія, повтореннымъ столько разъ, сколько единицъ въ показателѣ степени*

Эту теорему можно вывести другимъ путемъ. Пусть $\mathit{Ind}\ A = m$, а $\mathit{Ind}\ A^k = n$, значитъ: (1) $A \equiv g^m\ (\text{мод}\ p)$

Возвышаемъ обѣ части сравненія (1) въ k—тую степень. Тогда— $A^k = g^{mk}\ (\text{мод}\ p)$; (3)

сопоставляя (3) и (2) сравненія, находимъ:

$$g^n = g^{mk}\ (\text{мод}\ p)$$

Припоминая, что если двѣ степени сравнимы по модулю p, то показатели ихъ сравнимы по модулю $p-1$, заключаемъ, что—

$$n \equiv mk\ (\text{мод}\ p-1),$$

т. е. $\mathit{Ind}\ A^k \equiv k.\ \mathit{Ind}\ A\ (\text{мод}\ p-1)$.

§ 48. Приложенія теоріи индексовъ. Рѣшеніе сравненій I-й степени. Замѣтивъ эти главныя свойства индексовъ, мы перейдемъ къ ихъ приложеніямъ. Самое важное значеніе индексовъ въ практическихъ вопросахъ заключается въ томъ, что введеніе ихъ чрезвычайно ускоряетъ и упрощаетъ рѣшеніе сравненій, а слѣдовательно и неопредѣленныхъ уравненій.

Пусть дано сравненіе: $Ax = B\ (\text{мод}\ p)$,

гдѣ A и B—числа не дѣлящіяся на p, и p—число абсолютно простое.

Положимъ, что этому сравненію удовлетворяетъ $x = x_1$. По опредѣленію индексовъ, индексы двухъ чиселъ, сравнимыхъ между собою, должны быть тождественны, Значитъ,

$$\mathit{Ind}\ Ax_1 = \mathit{Ind}\ B.$$

Но мы знаемъ, что: $\mathit{Ind}\ Ax_1 \equiv [\mathit{Ind} A + \mathit{Ind} x_1] \equiv (\text{мод}\ p-1$

Слѣдовательно $\mathit{Ind} A + \mathit{Ind} x_1 \equiv \mathit{Ind} B\ (\text{мод}\ p-1)$.

Отсюда— $\mathit{Ind} x_1 \equiv \mathit{Ind} B - \mathit{Ind} A\ (\text{мод}\ p-1)$ *)

---

*) Этотъ результатъ вполнѣ отвѣчаетъ извѣстному въ теоріи логариѳмовъ положенію, что $\log \frac{b}{a} = \log b - \log a$.

Такимъ образомъ, зная индексы чиселъ A и B, мы простѣйшимъ вычисленіемъ можемъ опредѣлить $Indx_1$, а зная $Indx_1$ найдемъ весь тотъ классъ чиселъ, которому соотвѣтствуетъ этотъ индексъ, для котораго онъ является *инваріантою*

§ 49. Таблица индексовъ. Весь вопросъ, слѣдовательно, сводится къ тому, какъ возможно быстро опредѣлить *Ind* даннаго числа и, наоборотъ, по данному индексу опредѣлить число. Эта цѣль съ успѣхомъ достигается при помощи особыхъ таблицъ, въ которыхъ подъ одними рубриками помѣщены числа, вычисленныя соотвѣтственно даннымъ индексамъ, подъ другими—индексы, соотвѣтствующія различнымъ числамъ. Вотъ двѣ изъ такихъ таблицъ (заимствованныя изъ „Теоріи сравненій“ Чебышева. Спб 1849 г.)

Простое число 13.

I.

N	0	1	2	3	4	5	6	7	8	9
0 1	1 4	6 11	10	8	9	2	12	7	3	5

N.

I	0	1	2	3	4	5	6	7	8	9
0 1	1 4	6 11	10	8	9	2	12	7	3	5

Таблица подъ буквою I служитъ для опредѣленія индексовъ по данному числу, а подъ буквою *N* для отысканія чиселъ по Ind. Первый вертикальный столбецъ въ этихъ таблицахъ содержитъ десятки числа (таблица I) или индекса (таб. N), а первый горизонтальный рядъ—единицы. Искомое находится на пересѣченіи вертикальнаго и горизонтальнаго рядовъ. Напр., опредѣлимъ Ind 83; хотя этого числа нѣтъ въ таблицѣ (I), однако, зная, что $83 \equiv 5$ (*мод 13*), по опредѣленію индекса имѣемъ Ind 83=Ind 5 =9. Если, обратно, данъ индексъ числа, напр., Ind N=47, т. е. $N \equiv g^{47}$ (*мод 13*), то, желая уменьшить индексъ 47, положимъ, что $g^{47} \equiv g^x$ (*мод 13*) или $47 \equiv x$ (*мод 12*), т. е. $x=11$; этотъ индексъ принадлежитъ (см. § 44) числу N. По таблицѣ (N) видимъ, что N=11.

§ 50. Двучленныя сравненія. Положимъ, что дано сравненіе:

$$Ax^n \equiv B \text{ (мод } p\text{)}$$

(Сравненія такого вида называются *двучленными*). Спрашивается, какой способъ приложить для рѣшенія этого сравненія? По опредѣленію

$$Ind\ B = Ind\ (Ax^n)$$

Но— $Ind\ (Ax^n) \equiv Ind A + n Ind x$ (*мод* $p-1$).

Слѣдовательно — $Ind B \equiv Ind\ A + n.Ind x$ (*мод* $p-1$),

или— $n.Ind x \equiv Ind B - Ind A$ (*мод* $p-1$).

Отсюда уже нетрудно найти $Ind x$, а слѣдовательно и значеніе x. (Замѣтимъ между прочимъ, что данное сравненіе будетъ имѣть, вообще говоря, не одно рѣшеніе, а нѣсколько, какъ мы увидимъ ниже, на частномъ примѣрѣ).

Вотъ схема рѣшенія двучленныхъ сравненій. Приложимъ ее къ частному примѣру. Пусть дано сравненіе: $17x^1 \equiv 101$ (*мод* 13). Поступая по вышеуказанному, находимъ: $5\ Ind x \equiv Ind\ 101 - Ind\ 17$ (*мод* 12). Подыскивая въ таблицахъ соотвѣтственныя индексы, получимъ: $4\ Ind x \equiv 2 - 10 \equiv -8 \equiv 4$ (*мод* 12). Придавая $Ind x$ значенія, удовлетворяющія послѣднему сравненію, будемъ получать различныя значенія x. Итакъ, при $Ind x = 1$, x будетъ равно 6; при $Ind x = 4$, $x = 9$; при $Ind x = 7$, $x = 7$, при $Ind x = 10$, $x = 4$ и т. д. Подставимъ для провѣрки одно изъ значеній x въ данное сравненіе, положимъ $x = 4$; тогда получимъ: $17.4^4 \equiv 101$ (*мод* 13). Дѣйствительно, $17.4^4 - 10 \equiv 1251$ безъ остатка дѣлится на 13.

XI.

Квадратичные вычеты.

§ 51. Квадратичные вычеты. Изъ двучленныхъ сравненій особенно замѣчательны сравненія вида

$$z^2 \equiv q\ (\text{мод}\ p),$$

гдѣ мы можемъ предположить, что q не$\equiv 0$ (*мод* p), ибо въ такомъ случаѣ сравненіе имѣло бы лишь одно рѣшеніе: $z \equiv 0$ (*мод* p). Замѣчательно это сравненіе, во-первыхъ, по своей простотѣ и во-вторыхъ, особенно потому, что къ нему приводятся всѣ сравненія 2-й степени:

$$ax^2 + bx + c \equiv 0\ (\text{мод}\ p), \tag{1}$$

въ которомъ a можно считать взаимно простымъ съ p, а p не равнымъ 2, такъ какъ въ послѣднемъ случаѣ данное сравненіе можно было бы привести къ сравненію 1-й степени.

Умноживъ всѣ члены сравненія (1) на $4a$, прибавивъ и отнявъ въ первой части b^2, получимъ:

$$4a^2x^2+4abx+b^2+4ac-b^2\equiv0\ (\text{мод}\ p);$$

а отсюда $$(2ax+b)^2+4c-b^2\equiv0\ (\text{мод}\ p). \qquad (2).$$

Положимъ во (2) сравненіи: $2ax+b=z$ и $b^2-4ac=q$. Тогда оно приметъ видъ:

$$z^2\equiv q\ (\text{мод}\ p).$$

Слѣдовательно, для того, чтобы рѣшить (1) сравненіе, достаточно найти z, и тогда изъ уравненія: $2ax+b=z$ самыми простыми пріемами можно опредѣлить значенія x, удовлетворяющія (1) сравненію.

Поэтому мы займемся изслѣдованіемъ сравненій вида:

$$z^2\equiv q\ (\text{мод}\ p),$$

т. е. разсмотримъ, *какіе методы* приложить къ ихъ рѣшенію и *когда можно* рѣшить это сравненіе.

Если принять во вниманіе примѣчаніе о рѣшеніи сравненій вида $Ax^n\equiv B$ (*мод* p), то изъ нашего сравненія получимъ:

$$2Indz\equiv Indq\ (\text{мод}\ p-1). \qquad (3).$$

Такъ какъ $p-1$ число честное, то это сравненіе можетъ быть рѣшено только въ случаѣ $Indq$ четнаго; тогда q называется *квадратичнымъ вычетомъ* числа p; въ противномъ случаѣ q—*квадратичаый невычетъ* числа p.

Если подъ руками есть таблицы индексовъ, то рѣшеніе вопроса о томъ, есть-ли q квадратичный вычетъ или невычетъ, очень просто. Но таблицъ можетъ и не быть; тогда надо найти какой-нибудь другой критерій для рѣшенія этого вопроса.

Разсмотримъ отдѣльно, что имѣетъ мѣсто въ (3) сравненіи. Если q—квадратичный вычетъ, то $Indq=2t$ (кратному отъ 2-хъ). если же q—невычетъ, то $Indq=2t+1$ (t въ обоихъ случаяхъ различно). Слѣдовательно, обозначивъ первообразный корень числа p черезъ g, мы будемъ имѣть съ одной стороны—

(4) $g^{2t}\equiv q$ (*мод* p), съ другой $g^{2t+1}\equiv q$ (*мод* p). (5).

Возвышая обѣ части (4) сравненія въ степень $\frac{p-1}{2}$, получимъ:

$$g^{t(p-1)}\equiv q^{\frac{p-1}{2}}\ (\text{мод}\ p).$$

Но $g^{t(p-1)} \equiv 1$ (*мод* p).

Слѣдовательно, $q^{\frac{p-1}{2}} \equiv +1$ (*мод* p).

Обратимся теперь къ (5) сравненію. Возвысивъ его, такъ же какъ и (4), въ степень $\frac{p-1}{2}$, получимъ:

$$g^{t(p-1)+\frac{p-1}{2}} \equiv q^{\frac{p-1}{2}} \ (\textit{мод } p),$$

или: $g^{t(p-1)}.g^{\frac{p-1}{2}} \equiv q^{\frac{p-1}{2}}$ (*мод* p).

Такъ какъ— $g^{t(p-1)} \equiv 1$ (*мод* p),

то $g^{\frac{p-1}{2}} \equiv q^{\frac{p-1}{2}}$ (*мод* p).

По теоремѣ Фермата $g^{p-1} \equiv 1$ (*мод* p); другими словами:

$$\frac{g^{p-1}-1}{p} = \frac{(g^{\frac{p-1}{2}}-1)\ (g^{\frac{p-1}{2}}+1)}{p} = \text{цѣлому числу.}$$

Но въ виду того, что g есть первообразный корень числа p, $g^{\frac{p-1}{2}}$ не$\equiv 1$ (*мод* p), т. е. первый множитель полученнаго нами выраженія не можетъ дѣлиться на p; слѣдовательно, $(g^{\frac{p-1}{2}}+1)$

$$q^{\frac{p-1}{2}} \equiv -1 \ (\textit{мод } p).$$

Нетрудно убѣдиться, что и обратно, если $q^{\frac{p-1}{2}} \equiv +1$ (*мод* p), то q имѣетъ индексъ четный, т. е. (3) сравненіе, а слѣдовательно и сравненіе $z^2 \equiv q$ (*мод* p), имѣетъ рѣшеніе; наоборотъ, если $q^{\frac{p-1}{2}} \equiv -1$ (*мод* p), то $Ind q$—нечетный. Вотъ тѣ два критерія, которыми мы можемъ замѣнить нашъ первый критерій: все сводится къ тому, чтобы опредѣлить, какой изъ двухъ знаковъ выбрать въ сравненіи:

$$q^{\frac{p-1}{2}} \equiv \pm 1 \ (\textit{мод } p.) \qquad (6)$$

§ 52. Символъ Лежандра и его свойства. Для опредѣленія этого знака знаменитый Лежандръ ввелъ особый символъ, свойства котораго строго доказаны. Символъ этотъ выражается $\left(\frac{q}{p}\right)$ всегда равенъ 1, но со знакомъ (+) или (—), смотря по тому какой знакъ мы должны принять въ (6) сравненіи. Введеніемъ символа $\left(\frac{q}{p}\right)=\pm1$, задача наша не измѣняется, такъ какъ сопоставляя (6) сравненіе и значеніе символа, мы найдемъ, что $q^{\frac{p-1}{2}}\equiv\left(\frac{q}{p}\right)$ (*мод* p), а только сводится къ опредѣленію знака символа Лежандра.

Для этого разсмотримъ, какими свойствами обладаетъ символъ Лежандра.

1) *Если два числа сравнимы по модулю p, то символы ихъ равны.* Въ самомъ дѣлѣ, если $q\equiv q_1$ (*мод* p), то, возвышая обѣ части этого сравненія въ степень $\frac{p-1}{2}$, получимъ:

$$q^{\frac{p-1}{2}}\equiv q_1^{\frac{p-1}{2}} \text{ (мод } p).$$

А изъ опредѣленія символа Лежандра вытекаетъ, что

$$q^{\frac{p-1}{2}}\equiv\left(\frac{q}{p}\right) \text{ (мод } p) \text{ и } q_1^{\frac{p-1}{2}}\equiv\left(\frac{q_1}{p}\right) \text{ (мод } p).$$

Сопоставляя эти три сравненія находимъ:

$$\left(\frac{q}{p}\right)\equiv\left(\frac{q_1}{p}\right) \text{ (мод } p).$$

Если бы символы были различны, т. е. $\frac{q}{p}$ равнялось бы, положимъ, +1, а $\frac{q_1}{p}=-1$, то мы имѣли бы сравненіе:

$$+1\equiv-1 \text{ (мод } p), \text{ или } +2\equiv0 \text{ (мод } p).$$

Но этого быть не можетъ, такъ какъ p по условію не равно 2. Значитъ, теорема доказана.

Прежде чѣмъ показать значеніе этой теоремы для быстраго вычисленія символа, докажемъ еще вторую важную теорему:

2) *Если мы имѣемъ число, равное произведенію двухъ другихъ чиселъ, то символъ его равенъ произведенію символовъ этихъ двухъ чиселъ.*

Пусть $Q = q.q_1$, а символы ихъ: $\left(\frac{Q}{p}\right)$, $\left(\frac{q}{p}\right)$ и $\left(\frac{q_1}{p}\right)$.

Изъ опредѣленія символа слѣдуетъ, что—

$$q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \ (мод\ p), \quad q_1^{\frac{p-1}{2}} \equiv \left(\frac{q_1}{p}\right) \ (мод\ p).$$

Перемножимъ эти сравненія. Тогда получимъ.

$$q^{\frac{p-1}{2}} q_1^{\frac{p-1}{2}} \left(\frac{q}{p}\right)\left(\frac{q_1}{p}\right) \ (мод\ p).$$

или

$$(q.q_1)^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right)\left(\frac{q_1}{p}\right) \ (мод\ p).$$

Но такъ какъ $q.q_1 = Q$, то: $Q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right)\left(\frac{q_1}{p}\right)$ $(мод\ p)$.

Съ другой стороны, изъ того же опредѣленія символа выходитъ, что

$$Q^{\frac{v-1}{2}} \equiv \left(\frac{Q}{p}\right) \ (мод\ p).$$

Значитъ

$$\left(\frac{Q}{p}\right) \equiv \left(\frac{q}{p}\right)\left(\frac{q_1}{p}\right) \ (мод\ p).$$

А отсюда мы должны заключить, что—

$$\left(\frac{Q}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{q_1}{p}\right).$$

такъ какъ обратное привело бы насъ, какъ и въ первой теоремѣ, къ сравненію: $+1 \equiv -1$ $(мод\ p)$.

Легко видѣть, что (2) теорему можно распространить на любое число множителей, а затѣмъ, предположивъ всѣ эти множители равными, показать, что $\left(\frac{q^n}{p^n}\right) = \left(\frac{q}{p}\right)^n$.

Посмотримъ теперь, какъ, благодаря этимъ теоремамъ, облегчается задача отысканія значенія символа Лежандра. Пусть, напримѣръ, данъ символъ, $\left(\frac{1729}{101}\right)$. Замѣтивъ, что $1729 \equiv 12$ $(мод\ 101)$, мы на основаніи первой теоремы можемъ написать: $\left(\frac{1729}{101}\right) \equiv \left(\frac{12}{101}\right)$. Примѣняя теперь вторую теорему, находимъ: $\left(\frac{12}{101}\right) \equiv \left(\frac{2^2}{101}\right)$. $\left(\frac{3}{101}\right) \equiv \left(\frac{2}{101}\right)^2 \left(\frac{3}{101}\right)$. Но символомъ $\left(\frac{2}{101}\right)^2$ можно пренебречь, такъ какъ онъ всегда будетъ равенъ $+1$, и обратить вниманіе на символъ $\left(\frac{3}{101}\right)$, отъ котораго зависитъ знакъ $\left(\frac{12}{101}\right)$. Для нахожденія значенія $\left(\frac{3}{101}\right)$ изъ приведенныхъ двухъ теоремъ ничего извлечь нельзя, и потому надо найти еще какое-нибудь свойство символа Лежандра, которое позволило бы рѣшить нашу задачу. Такимъ свойствомъ является третья теорема, т. н. *законъ взаимности двухъ простыхъ чиселъ*, устанавливающій зависимость между значеніями символовъ $\left(\frac{q}{p}\right)$ и $\left(\frac{p}{q}\right)$.

§ 53. Лемма Гаусса. Есть очень много доказательствъ этого закона (и это болѣе всего указываетъ на тотъ интересъ, который возбуждалъ символъ Лежандра). Мы дадимъ одно изъ простѣйшихъ, которое основано на т. н. леммѣ Гаусса: *если i есть число отрицательныхъ наименьшихъ вычетовъ* *) *числа q по модулю p, то*

$$q^{\frac{p-1}{2}} \equiv (-1)^i \ (мод\ p),$$

такъ что, когда i—число четное, $\left(\frac{q}{p}\right) = +1$, если i—нечетное, то $\left(\frac{q}{p}\right) = -1$.

Эта лемма служитъ дополненіемъ къ теоремѣ Фермата, и доказательство ея сходно съ доказательствомъ послѣдней.

Составимъ, какъ мы это дѣлали въ теоремѣ Фермата, рядъ произведеній: $q.1, q.2, q.3, \dots, q.s, \dots q\frac{p-1}{2}$.

Пусть наименьшіе абсолютные вычеты этихъ произведеній будутъ: $r_1, r_2, r_3, \dots r_s, \dots r_{\frac{p-1}{2}}$.

Слѣдовательно, мы можемъ написать:

$q.1 \equiv r_1$ $(мод\ p)$; $q.2 \equiv r_2$ $(мод\ p)$; $q.4 \equiv r_3$ $(мод\ p), \dots q.s \equiv r_s$ $(мод\ p)$ $\dots\dots q\frac{p-1}{2} \equiv r_{\frac{p-1}{2}}$ $(мод\ p)$.

---

*) См. § 30.

Числа r_1, r_2, r_3,...r_s,...$r_{\frac{n-1}{2}}$ обладаютъ слѣдующими важными свойствами. 1) Всѣ они по абсолютной величинѣ $\leqq\frac{p-1}{2}$; 2) Ни одно изъ нихъ не можетъ равняться нулю, ибо, положивъ $r_s=0$, мы имѣли бы, что $\frac{s.q}{p}$=цѣлому числу, чего быть не можетъ, такъ какъ q—взаимно простое съ p, а $s<p$; 3) всѣ они взаимно простыя съ p, потому что только при этомъ условіи возможно сравненіе: $q.s\equiv r_s$ (*мод* p); 4) среди этихъ чиселъ нѣтъ двухъ, равныхъ между собою ни по абсолютной величинѣ, ни по знаку: если бы, положимъ $r_s=r_t$, то существовало бы сравненіе: $q.s-q.t$ (*мод* p), т. е. $\frac{q(s-t)}{p}$ было бы цѣлымъ числомъ; а этого быть не можетъ на томъ основаніи, что q—взаимно простое съ p, а s и t—каждое$<p$; а разность ихъ $s-t$ и подавно$<p$; точно также r_s не можетъ равняться $(-r_t)$, потому что это привело бы къ равенству: $\frac{q(s+t)}{p}$=цѣлому числу; но q—взаимно—простое съ p, а $s+t$ меньше p; значитъ, это равенство невозможно. Изъ всего этого можно заключить, что абсолютныя величины чиселъ рядовъ: $1,2,3,...s,...\frac{p-1}{2}$ и r_1, r_2, r_3,...r_s,...$r_{\frac{p-1}{2}}$ тождественны.

Перемножимъ теперь всѣ полученныя сравненія. Тогда мы найдемъ:

$$q^{\frac{p-1}{2}}(1.2.3....s...\frac{p-1}{2})\equiv r_1.r_2.r_3...r_s...r_{\frac{p-1}{2}}\ (\textit{мод}\ p).$$

Среди чиселъ $r_1.r_2,r_3...r_{\frac{p-1}{2}}$ есть несомнѣнно и отрицательныя, и если число ихъ будетъ, положимъ, i, то мы получимъ:

$$q^{\frac{p-1}{2}}\left(1.2.3...s...\frac{p-}{2}\right)\equiv(r_1)(r_2)(r_3)..(r_s)..(r_{\frac{p-1}{2}})(-1)^i\ (\textit{мод}\ p),$$

гдѣ (r_1), (r_2) и т. д. представляютъ абсолютныя значенія сооотвѣтствующихъ вычетовъ. Раздѣливъ обѣ части послѣдняго сравненія на тождественныя произведенія $\left(1.2.3....\frac{p-1}{2}\right)$ и $(r_1)(r_2)(r_3)...\left(r_{\frac{p-1}{2}}\right)$,

получимъ: $$q^{\frac{p-1}{2}}\equiv(-1)^i(\textit{мод}\ p).$$

Вслѣдствіе этого мы можемъ написать:

$$\left(\frac{q}{p}\right)=(-1)^i.$$

§ **54. Законъ взаимности двухъ простыхъ чиселъ.** На основаніи этой леммы Гаусса доказывается, какъ мы уже сказали, одна изъ самыхъ важныхъ теоремъ высшей ариѳметики—законъ взаимности двухъ простыхъ чиселъ: q и p—*числа взаимно простыя, нечетныя*; *если по крайней мѣрѣ одно изъ нихъ имѣетъ видъ* $4n+1$, *то* $\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)$; *если же оба они вида* $4n+3$, *то*

$$\left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right).$$

По § 47, символъ $\left(\frac{q}{p}\right)=(-1)^i$, если i обозначаетъ число отрицательныхъ вычетовъ въ ряду абсолютно малыхъ вычетовъ по модулю p чиселъ:

$$1.q,\ 2.q,\ 3.q, \ldots \frac{p-1}{2}q; \tag{1}$$

символъ $\left(\frac{p}{q}\right)=(-1)^j$, если j есть число наименьшихъ отрицательныхъ по модулю q произведеній:

$$1.p,\ 2.p,\ 3.p, \ldots \frac{q-1}{2}.p. \tag{2}$$

Перемноживъ эти символы, найдемъ:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{i+j}. \tag{3}$$

Опредѣлимъ теперь $(i+j)$, т. е. общее число отрицательныхъ вычетовъ между абсолютно малыми вычетами по модулю p чиселъ ряда (1) и по модулю q чиселъ ряда (2).

Предположимъ, что $q>p$. Тогда между вычетами не можетъ находиться такихъ, численная величиина которыхъ было бы болѣе $\frac{q}{2}$, но будутъ, во-первыхъ, вычеты съ численной величиной $<\frac{p}{2}$, и, во вторыхъ, такіе, численная величина которыхъ заключается между $\frac{p}{2}$ и $\frac{q}{2}$. Общее число отрицательныхъ вычетовъ $(i+j)$ равно суммѣ числа отрицательныхъ вычетовъ перваго рода и числа отрицательныхъ вычетовъ второго рода. Мы опредѣлимъ каждое изъ нихъ порознь.

1°. Вычеты, абсолютно численная величина которыхъ $<\frac{p}{2}$, могутъ находиться между вычетами чиселъ (1) ряда и вычетами чиселъ (2) ряда. Докажемъ, что если какой-нибудь вычетъ $(+r)$ находится между вычетами чиселъ ряда (1), то между вычетами чиселъ ряда (2) будетъ находиться отрицательный вычетъ съ тою же численною величиной $(-r)$. Пусть, напримѣръ, hq при дѣленіи на p даетъ остатокъ $+r$, такъ что $hq \equiv r$ (*мод* p), или

$$hq-kp=r \tag{4}$$

(k есть нѣкоторое цѣлое число въ ряду: 1,2,3,... $\frac{q-1}{2}$, такъ какъ $h<\frac{p}{2}$, а разность $hq-kp>0$). Изъ уравненія (4) получимъ

$$kp-hq=-r \tag{5}$$

—уравненіе, которое показываетъ, что число kp въ рядѣ (2) даетъ при дѣленіи на q абсолютно-малый вычетъ $-r$. Обратно, если kp ряда (2) даетъ положительный абсолютно-малый вычетъ $+r'$, то въ рядѣ (1) одно изъ чиселъ дастъ отрицательный абсолютно малый вычетъ $-r'$. Отсюда можно заключить, что число отрицательныхъ вычетовъ ряда (2) равняется числу положительныхъ вычетовъ ряда (1), а потому общее число отрицательныхъ вычетовъ въ (1) и (2) рядахъ, равно числу всѣхъ вычетовъ ряда (1), т. е. $\frac{p-1}{2}$.

2°. Теперь опредѣлимъ число тѣхъ отрицательныхъ вычетовъ, численная величина которыхъ заключается между $\frac{p}{2}$ и $\frac{q}{2}$. Эти вычеты могутъ находиться только между вычетами чиселъ ряда (2), Относительно отрицательныхъ вычетовъ этого рода можно доказать, что, вообще говоря, они представляются попарно, т. е, изъ существованія одного такого заключаемъ о существованіи другого, ему сопряженнаго. Въ самомъ дѣлѣ, пусть одно изъ чиселъ ряда (2), напр. $k.p$ при дѣленіи на q даетъ остатокъ $-r$, такъ что $\frac{p}{2}<r<\frac{q}{2}$; иначе говоря, $kp \equiv -r$ (*мод.* q).

или

$$kp-hq=-r. \tag{6}$$

(k меньше $\frac{q-1}{2}$, а h—нѣкоторое цѣлое число). Изъ равенства (6) можно вывести новое, которое покажетъ, что есть другое число въ ряду (2), вообще говоря, отличное отъ kp, имѣющее абсолютно малый вычетъ отрицательный и притомъ второго рода. Для этого положимъ, что

$$k'=\frac{q-1}{2}-k,\quad h'=\frac{p+1}{2}-h,$$

и введемъ k', h' вмѣсто k, h въ равенствѣ (6). Тогда получимъ

$$\frac{q-1}{2}.p-k'p-\frac{p+1}{2}.q+h'q=-r,$$

$$k'p-h'q=-\left(\frac{q+p}{2}-r\right)=-r'$$

(въ томъ, что $r'=\frac{p+q}{2}-r$ есть положительная величина $<\frac{q}{2}$ и $>\frac{p}{2}$, не трудно убѣдиться, принявъ во вниманіе что $\frac{q}{2}>r>\frac{p}{2}$. Такъ какъ $k<\frac{q-1}{2}$, то $k'p$ есть одно изъ чиселъ ряда (2). Такимъ образомъ дѣйствительно, предполагая существованіе $-r$, мы находимъ непремѣнно сопряженный ему—r'. Исключеніе представляется, повидимому, въ случаѣ, если $k=\frac{q-1}{2}$, такъ какъ тогда $k'=0$ и сопряженнаго вычета не существуетъ, но можно убѣдиться, что остатокъ отъ дѣленія $kp=\frac{q-1}{2}.\,p$ на q есть положительная величина. Дѣйствительно, абсолютно малый вычетъ, меньшій $\frac{q}{2}$, получится, если изъ $\frac{q-1}{2}.p$ вычтемъ $\frac{p-1}{2}.q$, и будетъ равенъ $\frac{q-p}{2}$ — величинѣ положительной. Такимъ образомъ, этотъ случай не представляетъ исключенія изъ доказаной теоремы, что „отрицательные вычеты второго рода попадаются попарно“, а потому число ихъ четно.

Единственное исключеніе можетъ быть только въ томъ случаѣ, когда $k'=k$, ибо тогда и $r'=r$, т. е. оба парные вычеты совпадаютъ. Тогда число вычетовъ нечетное. Такъ какъ $k'=k$, то $k=\frac{q-1}{4}$; такъ какъ $r'=r$; то $r=\frac{q+p}{4}$; но k и r должны быть числами цѣлыми; значитъ, послѣднія равенства могутъ быть соблюдены только тогда, когда q—число вида $4n+1$, а слѣдовательно p—вида $4n+3$.

Итакъ, вообще говоря, число отрицательныхъ вычетовъ второго рода четное, за исключеніемъ того, когда q имѣетъ видъ $4n+1$, а p видъ $4n+3$; тогда число отрицательныхъ вычетовъ нечетное.

На основаніи этихъ выводовъ можно легко опредѣлить $(i+j)$. Очевидно, тутъ могутъ быть три случая. Во-первыхъ, если $p=4n+1$, то число отрицательныхъ вычетовъ 1-го рода $=\frac{p-1}{2}=2n$ — четное, и 2-го рода тоже четное; слѣдовательно, сумма $(i+j)$— число четное. Во-вторыхъ, $p=4n+3$, а $q=4n+1$; тогда число отрицательныхъ вычетовъ 2-го рода тоже равно (по исключенію) нечетному числу; а потому $(i+j)$ равняется четному числу. Наконецъ, въ третьихъ, оба числа p и q имѣютъ видъ $4n+3$; въ этомъ случаѣ число отрицательныхъ вычетовъ 1-го рода—нечетное, а 2-го рода—четное; значитъ $(i+j)$ равняется нечетному числу. Обращаясь къ формулѣ (3), мы можемъ заключить, что въ первомъ и второмъ случаяхъ

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right)=+1, \text{ т. е. } \left(\frac{q}{p}\right)=\left(\frac{p}{q}\right) \qquad (7)$$

такъ какъ каждый изъ этихъ символовъ равенъ единицѣ съ однимъ и тѣмъ же знакомъ; а въ послѣднемъ случаѣ

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=-1, \text{ или: } \left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right), \qquad (8)$$

такъ какъ каждый символъ равенъ единицѣ, но съ различными знаками.

Такимъ образомъ, законъ взаимности двухъ простыхъ чиселъ можно считать доказаннымъ *): если q и p простыя нечетныя числа, то $\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)$, когда по крайней мѣрѣ одно изъ этихъ чиселъ имѣетъ видъ $4n+1$; и $\left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right)$, когда оба числа вида $4n+3$.

---

*) Законъ этотъ былъ открытъ индуктивно, на основаніи частныхъ примѣровъ, Эйлеромъ, какъ показалъ Чебышевъ,

§ 55. Опредѣленіе символовъ. $\left(\frac{\pm 1}{p}\right)$ и $\left(\frac{2}{p}\right)$. Благодаря этому закону, задача о нахожденіи значенія какого-угодно символа сводятся къ опредѣленію простѣйшихъ символовъ: $\left(\frac{\pm 1}{p}\right)$ и $\left(\frac{2}{p}\right)$. Обратимся хотя бы къ примѣру, взятому нами ранѣе (стр. 115). Мы нашли, что $\left(\frac{1729}{101}\right)=\left(\frac{3}{101}\right)$; по закону взаимности, мы можемъ написать: $\left(\frac{3}{101}\right)=\left(\frac{101}{3}\right)=\left(\frac{-1}{3}\right)$. Возьмемъ еще примѣры. Символъ

$$\left(\frac{17}{103}\right)=\left(\frac{1}{17}\right); \quad \left(\frac{17}{1847}\right)=\left(\frac{1847}{17}\right)=\left(\frac{11}{17}\right)=\left(\frac{6}{11}\right)=$$

$$=\left(\frac{2}{11}\right)\left(\frac{3}{11}\right)=\left(\frac{2}{11}\right)\left(\frac{-1}{3}\right).$$

Найдемъ теперь, чему равны символы: $\left(\frac{\pm 1}{p}\right)$ и $\left(\frac{2}{p}\right)$.

Нетрудно видѣть, что величина символа $\left(\frac{1}{p}\right)$ есть $+1$. Въ самомъ дѣлѣ, мы знаемъ, что

$$q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \ (\text{мод } p).$$

Подставивъ вмѣсто q единицу, получимъ: $1 \equiv \left(\frac{1}{p}\right)$ (*мод* p)

Очевидно, что $\left(\frac{1}{p}\right)=+1$, такъ какъ въ противномъ случаѣ, т. е. при $\left(\frac{1}{p}\right)=-1$, мы имѣли бы, что $2 \equiv 0$ (*мод* p), гдѣ p, по условію, число отличное отъ двухъ. Слѣдовательно

$$\left(\frac{1}{p}\right)=+1.$$

Точно такими же разсужденіями найдемъ, что: $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$.

Перейдемъ теперь къ опредѣленію символа $\left(\frac{2}{p}\right)$. По леммѣ Гаусса

$$2^{\frac{p-1}{2}}\equiv(-1)^{i}\ (\text{мод } p).$$

i представляетъ здѣсь число отрицательныхъ вычетовъ между абсолютно малымп вычетами произведенiй:

$$1.2,\quad 2.2,\quad 3.2,\ldots\ldots\frac{p-1}{2}.2. \qquad (1)$$

Всѣ числа этого ряда меньше p; тѣ изъ нихъ; которыя $<\frac{p}{2}$, будутъ сами абсолютно малые вычеты, т. е для нихъ абсолютные вычеты положительные; но для чиселъ $>\frac{p}{2}$ абсолютные вычеты отрицательны. Значитъ, вопросъ объ опредѣленiи i есть вопросъ о нахожденiи числа чиселъ, большихъ $\frac{p}{2}$ въ (1) ряду. А это число, очевидно, равно разности *между* $\frac{p-1}{2}$ и числомъ чиселъ, меньшихъ $\frac{p}{2}$, т. е. чиселъ: $1.2,\ 2.2,\ 3.2,\ldots\ldots x.2$,

при чемъ $x.2<\frac{p}{2}$ или $x<\frac{p}{4}$.

Слѣдовательно, послѣднее изъ этихъ чиселъ ($x.2$) получится, если мы придадимъ x'у значенiе, равное наибольшему цѣлому числу, заключающемуся въ дроби $\frac{p}{4}$ т. е. $E\left(\frac{p}{4}\right)$ *)

Итакъ, $$i=\frac{p-1}{2}-E\left(\frac{p}{4}\right).$$

Разсмотримъ теперь тѣ предположенiя, которыя можно сдѣлать относительно числа p. Какъ число нечетное, p можетъ быть представлено подъ однимъ изъ слѣдующихъ видовъ: $8n+1$, $8n+3$, $8n+5$ и $8n+7$. Подставляя эти значенiя въ выраженiе i, будемъ имѣть, что:

при $p=8n+1$, $i=4n-E\left(\frac{8n+1}{4}\right)=2n$,

„ $x=8n+3$, $i=4n+1-E\left(\frac{8n+3}{4}\right)=2n+1$.

---

*) Знакомъ Е (entier) принято обозначать цѣлое количество, содержащееся въ данной величинѣ.

при $\quad p=8n+5, \quad i+4n+2-E\left(\frac{8n+5}{4}\right)=2n+1,$

» $\quad p=8n+7, \quad i=5n+3-E\left(\frac{8n+7}{4}\right)=2n+2.$

Въ первомъ и послѣднемъ случаяхъ i является числомъ четнымъ, почему

$$2^{\frac{p-1}{2}} \equiv +1 \ (\text{мод } p).$$

и символъ $\left(\frac{2}{p}\right)$ будетъ равенъ $+1$. Во второмъ же и третьемъ случаяхъ i—число нечетное, и

$$2^{\frac{p-1}{2}} \equiv +1 \ (\text{мод } p), \text{ т. е.} \left(\frac{2}{p}\right)=-1$$

Зная все это, мы всегда можемъ опредѣлить значеніе любого символа. Такъ, во взятыхъ нами выше примѣрахъ,

$$\left(\frac{1729}{101}\right)=\left(\frac{-1}{3}\right).$$

Но $\left(\frac{-1}{3}\right)=-1$, такъ какъ $\frac{p-1}{2}=1$; значитъ

$$\left(\frac{1729}{101}\right)=-1$$

Другими словами, сравненіе: $z^2 \equiv 1729$ (*мод* 101), не имѣетъ рѣшенія, и 1729 есть квадратичный невычетъ числа z по модулю 101.

Наоборотъ, символъ $\left(\frac{17}{103}\right)=\left(\frac{1}{17}\right)=+1$:

значитъ 17 есть квадратичный вычетъ числа z по модулю 103. Точно также 17 есть квадратичный вычетъ z по модулю 1847, такъ какъ

$$\left(\frac{17}{1847}\right)=\left(\frac{3}{11}\right)\left(\frac{-1}{3}\right)$$

Но $\left(\frac{-1}{3}\right)$, какъ мы видѣли выше, равняется -1, и $\left(\frac{3}{11}\right)$

тоже равенъ—1; ибо 11 имѣетъ видъ $8n+3$, т. е.

$$\left(\frac{17}{1847}\right)=+1.$$

Въ тѣснѣйшей связи съ теоріей квадратичныхъ вычетовъ, находится слѣдующій отдѣлъ теоріи чиселъ—теорія бинарныхъ квадратичныхъ формъ. Бинарною квадратичною формою называется однородная функція отъ независимыхъ перемѣнныхъ 2-й степени $ax^2+2bxy+cy^2$; a, b, c—цѣлыя числа. Конечный вопросъ, который рѣшается въ теоріи бинарныхъ формъ, есть вопросъ о характерѣ, который должно имѣть число M для того, чтобы оно могло быть представлено формою $ax^2+bxy+cy^2$ (при x, y—цѣлыхъ), другими словами для того, чтобы неопредѣленное уравненіе $M=ax^2+2bxy+cy^2$ могло быть рѣшимо въ цѣлыхъ числахъ. Въ теоріи бинарныхъ формъ доказывается, что необходимое условіе для этого есть возможность сравненія:

$Z^2 \equiv D$ (*мод* M); D обозначаетъ *опредѣлитель* бинарной формы b^2—ac. Такъ, если M есть абсолютно простое число p и $D=-1$, то мы должны имѣть $\left(\frac{-1}{p}\right)=+1$.

Отсюда—только абсолютно-простыя числа вида $4k+1$ *могутъ* быть представлены подъ видомъ x^2+y^2. Также видно изъ § 55, что только простыя числа вида $8k+1$ и $8k+7$ могутъ быть представляемы подъ видомъ x^2+2y^2.

Въ теоріи бинарныхъ квадратичныхъ формъ основное значеніе имѣетъ понятіе объ эквивалентности формъ и о классѣ формъ.

Двѣ формы $$ax^2+2bxy+cy^2 \qquad (1)$$

$$a'x'^2+2b'x'y'+c'y'^2$$

называются *эквивалентными*, если,

полагая $\left.\begin{array}{l} x=\alpha x'+\beta y' \\ y=\gamma x'+\delta y' \end{array}\right\}$ гдѣ $\alpha,\beta,\gamma,\delta$, суть цѣлыя числа,

форма (1) переходитъ въ форму (2) и обратно, полагая

$\left.\begin{array}{l} x'=\lambda x+\mu y \\ y'=\nu x+\pi y \end{array}\right\}$ гдѣ λ,μ,ν,π суть цѣлыя числа, форма (2) переходитъ въ форму (1).

Для того, чтобы условія могли быть выполнены, необходимо, чтобы $\alpha\delta-\beta\gamma=\lambda\pi-\mu\nu=\pm1.$

Между опредѣлителями формъ (1) и (2) существуетъ тогда отношеніе

$$b^2-ac=b'^2-a'c'.$$

Всѣ формы, эквивалентныя между собою *собственно* ($\alpha\delta-\beta\gamma=+1$). составаяютъ одинъ *классъ*.

Всѣ формы, принадлежащія къ одному и тому же классу, тожественны по отношенію къ вопросу о представляемости чиселъ.

Такъ, напримѣръ, формы $65x^2+16xy+y^2$ и x^2+y^2 эквивалентны и потому простыя числа вида $4m+1$ могутъ быть представлены подъ видомъ

$$65x^2+16xy+y^2.$$

ПРИЛОЖЕНІЕ.

Историческій очеркъ теоріи чиселъ.

§ 56. Теорія чиселъ до Фермата. Китайцы, персы имѣли особенные гіероглифы для изображенія чиселъ; финикіянамъ, кажется, принадлежитъ особенный способъ изображать числа буквами, который отъ нихъ перешелъ къ грекамъ, а отъ грековъ уже къ болгарамъ. Несмотря на то, что при этомъ способѣ изображенія правила для производства операцій очень неудобны, у этихъ народовъ были уже задатки теоріи чиселъ. Такъ, китайцамъ приписываютъ теорему:

$$1^3+2^3+3^3+\ldots.+n^3=(1+2+3+\ldots.+n)^2.$$

Но въ особенности въ древности свойства чиселъ интересовали философовъ Италійской школы, основателемъ которой былъ знаменитый Пиѳагоръ (род. 570 г. до Р. Х.). Ихъ занятія этимъ предметомъ были въ связи съ ихъ ученіемъ о природѣ вещей. Они учили, что „числа суть причины существованія вещей; вещи только копіи съ чиселъ“. Въ умѣ Пиѳагора эти формы означали, можетъ быть, только увѣренность, что всѣ явленія подчинены строгимъ законамъ, выражающимся числами. Но въ его школѣ мало по малу эта здравая мысль замѣнилась мистическимъ ученіемъ, по которому всякому свойству цѣлаго числа подыскивалось какое-нибудь толкованіе.

Гораздо важнѣе по результатамъ стремленіе Пиѳагора отыскать цѣлыя числа, которыя могли бы быть катетами и гипотенузою прямоугольнаго треугольника, т. е. удовлетворяли бы условію:

$$x^2+y^2=z^2.$$

Онъ далъ рѣшеніе въ видѣ

$$a^2+\left(\frac{a^2-1}{2}\right)^2=\left(\frac{a^2+1}{2}\right)^2$$

гдѣ a можетъ быть какое угодно число цѣлое, нечетное.

Послѣ того знаменитый Платонъ далъ другое рѣшеніе въ видѣ:

$$b^2+\left(\frac{b^2}{4}-1\right)^2=\left(\frac{b^2}{4}+1\right)^2.$$

Платонъ оставилъ послѣ себя школу математиковъ, которые продолжали заниматься геометріей и, вѣроятно, свойствами чиселъ. Но отрывочность свѣдѣній, дошедшихъ до насъ, не позволяетъ судить о томъ, что было сдѣлано каждымъ изъ нихъ. О совокупности же достигнутыхъ результатовъ мы можемъ составить себѣ ясное понятіе, изучая сочиненіе Эвклида „Элементы". Эвклидъ (300 г. до Р. Х.) въ 7, 8 и 9 книгахъ этого сочиненія собралъ все, что было сдѣлано до него по теоріи чиселъ—изслѣдованія о дѣлимости чиселъ, общихъ дѣлителяхъ и кратныхъ. Въ 10-й книгѣ изложено принадлежащее ему ученіе о несоизмѣримыхъ величинахъ. Эвклидъ былъ одинъ изъ первыхъ ученыхъ Александрійской школы, которая обезсмертила себя многими великими открытіями.

Къ той же школѣ принадлежитъ Эратосѳенъ (род. 276 г. до Р. Х.), которому ариѳметика обязана извѣстною методою находить простыя числа, „рѣшетомъ Эратосѳена" *).

Тѣмъ не менѣе нужно замѣтить, что знаменитая Александрійская школа, къ которой принадлежали такіе астрономы, какъ Аристархъ, Гиппархъ и Птоломей, такіе геометры, какъ Аполлоній Пергійскій, не сдѣлала соотвѣтствующихъ успѣховъ въ алгебрѣ и теоріи чиселъ: единственное сочиненіе по этимъ наукамъ явилось только во время упадка Александрійской щколы. Но и геній величайшаго ариѳметика Греціи не могъ пробудить въ умахъ любви къ падающей наукѣ, противъ которой шли религіозный фанатизмъ и политическія событія; мы подразумѣваемъ Діофанта Александрійскаго, автора „Задачъ ариѳметическихъ" (13 книгъ, изъ которыхъ до насъ дошло только 6).

Но прежде, чѣмъ говорить о немъ, упомянемъ объ одномъ его предшественникѣ. Nicomachos (изъ Аравіи) былъ ревностный послѣдователь Пиѳагорейской школы и поэтому онъ съ любовью

---

*) См. Теорія чиселъ § 6.

занимался теоріей чиселъ. Одно изъ его сочиненій, совершенно свободное отъ той мистики, которая отличала Пиѳагорейскую школу, представляютъ ясный и подробный сводъ современныхъ ему ариѳметическихъ знаній грековъ. Онъ приводитъ много теоремъ относительно простыхъ и многоугольныхъ чиселъ; у него же въ первый разъ находится теорема, что сумма нечетныхъ чиселъ, начиная съ 1, всегда равняется квадрату. Зато заглавіе другого его сочиненія: „Ариѳметическія изслѣдованія о Богѣ и Божественныхъ вещахъ“ достаточно краснорѣчиво, чтобы дать понятіе объ его содержаніи. Nicomachos интересенъ въ томъ отношеніи, что онъ служитъ связью между Пиѳагорейпами и Діофантомъ, который жилъ въ половинѣ IV-го столѣтія. Въ своемъ сочиненіи онъ занимается рѣшеніемъ многихъ неопредѣленныхъ уравненій въ цѣлыхъ числахъ; поэтому неопредѣленный анализъ часто даже называется по его имени „Анализомъ Діофанта“.

Сочиненіе Діофанта по своей важности имѣло много комментаріевъ. Знаменитѣйшій комментарій въ древности, къ несчастью потерянный, принадлежитъ Гипатіи, дочери Ѳеона Александрійскаго, знаменитой своею смертью отъ рукъ разъяренной христіанской черни, фанатизированной противъ философіи и ея представителей.

Послѣ закрытія христіанскими императорами преподаванія въ Александрійскомъ музеумѣ, и истребленія Александрійской библіотеки наступило то время обскурантизма и фанатическихъ споровъ, которое называется средними вѣками. Наука сохранилась только у Арабовъ. Въ Европѣ же ея мѣсто замѣнили са́мые нелѣпые споры; здравыя научныя понятія, выработанныя греками, замѣнились предразсудками. Въ это время „мистеріи чиселъ“ занимали умы нѣсколько больше. чѣмъ другія математическія науки; появлялось нѣсколько комментаріевъ на „Ариѳметическія изслѣдованія о Богѣ“ Никомаха; магическіе квадраты считались талисманами. Очевидно, все это не могло содѣйствовать развитію методовъ и науки.

Только въ періодѣ возрожденія наукъ сдѣлала успѣхи и теорія чиселъ. Bachet de Meziriac (1587—1638) самостоятельно нашелъ извѣстный способъ рѣшать неопредѣленныя уравненія 1-й степени съ двумя неизвѣстными и опубликовалъ его въ сочиненіи: „Problèmes plaisants et délectables“*).

§ 57. **Ферматъ (1601—1655).** Отцомъ теоріи чиселъ по справедливости считается Ферматъ. Ему принадлежитъ громадное

---

*) Недавнія изслѣдованія показали однако, что подобное рѣшеніе было извѣстно еще Индійскимъ математикамъ (VI ст. по Р. X], Brahmagupta и Bhascara Acharya. (XII ст.)

множество чрезвычайно важныхъ теоремъ, которыя онъ оставилъ большею счастью безъ доказательствъ на поляхъ принадлежавшаго ему экземпляра сочиненій Діофанта.

Такова теорема его („малая теорема Фермата“), доказанная въ §§ 34—36, стр. 92: $x^p - x \equiv 0$ (*мод p*), если p есть абсолютно простое число, а x—какое угодно число. Такова знаменитая теорема его, относящаяся къ такъ называемымъ *многоугольнымъ числамъ*. Если мы составимъ ариѳметическую прогрессію, начинающуюся съ 1 и имѣющую разностью $k-2$, т. е. рядъ чиселъ:

$$1,\ k-1,\ 2k-3,\ 3k-5,\ 4k-7,\ldots$$

и затѣмъ изъ этого ряда чиселъ (1) составимъ новый, члены котораго послѣдовательно равны: первому члену ряда (1), суммѣ первыхъ двухъ членовъ, суммѣ первыхъ трехъ членовъ и т. д., т. е. рядъ:

$$1,\ k,\ 3k-3,\ 6k-8,\ 10k-15,\ldots.. \qquad (2)$$

Рядъ (2), общій членъ котораго имѣетъ форму

$$n+\frac{n^2-n}{2}(k-2),$$

и есть рядъ многоугольныхъ (k—угольныхъ) чиселъ; названіе это объясняется тѣмъ, что взявъ шары равнаго діаметра, въ числѣ, равномъ одному изъ этихъ чиселъ, мы можемъ составить изъ этихъ шаровъ правильный k—угольникъ. Еще древніе интересовались этими числами; Діофантъ написалъ о нихъ изслѣдованіе. Ферматъ далъ замѣчательную теорему: „Каждое число можетъ быть представлено подъ видомъ суммы k k—угольныхъ чиселъ, т. е. трехъ треугольныхъ *), четырехъ квадратовъ, пяти пятиугольныхъ и т. д.“ (1 и 0 считаются многоугольными числами). Доказательство этой общей теоремы дано Коши. Особенно интересенъ частный случай: „Каждое число можетъ быть представлено подъ видомъ суммы четырехъ квадратовъ“. Теорема эта доказана Якоби съ помощью теоріи эллиптическихъ функцій.

Знаменитѣйшая изъ всѣхъ теоремъ („большая теорема Фермата“), теорема, по которой уравненіе $x^n+y^n=z^n$ не можетъ быть рѣшено въ цѣлыхъ числахъ при $n>2$, до сихъ поръ еще не доказана вполнѣ. Послѣ того, какъ Эйлеръ далъ доказательство для

---

*) См. брошюру Е. Григорьева: «Къ теоремѣ Ферма о разложеніи всякаго числа въ сумму трехъ 3-угольныхъ чиселъ». Казань. 1903.

$n=3$ и $n=4$, Lejeune Dirichlet доказалъ для $n=5$ и Ламе для $n=7$. Наконецъ Куммеръ для доказательство для безконечнаго множества цѣлыхъ чиселъ, но доказательство Куммера не примѣнимо ко всѣмъ числамъ. Наконецъ, Ферматъ обратилъ вниманіе на важность рѣшенія въ цѣлыхъ числахъ уравненія $t^2-Dn^2=1$, гдѣ D есть нѣкоторое цѣлое число; уравненіе это часто носитъ названіе „Пеллевскаго уравненія".

§ 58. **Эйлеръ**. Послѣ Фермата наибольшія услуги теоріи чиселъ оказали Эйлеръ (1707—1783), Лежандръ и Лагранжъ. Мемуары Эйлера по теоріи чиселъ изданы въ двухъ большихъ томахъ Петербургскою Академіей Наукъ подъ именемъ: „Commentationes Arithmeticae collectae".

Эти два большіе тома содержатъ 94 мемуара по теоріи чиселъ, которые издатели (въ изданіи принимали участіе В. Я. Буняковскій и П. Л. Чебышевъ) располагали въ хронологическомъ порядкѣ; но вмѣстѣ съ тѣмъ издатели присоединили систематическій указатель, содержаніе котораго мы считаемъ полезнымъ привести, какъ дающаго представленіе о совокупности работъ Эйлера по теоріи чиселъ.

Отдѣлъ I-й. (*Дѣлимость чиселъ*). *a*) О цѣлыхъ числахъ по отношенію къ ихъ разложенію на множители. Таблицы простыхъ чиселъ. О числѣ чиселъ взаимно простыхъ съ даннымъ и меньшихъ даннаго. О суммахъ дѣлителей чиселъ. Дружественныя числа.

b) Дѣлимость различныхъ формулъ.

c) Теорія остатковъ и квадратичныхъ вычетовъ.

Отдѣлъ II-й. *Разложеніе чиселъ на суммы различныхъ формъ.* *a*) Разложеніе чиселъ на квадраты, на треугольныя числа и члены пропорціональные квадратамъ. *b*) Разбіеніе чиселъ.

Отдѣлъ III. *Анализъ Діофанта.* *a*) Опредѣленіе двухъ или многихъ неизвѣстныхъ, опредѣленныхъ однимъ уравненіемъ. *b*) Опредѣленіе многихъ неизвѣстныхъ, опредѣленныхъ двумя, тремя, четырмя или болѣе уравненіями. *c*) Неопредѣленные вопросы, приводящіе къ уравненіямъ, число которыхъ превышаетъ число неизвѣстныхъ (задача о магическихъ квадратахъ).

Интересныя изслѣдованія Эйлера по вопросу о представленіи чиселъ подъ видомъ суммъ—разбіеніи чиселъ—заключаются въ сочиненіи Эйлера: Introductio in Analysin infinitorum). Второй томъ „Алгебры" Эйлера также сполна посвященъ неопредѣленно му анализу; замѣчательныя „приложенія“, сдѣланныя къ этому тому Лагранжемъ, дѣлаютъ это сочиненіе однимъ изъ наиболѣе цѣнныхъ для изученія теоріи чиселъ.

Эйлеру принадлежитъ созданіе теоріи „степенныхъ вычетовъ“, изслѣдованіе по теоріи квадратичныхъ вычетовъ (см. § 51, стр. 114) и изслѣдованіе относительно представленія чиселъ въ видѣ x^2+my^2. Эти изслѣдованія были развиты Лежандромъ и Лагранжемъ и приведены въ систематическую форму Гауссомъ.

Лежандръ (1755—1833) оставилъ послѣ себя большое систематическое сочиненіе подъ заглавіемъ Théorie de nombres.

Труды **Лагранжа (1736—1855)** важны для теоріи чиселъ въ особенности тѣмъ, что они выяснили значеніе ученія о непрерывныхъ дробяхъ.

§ 59. Гауссъ (1777 - 1855). Этотъ знаменитый „princeps mathematicorum“ 24-хъ лѣтнимъ юношею издалъ (въ 1801 г). свое сочиненіе: „Disquisitiones arithmeticae“, которое до сихъ поръ должно быть изучаено всякимъ, кто желаетъ поппакомится съ теоріею чиселъ. Въ этомъ сочиненіи положены основанія такъ называемой *ариѳметической теоріи формъ.*

Формами называются однородныя цѣлыя функціи (многочлены) отъ нѣсколькихъ независимыхъ перемѣнныхъ, т. е. функціи $F\ (x,y,z,..)$, имѣющія то свойство, что.

$$F\ (tx,\ ty,\ tz,\ \ldots)=t^s.\ F\ (x,\ y,\ z,\ \ldots),$$

гдѣ s есть цѣлое число=степень формы. Напримѣръ:

$$x\ (tx)^2+2b\ (tx)\ (ty)+c\ (ty)^2=t^2\ (ax^2+2b\ xy+cy^2).$$

Формы раздѣляются 1) по числу перемѣнныхъ—на бинарныя (двѣ перемѣнныхъ), тернарныя и т. п., и 2) по степени формы—на линейныя (1-й степени), квадратичныя, кубичныя и т. д.

Теорія формъ можетъ быть *алгебрической*, когда и коэффиціенты и перемѣнныя могутъ принимать **какія угодно** численныя значенія, и *ариѳметической*, въ которой коэффиціенты и перемѣнныя предполагаются **цѣлыми** числами и который рѣшается съ помощью теоріи чиселъ. Главнѣйшій вопросъ, который рѣшается съ помощью теоріи формъ, есть вопросъ объ опредѣленіи чиселъ, которыя могутъ быть представлены формою. Говорятъ, что число n можетъ быть представлено выраженіемъ $F\ (x,\ y,\ z,..)$, когда существуютъ **цѣлыя** значенія $x,y,z,..$ которыя дѣлаютъ $F(x,y,z,...)$ равною n; имѣемъ, напр., слѣдующую теорему: *линейная форма* $mx+ny$

можетъ представить всякое число, дѣлящееся на общій наибольшій дѣлитель m и n, и она не можетъ представить никакихъ другихъ чиселъ. Въ частности, если *m* и *n* суть числа взаимно простыя, то линейная форма $mx+ny$ можетъ представить новое число.

Сочиненіе „Disquisitiones Arithmeticae“ раздѣляется на 7 отдѣловъ, изъ которыхъ первые четыре посвящены болѣе элементарнымъ вопросамъ (свойства сравненій, теорія степенныхъ вычетовъ, сравненія 2-й степени).

Въ 5-мъ отдѣлѣ изучается, только что упомянутая, теорія квадратичныхъ бинарныхъ и тернарныхъ формъ, но въ особенности замѣчателенъ послѣдній, седьмой отдѣлъ сочиненія, содержащій приложеніе теоріи чиселъ (именно теоріи первообразныхъ корней) къ рѣшенію знаменитой еще съ древности задачи о дѣленіи круга на *m* равныхъ частей, или о построеніи съ помощью циркуля и линейки правильнаго многоугольника о *m* сторонахъ. Греческимъ математикамъ были извѣстны построенія правильнаго треугольника и правильнаго пятиугольника; такъ какъ кромѣ того имъ извѣстно было дѣленіе всякаго угла на два, то съ помощью циркуля и линейки можно было на основаніи этихъ результатовъ раздѣлить кругъ на 2γ, $2\gamma.\ 3$, $2\gamma.\ 5$, $2\gamma.\ 3.5$ равныхъ частей ($\gamma=0,1,2,\ldots$). Гауссъ съ помощью теоріи чиселъ показалъ, что кругъ съ помощью циркуля и линейки можетъ быть раздѣленъ на *p* равныхъ частей если *p* есть абсолютно-простое число вида $2^{2^\mu}+1$, и вмѣстѣ съ тѣмъ показалъ, что дѣленіе съ помощью круга и линейки не выполнимо для всѣхъ другихъ простыхъ чиселт и степеней простыхъ чиселъ. Если положимъ $\mu=0$, то $p=3$; для $\mu=1$ получимъ $p=5$, т. е. имѣемъ случаи, извѣстные еще въ древности. Далѣе, при $\mu=2$ имѣемъ $p=2^{2^2}+1=17$—случай. для котораго Гауссъ выполнилъ дѣленіе. Для $\mu=3$ имѣемъ $p=2^{2^3}+1=257$—также простое число, слѣдовательно 257-угольникъ построить можно. Тоже самое имѣетъ мѣсто для 65537—угольника, такъ какъ $p=2^{2^4}+1=65537$—число простое. $\mu=5$, 6, 7, 13 и 23 не даютъ простыхъ чиселъ; случаи μ, равнаго остальнымъ числамъ до 23—и подавно, а болѣе 23 еще никѣмъ не изслѣдованы, и мы незнаемъ, будетъ ли *p* въ этихъ случаяхъ простымъ числомъ или нѣтъ. Уже доказательства, что получаемыя $\mu=5$, 6, 7, 13 и 23 громадныя числа не суть простыя, потребовали затраты большихъ усилій и навыка. Весьма возможно, что $\mu=4$ есть послѣднее число, которое даетъ рѣшеніе. Относительно 257-угольника Richelot напечаталъ обширную работу въ журналѣ Crelle'я *). На 65537-угольникъ потратилъ десять лѣтъ своей жизни профессоръ Hermes въ Lingen'ѣ, чтобы изслѣдовать точно всѣ корни, являющіеся въ методѣ Гаусса **).

Въ своихъ дальнѣйшихъ работахъ Гауссъ нашелъ нужнымъ разсматривать въ „Теоріи чиселъ", кромѣ ряда цѣлыхъ положительныхъ чиселъ, цѣлыя комплексныя числа вида $a+b\,i$, гдѣ $i=\sqrt{-1}$, a и b—цѣлыя вещественныя числа. Введеніе этихъ чиселъ привело не къ усложненію, а напротивъ, къ упрощенію напр. теоріи биквадратичныхъ вычетовъ.

§ **60**. Поэтому, послѣ Гаусса,—Якоби, Леженъ Диришле, Куммеръ начали изучать комплексныя числа болѣе общія, а именно вида

$$a_0+a_1\ \varepsilon_1+a_2\ \varepsilon_2+\ldots.+a_{n-1}\ \varepsilon_{n-1},$$

гдѣ ε, $\varepsilon_2,\ldots.\varepsilon_{n-1}$ —суть мнимые корни *изъ единицы*, т. е. корни уравненія $\dfrac{x^p-1}{x-1}=0$; коэффиціенты же a_0, a,.....a_{n-1} суть цѣлыя вещественныя числа.

Наконецъ, Кронекеръ и Дедекиндъ создали общую теорію цѣлыхъ алгебрическихъ чиселъ, свойства которыхъ суть обобщеніе свойствъ цѣлыхъ вещественныхъ чиселъ.

Изслѣдованія Гаусса относительно формъ также получили значительное обобщеніе. Эрмитъ и другіе разсматривали общую теорію квадратичныхъ формъ съ n перемѣнными. Многіе замѣчательные результаты были получены въ теоріи чиселъ отъ сближенія ея съ такъ называемой теоріей эллиптическихъ функцій, и въ этомъ отношеніи начало положилъ Якоби. Приведу одинъ примѣръ. Въ теоріи эллиптическихъ функцій изучается зависимость K отъ нѣкоторой величины q и получаются двѣ строки:

$$\sqrt[4]{\frac{2K}{\pi}}=1+2q+2q^4+2q^9+2q^{16}+2q^{(n-1)^2}+2q^{n^2}+\ldots$$

$$\frac{2K}{\pi}=1+A_1q+A_2q^2+A_3q^3+A_4q^4+\ldots$$

---

*) «De resolutione atgebraica aequationis $x^{257}=1$, sive de divizione circuli per bisectionem anguli septies repetitam in partes 257 inter se aequales commentatio coronata». Crlle's journ. IX, 1898.

**) Желающихъ познакомиться съ методомъ Гаусса и построеніемъ стороны правильнаго 17-угольника мы отсылаемъ къ изданію Физико-математическаго общества: «*Ф. Клейнъ.* Лекціи по избраннымъ вопросамъ элементарной геометріи. Перев. Н. Н. Парфентьева подъ редакцію *Д. М. Синцова*. Казань. 1898».

(т. е. первая строка содержитъ въ себѣ степени, показатель которыхъ суть самый квадратъ, между тѣмъ какъ вторая строка содержитъ всѣ степени безъ исключенія).

Сопоставленіе этихъ двухъ формулъ даетъ доказательство теоремы, что число можетъ быть представлено подъ видомъ суммы четырехъ квадратовъ.

Ліувиль далъ безъ доказательства весма большое число формулъ теоріи чиселъ, основанныхъ на такомъ же приложеніи теоріи эллиптическихъ функцій. Доказательства этихъ теоремъ были даны профессоромъ Казанскаго университета П. С. Назимовымъ.

Кромѣ вышеупомянутыхъ въ историческомъ очеркѣ, важные вклады въ теорію чиселъ сдѣлали Эйзенштейнъ, Риманъ, Эд. Лукасъ и др.

Въ Россіи въ области теоріи чиселъ работали Чебышевъ, Буняковскій, Бугаевъ, Золотаревъ. Ю. В. Сохоцкій и др.

Лучшими учебниками по теоріи чиселъ являются въ настоящее время, кромѣ вышеупомянутыхъ классическихъ сочиненій Гаусса и Лежандра, слѣдующее:

Lejeune-Dirichlet. Vorlesungen über die Zahlentheorie.
Bachmann. Zahlentheorie.
Kronecker. Vorlesungen über Zahlentheorie.
Lucas. Théorie des nombres.
Cahen. Théorie des nombres.

На **русскомъ языкѣ** мы имѣемъ замѣчательную по ясности изложенія „Теорію Сравненій“ Чебышева и второй томъ сочиненія Ю. В. Сохоцкаго Высшая Алгебра. Для подробнаго знакомства съ теоріей чиселъ необходимо рекомендовать также: Report on the theory of numbers—Стефана Смита, помѣщавшееся въ Reports of the British Association за 1850 и слѣд. годы.

I. Prof. G. Papelier.

НАЧАЛА АНАЛИЗА.

Перев. съ франц. подъ редакціей орд. профессора
А. П. Котельникова,

СЪ ИСТОРИЧЕСКИМЪ ОЧЕРКОМЪ АНАЛИЗА Б.-М.

Заслуженнаго ординарнаго профессора
А. В. Васильева.

II. **А. В. Васильевъ**, засл. проф. Казанск. Университета.

ДИФФЕРЕНЦІАЛЬНАЯ ГЕОМЕТРІЯ.

По лекціямъ и подъ ред. профессора составилъ студентъ
Н. Н. Іовлевъ.

III. Приватъ-доцентъ Н. Н. Іовлевъ.. **Элементарная Геометрія**. Курсъ среднихъ учебныхъ заведеній. Часть I, геометрія соизмѣримыхъ протяженій. Ц. 80 к.

То-же. Часть 2. Цѣна 20 к.

Сборникъ научно-популярныхъ статей по основаніямъ Ариѳметики (философія числа) Гельмгольца, Кронекера, Дедекинда и др. Изданіе Студенческаго Математическаго кружка.

Складъ въ магазинѣ **М. А. Голубева** въ Казани, Воскресенская ул., д. Матвѣевскаго.