Министерство образования Республики Беларусь
Учреждение образования «Витебский государственный университет имени П.М. Машерова»
Кафедра алгебры и методики преподавания математики

**Н.Н. Воробьев, С.Н. Воробьев,
М.И. Наумик**

ТЕОРИЯ ЧИСЕЛ:
СРАВНЕНИЯ И ИХ ПРИЛОЖЕНИЯ

Сборник заданий

Витебск
ВГУ имени П.М. Машерова
2017

УДК 511(076.5)
ББК 22.13я73
В75

Печатается по решению научно-методического совета учреждения образования «Витебский государственный университет имени П.М. Машерова». Протокол № 2 от 28.12.2016 г.

Авторы: профессор кафедры алгебры и методики преподавания математики ВГУ имени П.М. Машерова, доктор физико-математических наук, доцент **Н.Н. Воробьев;** доценты кафедры алгебры и методики преподавания математики ВГУ имени П.М. Машерова, кандидаты физико-математических наук **С.Н. Воробьев, М.И. Наумик**

Научный редактор:
заведующий кафедрой алгебры
и методики преподавания математики ВГУ имени П.М. Машерова,
доктор физико-математических наук, профессор *Н.Т. Воробьев*

Рецензент:
профессор кафедры геометрии и математического анализа
ВГУ имени П.М. Машерова, доктор физико-математических наук,
профессор *Ю.В. Трубников*

Воробьев, Н.Н.

В75 Теория чисел: сравнения и их приложения : сборник заданий / Н.Н. Воробьев, С.Н. Воробьев, М.И. Наумик. – Витебск : ВГУ имени П.М. Машерова, 2017. – 67 с.

Предлагаемое издание адресовано студентам физико-математических специальностей. В начале каждого параграфа даются основные теоретические сведения (определения и формулировки некоторых теорем). Затем приведены подробно разобранные решения ряда задач. В заключение читателю предложены задачи для самостоятельного решения (их в издании свыше тысячи) и контрольные вопросы.

Адресовано студентам физико-математических специальностей и может успешно использоваться для проведения практических и самостоятельных (контрольных) работ по дисциплинам «Теория чисил», «Алгебра и теория чисел», «Геометрия и алгебра».

УДК 511(075.8)
ББК 22.13я73

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ

Предлагаемый сборник заданий, являясь по сути практикумом по решению задач, дополняет вышедшие ранее пособи [7,8] и содержит свыше тысячи задач. Настоящее издание посвящено элементарной теории чисел, а именно, изучению основ теории сравнений и ее некоторым первоначальным приложениям в криптографии. Весь материал разбит на двадцать семь параграфов. Каждый параграф, как правило, предваряют краткими теоретическими сведениями: излагаются и иллюстрируются на примерах соответствующие математические понятия, формируются ключевые свойства и теоремы. Затем приводятся подробные решения ряда стандартных задач. В параграфе 26 содержит контрольные вопросы. В параграфе 27 читателю предложены задачи для самостоятельного решения.

Настоящий сборник заданий составлен в соответствии с учебными программ дисциплин «Теория чисел», «Алгебра и теория чисел», «Геометрия и алгебра» и предназначен студентам физико-математических специальностей университетов. Вместе с тем отдельные его параграфы доступны также учащимся старших классов средней школы»[1].

[1] На обложке изображены две почтовые марки, изданные в ФРГ и ССР, посвященные К. Гауссу и П.Л. Чебышеву. Карл Фридрих Гаусс (Johann Carl Friedrich Gauβ) с 30.04.1777, Брауншвейг, Нижняя Саксония – 23.02.1855, Геттинген, Ганновер] – немецкий математик, механик, физик, астролог и геодезист. Считается одним из величайших математиков всех времен, «королем математиков». Создал основные методы и завершил построение теории сравнений.
Пафнутий Львович Чебышев [04.05.1821, село Окатово, Боровский уезд, Калужская губерния – 26.11.1894, Санкт-Петербург] – русский математик и механик, основоположник петербургской математической школы, академик Петербургской академии наук (1859) и еще двадцати четырех академий мира. П.Л. Чернышев – гениальный математик и «один из величайших математиков Европы» (Ш. Эрмит). Получил фундаментальные результаты в теории чисел (распределение простых чисел). В 1849 году вышла книга Чебышева «Теория сравнений», по которой автор в том же году стал профессором Петербургского университета. Этот труд стал первой изданной в росии монографией по теории чисел, неоднократно переиздавался и был переведен на немецкий и итальянский языки.

1 Определение и простейшие свойства сравнений

1.1 Определение. Пусть $a, b, m \in Z$ и $m \neq 0$. Целые числа a и b называются сравнимыми по модулю m, если разность $a - b$ делится на m, т.е. $(a - b)$ ε m.

Что a сравнимо с b по модулю m и записывают так: a В b ($mod\ m$).

1.2 Теорема.

1. a В b ($mod\ m$) *тогда и только тогда, когда a и b при делении на m дают одинаковые остатки.*

2. *Отношение сравнения является отношением эквивалентности.*

3. a В b ($mod\ m$) / c В d ($mod\ m$) Λ $a + c$ В $b = d$ ($mod\ m$).

4. a В b ($mod\ m$) / c В d ($mod\ m$) Λ ac В bd ($mod\ m$).

1.3 Следствие.

1. $a + b$ В c ($mod\ m$) Λ a В $c - b$ ($mod\ m$);

2. a В b ($mod\ m$) Λ a В $b + km$ ($mod\ m$), где $k \in Z$;

3. При любом натуральном n a В b ($mod\ m$) Λ a^n В b^n ($mod\ m$);

4. При любом натуральном k a В b ($mod\ m$) Λ ka В kb ($mod\ m$).

5. Если a_i В b_i ($mod\ m$) / c_i В d_i ($mod\ m$), то $\sum_{i=1}^{n} a_i c_i \equiv \sum_{i=1}^{n} b_i d_i \pmod{m}$.

1.4 Теорема.

1. ac В bc ($mod\ m$) / $(c, m) = 1$ Λ a В b ($mod\ m$);

2. *Пусть c натуральное число, тогда* a В b ($mod\ m$) ⇔ ac В bc ($mod\ m$).

3. *Пусть c натуральный делитель числа m, тогда* a В b ($mod\ m$) Λ a В b ($mod\ c$).

4. a В b ($mod\ m_1$) / a В b ($mod\ m_2$) Λ a В b ($mod\ [m_1; m_2]$).

5. Пусть a В b ($mod\ m$), тогда $a \times x$ / $m \times x$ _ $b \times x$ / $m \times x$ в частности $(a; m) = (b; m)$.

1.5 Пример. Доказать, что числа $6^{1001} + 1$ и $6^{1000} - 1$ делятся на 7.

Решение. Так как 6 В –1 (mod 7), то 6^{1000} В 1 (mod 7), т.е. $6^{1000} - 1$ делится на 7.

Из 6^{1000} В 1 (mod 7) и 6 В –1 (mod 7) следует 6^{1001} В –1 (mod 7), т.е. $6^{1001} + 1$ делится на 7.

1.6 Пример. Найти остаток от деления числа $29^{2929} + 6^{231}$ на 31.

Решение. Необходимо найти число r, удовлетворяющее условиям $29^{2929} + 6^{231}$ В r (mod 31), $0 \leq r < 31$.

Воспользуемся свойствами сравнений. Так как 29 В –2 (mod 31), то 29^{2929} В $(-2)^{2929}$ (mod 31). Поскольку $(-2)^5 = -32$ В –1(mod 31), то $(-2)^{2929} = ((-2)^5)^{585} \cdot (-2)^4$ В $(-1)^{585} \cdot (-2)^4$ (mod 31). Поэтому $(-2)^{2929}$ В –16 (mod 31) и 29^{2929} В –16 (mod 31). Так как $6^2 = 36$ В 5 (mod 31), то $6^{231} = (6^2)^{115} \cdot 6$ (mod 31). Поскольку $5^3 = 125$ В 1 (mod 31), $5^{115} \cdot 6 = (5^3)^{38} \cdot 5 \cdot 6$ В $1^{38} \cdot 30$ (mod 31).

Таким образом, 6^{231} В 30 (*mod* 31). Теперь, складывая сравнения 29^{2929} В – 16 (*mod* 31) и 6^{231} В 30 (*mod* 31), получим $29^{2929} + 6^{231}$ В –16 + 30 (*mod* 31), откуда $29^{2929} + 6^{231}$В 14 (*mod* 31), т.е. остаток от деления этого выражения на 31 равен 14.

Ответ: 14.

1.7 Пример. Найдите последние две цифры десятичной записи числа 5^n, $n \geq 2$.

Решение. Последние две цифры совпадают с остатком отделения этого числа на 100. Проверим, что при $n \geq 2$ последние две цифры десятичной записи числа 5^n будет 2 и 5. Воспользуемся индукцией по n. При $n = 2$ утверждение справедливо. Пусть $n \geq 3$. Предположим, что утверждение верно для $n - 1$ и докажем его для n. Так 5^{n-1} В 25 (mod 100), то $5^n = 5^{n-1} \cdot 5$ В $25 \cdot 5 = 125$ В 25 (mod 100) значит, утверждение справедливо для любого $n \geq 2$.

Ответ: 2 и 5.

1.8 Пример. Построить таблицу умножения по модулю 5.

Решение.

mod 5	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

1.9 Пример. Построить таблицу умножения по модулю 6.

Решение.

mod 6	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

1.10 Вопросы по таблицам:

1) Почему в первой таблице не было нулей, а во второй они есть?

2) Почему в каждой строчке первой таблицы никакое число не повторяется дважды?

3) Для каких модулей в пределах первого десятка таблицы умножения будут похожи на таблицу по модулю 5, а для каких – на таблицу по модулю 6?

4) Сколько в таблице по модулю 12 таких строчек, в которых нет нулей?

Ответы на вопросы:

1) Потому что 5 – простое число, а 6 – составное. Когда перемножаются два числа, одно из которых кратно 2, а другое кратно трем, то в результате (в таблице по модулю 6) получается 0.

2) Ровно по той же причине: если бы ab В ac при равных b и c, то в этой же строке должен был быть о: а$(b - c)$ В 0. Но по простому модулю это невозможно.

3) По-видимому, для простых модулей (то есть чисел 2, 3, 7) таблицы будут аналогичны таблице по модулю 5 (нет нулей, все числа в каждом столбце и каждой строке различные), а для составных – аналогичны таблицы по модулю 6.

4) Этот вопрос сформулируем по-другому: для каких множителей $m < 12$ не может выполняться равенство $m \cdot n$ В 0 ни при каких $n < 12$? Невозможность такого равенства равносильна условию НОД $(m, 12) = 1$. Иначе говоря, m + 1, 5, 7 или 11.

Ответ: 4 строки.

2 Признаки делимости

Теорема 2.1 Признак делимости Паскаля (общий признак равнозначности). *Пусть для степени основания системы счисления g имеет место сравнение* g^k В s_k (mod m), *тогда* $\overline{(a_n \ldots a_1 a_0)}_g \equiv g_0 s_0 + a_1 s_1 + \ldots a_n s_n \pmod m$.

2.2 Задача. Найти признак делимости на 3 в системе счисления 10.

Решение. Имеем $m = 3$, $g = 10$, 10 В 1 (mod 3), 10^2 В 1 (mod 3), … . $\overline{(a_n \ldots a_2 a_1 a_0)}_{10} \equiv a_0 + a_1 + \ldots a_n \pmod 3$.

Число в обычной (десятичной) системе счисления при делении на три дает тот же остаток, что и сумма его цифр.

2.3 Задача. Найти признак делимости на 4 в системе счисления 10.

Решение. Имеем $m = 4$, $g = 10$, 10 В 2 (mod 4), 10^2 В 0 (mod 4), … , т.е. g^k В 0 (mod 4) для всех $k \geq 2$.

$\overline{(a_n \ldots a_1 a_0)}_{10} \equiv a_0 + 2a_1 \pmod 4$.

Число делится на 4 в системе счисления 10, если число составленное из суммы последней цифры его плюс удвоенной предпоследней цифры делится на 4.

2.4 Задача. Найти признак делимости на 11 в системе счисления 10.

Решение. m = 11, g = 10. 1 В 1 (mod 11), 10 В –1 (mod 11), 10^2 В 1 (mod 11), 10^3 В –1 (mod 11), …, 10^k В $(-1)^k$ (mod 11).

Имеем $\overline{(a_n \ldots a_1 a_0)}_{10} \equiv a_0 - a_1 + \ldots + (-1)^n a_n \pmod{11}$.

2.5 Задача. Найти признак делимости на 11 в системе счисления 100.

Решения. m = 11, g = 100. 100 В 1 (mod 11), …, 100^κ В 1 (mod 11).

Признак равноостаточности на 11 по основанию 100. Сумма двухзначных граней числа считая справа налево должны делится на 11.

3 Полная система вычетов

a. Отношение сравнимости по модулю m обладает свойствами рефлексивности, симметричности и транзитивности, т.е. является отношением эквивалентности.

b. Отношение сравнимости индуцирует разбиение множества **Z** целых чисел на классы эквивалентности, которые называются классами вычетов по модулю m.

c. **Свойство.** Любые два класса вычетов по модулю либо совпадают, либо не пересекаются. Объединение всех классов вычетов по модулю m совпадают с множеством **Z** всех целых чисел.

d. **Свойство.** Пусть A и B – классы вычетов по модулю m, $a \in A$ и $b \in B$. Смежные классы A и B совпадают тогда и только тогда, когда a B b (mod m).

e. **Свойство.** Если A – класс вычетов по модулю m и a – любой элемент из A, то $A = a + mZ$, т.е. $A = \{a + mk / k \in Z\}$.

f. Любое число, принадлежащее классу вычетов a по модулю m называется представителем этого класса.

g. Определение. Если из каждого класса вычетов по модулю m выбрать по одному представителю, то полученное множество чисел называется полной системой вычетов по модулю m, а его элементы вычетами по модулю m.

h. Задача. Найти полную систему вычетов по модулю 4.

Решение. 0, 1, 2, 3, 4 – полная система вычетов.

3.9. Ясно, что полная система вычетов содержит m чисел.

3.10 Если в качестве полной системы вычетов по модулю m выбрать числа 1, 2, …, $m - 1$, то она называется полной системой наименьших неотрицательных вычетов, а 1, 2, 3, …, $m - 1$, m называется полной системой наименьших положительных вычетов.

3.11 Полная система наименьших по абсолютной величине вычетов при нечетном m: $-k$, …, –2, –1, 0, 1, 2, …, k, где $k = \frac{m-1}{2}$; при четном m: $k - 1$, …, –2, –1, 0, 1, 2, … k, $k = \frac{m}{2}$.

3.12 Теорема. *Любая совокупность m чисел* ($m > 1$) *попарно несравнимых по модулю m, есть полная система вычетов по модулю m.*

3.13 Теорема. *Пусть a и b – целые положительные числа и* $(a, m) = 1$. *Если x пробегает полную систему вычетов по модулю m, то ax + b тоже пробегает полную систему вычетов по модулю m.*

3.14 Задача. Проверить, образуют ли числа 13, 8, –3, 10, 35, 60 полную систему вычетов по модулю 6.

Решение. Числа образуют полную систему вычетов по модулю 6 тогда и только тогда, когда их точно 6 и они попарно несравнимы по модулю 6. Попарную несравнимость можно проверить, заменив каждое числа наименьшим неотрицательным вычетом: если повторений не будет, то это полная система вычетов. Получаем 13 В –1 (6), 8 В 2 (6), –3 В 3(6), 10 В 4 (6), 35 В 5 (6), 60 В 0 (6). Следовательно, данные числа образуют полную систему вычетов по модулю 6.

4 Аддитивная группа классов вычетов

4.1 Любое число, принадлежащее классу вычетов a по модулю m называется представителем этого класс, а сам класс обозначается знаком $\overline{a}$.

4.2 По модулю 6 имеется всего 6 классов, а именно:

$\overline{a}$ = {…, –12, –6, 0, 6, 12, 18, …},
$\overline{1}$ = {…, –11, –5, 1, 7, 13, 19, …},
$\overline{2}$ = {…, –10, –4, 2, 8, 14, 20, …},
$\overline{3}$ = {…, –9, –3, 3, 9, 15, 21, …},
$\overline{4}$ = {…, –8, –2, 4, 10, 16, 22, …},
$\overline{5}$ = {…, –7, –1, 5, 11, 17, 23, …},

4.3 На множестве классов по модулю m определим операцию, которую будем называть сложением классов.

Определение. Суммой классов $\overline{a}$ и $\overline{b}$ называется $\overline{a+b}$, т.е. класс чисел, содержащий число $a + b$.

4.4 Задача. Составить таблицу сложения классов по модулю 6.

Решение.

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

4.5 Теорема. *Множество классов $Z_m = Z/_mZ$ по модулю m с операцией сложения является аддитивной группой.*

5 Кольцо классов вычетов

5.1 На множестве классов $Z_m = Z/_mZ$ по модулю m определим операцию, которую будем называть умножением классов.

Определение. Произведением классов $\overline{a}$ и $\overline{b}$ называется класс $\overline{ab}$, т.е. класс чисел, содержащий число ab.

5.2 Задача. Составить таблицу умножения классов по модулю 6.

Решение.

·	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

5.3 Теорема. *Множество классов $Z_m = Z/_mZ$ с операциями сложения и умножения классов является коммутативным кольцом.*

5.4 Теорема. *Кольцо классов вычетов по составному модулю является кольцом с делителем нуля.*

5.5 Теорема. *Кольцо классов вычетов по простому модулю является кольцом без делителей нуля.*

5.6 Задача. Пусть $\overline{a}$ – класс вычетов по модулю m, содержащий число a. При каком m в кольце $Z/_mZ$ возможно равенство $\overline{2} - \overline{3} = \overline{5}$?

Решение. Равенству $\overline{2} - \overline{3} = \overline{5}$ из кольца $Z/_mZ$ соответствует сравнение $2 - 3 \equiv 5 \pmod m$ в кольце Z целых чисел. Отсюда $6 \equiv 0 \pmod m$. Следовательно, $6 \times m$, т.е. $m = 6; 2; 3$ ($m = 1$ исключаем из рассмотрения).

Ответ: 2, 3, 6.

6 Приведенная система вычетов

6.1 Согласно 2-й теореме из п. 1 все числа из одного и того же класса вычетов имеют с m один и тот же делитель наибольший общий делитель. В частности, если одно из этих чисел взаимно просто с модулем, то и все они взаимно простые с модулем.

6.2 Определение. Классом вычетов взаимно простых с модулем m называют класс вычетов содержащий числа взаимно простые с этим модулем.

6.2 Пример. При $m = 35$, класс $\overline{6}$ – взаимно прост с модулем.

6.4 Определение. Если из каждого класса вычетов взаимно простого с модулем m выбрать по одному представителю, то полученное множество чисел называется приведенной системой вычетов по модулю m.

6.5 При $m = 12$. Приведенной системой вычетов по модулю 12 будет множество 1; 5; 7; 11.

6.6 Обозначение: число чисел в приведенной системе вычетов по модулю m обозначается через $\varphi(m)$.

6.7 Теорема. *Любая совокупность $\varphi(m)$ чисел $m > 1$, взаимно простых с m и попарно несравнимых по модулю m, есть приведенная система вычетов по модулю m.*

6.8 Теорема. *Пусть a – целое число, взаимно простое с m и $b_1, b_2, \ldots, b_{\varphi(m)}$ – приведенная системы вычетов по модулю m. Тогда совокупность $ab_1, ab_2, \ldots, ab_{\varphi(m)}$ тоже приведенная системы вычетов по модулю m.*

6.9 Задача. В кольце классов вычетов по модулю 12 отыскать подполе.

Решение. Кольцо $S = Z/_{12}Z$ имеет 12 элементов, число элементов конечного поля есть степень простого числа. Кроме того, аддитивная группа подполя должно быть подгруппой аддитивной группы кольца S. По теореме Лагранжа порядок подгруппы есть делитель порядка группы. Так как аддитивная группа кольца S циклическая (порождена элементом $\overline{1}$), то надо проверить, порождают ли подполе ее элементы второго, четвертого и третьего порядков.

Единственным элементом второго порядка является $\overline{6} : \overline{6} + \overline{6} = \overline{0}$. Но 6 не может входить в мультипликативную группу, ибо $\overline{6} \cdot \overline{6} = \overline{0}$. Поэтому S не содержит подполе порядка 2; S не содержит и подполя порядка 4, такое подполе должно само содержать подполе порядка 2. Этот же факт виден, если рассмотреть аддитивную подгруппу, порожденную элементом $\overline{3}$:{ $\overline{3}$, $\overline{6}$, $\overline{9}$, $\overline{0}$ }. Эта подгруппа не может быть подполем, так как $\overline{6} \cdot \overline{6} = \overline{0}$.

Возьмем элемент порядка 3. Это $\overline{4}$. Аддитивная подгруппа $\{\overline{4}, \overline{8}, \overline{0}\} = P$ является полем. Действительно, $\overline{4} \cdot \overline{8} = \overline{8}$; $\overline{4} \cdot \overline{4} = \overline{4}$; $\overline{8} \cdot \overline{8} = \overline{4}$. Поэтому $\overline{4}$ в P является нейтральным элементом по умножению, $\overline{8}$ обратно себе по умножению. Итак, P – подполе третьего порядка; его мультипликативная группа, естественно, второго порядка.

Ответ: $P = \{\overline{4}, \overline{8}, \overline{0}\}$.

7 Мультипликативная группа классов вычетов, взаимно простых с модулем

7.1 Теорема. *Множество классов вычетов по модулю m, взаимно простых с модулем, образуют относительно умножения группу.*

7.2 Определение. Группа из 7.1 называется мультипликативной группой классов вычетов по модулю m, взаимно простых с модулем.

7.3 Теорема. *Если p – простое число, то множество ненулевых классов вычетов является абелевой группой относительно умножения.*

7.4 Теорема. *Кольцо классов вычетов по модулю m тогда и только тогда является полем, когда m есть простое число.*

7.5 Определение. Число a называться обратным к числу b по модулю m, если ab В 1 (mod m). Числа a и b будем также называть взаимно обратными по модулю m.

7.6 Теорема. *Пусть число a взаимно простое с модулем m и* P_{n-1} *– числитель предпоследней подходящей дроби для числа* $\frac{m}{a}\left(\frac{m}{a}=\frac{P_n}{Q_n}\right)$. *Тогда* $a \cdot (-1)^{n-1} P_{n-1}$ В 1 (mod *m*), *т.е. число* $(-1)^{n-1} P_{n-1}$ *является обратным к элементу a по модулю m.*

7.7 Задача. Найдите число, обратное числу 79 по модулю *m* В 273.

Решение. Разложим число $\frac{273}{79}$ в цепную дробь, тогда $\frac{273}{79}$ = [3; 2, 5, 7].

Вычислим числители подходящих дробей к числу $\frac{273}{79}$ по схеме

k		1	2	3	4
g_k		2	2	5	7
P_k	1	3	7	38	273

P_3 = 38 есть числитель предпоследней подходящей дроби для числа $\frac{273}{79}$. Следовательно, число $(-1)^3 \cdot P_3 = -38$ является обратным к числу 79, т.е. 79 · (–38) В 1 (mod 273).

Ответ. –38.

8 Функция Эйлера

8.1 Определение. Функцией Эйлера называется функция φ определенная на множестве натуральных чисел следующим образом:

$\varphi(m)$ равно числу натуральных чисел не превосходящих *m* и взаимно простых с *m*.

8.2 Пример. $\varphi(1)=1$, $\varphi(2)=1$, $\varphi(6)=2$, $\varphi(5)=4$, $\varphi(12)=4$.

8.3 Ясно, что $\varphi(m)$ это число чисел в приведенной системе вычетов или другими словами $\varphi(m)$ это число классов взаимно простых с *m*.

8.4 Теорема. Пусть *a* и *b* взаимно простые натуральные числа. $u_1, u_2, ..., u_{\varphi(a)}$ и $\upsilon_1, \upsilon_2, ..., \upsilon_{\varphi(b)}$ приведенные системы вычетов соответственно по модулям *a* и *b*. Тогда множество $M = \{a\upsilon_i + b\upsilon_k / i = 1, 2, ..., \varphi(b); k = 1, 2, ..., \varphi(a)\}$ является приведенной системой вычетов по модулю *ab*.

8.5 Следствие. Если НОД(*a, b*) = 1, то $\varphi(ab) = \varphi(a) \cdot \varphi(b)$.

8.6. Следствие. Если $a_1, a_2, \ldots, a_n$ попарно взаимно простые, то $\varphi(a_1 \cdot a_2, \cdot \ldots, \cdot a_n) = \varphi(a_1) \cdot \varphi(a_2) \cdot \varphi(a_2) \cdot \varphi(a_n)$.

8.7 Следствие. Пусть $m = p_1^{\alpha_1} p_2^{\alpha_1} \ldots p_k^{\alpha_k}$ – каноническое разложение числа *m*, то

$$\varphi(m) = (p_1^{\alpha_1} - p_k^{\alpha_k - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \ldots (p_k^{\alpha_k} - p_k^{\alpha_k - 1}) =$$
$$= p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \ldots p_k^{\alpha_k - 1} (p_1 - 1)(p_2 - 1) \ldots (p_k - 1) =$$
$$= p_1^{\alpha_1} p_2^{\alpha_1} \ldots p_k^{\alpha_k} \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_k}\right) = m \prod_{m:\, p_i} \left(1 - \frac{1}{p_i}\right).$$

8.9 Пример. Найти $\varphi(270)$.

Решение. $\varphi(270) = \varphi(2 \cdot 3^3 \cdot 5) = 2^0(2 - 1) \cdot 3^2(3 - 1) \cdot 5^0(5 - 1) = 3^2 \cdot 2 \cdot 4 = 72$.

Ответ. 72.

8.10 Пример. Найти $\varphi(1800)$.

Решение. $\varphi(1800) = \varphi(2^3 \cdot 3^2 \cdot 5^2) = \varphi(2^3)\ \varphi(3^2)\varphi(5^2) = 2^2(2 - 1) \cdot 3(3 - 1) \cdot 5(5 - 1) = 4 \cdot 1 \cdot 3 \cdot 2 \cdot 5 \cdot 4 = 12 \cdot 2 \cdot 20 = 24 \cdot 20 = 480$.

Ответ: 480.

8.11 Пример. Найти $\varphi(30)$.

Решение. $\varphi(30) = \varphi(2 \cdot 3 \cdot 5) = 30 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 30 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 8.$

Ответ. 8.

9 Теоремы Эйлера, Ферма, Вильсона и формула Гаусса

9.1 Теорема Эйлера. *Если целое число a взаимно простое с m, то* $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\ m)$.

9.2 Теорема Ферма. *Если целое число a не делится на простое число p,* то $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$.

9.3 Вторая формулировка теоремы Ферма. *Если p – простое и a – любое целое число, то* $a^p \equiv a (\mathrm{mod}\ p)$.

9.4 Теорема Вильсона. *Если p – простое число, то* $(p-1)! + 1 \equiv 0 (\mathrm{mod}\ p)$.

9.5 Теорема (Формула Гаусса). $\sum_{m:x} \varphi(x) = m.$

9.6 Задача. Найти $\sum_{15:x} \varphi(x)$, при $m = 15$.

Решение. $\sum_{15:x} \varphi(x) = \varphi(1) + \varphi(3) + \varphi(5) + \varphi(15) = 1 + 2 + 4 + 8 = 15.$

Ответ: 15.

9.7 Задача. Найти остаток отделения 171^{2147} на 52.

Решение. Обозначим искомый остаток через x. Имеем $\varphi(52) = 24$, x В 171^{2147} В $15^{24 \cdot 99 + 11}$ В 15^{11} В $(3375)^3 \cdot 225$ В$(-5)^3 \cdot 17$ В$-21 \cdot 17$ В 7 (mod 52).

Ответ: 7.

9.8 Задача. Найти остаток от деления 126^{1020} на 138.

Решение. Здесь НОД(126. 138) = 6. Если x В 126^{1020} (mod 138), то $x = 6\,x$, x_1 В $21 \cdot 126^{1019}$ В $21 \cdot 11^{22 \cdot 4677}$ В $-2 \cdot 11^{7}$В 11^{6} В 6 В9 (mod 23), $x = 54$ В 2 (mod 52). Остаток равен 2.

Ответ: 2.

9.9 Функция Эйлера $\varphi(m)$ не всегда является наименьшим положительным значением k, таким, что a^k В 1 (mod m). Для нахождения значений k, меньших, чем $\varphi(m)$, удовлетворяющих этому сравнению, имеет смысл ввести в рассмотрение обобщенную функцию Эйлера $L(m)$.

9.10 Определение. Обобщенной функцией Эйлера $L(m)$ называется функция, определенная для всех натуральных значений m следующим образом: $L(1) = 1$, а при $m > 1$

$$L(m)=\text{НОК}[p_1^{\alpha_1-1}(p_1-1),\ p_2^{\alpha_2-1}(p_2-1),\ ...,\ p_s^{\alpha_s-1}(p_s-1)],$$

где $m = p_1^{\alpha_1} p_2^{\alpha_1} ... p_s^{\alpha_s}$ – каноническое разложение m.

9.11 Задача. Найти $L(360)$.

Решение. $L(360) = L(2^3 \cdot {}^2 3 \cdot 5) = \text{НОК}[4, 6, 4] = 12$.

Ответ: 12.

9.12 Задача. Найти $L(45551)$.

Решение. $L(45551) = L(11 \cdot 21 \cdot 101) = \text{НОК}[10, 40, 100] = 200$.

Ответ: 200.

9.13 При $m = p^{\alpha}$ функция $L(m)$ и $\varphi(m)$, очевидно, совпадают.

9.14 Теорема. *При любом модуле* m *и* НОД(a, m) = 1. *Имеет место сравнение* $a^{L(m)}$ В 1 (mod m).

9.15 Пример. Показать, что $5^{L(546)}$ В 1 (mod 546).

Решение. Имеем $L(546) = L(2 \cdot 3 \cdot 7 \cdot 13) = \text{НОК}[1, 2, 6, 12] = 12$. 5^{12} В 625^3 В 79^3 В 1 (mod 546).

10 Сравнения с одним неизвестным

10.1 В кольце $Z/_mZ$ рассмотрим уравнение с одним неизвестным

$$\bar{a}_n \bar{x}^n + \bar{a}_{n-1}\bar{x}^{n-1} + ... + \bar{a}_1\bar{x}^1 + \bar{a}_0 = \bar{0} \qquad (*).$$

10.2 Теорема. *Класс* $\bar{c}$ *является решением уравнения* (*) *тогда и только тогда когда*

$$a_n c^n + a_{n-1}c^{n-1} + ... + a_1 c + \bar{a}_0 \equiv 0 (\text{mod } m) \qquad (**).$$

10.3 Определение. Сравнение (**) называется сравнением с одним неизвестным.

Если a_n не делится на m, то число n называется степенью сравнения (**). Если c такое число, что $a_n c^n + a_{n-1}c^{n-1} + ... + a_1 c + \bar{a}_0 \equiv 0 (\text{mod } m)$, то говорят, что c удовлетворяет сравнению (**), а решением сравнения (**) называется класс $\bar{c}$.

10.4 Следствие. Если один представитель из класса вычетов удовлетворяет сравнению (**), то и любой другой представитель удовлетворяет

этому сравнению.

Чтобы найти все решения сравнения (**) достаточно найти все числа из полной системы вычетов удовлетворяющие этому сравнению, а соответствующие им классы являются решениями этого сравнения (**).

10.5 Если $\overline{c}_1$, $\overline{c}_2$,..., $\overline{c}_k$ решение сравнения (**), то записывается это так

$x \equiv c_1 \pmod m$,

$x \equiv c_2 \pmod m$,

……

$x \equiv c_2 \pmod m$.

10.6 Задача. Найти решения сравнения $x^4 - 3x^3 + x^2 - 2 \equiv 0 \pmod 7$.

Решение. Запишем полную систему вычетов наименьших по абсолютной величине по модулю $\overline{x}$: –3, –2, –1, 0, 1, 2, 3.

Ответ: $-\overline{2}, \overline{3}$ или $x \equiv 5 \pmod 7$, $x \equiv 3 \pmod 7$.

10.7 Задача. Найти решения сравнения $x^4 - x^2 + 3x - 1 \equiv 0 \pmod 4$.

Решение. Запишем полную систему вычетов наименьших по абсолютной величине по модулю 4: –1, 0, 1, 2.

Ответ: $-\overline{1}$ или $x \equiv 3 \pmod 4$.

10.8 Задача. Решить сравнение $x^3 - 7x + 3 \equiv 0 \pmod 5$.

Решение. Запишем полную систему вычетов наименьших по абсолютной величине по модулю 5: –2, –1, 0, 1, 2. Это сравнение решений не имеет.

Ответ: нет решений.

10.9 Определение. Два сравнения называются эквивалентными или равносильными, если множество чисел, удовлетворяющее этим сравнениям, совпадают.

10.10 Теорема. 1. *Если* НОД(c, m) = 1, то *сравнения* $f(x) \equiv 0 \pmod m$ *и* $c \cdot f(x) \equiv 0 \pmod m$ *эквиваленты.*

2. *Если при* $i = 0, 1, \ldots, n$ $a_i \equiv b_i \pmod m$, *то сравнения* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 \pmod m$ *и* $g(x) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0 \equiv 0 \pmod m$ *эквиваленты.*

10. 11 Следствие. Если в сравнении добавить или отбросить слагаемые с коэффициентами делящимися на модуль, то полученное сравнение эквивалентно данному.

10.12 Следствие. Сравнение $f(x) \equiv 0 \pmod p$, где p – простое число можно заменить эквивалентным сравнением со старшим коэффициентом равным единице.

10.13 Замечание. Сравнения разных степеней могут быть эквивалентными.

10.14 Пример. Сравнения $2x + 1 \equiv 0 \pmod 3$ и $x^3 - 1 \equiv 0 \pmod 3$ эквивалентны. Имеют решения $x \equiv 0 \pmod 3$.

10.5 Замечание. Сравнения по разным модулям тоже могут быть эквивалентны.

10.16 Задача. Найти два эквивалентных сравнения по разным модулям.

11 Линейные сравнения с одним неизвестным

11.1 Рассмотрим сравнение $a_0x + a_1 \equiv 0 \pmod{m}$, где $a_0 \not\vdots m$. Такое сравнение называется сравнением первой степени или линейным сравнением.

11.2 Линейные сравнения обычно будем записывать в виде

$$ax \equiv b \pmod{m}.$$

11.3 Теорема. *Пусть* НОД$(a, m) = d$, $d > 0$. *Сравнение* $ax \equiv b \pmod{m}$ *не имеет решений, если* $b \not\vdots m$ *и имеет d решений, если* $b \vdots d$.

11.4 Задача. Решить сравнение $12x \equiv 5 \pmod{21}$.

Решение. Имеем НОД$(12, 21) = 3$ и $5 \not\vdots 3$, то наше сравнение не имеет решений.

Ответ: нет решений.

11.5 Задача. Решить сравнение $11x \equiv 21 \pmod{15}$.

Решение. Имеем НОД$(12, 15) = 3$ и $21 \vdots 3$. Следовательно сравнение имеет три решения. Получаем сравнение $4x \equiv 7 \pmod 5$, т.е. $x \equiv 3 \pmod 5$ и $x \equiv 3 \pmod{15}$, $x \equiv 8 \pmod{15}$, $x \equiv 13 \pmod{15}$.

Ответ: $x \equiv 3 \pmod{15}$, $x \equiv 8 \pmod{15}$, $x \equiv 13 \pmod{15}$.

12 Способы решения линейных сравнений

12.1 Решение методом подбора. Решить сравнение $5x \equiv 7 \pmod 8$.

Решение. НОД$(5, 8) = 1$ и следовательно существует единственное решение. Испытывая вычета $0, \pm1, \pm2, \pm3, 4$ находим решение $x \equiv 3 \pmod 8$.

Ответ: $x \equiv 3 \pmod 8$.

12.2.1 Решение сравнений первой степени методом преобразования коэффициентов. Решение сравнений первой степени методом подбора не является эффективным. На практике для небольших модулей m целесообразно, используя общие свойства сравнений попытаться преобразовать коэффициенты так, чтобы правую часть можно было бы разделить на коэффициент у неизвестного x.

Преобразования о которых идет речь, следующие: замена коэффициентов абсолютно наименьшим вычетом, замена b (алгебраическим добавлением кратного модуля) сравнимым по модулю m числом с тем, чтобы последнее делилось на a, переход от a и b к другим, сравнимым с ними по модулю m числом, у которых оказался бы общий делитель и т.п.

Преобразованию можно подвергать a или b, а также a и b сразу.

12.2.2 Задача. Решить сравнение $5x \equiv 7 \pmod 8$.

Решение. Так как НОД$(5, 8) = 1$, то сравнение имеет единственное решение $5x \equiv 7 + 8 = 15 \pmod 8$, т.е. $x \equiv 3 \pmod 8$.

Ответ: $x \equiv 3 \pmod 8$.

12.2.3 Задача. Решить сравнение $7x \equiv 6 \pmod{15}$.

Решение. НОД(7, 15) = 1. Следовательно сравнение имеет единственное решение.

1-й способ. $7x \equiv 6 + 21(15)$, т.е. $x \equiv 3 \pmod{15}$.

2-й способ. Так как НОД(6, 15) = 3 делаем подстановку $x = 3y$. Имеем $7 \cdot 3y \equiv 6 \pmod{15}$, т.е. $7y \equiv 2 \pmod 5$. Имеем $2y \equiv 2 \pmod 5$ или $y \equiv 1 \pmod 5$. Отсюда получаем $3y \equiv 3 \pmod{15}$ или $x \equiv 3 \pmod{15}$.

Ответ: $x \equiv 3 \pmod{15}$.

12.2.4 Задача. Решить сравнение $17x \equiv 25 \pmod{28}$.

Решение. Имеем НОД(17, 28) =1, то сравнение имеет единственное решение $(17 + 28)x \equiv 25 \pmod{28}$, т.е. $9x \equiv 5 \pmod{28}$, т.е. $9x \equiv 5 - 5 \cdot 28 \equiv -135 \pmod{28}$, т.е. $x \equiv -15 \equiv 13 \pmod{28}$.

Ответ: $x \equiv 13 \pmod{28}$.

12.3.1 Решение сравнений 1-ой степени при помощи теоремы Эйлера. Если НОД(a, m) =1, тогда $a^{\varphi(m)} \equiv 1 \pmod m$. Отсюда $a^{\varphi(m)} \cdot b \equiv b \pmod m$.

Сравнивая это сравнение со сравнением $ax \equiv b \pmod m$, видно, что $x \equiv a^{\varphi(m)-1} \cdot b \pmod m$ является его решением.

Мы получили решение в виде готовой формулы. Однако задачу можно считать эффективно решенной лишь тогда, когда для $a^{\varphi(m)-1} \cdot b$ будет найден наименьший неотрицательный или абсолютно наименьший вычет по модулю m.

12.3.2 Задача. Решить сравнение $3x \equiv 7 \pmod{11}$.

Решение. Так как НОД(3, 11) = 1, то существует единственное решение и $x \equiv 3a^{\varphi(11)-1} \cdot 7 \pmod{11}$. Имеем $\varphi(11) = 10$, т.к. $\varphi(p) = p - 1$, и $x \equiv 3a^9 \cdot 7 \pmod{11}$. Находим абсолютно наименьший вычет для 3^9 по модулю 11. Получаем $3^2 \equiv 9 \equiv -2(11)$, $3^4 \equiv 4 \pmod{11}$, $3^5 \equiv 12 \equiv 1(\mathrm{mod}\ 11)$, $3^9 \equiv 4 \pmod{11}$. Теперь $3^9 \cdot 7 \equiv 4 \cdot 7 = 28 \equiv 6 \pmod{11}$. Итак, $x \equiv 6 \pmod{11}$.

Ответ: $x \equiv 6 \pmod{11}$.

12.4.1 Решение уравнений первой степени с помощью цепных дробей. Это эффективный способ.

Теорема. *Пусть* НОД(a, m) = 1 и $\frac{P_0}{Q_0}, \frac{P_1}{Q_1}, ..., \frac{P_{s-1}}{Q_{s-1}}, \frac{P_s}{Q_s}$ *последовательность подходящих дробей разложения* $\frac{m}{a}$ *в цепную дробь. Тогда решением сравнения* $ax \equiv b \pmod m$ *является класс* $x \equiv (-1)^s \cdot b \cdot P_{s-1} \pmod m$.

12.4.2 Задача. Решить сравнение $91x \equiv 322 \pmod{763}$.

Решение. Имеем НОД(91, 763) = 7 и $322 \vdots 7$. Отсюда следует, что сравнение имеет 7 решений. $13x \equiv 46 \pmod{109}$. Разложим дробь $\frac{109}{13}$ в

цепную дробь

$$
\begin{array}{r|l}
109 & 13 \\
\cline{2-2}
104 & 8 \\
\cline{1-1}
13 & 5 \\
\cline{1-1}
10 & 2 \\
\cline{1-1}
5 & 3 \\
\cline{1-1}
3 & 1 \\
\cline{1-1}
3 & 2 \\
\cline{1-1}
2 & 1 \\
\cline{1-1}
2 & 1 \\
\cline{1-1}
2 & 2 \\
\cline{1-1}
0 &
\end{array}
$$

		0	1	2	3	4
q_i		8	2	1	1	2
p_i	1	8	17	25	42	109

Итак, $\frac{109}{13} = [8; 2, 1, 1, 2]$.

Имеем $x \equiv (-1)^4 \cdot 46 \cdot 42 \equiv 79 \pmod{109}$.

Отсюда $x \equiv 79, 188, 297, 406, 515, 624, 733 \pmod{763}$.

Ответ: $x \equiv 79, 188, 297, 406, 515, 624, 733 \pmod{763}$.

13 Применение цепных дробей к решению неопределенных уравнений первой степени с двумя переменными

13.1 Определение. Диофантовым уравнением 1-й степени с n переменными называется уравнение вида $a_1x_1 + a_2x_2 + a_nx_n = b$, где все коэффициенты a неизвестные – целые числа и хотя бы одно $a_i \neq 0$.

13.2 Определение. Решение диофантова уравнения называется n-ка целых чисел $(x_1', x_2', ..., x_n')$, удовлетворяющая этому уравнению.

13.4 Теорема. *Если x_0 удовлетворяет уравнению $ax \equiv c \pmod{b}$, то пара $\left(x_0, \frac{c - ax_0}{b}\right)$ есть решение диофантова уравнения $ax + by = c$.*

13.5 Теорема. *Пусть d – наибольший общий делитель a и b, $a \neq 0$, $b \neq 0$, $(c \vdots d)$ и (x_0, y_0) некоторое решение диофантова уравнения: $ax + by = c$. Тогда множество решений этого уравнения в целых числах совпадает со множеством пар (x', y'), где $x' = x_0 - \frac{b}{d}t$, $y' = y_0 + \frac{a}{d}t$, a t – любое целое*

число.

13.6 Задача. Решить уравнение $50x + 42y = 34$.

Решение. Здесь НОД(50, 42) = 2, 34×2. Рассмотрим сравнения $50x \equiv 34 \pmod{42}$, находим последовательно: $4x \equiv 17 \pmod{21}$, $2x \equiv 19 \pmod{21}$, $x \equiv 20 \pmod{21}$, $x_0 = 20$, так, что $25 \cdot 20 - 21y_0 = 17$, $y_0 = 23$. Любое решение данного диофантова уравнения имеет вид: $x = 20 + 21t$, $y = 23 - 25t$, где $t \in Z$.

Ответ: $x = 20 + 21t$, $y = 23 - 25t$, где $t \in Z$.

14 Системы сравнений первой степени

14.1 Задача. Решить систему сравнений $\begin{cases} x \equiv 2 \pmod 7, \\ x \equiv 5 \pmod 9, \\ x \equiv 11 \pmod{15}. \end{cases}$

Решение. Из второго сравнения $x = 5 + 9t$, где $t \in Z$. Подставляем в первое сравнение и получаем $5 + 9t_1 \equiv 2 \pmod 7$, $2t_1 \equiv -3 \pmod 7$, $t_1 \equiv 2 \pmod 7$, т.е. $t_1 = 2 + 7t_2$, $x = 5 + 9(2 + 7t_2) = 23 + 63\,t_2$.

Имеем $23 + 63\,t_2 \equiv 11 \pmod{15}$, $63\,t_2 \equiv -12 \pmod{15}$, т.е. $63\,t_2 \equiv 18 \pmod{15}$, $21t_2 \equiv 6 \pmod{15}$ или $7t_2 \equiv 2 \pmod 5$, $2t_2 \equiv 2 \pmod 5$, $t_2 \equiv 1 \pmod 5$.

Итак, $t_2 = 1 + 5t_3$, т.е. $x = 23 + 63\,(1 + 5t_3) = 86 + 315\,t_3$. Итак, $x \equiv 86 \pmod{315}$.

Ответ: $x \equiv 86 \pmod{315}$.

14.2 Мы рассмотрим лишь простейшую системы сравнений

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \quad (1) \\ \ldots\ldots \\ x \equiv b_k \pmod{m_k}, \end{cases}$$

, с одним неизвестным, но с разными и притом взаимно простыми модулями.

14.3 Теорема. *Пусть числа* M_s и M'_s *определены из условий* $m_1 m_2 \ldots m_s = M_s m_s$, $M_s M'_s \equiv 1 \pmod{m_s}$ *и пусть* $x_0 = M_1 M'_1 b_1 + M_2 M'_2 b_2 + \ldots + M_k M'_k b_k$. *Тогда совокупность значений x, удовлетворяющих системе (1), определяется сравнением* $x \equiv x_0 \pmod{m_1 m_2 \ldots m_k}$.

14.4.1 Задача. Решить систему $\begin{cases} x \equiv b_1 \pmod 4, \\ x \equiv b_2 \pmod 5, \\ x \equiv b_3 \pmod 7. \end{cases}$

Решение. Здесь $4 \cdot 5 \cdot 7 = 35 \cdot 4 = 28 \cdot 5 = 20 \cdot 7$, причем $35 \cdot 3 \equiv 1 \pmod 4$, $28 \cdot 2 \equiv 1 \pmod 5$, $20 \cdot 6 \equiv 1 \pmod 7$. Поэтому $x_0 = 35 \cdot 3b_1 + 28 \cdot 2b_2 + 20 \cdot 6b_3 = 105\ b_1 + 56\ b_2 + 120b_3$, и, следовательно, совокупность значений x, удовлетворяющих системе, может быть представлена в виде $x \equiv 105\ b_1 + 56\ b_2 + 120b_3 \pmod{140}$.

Ответ: $x \equiv 105\ b_1 + 56\ b_2 + 120b_3 \pmod{140}$.

14.4.2 Так, например, совокупность значений x, удовлетворяющих системе $\begin{cases} x \equiv 1 \pmod 4, \\ x \equiv 3 \pmod 5, \\ x \equiv 2 \pmod 7, \end{cases}$ будет $x \equiv 105 \cdot 1 + 56 \cdot 3 + 120 \cdot 2 \equiv 93 \pmod{140}$.

Ответ: $x \equiv 93 \pmod{140}$.

14.4.3 Задача. Решить систему $\begin{cases} x \equiv 3 \pmod 4, \\ x \equiv 3 \pmod 5, \\ x \equiv 6 \pmod 7. \end{cases}$

Решение. $x \equiv 105 \cdot 3 + 56 \cdot 2 + 120 \cdot 6 \equiv 27 \pmod{140}$.

Ответ: $x \equiv 27 \pmod{140}$.

15 Сравнения высших степеней по простому модулю

15.1 Сравнение (*) $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 \pmod p$, где $a_n \not\equiv p$ и $\overline{a}_n \overline{x}^n + \overline{a}_{n-1}\overline{x}^{n-1} + \ldots + \overline{a}_1 \overline{x} + x_0 = \overline{0}$ в $Z/_pZ$ равносильны.

15.2 Теорема. *Сравнение n-ой степени* (*) *эквивалентно некоторому сравнению степени не выше p – 1-ой.*

15.3 Пример. Сравнение $x^{13} - 3x^{10} + x^8 - 6x^3 + x^2 - x + 4 \equiv 0 \pmod 5$ заменить сравнением не выше 4 степени.

Решение. Применим малую теорему Ферма $x^5 \equiv x \pmod 5$, получим $x^{13} \equiv x^{5 \cdot 2 + 3} \equiv x^{2+3} \equiv x \pmod 5$, т.е. $x - 3x^2 + x^4 - 6x^3 + x^2 - x + 4 \equiv 0 \pmod 5$ или $x^4 - 6x^3 + 2x^2 + 4 \equiv 0 \pmod 5$.

Ответ: $x^4 - 6x^3 + 2x^2 + 4 \equiv 0 \pmod 5$.

15.4 Теорема. Сравнение n-ой степени по простому модулю имеет не более n решений.

Другими словами. Уравнение n-ой степени с коэффициентами из поля $Z/_pZ$ имеет не более n решений.

15.5 Теорема. *Если p – простое число, то сравнение* $x^{p-1} - 1 \pmod p$ *имеет точно p – 1 решение.*

15.6 Теорема Вильсона. *Если p – простое число, то* $(p-1)! + 1 \equiv 0 \pmod p$.

15.7 Теорема. Если *p – простое число и d натуральный делитель числа p – 1, то сравнение* $x^d - 1 \pmod p$ *имеет точно d решений.*

16 Сравнение любой степени по составному модулю

16.1 Теорема. *Если* $m_1, m_2, \ldots, m_k$ *попарно взаимно простые, то сравнение* $f(x) \equiv 0 \pmod{m_1, m_2, \ldots, m_k}$ *(1) равносильно системе*

$$\begin{cases} f(x) \equiv 0 \pmod{m_1}, \\ f(x) \equiv 0 \pmod{m_2}, \\ \ldots\ldots \\ f(x) \equiv 0 \pmod{m_k}. \end{cases}$$

При этом, обозначая через $T_1, T_2, \ldots, T_k$ *число решений отдельных сравнений этой системы по соответствующим модулям и через* T *– число решений сравнения* (1), *будем иметь* $T = T_1, T_2, \ldots, T_k$.

16.2 Задача. Решить сравнение $f(x) \equiv 0 \pmod{35}$, $f(x) = x^4 + 2x^3 + 8x + 9$ (2).

Решение. Наше сравнение равносильно системе $\begin{cases} f(x) \equiv 0 \pmod 5, \\ f(x) \equiv 0 \pmod 7. \end{cases}$

Легко убедиться, что первое уравнение этой системы имеет два решения: $x \equiv 1; 4 \pmod 5$, второе сравнение имеет 3 решения $x \equiv 3; 5; 6 \pmod 7$. Поэтому сравнение (2) имеет $2 \cdot 3 = 6$ решений. Чтобы найти 6 решений надо решить 6 систем вида $\begin{cases} x \equiv b_1 \pmod 5, \\ x \equiv b_2 \pmod 7 \end{cases}$ (3), которые получим, заставляя b_1 пробегать значения $b_1 = 1; 4$, а b_2 пробегать значения $b_2 = 3; 5, 6$. Но ввиду $35 = 7 \cdot 5 = 5 \cdot 7$, $7 \cdot 3 \equiv 1 \pmod 5$, $5 \cdot 3 \equiv 1 \pmod 7$, совокупность значений x, удовлетворяющих системе (3) представим в виде (14.4.1) $x \equiv 21b_1 + 15b_2 \pmod{35}$. Поэтому решение сравнения (2) будет $x \equiv 31; 26; 6; 24; 19; 34 \pmod{35}$.

Ответ: $x \equiv 31; 26; 6; 24; 19; 34 \pmod{35}$.

16.3 Ввиду теоремы 16.1 исследование и решение сравнения $f(x) \equiv 0 \pmod{p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_1}}$ сводится к исследованию и решению сравнений вида $f(x) \equiv 0 \pmod{p^{\alpha}}$; (4) это же сравнение сводится вообще, как мы сейчас увидим, к сравнению $f(x) \equiv 0 \pmod p$ (5).

Действительно, всякое x, удовлетворяющее сравнению (4) необходимо должно удовлетворять и сравнению (5).

Пусть $x \equiv x_1 \pmod p$ – какое-либо решение сравнения (5). Тогда $x = x_1 + pt_1$, где t_1 – целое. Вставляя это значение x в сравнение $f(x) \equiv 0 \pmod{p^2}$ и разлагая левую часть по формуле Тейлора, найдем (принимая во внимание, что $\frac{1}{k!} f^{(k)}(x_1)$ – целое, и отбрасывая члены кратные p^2)

$f(x)+ pt_1'(x_1) \equiv 0 \pmod{p^2}$; $\frac{f(x_1)}{p} + t_1 f'(x_1) \equiv 0 \pmod{p}$.

Ограничиваясь здесь случаем, когда $f'(x_1)$ не делится на p, имеет одно решение: $t_1 \equiv t_1' \pmod{p}$; $t_1 = t_1' + pt_2$.

Выражение для x принимает вид $x = x_1 + pt_1' + p^2 t_2 = x_2 + p^2 t_2$; вставляя его в выражение $f(x) \equiv 0 \pmod{p^3}$, получим $f(x_2) + p^2 t_2 f'(x_2) \equiv 0 \pmod{p^3}$; $\frac{f(x_2)}{p^2} + t_2 f'(x_2) \equiv 0 \pmod{p}$. Здесь $f'(x_2)$ не делится на p, так как $x_2 \equiv x_1 \pmod{p}$, $f'(x_2) \equiv f'(x_1) \pmod{p}$, и потому последнее сравнение имеет одно решение: $t_2 = t_2' \pmod{p}$; $t_2 = t_2' + pt_3$.

Выражение для x принимает вид $x = x_2 + p^2 t_2' + p^3 t_3 = x_3 + p^3 t_3$ и т.д. Таким путем по данному решению сравнения (5) постепенно найдем сравниваемое с ним решение сравнения (4).

Итак, всякое решение $x \equiv x_1 \pmod{p}$ сравнения (5) при условии, что $f'(x_1)$ не делится на p, даст одно решение сравнения (4) $x = x_\alpha + p^\alpha \cdot t_\alpha$; $x \equiv x_\alpha \pmod{p^\alpha}$.

16.4 Задача. Решить сравнение $f(x) \equiv 0 \pmod{27}$, $f(x) = x^4 + 7x + 4$. (6)

Решение. Сравнение $f(x) \equiv 0 \pmod{3}$ имеет одно решение $x \equiv 1 \pmod{3}$, при этом $f'(1) \equiv 2 \pmod{3}$ и, следовательно, не делится на 3.

Находим: $x = 1 + 3t_1$, $f(1) + 3t_1 f'(1) \equiv 0 \pmod{9}$, $3 + 3t_1 \cdot 2 \equiv 0 \pmod{9}$, $2t_1 + 1 \equiv 0 \pmod{3}$, $t_1 \equiv 1 \pmod{3}$, $t_1 = 1 + 3t_2$, $x = 4 + 9t_2$, $f(4) + 9t_2 f'(4) \equiv 0 \pmod{27}$, $18 + 9t_2 \cdot 2 \equiv 0 \pmod{27}$, $2t_2 + 2 \equiv 0 \pmod{3}$, $t_2 \equiv 2 \pmod{3}$, $t_2 = 2 + 3t_3$, $x \equiv 22 + 27t_3$. Таким образом, сравнение (6) имеет одно решение $x \equiv 22 \pmod{27}$.

Ответ: $x \equiv 22 \pmod{27}$.

17 Квадратичные вычеты

17.1 Рассмотрим сравнение второй степени $ax^2 + bx + c \equiv 0 \pmod{p}$ простому модулю $p \neq 2$.

17.2 Легко проверить, что это сравнение эквивалентно сравнению $(2ax + b^2) \equiv b^2 - 4ac \pmod{p}$.

17.3 Таким образом вопрос сводится к решению сравнения (*) $x^2 \equiv a \pmod{p}$, причем будем считать, что $a \nmid p$.

17.4 Определение. Если сравнение (*) имеет решение, то число a называется *квадратичным вычетом*, в противном случае число a называется *квадратичным невычетом*.

17.5 Теорема. Если a квадратичный вычет, то сравнение (*) имеет два решения.

17.6 Теорема (критерий Эйлера). Число a является квадратичным вычетом по модулю p тогда и только тогда, когда $a^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p)$.

Число a является квадратичным невычетом по модулю p, тогда и только тогда, когда $a^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\, p)$.

17.7 Следствие. Для нечетного простого p число его квадратичных вычетов всегда равно числу его квадратичных невычетов, а именно: $\frac{p-1}{2}$.

17.8 Теорема. *Произведение двух квадратичных вычетов или двух невычетов есть вычет; произведение вычета на невычет есть невычет.*

17.9 Задача. Найти класс квадратичных вычетов по модулю $p = 13$.

Решение. Имеем 1, 2, 3, … , 12, $p = 13$, $\frac{p-1}{2} = 6$.

$1^6 \equiv 1 \pmod{13}$ – квадратичный вычет 1,
$2^6 \equiv -1 \pmod{13}$ – квадратичный невычет 2,
$3^6 \equiv 1 \pmod{13}$ – квадратичный вычет 3,
$4^6 \equiv 2^{12} \equiv 1 \pmod{13}$ – квадратичный вычет 4,
$5^6 \equiv -1 \pmod{13}$ – квадратичный невычет 5,
$6^6 = 2^6 \cdot 3^6 \equiv -1 \pmod{13}$ – квадратичный невычет 6,
$7^6 \equiv (-3)^3 \equiv -1 \pmod{13}$ – квадратичный невычет 7,
$8^6 = 2^{18} \equiv -1 \pmod{13}$ – квадратичный невычет 8,
$9^6 = 3^{18} \equiv 1 \pmod{13}$ – квадратичный вычет 9,
$10^6 = 2^6 \cdot 5^6 \equiv 1 \pmod{13}$ – квадратичный вычет 10,
$11^6 \equiv (-2^6) = \cdot 2^6 \equiv -1 \pmod{13}$ – квадратичный невычет 11,
$12^6 = 2^{12} \cdot 3^6 \equiv 1 \pmod{13}$ – квадратичный вычет 12.

.

18 Символ Лежандра

18.1 Сравнение $a^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p)$ и $a^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\, p)$, где НОД($a$, p) = 1 и p – нечетное простое число объединяются в одно сравнение вида $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) (\mathrm{mod}\, p)$, где $\left(\frac{a}{p}\right)$ называется *символом Лежандра* и обозначает +1 или –1. Число a называется *числителем, p – знаменателем* символа Лежандра.

18.2 Теперь, если $\left(\frac{a}{p}\right) = 1$, то a квадратичный вычет по модулю p и

сравнение $x^2 \equiv a \pmod p$ имеет два различных решения; если же $\left(\frac{a}{p}\right) = -1$, то a – квадратичный невычет по модулю p и сравнение $x^2 \equiv a \pmod p$ неразрешимо.

18.3 Символ Лежандра можно находить с помощью критерия Эйлера: $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \equiv \pm 1 (\mathrm{mod}\, p)$, но при больших значениях a и p вычисление является громоздким. Вычисление значительно упрощается, если использовать некоторые его свойства.

18.4 Свойства символа Лежандра:

1) Если $a \equiv b \pmod p$, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

2) $\left(\frac{1}{p}\right) = 1$.

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

4) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

5) $\left(\frac{ab\ldots l}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\ldots\left(\frac{l}{p}\right)$, где $a, b, \ldots, l$ взаимно просты с p; в частности $\left(\frac{a^n}{p}\right) = \left(\frac{a}{p}\right)^n$, $\left(\frac{a^2}{p}\right) = 1$, $\left(\frac{ab^2}{p}\right) = \frac{a}{p}$.

6) *Закон взаимности квадратичных вычетов*: если p и g – различные простые нечетные числа, то $\left(\frac{g}{p}\right)\cdot\left(\frac{p}{g}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{g-1}{2}}$, или $\left(\frac{g}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{g-1}{2}}\left(\frac{p}{g}\right)$, так как $\left(\frac{p}{g}\right)^2 = 1$.

18.5 Задача. Вычислить $\left(\frac{438}{593}\right)$.

Решение. Сначала разложим числитель 438 на простые множители: $438 = 2 \cdot 3 \cdot 73$; далее по 5) свойству имеем $\left(\frac{438}{593}\right) = \left(\frac{2}{593}\right)\cdot\left(\frac{3}{593}\right)\cdot\left(\frac{73}{593}\right)$. Вычислим отдельно каждый символ правой части: $\left(\frac{2}{593}\right) = +1$, применяя

свойство 4). Для вычисления $\left(\frac{3}{593}\right)$ сначала применим закон взаимности, а затем свойство 1): $\left(\frac{3}{593}\right)=\left(\frac{593}{3}\right)=\left(\frac{2}{3}\right)=-1$ и свойство 4).

Далее по закону взаимности и по свойству 1) и 2):
$\left(\frac{73}{593}\right)=\left(\frac{593}{73}\right)=\left(\frac{9}{73}\right)=\left(\frac{3^2}{73}\right)=\left(\frac{3}{73}\right)^2=+1$. Следовательно, $\left(\frac{438}{533}\right)=+1(-1)\cdot 1=-1$.
Таким образом, сравнение $x^2 \equiv 438 \pmod{593}$ не имеет решений.

Ответ: –1.

18.6 Задача. Вычислить $\left(\frac{2023}{1231}\right)$.

Решение. Сначала приведем числитель по модулю 1231: $\left(\frac{2023}{1231}\right)=\left(\frac{792}{1231}\right)$; разложим 792 на простые множители: $792 = 2^3 \cdot 3^2 \cdot 11$;
$\left(\frac{792}{1231}\right)=\left(\frac{2^3}{1231}\right)\cdot\left(\frac{3^2}{1231}\right)\cdot\left(\frac{11}{1231}\right)=\left(\frac{2}{1231}\right)\cdot\left(\frac{11}{1231}\right)$; $\left(\frac{2^3}{1231}\right)=+1$ ибо 1231 вида $8k + 7$, ибо здесь оба числа 1231 и 11 вида $4k + 3$; далее: $\left(\frac{1231}{11}\right)=\left(\frac{-1}{11}\right)=-1$ ибо 11 вида $4k + 3$. Следовательно, $\left(\frac{792}{1231}\right)=+1$, т.е. сравнение $x^2 \equiv 792 \pmod{1231}$ имеет решения.

Ответ: +1.

19 Символ Якоби

19.1 Полезным обобщением символа Лагранжа является *символ Якоби*. Пусть P – нечетное, большее единицы, и $P = p_1 p_2 \ldots p_r$ – разложение его в простые сомножители (среди них могут быть и равные). Пусть далее НОД(a, P) = 1. Тогда символ Якоби $\left(\frac{a}{P}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\ldots\left(\frac{a}{p_r}\right)$.

19.2 Свойства символа Якоби:

1) $a \equiv a_1 \pmod{P}$, то $\left(\frac{a}{P}\right)=\left(\frac{a_1}{P}\right)$.

2) $\left(\frac{1}{P}\right)=1$.

3) $\left(\frac{-1}{P}\right)=(-1)^{\frac{P-1}{2}}$.

4) $\left(\frac{ab...l}{P}\right)=\left(\frac{a}{P}\right)\left(\frac{b}{P}\right)...\left(\frac{l}{P}\right)$.

5) $\left(\frac{2}{P}\right)=(-1)^{\frac{p^2-1}{8}}$.

6) Если P и Q – положительные нечетные взаимно простые, то $\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right)$.

19.3 Задача. Сколько решений имеет сравнение $x^2 \equiv 219 \pmod{383}$.

Решение. $\left(\frac{219}{383}\right)=-\left(\frac{383}{219}\right)=-\left(\frac{164}{219}\right)=-\left(\frac{41}{219}\right)=-\left(\frac{219}{41}\right)=$

$$-\left(\frac{14}{41}\right)=-\left(\frac{2}{41}\right)\cdot\left(\frac{7}{41}\right)=-\left(\frac{7}{41}\right)=-\left(\frac{41}{7}\right)=-\left(\frac{-1}{7}\right)=1.$$

Следовательно, рассматриваемое сравнение имеет два решения.

Ответ: 2.

20 Числа и классы чисел принадлежащие показателю

20.1.1 При НОД(a, m) = 1 существует натуральный показатель s, что $a^s \equiv 1 \pmod{m}$.

20.1.2 Пример. $a^{\varphi(m)} \equiv 1 \pmod{m}$, при НОД($a$, m) = 1.

20.2 Определение. Наименьший из натуральных s удовлетворяющих условию $a^s \equiv 1 \pmod{m}$, при НОД(a, m) = 1 называется показателем которому a принадлежит по модулю m.

20.3 Теорема. *Число a принадлежит показателю k по модулю m тогда и только тогда, когда порядок элемента $\bar{a} \in Z_m^*$ равен k.*

20.4 Следствие. Пусть a принадлежит показателю k по модулю m. Тогда:

1) Числа $a^0, a, a^2, \ldots, a^{k-1}$ попарно несравнимы по модулю m.

2) $a^s \equiv 1 \pmod{m}$ тогда и только тогда, когда $s \vdots k$. .

3) $a^s \equiv a^t \pmod{m}$ тогда и только тогда, когда $s \equiv t \pmod{k}$.

4) $\varphi(m) \vdots k$.

5) a^s принадлежит показателю $\frac{k}{\text{НОД}(k,s)}$ по модулю m.

20.5 Задача. Найти порядок числа 2 по модулю 29, т.е. $P_{29}(2)$.

Решение. Порядок любого вычета есть делитель функции Эйлера от модуля $\varphi(29) = 28$. Делители 28 следующие: 1, 2, 4, 7, 14, 28. Нам надо найти наименьшее из этих чисел, удовлетворяющее сравнению $2^x \equiv 1 \pmod{29}$. Для этого степени числа 2 последовательно заменяем абсолютно наименьшим вычетом, пока не получим вычет 1: $2^2 = 4$; $2^4 = 16 \equiv -13 \pmod{29}$.

Умножим обе части $2^3 : 2^7 \equiv -13 \cdot 2^3 \equiv 12 \pmod{29}$. Возведем обе части в квадрат: $2^{14} \equiv 144 \equiv -1 \pmod{29}$. $2^{28} \equiv 1 \pmod{29}$. Итак, $P_{29}(2) = 28$.

Ответ: $P_{29}(2) = 28$.

21 Первообразные корни

21.1.1 Определение. Число принадлежащее показателю $\varphi(m)$ называется первообразующим корнем по модулю m.

21.1.2 Пример. При m =13, $\varphi(m) = 12$. Число 2 первообразующий корень по модулю 13.

21.1.3 Пример. При m =8. Имеем $1^1 \equiv 1 \pmod{8}$; $3^2 \equiv 1 \pmod{8}$; $5^2 \equiv 1 \pmod{8}$; $7^2 \equiv 1 \pmod{8}$. Таким образом по модулю 8 нет первообразных корней.

21.2 Теорема. *Число a является первообразным корнем по модулю m тогда и только тогда, когда группа* Z_p^* *циклическая с образующей* $\bar{a}$.

21.3 Теорема. *По любому простому модулю p существуют первообразные корни, число их равно* $\varphi(p-1)$.

21.4 Замечание. Первообразные корни существуют не для всякого модуля m, лишь для $m = 2, 4, p^k, 2p^k$ (p – простое нечетное число).

21.5 Задача. Найти все первообразные корни по модулю $p = 13$.

Решение. Число $p - 1 = 12$ имеет 6 натуральных делителей 1, 2, 3, 4, 5, 6. $\varphi(1) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(6) = 2$, $\varphi(12) = 1$. Числа 2, 6, 7, 11 являются первообразными корнями по модулю 13. Число 12 имеет порядок 2, число 3 – порядок 3, число 5 – порядок 5, число 8 – порядок 4, числа 4, 10 – порядок 6, число 1 – порядок 1.

22 Индексы по простому модулю

22.1 Поскольку Z_p^* циклическая группа с $\bar{g}$ образующей, то для любого $\bar{a} \in Z_p^*$ существует показатель s, что $\bar{a} = \bar{g}^s$, $s = ind_g a$. Иными словами $a \equiv g^s \pmod{p}$.

22.2 Определение. Пусть g первообразный корень по модулю p и $a \equiv g^s \pmod{p}$. Тогда s называется индексом числа a по модулю p и основанию g.

22.3 Обозначение $s = ind_g a$. Отсюда $a = g^{ind_g a} \pmod{p}$.

22.4 Следует иметь в виду, что индекс определяется не однозначно.

22.5 Задача. Составить таблицу индексов по модулю 29 с основанием 2 (2 – первообразный корень по модулю 2).

Решение. Вычислим последовательно наименьшие отрицательные вычеты всех степеней числа 2 от 2^0 до 2^{27} по модулю 29. Так как 2 есть

первообразный корень по простому числу 29, то эти вычеты пробегают все натуральные числа от 1 до 28 в каком-то порядке. При прочтении справа налево будут получены индексы всех классов вычетов, взаимно простых с модулем:

$2^0 \equiv 1 \pmod{29}$, $2^7 \equiv 12 \pmod{29}$,
$2^1 \equiv 2 \pmod{29}$, $2^8 \equiv 24 \pmod{29}$,
$2^2 \equiv 4 \pmod{29}$, $2^9 \equiv 19 \pmod{29}$,
$2^3 \equiv 8 \pmod{29}$, $2^{10} \equiv 9 \pmod{29}$,
$2^4 \equiv 16 \pmod{29}$, $2^{11} \equiv 18 \pmod{29}$,
$2^5 \equiv 3 \pmod{29}$, $2^{12} \equiv 7 \pmod{29}$,
$2^6 \equiv 6 \pmod{29}$, $2^{13} \equiv 14 \pmod{29}$,

$2^{14} \equiv 28 \pmod{29}$, $2^{21} \equiv 46 \equiv 17 \pmod{29}$,
$2^{15} \equiv 14 \equiv 27 \pmod{29}$, $2^{22} \equiv 34 \equiv 5 \pmod{29}$,
$2^{16} \equiv 54 \equiv 25 \pmod{29}$, $2^{23} \equiv 10 \pmod{29}$,
$2^{17} \equiv 50 \equiv 21 \pmod{29}$, $2^{24} \equiv 20 \pmod{29}$,
$2^{18} \equiv 42 \equiv 13 \pmod{29}$, $2^{25} \equiv 40 \equiv 11 \pmod{29}$,
$2^{19} \equiv 26 \pmod{29}$, $2^{26} \equiv 22 \pmod{29}$,
$2^{20} \equiv 52 \equiv 23 \pmod{29}$, $2^{27} \equiv 44 \equiv 25 \pmod{29}$,

Сведем результаты в таблицу

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\text{ind}_2 a$	0	1	5	2	22	6	12	3	10	23	25	7	18	13	27	4	21	11

19	20	21	22	23	24	25	26	27	28
9	24	17	26	20	8	16	19	15	14

Класс нуля индекса не имеет. Например $ind\ 25 \equiv 16 \pmod{28}$, $ind\ 15 \equiv 27 \pmod{28}$.

22.6 Задача. Составить таблицу антииндексов по модулю 29 с основанием 2.

Решение. Эта таблица позволяет по данному индексу находить соответствующие числа. Используя задачу 22.5 составим таблицу:

$\text{ind}_2 a$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
a	1	2	4	8	16	3	6	12	24	19	9	18	7	14	28	27	25	21

18	19	20	21	22	23	24	25	26	27
13	26	23	17	5	10	20	11	22	14

22.7 Теорема. Пусть g первообразный корень по модулю p (p – простое число).

Тогда 1) $a \equiv b \pmod{p}$ тогда и только тогда, когда 1) $ind_g a \equiv ind_g b \pmod{p-1}$.

2) $ind_g(ab) \equiv ind_g a + ind_g b (\mathrm{mod}\, p-1)$.

22.7 Следствия. 1) $ind\ 1 = 0$, так как всегда $1 \equiv g^0 (\mathrm{mod}\ p)$.

2) $ind_g(a_1 a_2 \ldots a_n) \equiv ind_g a_1 + ind_g a_2 + ind_g a_n (\mathrm{mod}\, p-1)$.

3) $ind_g a^n \equiv n\, ind_g a\ (\mathrm{mod}\, p-1)$.

4) $ind_g \frac{a}{b} \equiv ind_g a - ind_g b (\mathrm{mod}\, p-1)$.

5) $ind_g a \equiv ind_g a \cdot ind_g g (\mathrm{mod}\, p-1)$.

23 Двухчленные сравнения

23.1 Определение. Двухчленное сравнение по простому модулю p называется сравнение вида $ax^n \equiv b (\mathrm{mod}\, p)$, где НОД($a$, p) = 1.

23.2 Будем считать, что $p \neq 2$.

23.3 Теорема. *Пусть* $ax^n \equiv b (\mathrm{mod}\, p)$ *и* $d = (n, p-1)$. *Если* $indb - inda$ *не делится на* d, *сравнение не имеет решения.*

Если $indb - inda$ *делится на* d, *то сравнение имеет* d *решений.*

23.4 Теорема. *Пусть* $x^n \equiv a (\mathrm{mod}\, p)$ – *двухчленное сравнение и* НОД(n, p – 1) = b (d > 0). *Сравнение имеет решение тогда и только тогда, когда* $a^{\frac{p-1}{d}} \equiv 1 (\mathrm{mod}\, p)$.

23.5 Задача. Решить сравнение $x^8 \equiv 23 (\mathrm{mod}\ 41)$.

Решение. Имеет НОД(8, 40) = 8, причем *ind*23 = 36 не делится на 8. Поэтому наше сравнение неразрешимо.

Ответ: нет решений.

23.6 Задача. Решить сравнение $x^{12} \equiv 37 (\mathrm{mod}\ 41)$.

Решение. Имеем НОД(12, 40) = 4, причем *ind*37 = 32 делится на 4. Поэтому наше сравнение разрешимо, причем это сравнение имеет 4 решения. Указанные решения найдем следующим образом. Наше сравнение равносильно таким: $12\ indx \equiv 32 (\mathrm{mod}\ 40)$, $indx \equiv 6 (\mathrm{mod}\ 10)$. Отсюда для *indx* найдем 4 несравнимых по модулю 40 значений: *indx* = 6, 16, 26, 36, соответственно чему найдем 4 решения нашего сравнения. $x \equiv 39; 18; 2; 23$ (mod 41),

Ответ: $x \equiv 39; 18; 2; 23$ (mod 41).

23.7 Задача. Решить сравнение $6x^8 \equiv 5 (\mathrm{mod}\ 13)$.

Решение. В нашем случае имеем 8*indx* = *ind*5 – *ind*6 (mod 12). Это сравнение совместно, так как НОД(8, 12) = 4 делит 4, и имеет следующие четыре решения: $indx \equiv 2, 5, 8, 11$ (mod 12). Поэтому наше сравнение имеет четыре решения: $x \equiv 4, 6, 9, 7$ (mod 13).

Ответ: $x \equiv 4, 6, 9, 7 \pmod{13}$.

23.8 Задача. При помощи индексов решить сравнение $21^{3x} \equiv 50^5 \pmod{29}$.

Решение. I способ. Индексируем сравнение: $3x ind 21 \equiv 5 ind 50 \pmod{28}$. Чтобы найти $ind 50$ заменяем 50 наименьшим неотрицательным вычетом по модулю 29, т.е. $50 \equiv 21 \pmod{29}$, $ind 50 \equiv ind 21 \equiv 17 \pmod{28}$. Тогда $3x \cdot 17 \equiv 5 \cdot 17 \pmod{28}$. Сократив на 17, найдем $3x \equiv 5 \pmod{28}$. Отсюда $x \equiv 11 \pmod{28}$. Так как по смыслу задачи x должен быть неотрицательным, то от сравнения перейдем к равенству $x = 11 + 28t$. Теперь видно, что t может быть любым неотрицательным целым.

II способ. Данное сравнение равносильно сравнению $21^{3x} \equiv 21^5 \pmod{29}$, ибо $50 \equiv 21 \pmod{29}$. Из теоремы о сравнимости степеней одного и того же числа следует, что решение последнего сравнения в точности являются неотрицательными решениями сравнения $3x \equiv 5 \pmod{\delta}$, где δ – порядок 21 по модулю 29. Для нахождения δ решим сравнение $21^y \equiv 1 \pmod{29}$. Получаем $y \cdot ind 21 \equiv ind 1 \pmod{28}$; $17y \equiv 0 \pmod{28}$; $y \equiv 0 \pmod{28}$. Максимальное неотрицательное решение есть 28, т.е. $P_{29}(21) = 28$. Получаем сравнение $3x \equiv 5 \pmod{28}$, т.е. $x \equiv 11 \pmod{28}$, $x \equiv 11 + 28t$, где $t \in N_0$.

Ответ: $x \equiv 11 + 28t$, где $t \in N_0$.

24 Обращение обыкновенной дроби в систематическую и определение длины периода систематической дроби

24.1 Определение. $a_1, a_2, \ldots, a_n, \ldots$бесконечная последовательность цифр, допускается чтобы начиная с некоторого номера все a_n равны $g - 1$. Тогда бесконечный ряд:

$$\sum_{k=1}^{\infty} \frac{a_k}{g^k} \qquad (1)$$

называется g-ичной дробью (или просто дробью).

24.2 Определение. Дробь (1) называется конечной, если начиная с некоторого номера все $a_k = 0$.

24.3 Определение. Дробь (1) называется периодической, если можно указать такие числа $t \geq 0$ и $s \geq 1$, что для любых $n > t$, $a_n = a_{n+s}$.

24.4 Задача. Записать в виде периодической дроби $\frac{1}{14}$.

Решение. $\frac{1}{14} = 0{,}07142142142\ldots = 0{,}07\,(142)$.

Ответ: $\frac{1}{14} = 0{,}07\,(142)$.

24.5 Определение. Наименьшее из таких s называется длиной периода.

24.6 Определение. Периодическая дробь называется чисто периодической, если можно принять $t = 0$ и смешенно периодической в противном случае.

24.7 Примеры. 1) $0, a_1a_2a_3a_1a_2a_3 \ldots = 0, (a_1a_2a_3)$ – чисто периодическая дробь.

2) $0, a_1a_2a_3a_4a_5a_4a_5a_4a_5 \ldots = 0, a_1a_2a_3(a_4a_5)$ смешенно периодическая дробь.

3) 0, 12121212 … = 0, (12) – чисто периодическая дробь.

4) 0, 1257343434 … = 0, 1257 (34) – смешенно периодическая дробь.

24.8 Теорема. *Всякая периодическая дробь представляет некоторое рациональное число.*

24.9 Следствие. Чисто периодическая дробь представляет рациональное число $\frac{a}{b}$ в котором НОД(b, g) = 1.

24.10 Теорема. *Пусть* $\frac{a}{b}$ *несократимая дробь и* НОД(b, g) = 1. *Тогда* $\frac{a}{b}$ *представляется чисто периодической дробью, длина периода которой равна показателю числа* g *по модулю* b.

24.11 Теорема. *Пусть* g *– фиксированное натуральное, большее единицы число. Для любого заданного положительного рационального числа* $\frac{a}{b}$ *существует число* t *и натуральные числа* c, n *такие, что* $\frac{a}{b} = g^t \cdot \frac{c}{n}$, *НОД(*$g$, n*),* $c \not\vdots g$, НОД(c, n) = 1.

При этом, если целое число t_1, *и натуральные числа* c_1 *и* n_1 *удовлетворяют условиям* $\frac{a}{b} = g^{t_1} \cdot \frac{c_1}{n_1}$, НОД($g$, n_1) = 1, $c_1 \not\vdots g$, НОД(c_1, n_1) = 1, *то* $t = t_1$, $c = c_1$ *и* $n = n_1$.

24.12 Теорема. *Пусть* $\frac{a}{b}$ *несократимая дробь и* НОД(b, g) = 1. *Пусть* t *– наименьшее положительное число удовлетворяющее условию в несократимой дроби:* $\frac{a_1}{b_1} = \frac{a}{b} g^t$, *где* НОД($b_1$, g) = 1. *Тогда* $\frac{a}{b}$ *представляется смешенно периодической дробью с* t *– цифрами между запятой и первым периодом (предпериод), а длина периода дроби* $\frac{a}{b}$ *равна показателю числа* g *по модулю* b_1.

24.13 Задача. Определить длину периода и предпериода при обращении $\frac{1}{12}$ в g-ичную систематическую дробь при $g = 10$.

Решение. При $g = 10 = 2 \cdot 5$ и $12 = 2^2 \cdot 3$, и длины предпериода равна

2 (максимальный показатель 2 или 5 в каноническом разложении знаменателя несократимой дроби, т.е. 12). Длина периода равна $P_3(10)$, где 3 – максимальный делитель знаменателя, взаимно простой с основанием счисления. Так как $P_3(10) = 1$, то в периоде одна цифра. В самом деле, $\frac{1}{12}=0,08(3)$.

Ответ: длина предпериода 2, а периода 1.

24.14 Задача. Определить длину периода и предпериода при обращении $\frac{1}{12}$ в g-ичную систематическую дробь при $g = 14$.

Решение. При $g = 14 = 2 \cdot 7$, $12 = 2^2 \cdot 3$ максимальный делитель знаменателя, взаимно простой с g, опять 3, т.е. $P_3(14) = 2$ есть длина периода. Длина предпериода находится как минимальное n из условия $g^n \vdots d$, где d – частное от деления знаменателя на его наибольший делитель, взаимно простой с основанием счисления, т.е. $\frac{12}{3}=4=d; 14^n \vdots 4$ верно уже при $n = 2$. Итак, предпериод тоже содержит 2 цифры. Можно проверить, что $\frac{1}{12}=0,12(49)_{14}$.

Ответ: длина предпериода равна 2, длина периода равна 2.

24.15 Задача. Определить длину периода и предпериода при обращении $\frac{1}{12}$ в g-ичную систематическую дробь при $g = 35$.

Решение. Имеем $12 = 2^2 \cdot 3$ и $g = 35 = 5 \cdot 7$. При НОД(12, 35) =1 следует, что дробь получится чисто периодической с длиной периода $P_{12}(35) = 2$. Можно проверить, что $\frac{1}{12}=0,(2(32))_{35}$, где (32) – цифра в 35-ричной системе счисления.

Ответ: $\frac{1}{12}=0,(2(32))_{35}$.

24.16 Задача. В позиционной системе счисления с основанием $g < 20$ дробь $\frac{1}{12}$ обращается в конечную систематическую дробь. Определить g и соответствующую систематическую дробь.

Решение. Так как $12 = 2^2 \cdot 3$, то из условия конечности систематической дроби получаем: $g \vdots 2$, $g \vdots 3$, т.е. g кратно 6. Так как $g < 20$, то $g = 6, 12, 18$. При $g = 6$ уже $g^2 \vdots 12$, т.е. $\frac{1}{12}=\frac{6^2}{12\cdot 6^2}=0,03_6$. При $g = 12$ получаем

$\frac{1}{12} = 0{,}1_{12}$. При $g = 18$ имеем $g^2 \vdots 12$, т.е. $\frac{1}{12} = \frac{18^2}{12 \cdot 18^2} = \frac{27}{18^2} = \frac{19_{18}}{100_{18}} = 0{,}19_{18}$.

Ответ: $\frac{1}{12} = 0{,}03_6$; $\frac{1}{12} = 0{,}1_{12}$; $\frac{1}{12} = 0{,}19_{18}$.

25 Другие применения теории сравнений

25.1 Шифрование с открытым ключом. Наука о шифровании – криптография – в течение многих веков служила людям для передачи секретных сообщений. Были придуманы десятки разных шифров, с помощью которых отправитель, знающий способ шифровки, мог закодировать свое сообщение, а получатель, знающий способ дешифровки, мог это сообщение раскодировать и прочитать. Как правило, все эти способы основывались на понятии «секретного» (или закрытого) ключа, т.е. опирались сведения, известные только отправителю или получатель, но не постороннему человеку. Стойкость шифров определялось тем, какое время могло понадобиться постороннему для его вскрытия, то есть для того, чтобы суметь раскодировать и прочитать сообщение, не зная поначалу секретного ключа. Во все времена случались проколы, в результате которых секреты оказались раскрытыми, а обладание секретами противника давало ощутимый перевес и в военных действиях, и в мирной дипломатии.

Опишем один из способов ассиметричного шифрования, основанный на теории чисел. Пусть p – простое число, а e – число, взаимно простое с $p - 1$. Если P – «исходное сообщение» – натуральное число, меньшее p, то ему можно сопоставить «шифрованное сообщение» – число C, равное остатку от деления P^e на p: $C \equiv P^e \pmod p$. Таким образом, для шифрования нужно знать только два числа – p и e.

Теперь разберемся с дешифрованием. По алгоритму Евклида, существует число $d < p$, для которого

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

Вычислим C^d по модулю p: $C^d \equiv P^{ed} \equiv P^{ed} \pmod p$ (в последнем сравнении использована МТФ). Таким образом, дешифрование сообщения C состоит в вычислении остатка от деления C^d на p. Тот, кто знает p и d, сможет прочитать любое сообщение, закодированное этим шрифтом. Асимметричность шифрования здесь проявляется в том, что человек, знающий ключ шифрования, не сможет тем не менее расшифровать чужие сообщения, зашифрованные с этим же ключом, а человек, знающий ключ для дешифровки, не сможет ничего зашифровать. Впрочем, вычисление d по известному p и e (равно как и вычисление e по известному p и d) не является сложной задачей, так как надежность такой системы невелика.

Однако во второй половине XX века появились действительно надежные системы шифрования с публичным (открытым) ключом, то есть такие, для которых способ шифрования не нужно держать в секрете, – обладание общеизвестным ключом шифрования позволяет любому написать и зашифровать сообщение, но не позволяет расшифровать и прочитать сообщения, написанные другими. Эти системы также были основаны на некоторых фактах из теории чисел.

Метод RSA (названный по первым буквам фамилий авторов[2]) основан на следующим: Пусть $m = pg -$ составное число, равное произведению *двух больших*[3] простых чисел p и g. Зная эти числа мы можем вычислить

$$\varphi(m) = (p-1)(g-1).$$

Выберем произвольное число e, взаимно простое с $\varphi(m)$. Открытым ключом является пара (p, m). Как и раньше, шифровании сообщения P состоит в вычислении остатка от деления P^e на m: $C \equiv (\mathrm{mod}\, m)$, $0 < C < m$. Однако знание открытого ключа не позволяет никому самостоятельно вычислить ни множители p и g, ни значение $\varphi(m)$. Мы же, зная $\varphi(m)$, можем вычислить такое d, для которого $de \equiv 1 (\mathrm{mod}\, \varphi(m))$, и с его помощью расшифровать полученное сообщение C: $P = C^d = P^{ed} (\mathrm{mod}\, m)$ (здесь использована теорема Эйлера).

Еще раз поясним, почему этот способ считается надежным. Ключ дешифрования состоит из чисел m и d. Число m известно (является частью открытого ключа), но число d держится в секрете. Если предположить, что злоумышленник вычислил d, то он будет знать

$$de - 1 (\mathrm{mod}\, m) \equiv \varphi(m),$$

а так как $\varphi(m) = m - p - g + 1$, то это, в свою очередь, даст ему сумму $p + g$. Зная сумму двух простых чисел и их произведение, он сможет найти эти числа, то есть разложить число m на простые множители. Надежность (стойкость) системы RSA основана на том, что разложение большого составного числа на два (также больших) простых множителя требует очень значительных вычислительных ресурсов.

25.2 Задача. Найдите ключ дешифровки d для системы асимметричного шифрования, если известно, что p = 2017, e =13.

---

[2] Большая часть работ XX века по криптографии до сих пор засекречена. Поэтому имена первооткрывателей алгоритмов криптографии не всегда известны. Это, разумеется, не умаляет заслуг тех ученых, которые переоткрыли их и сделали свои работы достоянием общественности.

[3] Слово «больших» здесь означает буквально следующее: если число m известно, должно быть затруднительно разложить его на множители за разумное время даже на мощной вычислительной технике. Поскольку это свойство, очевидно, зависит от мощности вычислительной техники, величина чисел, используемых для кодирования RSA, также от нее зависит. Тем не менее, так как убедиться в простоте числа проще, чем отыскать разложение составного числа на множители, фактически алгоритм RSA основан на том, что всегда будут существовать такие пары чисел, простоту которых мы проверим еще можем, а вот найти разложение на множители их произведения, не зная заранее этих множителей, уже на можем

Решение. Нужно решить уравнение $13d \equiv 1 \pmod{2016}$. Это можно сделать даже не раскладывая 2016 на множители – с помощью алгоритма Евклида для пары чисел НОД(2016, 13). Собственно, поскольку 2016 = 13 ·155 + 1, имеет $13 \cdot 155 \equiv -1 \pmod{2016}$ и, следовательно,

$$13 \cdot (2016 - 155) \equiv 1 \pmod{2016}.$$

Ответ: $d = 1861$.

25.3 Задача. Сгенерируйте ключи RSA по следующим исходным данным: $p = 3557$, $g = 2579$, $e = 3$.

Ответ: $m = pg = 9173503$, $\varphi(m) = (p-1)(g-1) = 9167368$, $de \equiv 1 / e \pmod{\varphi(m)} = 6111579$ (последнее вычисление делается с помощью алгоритма Евклида).

25.4 Задача. Протокол Диффи–Хеллмана служит для того, чтобы создавать секретные ключи, пользуясь открытыми (общедоступными, незащищенными, иначе говоря, ненадежными) каналами связи. Пусть Алиса и Боб[4] знают два простых числа – p и g. Эти числа[5] не секретны, они могут быть известны кому угодно. Чтобы создать общий и неизвестный более никому секретный ключ, Алиса сама генерирует большое случайное число a, а Боб – большое случайное число b. Затем Алиса вычисляет значение $A \equiv g^a \pmod{p}$ и пересылает его Бобу, а Боб вычисляет $B \equiv g^b \pmod{p}$ и пересылает Алисе. Числа A и B называются *открытыми ключами*, потому что предполагается, что пересылка происходит по открытому каналу связи, то есть злоумышленник может перехватить оба этих значения. Затем Алиса на основе имеющегося у нее закрытого ключа a и полученного открытого ключа B вычисляет значение $B^a \pmod{p}$, а Боб аналогично вычисляет $A^b \pmod{p}$. Докажите, что у Алисы и Боба получается одно и то же число. Объясните, почему это число действительно является секретным для всех остальных.

Решение. Полученное число – это $K \equiv g^{ab} \pmod{p}$. Злоумышленник при этом знает, что оно является какой-то степенью известного ему числа A по известному модулю p и какой-то другой степенью известного ему числа B по модулю p, однако такие степени в результате могут давать любые остатки.

Комментарий. Задача вычисления ключа K по известным A и B называется задачей дискретного логарифмирования и считается трудноразрешимой. В статье Википедии «Discrete logarithm records» приведены текущие достижения в решении этой задачи.

[4] Традиционные имена персонажей криптографических протоколов. Впервые появились в работе Р. Ривеста в 1978 году.

[5] Для повышения надежности число p выбирают очень большим и дополнительно требуют, чтобы (p – 1)/2 также было простым числом. От числа g ничего такого не требуется, поэтому, чаще всего используются простые числа первого десятка.

25.5 Задача. Придумайте, как расшифровать протокол Диффи–Хеллмана на трех участников – Алису, Бобо и Чарли.

Указание. В итоге у всех должен оказаться ключ, равный g^a, g^b, g^c, g^{ab}, g^{ac}, g^{bc} (mod p), но это не даст ему никакого знания об общем секретном ключе.

25.6.1 Вечный календарь. Обозначим число в месяце буквой g, а день недели буквой h. Пронумеруем дни недели числами от 0 (суббота) до 6 (пятница). Месяцы обозначим m и пронумеруем от 3 (март) до 14 (феарвль), причем *будем относить январь и февраль к предыдущему году*. Номер года (обозначим его Y) разделим на 100 с остатком: B^a (mod p) = $100J + K$.

25.6.2 Задача. Докажите, что для вычисления дня недели в григорианском календаре можно использовать *сравнение Зеллера*:

$$h \equiv g + [13(m + 1)/5] + K + [K/4] + [J/4] - 2J \pmod 7.$$

25.6.3 Задача. Докажите, что в юлианском календаре[6] аналогичное сравнение имеет вид

$$h \equiv g + [13(m + 1)/5] + K + [K/4] + 5 - J \pmod 7.$$

25.7.1 Организация турниров по круговой системе. Во многих игровых видах спорта (например, в шахматах и футболе) одна игра – это соревнование между двумя участниками, поэтому естественно возникает задача организации турниров для многих участников по круговой системе, то есть таких, чтобы в результате проведения нескольких последовательных туров каждый игрок (или команда) сыграл с каждым из остальных ровно один раз и при этом в турах не было большего числа свободных от игры участников.

Разумеется, если общее число участников нечетно, то в каждом туре хотя бы один из них вынужден отдыхать. Проще всего обеспечить это следующим способом: добавим одного «виртуального» участника, после чего общее количество участников станет четным, а свободном от игры в каждом туре объявим того, кто в этом туре должен играть против виртуального участника.

Таким образом, достаточно разобраться со случаем четного числа участников (команд). Перенумеруем их числами от 1 до N и составим расписание игр по следующей схеме: команды с номерами i, j, отличными от N, играют между собой в туре с номером $(i + j) \bmod (N - 1)$. Далее, существует ровно одна команда, номер которой удовлетворяет условию $2i \equiv k \pmod{N - 1}$. Именно эту команду в k-м туре назначим играть против команды N.

[6] Юлианский календарь («старый стиль») отличается от григорианского («нового стиля») тем, что все годы, номера которых заканчиваются на 00, являются високосными. В григорианском календаре из годов, номера которых заканчиваются на 00, високосным является только каждый четвертый. В частности 2000 год был високосным, а 2100, 2200 и 2300 – не будут. Сейчас юлианский календарь отстает от григорианского на 13 дней.

25.7.2 Задача. Докажите, что если туры 1, 2, …, $N - 1$ устроены описанным выше образом, то каждая команда играет с каждой из остальных ровно один раз.

25.7.3 Задача. Постройте расписание кругового турнира для 5 команд.

25.7.4 Задача. Пусть кроме расписание игр, мы должны выбрать, какой из игроков проводит игру «дома», а какой «на выезде». Сделаем это следующим образом: если $i + j$ нечетно, то «дома» играет игрок с меньшим номером, а если $i + j$ четно – то с большим. Докажите, что при четном числе туров (то есть при нечетном n) такое расписание обеспечивает, что каждый игрок проводит «дома» и «на выезде» поровну игр.

25.8.1 Контрольные цифры. Задача. Международный стандарт книжной нумерации (ISBN-10) задает 10-значный код для каждой книги, в котором 10-й знак вычисляется по правилу $a_{10} = a_1 + 2a_2 + \ldots + 9a_9 \pmod{11}$. (Если результат оказывается равным 10, то вместо цифры на месте a_{10} пишут букву X).

а) При печати ISBN-10 две соседних цифры были переставлены. Докажите, что полученный таким образом код будет некорректным.

б) При печати ISBN-10 в одной из цифр была допущена ошибка. Докажите, что полученный код также будет некорректным.

25.8.2 Задача. Международный стандарт нумерации музыкальных произведений (ISMN) задает 13-значный код, в котором 13-й знак вычисляется так, чтобы контрольная сумма

$$a_1 + 3a_2 + a_3 + 3a_4 + \ldots a_{11} + 3a_{12} + a_{13}$$

делилось на 10. Аналогичным образом, только с 11 знаками вместо 13, устроен Universal Product Code – всем нам хорошо известный штрих-код на товарах. Докажите, что оба этих кода не обладают ни одним из свойств ISMN, доказанных в задаче Г1, пункты б) и в).

25.8.3 Задача. Номер лицевого счета для собственников квартир в Санкт-Петербурге – 9-значное число, в котором контрольная цифра стоит на последнем месте и определяется по следующему алгоритму: каждая цифра умножается на 2 в степени номера позиции (начиная с конца). Остаток от деления на 11 суммы произведений затем вычитается из 11. Если результат больше 9, то результат принимается равным 0. Например, для номера 12345678 контрольная цифра равна 8: $11 - ((8 \cdot 2^1 + 7 \cdot 2^2 + 6 \cdot 2^3 + 5 \cdot 2^4 + 4 \cdot 2^5 + 3 \cdot 2^6 + 2 \cdot 2^7 + 1 \cdot 2^8) \bmod 11) = 8$. Хорош ли этот алгоритм с точки зрения чувствительности к ошибкам?

26 Вопросы

1. Отношение делимости в кольце целых чисел.
2. Деление с остатком.
3. Наибольший общий делитель. Алгоритм Евклида.
4. Основные свойства наибольшего общего делителя.
5. Взаимно простые числа.
6. Наименьшее общее кратное.
7. Конечные цепные дроби.
8. Простые числа.
9. Разложение на простые множители.
10. Делимость целых чисел, разложенных на простые множители.
11. Числовые функции.
12. Целые систематические числа.
13. Арифметические операции над целыми систематическими числами.
14. Кольцо целых Гауссовых чисел.
15. Кольцо целых Гауссовых чисел. Свойства Евклидовых колец.
16. Определение и простейшие свойства сравнений.
17. Признаки делимости.
18. Полная система вычетов.
19. Аддитивная группа классов вычетов.
20. Кольцо классов вычетов.
21. Приведенная система вычетов.
22. Мультипликативная группа классов вычетов, взаимно простых с модулем.
23. Функция Эйлера.
24. Теорема Эйлера, Ферма, Вильсона и формула Гаусса.
25. Сравнение с одним неизвестным.
26. Линейные сравнения с одним неизвестным.
27. Способы решения линейных сравнений.
28. Применение цепных дробей к решению неопределенных уравнений первой степени с двумя переменными.
29. Системы сравнений первой степени.
30. Сравнения высших степеней по простому модулю.
31. Сравнение любой степени по составному модулю.
32. Квадратичные вычеты.
33. Символ Лежандра.
34. Символ Якоби.
35. Числа и классы чисел принадлежащие показателю.
36. Первообразные корни.
37. Индексы по простому модулю.
38. Двухчленные сравнения.
39. Обращение обыкновенной дроби в систематическую и определение длины периода систематической дроби.
40. Другие приложения теоремы сравнений.

27 Задачи

Пусть $n \in \square$. Найдите последние два цифры две цифры десятичной записи числа a и остаток от деления числа b на m.

1. $a = 5^{40}$, $b = 48^{5n+3}$, $m = 11$.
2. $a = 6^{32}$, $b = 48^{5n+4}$, $m = 11$.
3. $a = 8^{18}$, $b = 7 \cdot 3^{3n+1} - 2^{3n+1}$, $m = 19$.
4. $a = 3^{12}$, $b = 25 \cdot 7^{2n} + 2^{3n+1}$, $m = 41$.
5. $a = 2^{33}$, $b = 11 \cdot 3^{5n} + 2^{2n+1} \cdot 13^{2n+1}$, $m = 37$.
6. $a = 4^{20}$, $b = 75^{6n+7}$, $m = 13$.
7. $a = 2^{78}$, $b = 40^{3n+3}$, $m = 19$
8. $a = 3^{63}$, $b = 128^{6n+7}$, $m = 9$.
9. $a = 5^{37}$, $b = 88^{9n+5}$, $m = 9$.
10. $a = 6^{47}$, $b = 104^{8n+3}$, $m = 7$.
11. $a = 8^{39}$, $b = 261^{3n+5}$, $m = 7$.
12. $a = 4^{48}$, $b = 108^{3n+1}$, $m = 7$.
13. $a = 2^{56}$, $b = 130^{10n+3}$, $m = 11$.
14. $a = 3^{73}$, $b = 180^{5n+2}$, $m = 11$.
15. $a = 7^{32}$, $b = 36^{20n+3}$, $m = 11$.

Укажите полную систему неотрицательных вычетов и полную систему наименьших по абсолютной величине вычетов по модулю m.

16. $m = 5$.
17. $m = 8$.
18. $m = 11$.
19. $m = 14$.
20. $m = 17$.
21. $m = 6$.
22. $m = 9$.
23. $m = 12$.
24. $m = 9$.
25. $m = 18$.
26. $m = 7$.
27. $m = 10$.
28. $m = 13$.
29. $m = 16$.
30. $m = 19$.

Составьте из чисел, кратных p, полную систему вычетов по модулю m.

31. $m = 11$, $p = 3$.
32. $m = 14$, $p = 3$.
33. $m = 6$, $p = 5$.
34. $m = 13$, $p = 8$.
35. $m = 13$, $p = 7$.
36. $m = 12$, $p = 7$.
37. $m = 15$, $p = 7$.
38. $m = 14$, $p = 5$.
39. $m = 12$, $p = 5$.
40. $m = 10$, $p = 7$.
41. $m = 9$, $p = 4$.
42. $m = 15$, $p = 4$.
43. $m = 17$, $p = 6$.
44. $m = 13$, $p = 5$.
45. $m = 11$, $p = 6$.

В аддитивной группе кольца $\mathbb{Z}_m$ найдите порядки всех элементов. Для каждого элемента укажите противоположный.

46. m =16.
47. m = 21.
48. m = 15.
49. m = 11.
50. m = 18.
51. m = 20.
52. m = 13.
53. m = 14.
54. m = 22.
55. m = 12.
56. m = 19.
57. m = 17.
58. m = 10.
59. m = 14.
60. m = 24.

В кольце $\mathbb{Z}_m$ перечислите обратимые элементы и делители нуля. Для каждого обратимого элемента укажите обратный.

61. m =12.
62. m =14.
63. m =28.
64. m =18.
65. m =36.
66. m =10.
67. m =15.
68. m =30.
69. m =20.
70. m =42.
71. m =21.
72. m =27.
73. m =16.
74. m =26.
75. m = 22.

Найдите все идемпотентны в кольце $\mathbb{Z}_m$.

76. m = 1183.
77. m = 147.
78. m = 845.
79. m = 867.
80. m = 1083.
81. m = 507.
82. m = 245.
83. m = 847.
84. m = 637.
85. m = 275.
86. m = 605.
87. m =363.
88. m = 539.
89. m = 175.
90. m = 325.

Найдите все нильпотентные элементы в кольце $\mathbb{Z}_m$.

91. m = 147.
92. m = 136.
93. m = 220.
94. m = 650.
95. m = 900.
96. m = 224.
97. m = 441.
98. m = 490.
99. m = 882.
100. m = 440.
101. m = 448.
102. m = 550.
103. m = 726.
104. m = 408.
105. m = 980.

Найдите порядки всех обратимых элементов в $\mathbb{Z}_m$. Является ли циклической мультипликативная группа $\mathbb{Z}_m$?

106. m = 22.
107. m = 20.
108. m = 24.
109. m = 28.
110. m = 10.
111. m = 18.
112. m = 12.
113. m = 27.
114. m = 36.
115. m = 30.
116. m = 21.
117. m = 26.
118. m = 42.
119. m = 15.
120. m = 16.

Найдите значение $t \in \square_m$ при которых отношение корней уравнения равно k.

121. $2x^2 + (t - 10)x + 6 = 0$, $m = 5$. $k = 13$.
122. $x^2 + tx + 7 = 0$, $m = 19$. $k = 6$.
123. $x^2 + (t + 1)x + 30 = 0$, $m = 7$. $k = 4$.
124. $x^2 + 6x + t = 0$, $m = 11$. $k = 9$.
125. $3x^2 - 18x + t + 1 = 0$, $m = 11$. $k = 13$.
126. $x^2 - (t + 3)6 + 1 = 0$, $m = 5$. $k = 24$.
127. $x^2 - 4x + 2t = 0$, $m = 7$. $k = 5$.
128. $x^2 + 3tx + 3 = 0$, $m = 11$. $k = 9$.
129. $x^2 + 2x + t - 2 = 0$, $m = 7$. $k = 9$.
130. $x^2 + (t - 6)x + 8 = 0$, $m = 7$. $k = 4$.
131. $x^2 - 8x - t = 0$, $m = 13$. $k = 10$.
132. $x^2 + 2tx + 2 = 0$, $m = 13$. $k = 5$.
133. $x^2 - 4x - t - 1 = 0$, $m = 11$. $k = 8$.
134. $x^2 + (t + 3) - 1 = 0$, $m = 7$. $k = 3$.
135. $2x^2 - x + t = 0$, $m = 7$. $k = 3$.

Даны числа a_1, a_2, …, a_{m-1}. Найти такое натуральное число a_m, $a_m \le m$, чтобы числа a_1, … a_m составили полную систему вычетов по модулю m.

136. $a_1 = 3$, $a_2 = -14$, $a_3 = -1$, $a_4 = 100$,
137. $a_1 = 6$, $a_2 = 7$, $a_3 = -12$, $a_4 = -101$,
138. $a_1 = 41$, $a_2 = -50$, $a_3 = -13$, $a_4 = -21$,
139. $a_1 = 61$, $a_2 = 82$, $a_3 = -72$, $a_4 = -34$,
140. $a_1 = 100$, $a_2 = 102$, $a_3 = 104$, $a_4 = 101$,
141. $a_1 = -87$, $a_2 = -78$, $a_3 = 51$, $a_4 = -51$,
142. $a_1 = 25$, $a_2 = -34$, $a_3 = 33$, $a_4 = 76$, $a_5 = -37$,
143. $a_1 = -12$, $a_2 = 43$, $a_3 = 56$, $a_4 = -33$, $a_5 = 48$,
144. $a_1 = 241$, $a_2 = -242$, $a_3 = 15$, $a_4 = 150$, $a_5 = -82$,
145. $a_1 = 11$, $a_2 = 12$, $a_3 = 14$, $a_4 = 75$, $a_5 = 22$,
146. $a_1 = 101$, $a_2 = 102$, $a_3 = 103$, $a_4 = 104$, $a_5 = 105$,
147. $a_1 = -1$, $a_2 = -2$, $a_3 = -3$, $a_4 = -4$, $a_5 = -5$,
148. $a_1 = 102$, $a_2 = 115$, $a_3 = 128$, $a_4 = -7$, $a_5 = -123$,
149. $a_1 = 1$, $a_2 = -22$, $a_3 = 57$, $a_4 = -38$, $a_5 = -31$,
150. $a_1 = -7$, $a_2 = -50$, $a_3 = 30$, $a_4 = 80$, $a_5 = 60$, $a_6 = 40$,
151. $a_1 = 35$, $a_2 = -36$, $a_3 = 44$, $a_4 = -44$, $a_5 = 71$, $a_6 = 18$,
152. $a_1 = 105$, $a_2 = 1$, $a_3 = -46$, $a_4 = -8$, $a_5 = 48$,
153. $a_1 = 109$, $a_2 = -35$, $a_3 = -65$, $a_4 = 15$, $a_5 = -4$, $a_6 = 51$,
154. $a_1 = -77$, $a_2 = -8$, $a_3 = -47$, $a_4 = -60$, $a_5 = -10$, $a_6 = -30$, $a_7 = -51$,

155. $a_1 = -7$, $a_2 = 43$, $a_3 = 71$, $a_4 = 38$, $a_5 = 109$, $a_6 = -6$, $a_7 = -16$,
156. $a_1 = -71$, $a_2 = -69$, $a_3 = -45$, $a_4 = -4$, $a_5 = 5$, $a_6 = -70$,
157. $a_1 = 18$, $a_2 = -12$, $a_3 = 64$, $a_4 = -5$, $a_5 = 29$, $a_6 = -23$, $a_7 = -42$,
158. $a_1 = 0$, $a_2 = 1$, $a_3 = 2$, $a_4 = 3$, $a_5 = 214$, $a_6 = -129$, $a_7 = -68$,
159. $a_1 = -7$, $a_2 = 10$, $a_3 = -20$, $a_4 = 30$, $a_5 = 55$, $a_6 = -59$,
160. $a_1 = 107$, $a_2 = -50$, $a_3 = 39$, $a_4 = -60$, $a_5 = 44$,

Найти такое натуральное число $a_n < m$, чтобы числа $a_1, \ldots, a_n$ составили приведенную систему вычетов по модулю m.

161. $m = 13$, $a_1 = -101$, $a_2 = 121$, $a_3 = 31$, $a_4 = 422$, $a_5 = 14$, $a_6 = 61$ $a_7 = 50$, $a_8 = -31$, $a_9 = 23$, $a_{10} = 25$, $a_{11} = 20$.
162. $m = 16$, $a_1 = -11$, $a_2 = 23$, $a_3 = 43$, $a_4 = -65$, $a_5 = 45$, $a_6 = -63$ $a_7 = 115$.
163. $m = 20$, $a_1 = -39$, $a_2 = -83$, $a_3 = 23$, $a_4 = -127$, $a_5 = 107$, $a_6 = 9$ $a_7 = -29$.
164. $m = 15$, $a_1 = 37$, $a_2 = -22$, $a_3 = -146$, $a_4 = -119$, $a_5 = 44$, $a_6 = 77$ $a_7 = 26$.
165. $m = 16$, $a_1 = 105$, $a_2 = -95$, $a_3 = 123$, $a_4 = -61$, $a_5 = -19$, $a_6 = 85$ $a_7 = 167$.
166. $m = 22$, $a_1 = 65$, $a_2 = 41$, $a_3 = 25$, $a_4 = -17$, $a_5 = -29$, $a_6 = 45$ $a_7 = -97$, $a_8 = -103$, $a_9 = 31$.
167. $m = 20$, $a_1 = 37$, $a_2 = -7$, $a_3 = 31$, $a_4 = -71$, $a_5 = -39$, $a_6 = -93$ $a_7 = 103$.
168. $m = 14$, $a_1 = 25$, $a_2 = -13$, $a_3 = 17$, $a_4 = 33$, $a_5 = 23$.
169. $m = 15$, $a_1 = 164$, $a_2 = -43$, $a_3 = 49$, $a_4 = 28$, $a_5 = -64$, $a_6 = -38$ $a_7 = 31$.
170. $m = 8$, $a_1 = 11$, $a_2 = 13$, $a_3 = 23$, $a_4 = 79$, $a_5 = -116$.
171. $m = 16$, $a_1 = -47$, $a_2 = 117$, $a_3 = -51$, $a_4 = -25$, $a_5 = 89$, $a_6 = -37$ $a_7 = 31$.
172. $m = 20$, $a_1 = 81$, $a_2 = 111$, $a_3 = -27$, $a_4 = -193$, $a_5 = 139$, $a_6 = -71$ $a_7 = 23$.
173. $m = 11$, $a_1 = -9$, $a_2 = 116$, $a_3 = 122$, $a_4 = 19$, $a_5 = -41$, $a_6 = 5$ $a_7 = -51$, $a_8 = -46$, $a_9 = 87$.
174. $m = 14$, $a_1 = -29$, $a_2 = 145$, $a_3 = -97$, $a_4 = 53$, $a_5 = -109$.
175. $m = 16$, $a_1 = 43$, $a_2 = -1$, $a_3 = -109$, $a_4 = 17$, $a_5 = -43$, $a_6 = -55$ $a_7 = 77$.
176. $m = 22$, $a_1 = 23$, $a_2 = -17$, $a_3 = -201$, $a_4 = 31$, $a_5 = -103$, $a_6 = 77$ $a_7 = -51$, $a_8 = 39$, $a_9 = -23$.
177. $m = 15$, $a_1 = 122$, $a_2 = 23$, $a_3 = -14$, $a_4 = 43$, $a_5 = -41$, $a_6 = -109$ $a_7 = 37$.
178. $m = 16$, $a_1 = -1$, $a_2 = -21$, $a_3 = 273$, $a_4 = -103$, $a_5 = -77$, $a_6 = 39$ $a_7 = 21$.

179. $m = 20$, $a_1 = -11$, $a_2 = -13$, $a_3 = 3$, $a_4 = -49$, $a_5 = 101$, $a_6 = -87$ $a_7 = 219$.

180. $m = 14$, $a_1 = -25$, $a_2 = -57$, $a_3 = 79$, $a_4 = -41$, $a_5 = -73$.

181. $m = 16$, $a_1 = -37$, $a_2 = -41$, $a_3 = 49$, $a_4 = -33$, $a_5 = 163$, $a_6 = -151$ $a_7 = 29$.

182. $m = 13$, $a_1 = 27$, $a_2 = -11$, $a_3 = 42$, $a_4 = -9$, $a_5 = 31$, $a_6 = -20$ $a_7 = 46$, $a_8 = 731$, $a_9 = 179$, $a_{10} = 48$, $a_{11} = 103$.

183. $m = 13$, $a_1 = 1$, $a_2 = -1$, $a_3 = 2$, $a_4 = -2$, $a_5 = 3$, $a_6 = -3$ $a_7 = 4$, $a_8 = -4$, $a_9 = 5$, $a_{10} = -5$, $a_{11} = 6$.

184. $m = 15$, $a_1 = 62$, $a_2 = -94$, $a_3 = -83$, $a_4 = -46$, $a_5 = 79$, $a_6 = 68$ $a_7 = 43$.

185. $m = 13$, $a_1 = -46$, $a_2 = 62$, $a_3 = -83$, $a_4 = 69$, $a_5 = 93$, $a_6 = 90$ $a_7 = 7$, $a_8 = -49$, $a_9 = -21$, $a_{10} = 66$, $a_{11} = 35$.

Найти значения функции Эйлера от числа a:

186. $a = 121$.
187. $a = 137$.
188. $a = 141$.
189. $a = 157$.
190. $a = 168$.
191. $a = 202$.
192. $a = 222$.
193. $a = 278$.
194. $a = 486$.
195. $a = 341$.
196. $a = 356$.
197. $a = 380$.
198. $a = 399$.
199. $a = 432$.
200. $a = 468$.
201. $a = 528$.
202. $a = 621$.
203. $a = 725$.
204. $a = 901$.
205. $a = 845$.
206. $a = 768$.
207. $a = 697$.
208. $a = 648$.
209. $a = 578$
210. $a = 535$

Решить уравнение $\varphi(P^x) = a$:

211. $a = 500$, $P = 5$.
212. $a = 2500$, $P = 5$.
213. $a = 12500$, $P = 5$.
214. $a = 18$, $P = 3$.
215. $a = 541$, $P = 3$.
216. $a = 162$, $P = 3$.
217. $a = 486$, $P = 3$.
218. $a = 4374$, $P = 3$.
219. $a = 67240$, $P = 41$.
220. $a = 13122$, $P = 3$.
221. $a = 500$, $P = 5$.
222. $a = 294$, $P = 7$.
223. $a = 14406$, $P = 7$.
224. $a = 1210$, $P = 11$
225. $a = 2028$, $P = 13$.
226. $a = 4624$, $P = 17$.
227. $a = 6498$, $P = 19$.
228. $a = 11638$, $P = 23$.
229. $a = 23548$, $P = 29$.
230. $a = 28830$, $P = 31$.
231. $a = 49284$, $P = 37$.
232. $a = 13310$, $P = 11$.
233. $a = 26364$, $P = 13$.
234. $a = 12500$, $P = 5$.
235. $a = 123462$, $P = 19$.

Решить уравнение $\varphi(x)=a$, $x = P^{\alpha}$

236. a = 4970.
237. a = 64.
238. a = 54.
239. a = 930.
240. a = 42.
241. a = 128.
242. a = 1640.
243. a = 162.
244. a = 110.
245. a = 256.
246. a = 812.
247. a = 1806.
248. a = 8.
249. a = 512.
250. a = 156.
251. a = 3422.
252. a = 294.
253. a = 32.
254. a = 272.
255. a = 3660.
256. a = 506.
257. a = 100.
258. a = 342.
259. a = 15.
260. a = 2756.

Найти остаток от деления числа a^m на число b:

261. a = 126, m = 201, b = 67.
262. a = 401, m = 206, b = 31.
263. a = 221, m = 102, b = 42.
264. a = 843, m = 326, b = 68.
265. a = 297, m = 79, b = 70.
266. a = 262, m = 114, b = 51.
267. a = 311, m = 465, b = 50.
268. a = 257, m = 182, b = 45.
269. a = 257, m = 191, b = 61.
270. a = 229, m = 127, b = 143.
271. a = 187, m = 88, b = 43.
272. a = 383, m = 175, b = 45.
273. a = 478, m = 113, b = 27.
274. a = 217, m = 348, b = 66.
275. a = 137, m = 113, b = 45.
276. a = 337, m = 169, b = 83.
277. a = 239, m = 149, b = 74.
278. a = 271, m = 261, b = 85.
279. a = 199, m = 125, b = 45.
280. a = 225, m = 111, b = 53.
281. a = 343, m = 101, b = 64.
282. a = 231, m = 148, b = 104.
283. a = 292, m = 150, b = 95.
284. a = 426, m = 101, b = 105.
285. a = 280, m = 183, b = 77.

Найти остаток от деления a^m на число b:

286. $a = 444$, $m = 144$, $b = 44$.
287. $a = 102$, $m = 151$, $b = 74$.
288. $a = 365$, $m = 62$, $b = 95$.
289. $a = 400$, $m = 52$, $b = 68$.
290. $a = 195$, $m = 197$, $b = 85$.
291. $a = 190$, $m = 281$, $b = 42$.
292. $a = 345$, $m = 147$, $b = 33$.
293. $a = 539$, $m = 60$, $b = 99$.
294. $a = 333$, $m = 152$, $b = 39$.
295. $a = 445$, $m = 66$, $b = 65$.
296. $a = 231$, $m = 52$, $b = 69$.
297. $a = 25$, $m = 2004$, $b = 55$.
298. $a = 88$, $m = 183$, $b = 209$.
299. $a = 206$, $m = 127$, $b = 66$.
300. $a = 180$, $m = 106$, $b = 106$.
301. $a = 91$, $m = 125$, $b = 385$.
302. $a = 57$, $m = 674$, $b = 192$.
303. $a = 44$, $m = 126$, $b = 100$.
304. $a = 135$, $m = 41$, $b = 39$.
305. $a = 50$, $m = 111$, $b = 74$.
306. $a = 50$, $m = 155$, $b = 78$.
307. $a = 147$, $m = 155$, $b = 117$.
308. $a = 98$, $m = 147$, $b = 78$.
309. $a = 90$, $m = 123$, $b = 82$.
310. $a = 126$, $m = 87$, $b = 86$.

Найти три последние цифры a^6:

311. $a = 221$, $b = 201$.
312. $a = 241$, $b = 301$.
313. $a = 517$, $b = 201$.
314. $a = 327$, $b = 301$.
315. $a = 277$, $b = 501$.
316. $a = 601$, $b = 601$.
317. $a = 289$, $b = 601$.
318. $a = 301$, $b = 301$.
319. $a = 387$, $b = 201$.
320. $a = 399$, $b = 201$.
321. $a = 401$, $b = 301$.
322. $a = 461$, $b = 201$.
323. $a = 497$, $b = 501$.
324. $a = 501$, $b = 501$.
325. $a = 537$, $b = 601$.
326. $a = 317$, $b = 501$.
327. $a = 279$, $b = 101$.
328. $a = 419$, $b = 201$.
329. $a = 819$, $b = 301$.
330. $a = 717$, $b = 501$.
331. $a = 317$, $b = 601$.
332. $a = 403$, $b = 201$.
333. $a = 517$, $b = 101$.
334. $a = 313$, $b = 101$.
335. $a = 113$, $b = 301$.
336. $a = 105$, $b = 101$.
337. $a = 126$, $b = 203$.
338. $a = 135$, $b = 301$.
339. $a = 262$, $b = 104$.
340. $a = 206$, $b = 205$.

341. $a = 325$, $b = 101$.
342. $a = 435$, $b = 101$.
343. $a = 425$, $b = 301$.
344. $a = 475$, $b = 401$.
345. $a = 485$, $b = 101$.
346. $a = 345$, $b = 101$.
347. $a = 385$, $b = 101$.
348. $a = 485$, $b = 301$.
349. $a = 165$, $b = 103$.
350. $a = 385$, $b = 102$.
351. $a = 595$, $b = 202$.
352. $a = 42$, $b = 103$.
353. $a = 286$, $b = 203$.
354. $a = 42$, $b = 204$.
355. $a = 568$, $b = 101$.
356. $a = 66$, $b = 202$.
357. $a = 78$, $b = 203$.
358. $a = 154$, $b = 203$.
359. $a = 182$, $b = 203$.
360. $a = 28$, $b = 303$.

Решите сравнения.

361. $3x \equiv 1 \pmod 7$, $15x \equiv 9 \pmod{11}$, $42x \equiv 12 \pmod{90}$.
362. $5x \equiv 9 \pmod 6$, $29x \equiv 15 \pmod{19}$, $55x \equiv 35 \pmod{75}$
363. $13x \equiv 20 \pmod 4$, $6x \equiv 22 \pmod{13}$, $42x \equiv 12 \pmod{90}$.
364. $16x \equiv -6 \pmod 9$, $14x \equiv -9 \pmod{17}$, $25x \equiv 45 \pmod{60}$.
365. $17x \equiv -30 \pmod 9$, $9x \equiv -8 \pmod{23}$, $21x \equiv 7 \pmod{49}$.
366. $5x \equiv 7 \pmod 8$, $10x \equiv 15 \pmod{17}$, $10x \equiv 25 \pmod{35}$.
367. $7x \equiv 6 \pmod{15}$, $18x \equiv 12 \pmod{19}$, $10x \equiv 12 \pmod{14}$.
368. $27x \equiv -14 \pmod{25}$, $2x \equiv 14 \pmod{23}$, $26x \equiv 2 \pmod{30}$.
369. $13x \equiv 10 \pmod{11}$, $24x \equiv 16 \pmod{25}$, $15x \equiv 21 \pmod{24}$.
370. $5x \equiv -2 \pmod{11}$, $15x \equiv 10 \pmod{19}$, $10x \equiv 14 \pmod{22}$.
371. $4x \equiv 7 \pmod{17}$, $14x \equiv 35 \pmod{37}$, $15x \equiv 25 \pmod{35}$.
372. $2x \equiv 5 \pmod 8$, $22x \equiv 33 \pmod{39}$, $12x \equiv 21 \pmod{27}$.
373. $5x \equiv 6 \pmod 7$, $21x \equiv 35 \pmod{37}$, $10x \equiv -4 \pmod{22}$.
374. $3x \equiv -8 \pmod{13}$, $26x \equiv 39 \pmod{41}$, $14x \equiv 12 \pmod{30}$.
375. $3x \equiv -7 \pmod{11}$, $15x \equiv 20 \pmod{23}$,

$16x \equiv 28 \pmod{36}$.

Решите сравнение первой степени.

376. $114x \equiv 42 \pmod{87}$.
377. $39x \equiv 84 \pmod{93}$.
378. $111x \equiv 81 \pmod{447}$.
379. $186x \equiv 374 \pmod{442}$.
380. $375x \equiv 196 \pmod{501}$.
381. $129x \equiv 321 \pmod{471}$.
382. $117x \equiv 168 \pmod{186}$.
383. $132x \equiv 147 \pmod{189}$.
384. $112x \equiv 140 \pmod{252}$.
385. $176x \equiv 196 \pmod{252}$.
386. $273x \equiv 161 \pmod{343}$.
387. $294x \equiv 131 \pmod{450}$.
388. $210x \equiv 180 \pmod{270}$.
389. $195x \equiv 147 \pmod{264}$.
390. $126x \equiv 210 \pmod{147}$.

Решить сравнение:

391. $48x \equiv 32 \pmod{115}$.
392. $131x \equiv 82 \pmod{64}$.
393. $60x \equiv 90 \pmod{203}$.
394. $125x \equiv 187 \pmod{312}$.
395. $131x \equiv 218 \pmod{136}$.
396. $66x \equiv 99 \pmod{199}$.
397. $113x \equiv 64 \pmod{312}$.
398. $427x \equiv 181 \pmod{300}$.
399. $40x \equiv 100 \pmod{363}$.
400. $20x \equiv 50 \pmod{91}$.
401. $131x \equiv 72 \pmod{70}$.
402. $23x \equiv 667 \pmod{963}$.
403. $271x \equiv 25 \pmod{119}$.
404. $113x \equiv 89 \pmod{311}$.
405. $221x \equiv 111 \pmod{360}$.
406. $48x \equiv 24 \pmod{125}$.
407. $54x \equiv 81 \pmod{125}$.
408. $80x \equiv 40 \pmod{231}$.
409. $80x \equiv 100 \pmod{121}$.
410. $78x \equiv 26 \pmod{101}$.
411. $41x \equiv 16 \pmod{37}$.

412. $60x \equiv 90 \pmod{103}$.
413. $58x \equiv 80 \pmod{111}$.
414. $35x \equiv 23 \pmod{72}$.
415. $67x \equiv 64 \pmod{183}$.

Решить сравнения:

416. $164x \equiv 68 \pmod{176}$.
417. $138x \equiv 42 \pmod{76}$.
418. $200x \equiv 104 \pmod{312}$.
419. $78x \equiv 42 \pmod{51}$.
420. $114x \equiv 42 \pmod{87}$.
421. $543x \equiv 93 \pmod{582}$.
422. $291x \equiv 99 \pmod{597}$.
423. $303x \equiv 93 \pmod{600}$.
424. $39x \equiv 84 \pmod{93}$.
425. $128x \equiv 84 \pmod{126}$.
426. $114x \equiv 52 \pmod{110}$.
427. $324x \equiv 88 \pmod{250}$.
428. $200x \equiv 208 \pmod{612}$.
429. $145x \equiv 390 \pmod{250}$.
430. $219x \equiv 120 \pmod{375}$.
431. $273x \equiv 99 \pmod{303}$.
432. $88x \equiv 40 \pmod{366}$.
433. $116x \equiv 174 \pmod{222}$.
434. $172x \equiv 28 \pmod{200}$.
435. $186x \equiv 30 \pmod{360}$.
436. $145x \equiv 80 \pmod{500}$.
437. $303x \equiv 78 \pmod{363}$.
438. $130x \equiv 100 \pmod{200}$.
439. $172x \equiv 92 \pmod{350}$.
440. $49x \equiv 56 \pmod{133}$.
441. $546x \equiv 36 \pmod{600}$.
442. $88x \equiv 55 \pmod{121}$.
443. $184x \equiv 56 \pmod{320}$.
444. $260x \equiv 68 \pmod{308}$.
445. $115x \equiv 95 \pmod{150}$.
446. $63x \equiv 39 \pmod{480}$.
447. $104x \equiv 156 \pmod{486}$.
448. $165x \equiv 21 \pmod{312}$.
449. $100x \equiv 80 \pmod{168}$.
450. $465x \equiv 65 \pmod{605}$.
451. $230x \equiv 200 \pmod{285}$.
452. $172x \equiv 28 \pmod{200}$.
453. $172x \equiv 24 \pmod{254}$.
454. $201x \equiv 48 \pmod{183}$.
455. $124x \equiv 88 \pmod{160}$.
456. $129x \equiv 321 \pmod{471}$.
457. $115x \equiv 85 \pmod{355}$.
458. $386x \equiv 32 \pmod{570}$.
459. $230x \equiv 190 \pmod{300}$.
460. $203x \equiv 91 \pmod{280}$.
461. $85x \equiv 45 \pmod{225}$.
462. $452x \equiv 68 \pmod{488}$.
463. $82x \equiv 110 \pmod{130}$.
464. $201x \equiv 39 \pmod{261}$.
465. $200x \equiv 64 \pmod{328}$.

Решите уравнение в кольце $\mathbb{Z}_m$.

466. $\overline{2}x^3 - \overline{3}x^2 + \overline{2}x - \overline{1} = \overline{0}$, $m = 7$.
467. $x^4 - \overline{4}x^2 + \overline{2} = \overline{0}$, $m = 5$.
468. $x^3 - \overline{2}x^2 + x - \overline{1} = \overline{0}$, $m = 3$.
469. $\overline{4}x^4 + x^2 + \overline{2}x + \overline{2} = \overline{0}$, $m = 5$.
470. $x^3 + \overline{5}x^2 - \overline{15}x + \overline{22} = \overline{0}$, $m = 7$.
471. $\overline{5}x^4 + x^2 - x + \overline{2} = \overline{0}$, $m = 7$.

472. $\overline{3}x^4+\overline{2}x^2-\overline{1}=\overline{0}$, $m=7$.

473. $\overline{7}x^3-\overline{5}x+\overline{1}=\overline{0}$, $m=13$.

474. $\overline{4}x^3-\overline{7}x^2+\overline{10}=\overline{0}$, $m=11$.

475. $\overline{2}x^4-\overline{5}x+\overline{3}=\overline{0}$, $m=6$.

476. $\overline{3}x^3+\overline{2}x^2-\overline{2}=\overline{0}$, $m=5$.

477. $\overline{5}x^3+\overline{3}x+\overline{3}=\overline{0}$, $m=7$.

478. $\overline{4}x^3+\overline{7}x-\overline{1}=\overline{0}$, $m=8$.

479. $\overline{4}x^4+\overline{3}x^2+\overline{2}=\overline{0}$, $m=6$.

480. $\overline{2}x^3-\overline{7}x+\overline{3}=\overline{0}$, $m=5$.

Решите уравнение в кольце $\mathbb{Z}_m$.

481. $\overline{132}x^3+\overline{143}x^2+\overline{23}x-\overline{19}=\overline{5}$, $m=11$.

482. $\overline{117}x^3+\overline{143}x^2+\overline{3}x-\overline{19}=\overline{5}$, $m=13$.

483. $\overline{153}x^3+\overline{187}x^2+\overline{11}x-\overline{9}=\overline{5}$, $m=17$.

484. $\overline{361}x^3+\overline{209}x^2+\overline{23}x-\overline{11}=\overline{5}$, $m=19$.

485. $\overline{253}x^3+\overline{115}x^2+\overline{12}x-\overline{9}=\overline{5}$, $m=23$.

486. $\overline{164}x^3-\overline{205}x^2+\overline{26}x-\overline{30}=\overline{9}$, $m=41$.

487. $\overline{273}x^3+\overline{195}x^2+\overline{22}x-\overline{22}=\overline{11}$, $m=39$.

488. $\overline{289}x^3-\overline{272}x^2+\overline{10}x-\overline{10}=\overline{5}$, $m=17$.

489. $\overline{342}x^3-\overline{228}x^2+\overline{18}x-\overline{18}=-\overline{6}$, $m=19$.

490. $\overline{437}x^3-\overline{184}x^2+\overline{21}x-\overline{21}=-\overline{7}$, $m=23$.

491. $\overline{225}x^3+\overline{325}x^2+\overline{24}x-\overline{16}=\overline{0}$, $m=25$.

492. $\overline{152}x^3-\overline{323}x^2+\overline{15}x-\overline{15}=-\overline{5}$, $m=19$.

493. $\overline{444}x^3+\overline{333}x^2+\overline{14}x-\overline{36}=\overline{0}$, $m=37$.

494. $\overline{228}x^3-\overline{304}x^2+\overline{29}x-\overline{10}=\overline{5}$, $m=19$.

495. $\overline{529}x^3+\overline{437}x^2+\overline{9}x-\overline{9}=-\overline{17}$, $m=23$.

Найдите все целочисленные решения уравнения.

496. $10x-15y=25$, $6x+10y+15z=7$.

497. $14x+21y=-49$, $4x-6y+11z=7$.

498. $12x-8y=-24$, $6x+10y-7z=7$.

499. $15x-18y=21$, $-7x+4y+9z=19$.

500. $22x+4y=-16$, $5x+12y+8z=14$.

501. $39x - 22y = 10$, $10x - 6y + 13z = 8$.
502. $17x - 25y = 117$, $7x - 4y + 8z = 11$.
503. $53x + 47y = 11$, $5x + 3y - 6z = 12$.
504. $43x + 37y = 21$, $6x + 5y - 3z = 7$.
505. $17x - 16y = 31$, $-3x + 7y + 6z = 15$.
506. $23x + 15y = 19$, $3x + 6y - 5z = 11$.
507. $12x - 37y = -3$, $11x - 3y + 6z = -5$.
508. $18x - 31y = 26$, $4x + 3y + 7z = -10$.
509. $11x + 16y = 156$, $-7x + 5y + 12z = 3$.
510. $45x - 37y = 25$, $3x - 7y + 2z = 5$.

Решить уравнения в целых числах.

511. $6x + 10y = 42$.
512. $4x + 5y = 60$.
513. $15x + 20y = 100$.
514. $6x + 7y = 43$.
515. $4x + 12y = 36$.
516. $7x + 8y = 115$.
517. $14x + 6y = 52$.
518. $2x + 5y = 33$.
519. $2x + 9y = 43$.
520. $6x + 8y = 86$.
521. $3x + 5y = 72$.
522. $2x + 9y = 43$.
523. $10x + 25y = 150$.
524. $6x + 10y = 42$.
525. $5x + 10y = 95$.
526. $9x + 15y = 105$.
527. $12x + 21y = 99$.
528. $6x + 16y = 92$.
529. $4x + 9y = 73$.
530. $5x + 8y = 83$.
531. $8x + 12y = 100$.
532. $5x + 9y = 95$.
533. $2x + 10y = 72$.
534. $2x + 9y = 43$.
535. $2x + 4y = 48$.

Решить сравнение, предварительно понизив его степень.

536. $41x^{31} + 17x^{14} + 7x^2 - 3 \equiv 0 \pmod 5$.
537. $32x^{20} + 15x^{10} - 111x^4 + x - 1 \equiv 0 \pmod 7$.
538. $43x^{18} + 27x^{14} + 15x^8 + 3x^3 + 2 \equiv 0 \pmod 7$.
539. $26x^{20} + 17x^{11} + 9x^4 + 2x^2 \equiv 0 \pmod 5$.
540. $82x^{32} - 27x^{11} + 11x^5 + x^2 - 2 \equiv 0 \pmod 5$.
541. $73x^{35} + 24x^{14} + 17x^3 + 8 \equiv 0 \pmod 7$.
542. $53x^{18} + 15x^{11} + 7x^5 - 3x + 1 \equiv 0 \pmod 7$.
543. $81x^{29} + 15x^{21} + 7x^2 - 3 \equiv 0 \pmod 5$.
544. $52x^{31} + 21x^{14} + 5x^4 + x^2 - 1 \equiv 0 \pmod 7$.
545. $81x^{21} + 42x^{11} - 10x^{10} - 3 \equiv 0 \pmod 5$.
546. $42x^8 + 36x^7 - x^6 + 12x^5 + 3x^4 - x^3 + 9x^2 + 8x - 2 \equiv 0 \pmod 5$.
547. $31x^{20} + 17x^{11} + 9x^8 + 15x^7 - 6x^4 + 3x^2 + 11 \equiv 0 \pmod 5$.
548. $27x^{32} + 17x^{21} + 24x^{16} + 17x^{10} + 21x^6 + 27x^4 + 3x^2 - 1 \equiv 0 \pmod 5$.
549. $71x^{31} + 27x^{20} - 18x^{16} - 3x^8 + 12x^7 - 10x^6 + 29x^4 - 17x + 4 \equiv 0 \pmod 5$.
550. $22x^{20} - 18x^{17} + 73x^{10} - 7x^2 - 1 \equiv 0 \pmod 5$.

551. $121x^{21} + 17x^{18} - 56x^{12} - 31x^9 - 12x^5 + 7x^3 - 3 \equiv 0 \pmod 5$.

552. $26x^{21} - 17x^{15} + 29x^{11} - 18x^7 + 11 \equiv 0 \pmod 5$.

553. $27x^{25} - 19x^{20} - 72x^{15} + 23x^{12} + 16x^3 - 1 \equiv 0 \pmod 7$.

554. $31x^{37} - 29x^{21} + 29x^{15} + 3x^2 + 1 \equiv 0 \pmod 7$.

555. $19x^{31} - 17x^{14} - 3x^{13} + 16x^2 - 1 \equiv 0 \pmod 7$.

556. $24x^{20} - 16x^{16} + 20x^8 - x + 1 \equiv 0 \pmod 7$.

557. $26x^{2o} - 50x^{16} + 47x^{15} - 27x^4 - 15x^2 - 2 \equiv 0 \pmod 7$.

558. $72x^{21} + 17x^{15} - 24x^{10} - x + 3 \equiv 0 \pmod 5$.

559. $-26x^{18} + 726x^{16} - 13x^{10} + 17x^2 + 6 \equiv 0 \pmod 5$.

560. $51x^{16} + 176x^{11} - 28x^9 + 16x^2 - 2x + 1 \equiv 0 \pmod 5$.

Решите системы сравнений.

561. $\begin{cases} 7x \equiv 3 \pmod{11} \\ 3x \equiv 1 \pmod 7 \\ 3x \equiv 2 \pmod 5, \end{cases} \quad \begin{cases} x \equiv 13 \pmod{16} \\ x \equiv 3 \pmod{10} \\ x \equiv 9 \pmod{14}. \end{cases}$

562. $\begin{cases} x \equiv 1 \pmod 3 \\ 3x \equiv 5 \pmod 7 \\ 2x \equiv 3 \pmod 5, \end{cases} \quad \begin{cases} 3x \equiv 5 \pmod{10} \\ 2x \equiv 5 \pmod{15} \\ 7x \equiv 5 \pmod{13}. \end{cases}$

563. $\begin{cases} 3x \equiv 2 \pmod 7 \\ x \equiv 8 \pmod{15} \\ 2x \equiv 9 \pmod{15}, \end{cases} \quad \begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 1 \pmod{12} \\ x \equiv 7 \pmod{14}. \end{cases}$

564. $\begin{cases} 7x \equiv 10 \pmod{11} \\ 12x \equiv 7 \pmod{13} \\ 7x \equiv 11 \pmod{15}, \end{cases} \quad \begin{cases} 4x \equiv 1 \pmod 9 \\ 5x \equiv 3 \pmod 7 \\ x \equiv 5 \pmod{12}. \end{cases}$

565. $\begin{cases} 2x \equiv 1 \pmod 3 \\ 2x \equiv 2 \pmod 7 \\ 17x \equiv 7 \pmod{11}, \end{cases} \quad \begin{cases} 5x \equiv 3 \pmod 8 \\ 7x \equiv 3 \pmod{11} \\ 5x \equiv 1 \pmod 6. \end{cases}$

566. $\begin{cases} 4x \equiv 7 \pmod{13} \\ x \equiv 2 \pmod{17} \\ 5x \equiv 3 \pmod 9, \end{cases} \quad \begin{cases} x \equiv 6 \pmod{15} \\ x \equiv 18 \pmod{21} \\ x \equiv 3 \pmod{12}. \end{cases}$

567. $\begin{cases} 4x \equiv 3 \pmod 7 \\ 5x \equiv 4 \pmod{11} \\ 11x \equiv 8 \pmod{13}, \end{cases} \quad \begin{cases} x \equiv 13 \pmod{14} \\ x \equiv 6 \pmod{35} \\ x \equiv 26 \pmod{45}. \end{cases}$

568. $\begin{cases} 2x \equiv 7 \pmod{13} \\ 5x \equiv 8 \pmod{17} \\ 14x \equiv 35 \pmod{19}, \end{cases} \quad \begin{cases} x \equiv 19 \pmod{56} \\ x \equiv 3 \pmod{24} \\ x \equiv 7 \pmod{20}. \end{cases}$

569. $\begin{cases} 2x \equiv 5 \pmod{11} \\ 7x \equiv 6 \pmod{13} \\ 3x \equiv 7 \pmod{17}, \end{cases} \quad \begin{cases} x \equiv 19 \pmod{22} \\ x \equiv 8 \pmod{33} \\ x \equiv 14 \pmod{21}. \end{cases}$

570. $\begin{cases} 2x \equiv 3 \pmod{7} \\ 3x \equiv 6 \pmod{11} \\ x \equiv 2 \pmod{5}, \end{cases} \quad \begin{cases} 3x \equiv 7 \pmod{10} \\ 2x \equiv 3 \pmod{7} \\ 7x \equiv 8 \pmod{15}. \end{cases}$

571. $\begin{cases} 3x \equiv 2 \pmod{7} \\ 3x \equiv 1 \pmod{5} \\ 7x \equiv 3 \pmod{11}, \end{cases} \quad \begin{cases} 3x \equiv 1 \pmod{10} \\ 4x \equiv 3 \pmod{5} \\ 2x \equiv 7 \pmod{9}. \end{cases}$

572. $\begin{cases} 7x \equiv 7 \pmod{13} \\ 2x \equiv 1 \pmod{3} \\ 3x \equiv 2 \pmod{5}, \end{cases} \quad \begin{cases} 7x \equiv 3 \pmod{15} \\ 3x \equiv 7 \pmod{10} \\ 3x \equiv 2 \pmod{7}. \end{cases}$

573. $\begin{cases} x \equiv 2 \pmod{9} \\ 5x \equiv 3 \pmod{3} \\ 4x \equiv 7 \pmod{11}, \end{cases} \quad \begin{cases} 3x \equiv 4 \pmod{5} \\ x \equiv 3 \pmod{10} \\ 7x \equiv 2 \pmod{11}. \end{cases}$

574. $\begin{cases} 2x \equiv 7 \pmod{17} \\ 5x \equiv 3 \pmod{13} \\ 14x \equiv 12 \pmod{5}, \end{cases} \quad \begin{cases} x \equiv 5 \pmod{12} \\ x \equiv 8 \pmod{15} \\ x \equiv 3 \pmod{11}. \end{cases}$

575. $\begin{cases} 11x \equiv 5 \pmod{17} \\ 6x \equiv 1 \pmod{11} \\ 3x \equiv 4 \pmod{7}, \end{cases} \quad \begin{cases} x \equiv 3 \pmod{10} \\ x \equiv 13 \pmod{15} \\ 7x \equiv 9 \pmod{11}. \end{cases}$

Решите систему сравнений.

576. $\begin{cases} x + 2y \equiv 3 \pmod{13} \\ 4x + y \equiv 5 \pmod{13}. \end{cases}$

577. $\begin{cases} 4x - 2y \equiv 1 \pmod{13} \\ 5x - 7y \equiv 3 \pmod{13}. \end{cases}$

578. $\begin{cases} x + 2y \equiv 0 \pmod{13} \\ 3x + 2y \equiv 2 \pmod{13}. \end{cases}$

579. $\begin{cases} x-7y\equiv 12 \pmod{16} \\ 4x+3y\equiv 13 \pmod{16}. \end{cases}$

580. $\begin{cases} 5x-y\equiv 3 \pmod{16} \\ 2x+3y\equiv -1 \pmod{16}. \end{cases}$

581. $\begin{cases} 2x+3y\equiv 1 \pmod{16} \\ 3x-4y\equiv 3 \pmod{16}. \end{cases}$

582. $\begin{cases} 9x-3y\equiv 5 \pmod{14} \\ 5x+6y\equiv 3 \pmod{14}. \end{cases}$

583. $\begin{cases} 8x-3y\equiv 1 \pmod{14} \\ 2x+5y\equiv 7 \pmod{14}. \end{cases}$

584. $\begin{cases} 3x+7y\equiv 13 \pmod{14} \\ 4x-5y\equiv 12 \pmod{14}. \end{cases}$

585. $\begin{cases} 2x-y\equiv 4 \pmod{15} \\ x+5y\equiv 3 \pmod{15}. \end{cases}$

586. $\begin{cases} 5x-y\equiv 9 \pmod{15} \\ 2x+4y\equiv 7 \pmod{15}. \end{cases}$

587. $\begin{cases} x-5y\equiv 10 \pmod{15} \\ 2x-2y\equiv -3 \pmod{15}. \end{cases}$

588. $\begin{cases} 3x+y\equiv 3 \pmod{17} \\ 4x-13y\equiv 1 \pmod{17}. \end{cases}$

589. $\begin{cases} 7x+5y\equiv 12 \pmod{17} \\ 2x-7y\equiv 4 \pmod{17}. \end{cases}$

590. $\begin{cases} 6x-8y\equiv 5 \pmod{17} \\ 3x+5y\equiv 7 \pmod{17}. \end{cases}$

Найдите все числа a, делящиеся на b.

591. $a=\overline{xy9z}$, $b=132$.

592. $a=\overline{xyz4}$, $b=252$.

593. $a=\overline{7xyz}$, $b=156$.

594. $a=\overline{xy86z}$, $b=693$.

595. $a=\overline{x67yz}$, $b=264$.

596. $a=\overline{4x8yz6}$, $b=504$.

597. $a=\overline{x5y6z6}$, $b=252$.

598. $a=\overline{xyz444}$, $b=693$.

599. $a=\overline{8xyz}$, $b=154$.

600. $a=\overline{x6yz}$, $b=308$.

601. $a=\overline{x4yz}$, $b=273$.

602. $a=\overline{3x5yz}$, $b=132$.

603. $a=\overline{42xyz}$, $b=792$.

604. $a=\overline{x396yz}$, $b=168$.

605. $a=\overline{xy35z2}$, $b=231$.

В кольце $\mathbb{Z}_n$ найдите обратные к элементам a и b

606. $n = 2020$. $a = 7$, $b = 13$.

607. $n = 2019$. $a = 17$, $b = 19$.

608. $n = 2016$. $a = 23$, $b = 11$.

609. $n = 2015$. $a = 17$, $b = 23$.

610. $n = 2013$. $a = 13$, $b = 19$.

611. $n = 2012$. $a = 7$, $b = 17$.

612. $n = 2009$. $a = 17$, $b = 5$.

613. $n = 2008$. $a = 19$, $b = 5$.

614. $n = 2007$. $a = 5$, $b = 10$.

615. $n = 2005$. $a = 11$, $b = 13$.

616. $n = 2004$. $a = 7$, $b = 11$.

617. $n = 2001$. $a = 19$, $b = 25$.

618. $n = 2000$. $a = 23$, $b = 13$.

619. $n = 1996$. $a = 29$, $b = 7$.

620. $n = 1992$. $a = 7$, $b = 23$.

Решите в поле $\mathbb{Z}_p$ квадратное уравнение.

621. $x^2 - 5x + 9 = 0$. $p = 11$.

622. $x^2 + 3x + 5 = 0$. $p = 11$.

623. $x^2 - 3x + 5 = 0$. $p = 11$.

624. $2x^2 - 7x + 5 = 0$. $p = 13$.

625. $x^2 + 7x - 4 = 0$. $p = 13$.

626. $x^2 + 6x + 10 = 0$. $p = 13$.

627. $x^2 + 10x + 4 = 0$. $p = 17$.

628. $x^2 + 14x - 2 = 0$. $p = 17$.

629. $x^2 + 13x + 5 = 0$. $p = 17$.

630. $x^2 + 6x + 12 = 0$. $p = 19$.

631. $3x^2 + 5x + 17 = 0$. $p = 19$.

632. $5x^2 + 6x + 17 = 0$. $p = 19$.
633. $2x^2 + 16x + 19 = 0$. $p = 23$.
634. $3x^2 + 18x + 19 = 0$. $p = 23$.
635. $4x^2 + 20x + 13 = 0$. $p = 23$.

Проверьте, что a является корнем кубического уравнения над полем $\mathbb{Z}_p$. Найдите оставшиеся корни.

636. $x^3 + 7x + 14 = 0$, $p = 17$, $a = 6$.
637. $x^3 + 5x + 16 = 0$, $p = 17$, $a = 2$.
638. $x^3 + 11x + 12 = 0$, $p = 17$, $a = 8$.
639. $x^3 + 16x + 8 = 0$, $p = 19$, $a = 12$.
640. $x^3 + 7x + 16 = 0$, $p = 19$, $a = 10$.
641. $x^3 + 8x + 22 = 0$, $p = 19$, $a = 2$.
642. $x^3 + 7x + 18 = 0$, $p = 23$, $a = 2$.
643. $x^3 + 6x + 17 = 0$, $p = 23$, $a = 6$.
644. $x^3 + 11x + 27 = 0$, $p = 23$, $a = 12$.
645. $x^3 + 9x + 25 = 0$, $p = 29$, $a = 3$.
646. $x^3 + 15x + 23 = 0$, $p = 29$, $a = 8$.
647. $x^3 + 18x + 29 = 0$, $p = 29$, $a = 17$.
648. $x^3 + 17x + 28 = 0$, $p = 31$, $a = 10$.
649. $x^3 + 7x + 14 = 0$, $p = 31$, $a = 15$.
650. $x^3 + 5x + 30 = 0$, $p = 31$, $a = 18$.

Найдите в поле $\mathbb{Z}_p$ коэффициенты многочлена $f(x) = ax^2 + bx + c$ такого, что:

651. $f(0) = 4$, $f(1) = 2$, $f(2) = 1$, $p = 5$.
652. $f(1) = 3$, $f(2) = 4$, $f(4) = 2$, $p = 5$.
653. $f(2) = 3$, $f(3) = 4$, $f(4) = 2$, $p = 5$.
654. $f(1) = 4$, $f(2) = 1$, $f(4) = 2$, $p = 5$.
655. $f(0) = 3$, $f(2) = 2$, $f(3) = 4$, $p = 5$.
656. $f(3) = 3$, $f(4) = 5$, $f(6) = 1$, $p = 7$.
657. $f(1) = 6$, $f(3) = 2$, $f(5) = 3$, $p = 7$.
658. $f(2) = 5$, $f(4) = 1$, $f(6) = 3$, $p = 7$.
659. $f(0) = 2$, $f(3) = 6$, $f(4) = 1$, $p = 7$.
660. $f(0) = 6$, $f(1) = 5$, $f(2) = 1$, $p = 7$.
661. $f(5) = 1$, $f(7) = 2$, $f(8) = 3$, $p = 11$.
662. $f(0) = 8$, $f(2) = 10$, $f(4) = 3$, $p = 11$.
663. $f(1) = 9$, $f(2) = 4$, $f(3) = 3$, $p = 11$.
664. $f(0) = 9$, $f(1) = 4$, $f(2) = 5$, $p = 11$.
665. $f(1) = 4$, $f(2) = 3$, $f(4) = 6$, $p = 11$.

Пусть α и β – корни многочлена $f(x)$ над полем $\mathbb{Z}_p$. Найдите многочлен корнями которого являются элементы α^{-1} и β^{-1}.

666. $f(x) = 3x^2 - 5x - 6$, $p = 11$.
667. $f(x) = 2x^2 - 7x + 5$, $p = 11$.
668. $f(x) = 5x^2 - 7x - 2$, $p = 11$.
669. $f(x) = 3x^2 - 7x + 7$, $p = 13$.
670. $f(x) = 4x^2 + 9x - 3$, $p = 13$.
671. $f(x) = 3x^2 + 2x - 4$, $p = 13$.
672. $f(x) = 4x^2 - 7x + 15$, $p = 17$.
673. $f(x) = 3x^2 - 8x + 14$ $p = 17$.
674. $f(x) = 7x^2 - 4x + 15$, $p = 17$.
675. $f(x) = 7x^2 + 6x + 12$, $p = 19$.
676. $f(x) = 3x^2 + 5x + 17$, $p = 19$.
677. $f(x) = 5x^2 + 6x + 17$, $p = 19$.
678. $f(x) = 3x^2 + 14x - 11$, $p = 23$.
679. $f(x) = 5x^2 + 11x - 16$, $p = 23$.
680. $f(x) = 4x^2 + 7x - 15$, $p = 23$.

В поле $\mathbb{Z}_p$ решите уравнение $f(x) = 0$.

681. $f(x) = 16x^7 + 11x^6 - 9x^5 - 11x^3 - x - 4$, $p = 5$.
682. $f(x) = x^{10}\, 2x^3 + 1$, $p = 5$.
683. $f(x) = x^8 + x^7 + x^5 - x^4 - x + 3$, $p = 5$.
684. $f(x) = x^{16} + 3x^8 - 5x^7 - x^4 + 6x - 2$, $p = 7$.
685. $f(x) = x^{10} + x^8 + x^7 - x^4 - x^2 + 4x - 3$, $p = 5$.
686. $f(x) = 2x^{11} + 22x^9 + x^8 - 2x^5 + 6x^3 + 2x + 4$, $p = 5$.
687. $f(x) = x^{101} + 3x^{15} - x^{11} - 3x^5 + 9x^2 + 10x - 5$, $p = 5$.
688. $f(x) = 13x^{93} + x^{92} + 9x^3 + 5x + 15$, $p = 5$.
689. $f(x) = x^{45} - x^{35} + x^{22} - 22x - 23$, $p = 5$.
690. $f(x) = x^{14} - x^{13} - x^2 + 2x + 1$, $p = 5$.
691. $f(x) = 6x^{26} - x^{25} - 31x^2 + 3x + 1$, $p = 5$.
692. $f(x) = x^{15} - 2x^{14} + 28x^2 + 26x - 1$, $p = 5$.
693. $f(x) = 2x^{84} + 2x^{67} - 2x^4 + 15x^3 + 4x^2 + 18$, $p = 5$.
694. $f(x) = x^{35} + 16x^{18} - 11x^2 + 4x$, $p = 5$.
695. $f(x) = 2x^{20} + x^{19} - 2x^4 - x^3 + x^2 + 2x + 18$, $p = 5$.

В поле $\mathbb{Z}_p$ методом Крамера решение систему линейных уравнений.

696. $\begin{cases} x_1 + x_2 = 1 \\ 2x_1 + 2x_3 = 1 \\ x_1 + x_2 + 2x_3 = 1. \end{cases}$ $p = 3$.

697. $\begin{cases} 2x_1 + x_2 + x_3 = 1 \\ 2x_1 + x_2 + 2x_3 = 2 \\ 2x_1 + 2x_2 + x_3 = 0. \end{cases}$ $p = 3.$

698. $\begin{cases} x_1 + 2x_2 = 1 \\ 2x_1 + 2x_3 = 1 \\ x_1 + 2x_2 + x_3 = 2. \end{cases}$ $p = 3.$

699. $\begin{cases} x_1 + 2x_2 + 4x_3 = 1 \\ x_1 + 3x_2 + 4x_3 = 2 \\ x_1 + 4x_2 + x_3 = 3. \end{cases}$ $p = 5.$

700. $\begin{cases} x_1 + 3x_2 + x_3 = 2 \\ 3x_1 + 3x_2 + 4x_3 = 1 \\ 3x_1 + 2x_3 = 0. \end{cases}$ $p = 5.$

701. $\begin{cases} 2x_1 + 3x_2 + x_3 = 2 \\ 3x_1 + 3x_2 + 4x_3 = 3 \\ 3x_1 + x_2 + 2x_3 = 1. \end{cases}$ $p = 5.$

702. $\begin{cases} 3x_2 + 4x_3 = 1 \\ 3x_1 + x_2 + 2x_3 = 3 \\ x_1 + x_3 = 4. \end{cases}$ $p = 5.$

703. $\begin{cases} 2x_1 + 2x_2 + x_3 = 2 \\ x_1 + x_2 + 3x_3 = 1 \\ 5x_1 + 6x_2 + 2x_3 = 3. \end{cases}$ $p = 7.$

704. $\begin{cases} 3x_1 + 2x_2 + 4x_3 = 1 \\ 2x_1 + 5x_2 + 3x_3 = 1 \\ 5x_1 + 3x_2 + 2x_3 = 4. \end{cases}$ $p = 7.$

705. $\begin{cases} x_1 + 2x_2 + 5x_3 = 4 \\ 2x_1 + 5x_2 + 4x_3 = 5 \\ 3x_1 + 3x_2 + 2x_3 = 3. \end{cases}$ $p = 7.$

706. $\begin{cases} 2x_1 + 5x_2 + 6x_3 = 1 \\ 2x_1 + 3x_2 + 4x_3 = 6 \\ 3x_1 + 3x_2 + 2x_3 = 2. \end{cases}$ $p = 7.$

707. $\begin{cases} 2x_1+9x_2+6x_3=10 \\ 10x_1+3x_2+4x_3=5 \\ 3x_1+3x_2+10x_3=7. \end{cases}$ p=11.

708. $\begin{cases} 5x_1+9x_2+6x_3=1 \\ 10x_1+3x_2+7x_3=3 \\ 4x_1+3x_2+8x_3=2. \end{cases}$ p=11.

709. $\begin{cases} x_1+x_2+6x_3=7 \\ 8x_1+5x_2+x_3=6 \\ 3x_1+3x_2+x_3=1. \end{cases}$ p=11.

710. $\begin{cases} x_1+9x_2+6x_3=1 \\ 8x_1+7x_2+7x_3=2 \\ 4x_1+3x_2+5x_3=1. \end{cases}$ p=11.

Найти показатель $P_m(a)$ по модулю m:

711. $P_{31}(4)$
712. $P_{21}(5)$
713. $P_{25}(4)$
714. $P_{28}(9)$
715. $P_{18}(5)$
716. $P_{31}(6)$
717. $P_{16}(5)$
718. $P_{31}(5)$
719. $P_{48}(11)$
720. $P_{22}(5)$
721. $P_{11}(5)$
722. $P_{17}(11)$
723. $P_{32}(3)$
724. $P_{21}(11)$
725. $P_{44}(3)$
726. $P_{32}(5)$
727. $P_{32}(11)$
728. $P_{21}(10)$
729. $P_{25}(6)$
730. $P_{22}(3)$
731. $P_{25}(9)$
732. $P_{36}(9)$
733. $P_{36}(7)$
734. $P_{30}(17)$
735. $P_{48}(5)$
736. $P_{29}(3)$
737. $P_{23}(10)$
738. $P_{37}(3)$
739. $P_{25}(4)$
740. $P_{37}(2)$
741. $P_{23}(12)$
742. $P_{23}(20)$
743. $P_{31}(14)$
744. $P_{23}(14)$
745. $P_{37}(4)$
746. $P_{23}(-4)$
747. $P_{29}(4)$
748. $P_{25}(3)$
749. $P_{29}(8)$
750. $P_{23}(4)$
751. $P_{23}(15)$
752. $P_{29}(5)$
753. $P_{31}(7)$
754. $P_{35}(4)$
755. $P_{23}(-3)$
756. $P_{22}(5)$
757. $P_{23}(7)$
758. $P_{64}(3)$
759. $P_{31}(10)$
760. $P_{37}(8)$

В кольце Z_m укажите обратимые элементы и делители нуля. Для каждого из обратимых элементов найдите обратный

761. $m = 8$, 762. $m = 9$, 763. $m = 10$, 764. $m = 14$, 765. $m = 6$,
766. $m = 18$, 767. $m = 16$, 768. $m = 20$, 769. $m = 24$, 770. $m = 30$,
771. $m = 15$, 772. $m = 5$, 773. $m = 4$, 774. $m = 7$, 775. $m = 11$,
776. $m = 13$, 777. $m = 12$, 778. $m = 21$, 779. $m = 22$, 780. $m = 23$.

Вычислить символ Лежандра

781. $\left(\frac{63}{131}\right)$, **784.** $\left(\frac{29}{383}\right)$, **787.** $\left(\frac{63}{97}\right)$, **790.** $\left(\frac{245}{593}\right)$, **793.** $\left(\frac{120}{73}\right)$,

782. $\left(\frac{35}{97}\right)$, **785.** $\left(\frac{241}{593}\right)$, **788.** $\left(\frac{57}{73}\right)$, **791.** $\left(\frac{194}{131}\right)$, **794.** $\left(\frac{412}{383}\right)$,

783. $\left(\frac{47}{73}\right)$, **786.** $\left(\frac{75}{131}\right)$, **789.** $\left(\frac{310}{383}\right)$, **792.** $\left(\frac{132}{97}\right)$, **795.** $\left(\frac{834}{593}\right)$.

Вычислением символа Лежандра установить, какие из следующих сравнений разрешимы, и найти их решения.

796. $x^2 \equiv 6 \pmod 7$,
797. $x^2 \equiv 2 \pmod 5$,
798. $x^2 \equiv 3 \pmod{11}$,
799. $x^2 \equiv 12 \pmod{13}$,
800. $x^2 \equiv 10 \pmod{13}$,
801. $x^2 \equiv 5 \pmod{11}$,
802. $x^2 \equiv 13 \pmod{17}$,
803. $x^2 \equiv 4 \pmod{13}$,
804. $x^2 \equiv 5 \pmod{13}$,
805. $x^2 \equiv 7 \pmod{11}$,
806. $x^2 \equiv 11 \pmod{17}$,
807. $x^2 \equiv 3 \pmod{13}$,
808. $x^2 \equiv 7 \pmod{17}$,
809. $x^2 \equiv 5 \pmod{17}$,
810. $x^2 \equiv 12 \pmod{17}$.

Вычислить символ Якоби.

811. $\left(\frac{63}{86}\right)$,
812. $\left(\frac{63}{92}\right)$,
813. $\left(\frac{122}{75}\right)$,
814. $\left(\frac{383}{755}\right)$,
815. $\left(\frac{125}{93}\right)$,
816. $\left(\frac{17}{124}\right)$,
817. $\left(\frac{63}{107}\right)$,
818. $\left(\frac{31}{150}\right)$,

819. $\left(\frac{33}{175}\right)$,

820. $\left(\frac{175}{93}\right)$,

821. $\left(\frac{2016}{2017}\right)$,

822. $\left(\frac{2015}{2016}\right)$,

823. $\left(\frac{2002}{2016}\right)$,

824. $\left(\frac{123}{735}\right)$,

825. $\left(\frac{175}{83}\right)$.

Найти наименьший первообразный корень g, больший a, по модулю m и построить таблицу индексов по первообразному корню g и модулю m:

826. $m = 13,\ a = 4$
827. $m = 13,\ a = 9$
828. $m = 17,\ a = 3$
829. $m = 17,\ a = 8$
830. $m = 17,\ a = 12$
831. $m = 19,\ a = 8$
832. $m = 19\ \ a = 11$
833. $m = 23,\ a = 5$
834. $m = 23,\ a = 8$
835. $m = 23,\ a = 12$
836. $m = 23,\ a = 15$
837. $m = 23,\ a = 17$
838. $m = 29,\ a = 6$
839. $m = 29,\ a = 8$
840. $m = 29,\ a = 12$
841. $m = 29,\ a = 16$
842. $m = 29,\ a = 19$
843. $m = 29,\ a = 24$
844. $m = 31,\ a = 8$
845. $m = 31,\ a = 15$
846. $m = 31,\ a = 19$
847. $m = 31,\ a = 22$
848. $m = 37,\ a = 3$
849. $m = 37,\ a = 11$
850. $m = 37,\ a = 13$

С помощью таблицы индексов для простого числа решить сравнение вида $ax^k \equiv b\ (mod\ p)$:

851. $5x^5 \equiv 10(mod\ 17)$
852. $15x^7 \equiv 9(mod\ 17)$
853. $11x^9 \equiv 9(mod\ 17)$
854. $6x^5 \equiv 2(mod\ 19)$
855. $2x^7 \equiv 12(mod\ 19)$
856. $16x^{11} \equiv 11(mod\ 19)$
857. $11x^7 \equiv 5(mod\ 23)$
858. $19x^9 \equiv 12(mod\ 23)$
859. $18x^5 \equiv 9(mod\ 23)$
860. $16x^5 \equiv 2(mod\ 29)$
861. $7x^9 \equiv 9(mod\ 29)$
862. $4x^{11} \equiv 13(mod\ 29)$
863. $19x^7 \equiv 9(mod\ 31)$
864. $9x^{11} \equiv 26(mod\ 31)$
865. $27x^{13} \equiv 20(mod\ 31)$
866. $17x^5 \equiv 2(mod\ 37)$
867. $15x^5 \equiv 4(mod\ 37)$
868. $31x^5 \equiv 2mod\ 37)$
869. $6x^5 \equiv 11(mod\ 41)$
870. $36x^5 \equiv 26(mod\ 41)$
871. $11x^5 \equiv 34(mod\ 41)$
872. $34x^5 \equiv 3(mod\ 43)$
873. $9x^5 \equiv 26(mod\ 43)$
874. $3x^{11} \equiv 27(mod\ 43)$

875. $11x^5 \equiv 5(mod\ 47)$
876. $11x^{13} \equiv 15(mod\ 43)$
877. $15x^{11} \equiv 52(mod\ 59)$
878. $17x^5 \equiv 13(mod\ 47)$
879. $13x^{17} \equiv 28(mod\ 73)$
880. $11x^5 \equiv 28(mod\ 59)$
881. $24x^9 \equiv 21(mod\ 47)$
882. $13x^{23} \equiv 45(mod\ 59)$
883. $53x^{11} \equiv 72(mod\ 83)$
884. $15x^{31} \equiv 11(mod\ 59$
885. $73x^{13} \equiv 15(mod\ 89)$
886. $61x^{23} \equiv 21(mod\ 71)$
887. $73x^{29} \equiv 15(mod\ 79)$
888. $23x^{41} \equiv 17(mod\ 53)$
889. $37x^{13} \equiv 71(mod\ 97)$
890. $24x^{23} \equiv 45(mod\ 67)$
891. $32x^7 \equiv 5(mod\ 37)$
892. $61x^{17} \equiv 73(mod\ 97)$
893. $24x^{11} \equiv 35(mod\ 53)$
894. $45x^{23} \equiv 15(mod\ 71)$
895. $63x^{31} \equiv 18(mod\ 73)$
896. $25x^{17} \equiv 42(mod\ 59)$
897. $44x^{23} \equiv 51(mod\ 59)$
898. $34x^{17} \equiv 41(mod\ 71)$
899. $61x^{16} \equiv 15(mod\ 43)$
900. $38x^{17} \equiv 49(mod\ 61)$

С помощью таблицы индексов для простого числа p решить сравнения вида $a^x \equiv b(mod\ p)$:

901. $2^x \equiv 13(mod\ 67)$
902. $3^x \equiv 19(mod\ 79)$
903. $2^x \equiv 71(mod\ 83)$
904. $3^x \equiv 41(mod\ 89)$
905. $2^x \equiv 31(mod\ 61)$
906. $2^x \equiv 17(mod\ 59)$
907. $3^x \equiv 15(mod\ 43)$
908. $3^x \equiv 18(mod\ 29)$
909. $2^x \equiv 15(mod\ 53)$
910. $27^x \equiv 4(mod\ 17)$
911. $2^x \equiv 43(mod\ 59)$
912. $3^x \equiv 18(mod\ 43)$
913. $2^x \equiv 51(mod\ 67)$
914. $3^x \equiv 71(mod\ 89)$
915. $2^x \equiv 24(mod\ 67)$
916. $13^x \equiv 12(mod\ 19)$
917. $2^x \equiv 43(mod\ 53)$
918. $3^x \equiv 14(mod\ 31)$
919. $2^x \equiv 45(mod\ 59)$
920. $3^x \equiv 24(mod\ 89)$
921. $2^x \equiv 23(mod\ 67)$
922. $3^x \equiv 41(mod\ 43)$
923. $2^x \equiv 18(mod\ 67)$
924. $3^x \equiv 47(mod\ 89)$
925. $2^x \equiv 38(mod\ 61)$.

С помощью таблицы индексов для простого числа p решить сравнения вида $ax \equiv b(mod\ p)$:

926. $36x \equiv 25(mod\ 71)$
927. $17x \equiv 16(mod\ 71)$
928. $19x \equiv 40(mod\ 71)$
929. $38x \equiv 14(mod\ 67)$
930. $25x \equiv 23(mod\ 67)$
931. $51x \equiv 9(mod\ 67)$
932. $57x \equiv 37(mod\ 59)$
933. $33x \equiv 20(mod\ 59)$
934. $23x \equiv 4(mod\ 59)$
935. $41x \equiv 33(mod\ 79)$
936. $28x \equiv 35(mod\ 79)$
937. $17x \equiv 60(mod\ 73)$
938. $59x \equiv 23(mod\ 73)$
939. $65x \equiv 33(mod\ 83)$
940. $37x \equiv 57(mod\ 83)$
941. $16x \equiv 56(mod\ 89)$
942. $32x \equiv 67(mod\ 89)$
943. $42x \equiv 6(mod\ 59)$

944. $50x \equiv 29(mod\ 59)$
945. $16x \equiv 30(mod\ 59)$
946. $43x \equiv 5(mod\ 53)$
947. $35x \equiv 29(mod\ 53)$
948. $36x \equiv 4(mod\ 47)$
949. $37x \equiv 35(mod\ 47)$
950. $39x \equiv 14(mod\ 47)$

Дано рациональное число $\frac{a}{b}$, которое требуется записать в виде g-ичной дроби, а) будет ли полученная дробь конечной или бесконечной; б) если полученная дробь бесконечная, то найти длину периода и число цифр между запятой и началом первого периода; в) записать число $\frac{a}{b}$ в виде g-ичной дроби; г) сделать проверку, обратив g-ичную дробь в рациональное число.

951. $\frac{a}{b} = \frac{3}{8}$ $g = 4$
952. $\frac{a}{b} = \frac{5}{9}$ $g = 6$
953. $\frac{a}{b} = \frac{7}{9}$ $g = 3$
954. $\frac{a}{b} = \frac{12}{25}$ $g = 5$
955. $\frac{a}{b} = \frac{33}{49}$ $g = 7$
956. $\frac{a}{b} = \frac{28}{81}$ $g = 9$
957. $\frac{a}{b} = \frac{11}{28}$ $g = 14$
958. $\frac{a}{b} = \frac{7}{16}$ $g = 4$
959. $\frac{a}{b} = \frac{5}{18}$ $g = 6$
960. $\frac{a}{b} = \frac{9}{25}$ $g = 5$
961. $\frac{a}{b} = \frac{5}{8}$ $g = 6$
962. $\frac{a}{b} = \frac{11}{32}$ $g = 8$
963. $\frac{a}{b} = \frac{11}{18}$ $g = 6$
964. $\frac{a}{b} = \frac{31}{54}$ $g = 6$
965. $\frac{a}{b} = \frac{11}{24}$ $g = 6$
966. $\frac{a}{b} = \frac{3}{4}$ $g = 6$
967. $\frac{a}{b} = \frac{5}{27}$ $g = 9$
968. $\frac{a}{b} = \frac{17}{32}$ $g = 8$
969. $\frac{a}{b} = \frac{11}{36}$ $g = 6$
970. $\frac{a}{b} = \frac{46}{121}$ $g = 11$
971. $\frac{a}{b} = \frac{13}{24}$ $g = 6$
972. $\frac{a}{b} = \frac{5}{9}$ $g = 3$
973. $\frac{a}{b} = \frac{4}{9}$ $g = 6$
974. $\frac{a}{b} = \frac{7}{16}$ $g = 8$
975. $\frac{a}{b} = \frac{17}{18}$ $g = 6$
976. $\frac{a}{b} = \frac{5}{7}$ $g = 6$

977. $\frac{a}{b}=\frac{3}{5}$ $g=4$

978. $\frac{a}{b}=\frac{3}{7}$ $g=6$

979. $\frac{a}{b}=\frac{8}{13}$ $g=12$

980. $\frac{a}{b}=\frac{2}{5}$ $g=9$

981. $\frac{a}{b}=\frac{2}{3}$ $g=8$

982. $\frac{a}{b}=\frac{5}{6}$ $g=11$

983. $\frac{a}{b}=\frac{6}{7}$ $g=11$

984. $\frac{a}{b}=\frac{5}{8}$ $g=7$

985. $\frac{a}{b}=\frac{3}{5}$ $g=4$

986. $\frac{a}{b}=\frac{4}{7}$ $g=6$

987. $\frac{a}{b}=\frac{7}{9}$ $g=8$

988. $\frac{a}{b}=\frac{3}{7}$ $g=9$

989. $\frac{a}{b}=\frac{2}{3}$ $g=5$

990. $\frac{a}{b}=\frac{2}{7}$ $g=9$

991. $\frac{a}{b}=\frac{7}{8}$ $g=3$

992. $\frac{a}{b}=\frac{4}{9}$ $g=7$

993. $\frac{a}{b}=\frac{3}{19}$ $g=11$

994. $\frac{a}{b}=\frac{3}{13}$ $g=9$

995. $\frac{a}{b}=\frac{5}{12}$ $g=11$

996. $\frac{a}{b}=\frac{5}{14}$ $g=9$

997. $\frac{a}{b}=\frac{5}{12}$ $g=7$

998. $\frac{a}{b}=\frac{5}{7}$ $g=9$

999. $\frac{a}{b}=\frac{3}{8}$ $g=7$

1000. $\frac{a}{b}=\frac{3}{7}$ $g=4$

1001. $\frac{a}{b}=\frac{13}{75}$ $g=5$

1002. $\frac{a}{b}=\frac{5}{14}$ $g=6$

1003. $\frac{a}{b}=\frac{13}{15}$ $g=5$

1004. $\frac{a}{b}=\frac{7}{10}$ $g=4$

1005. $\frac{a}{b}=\frac{5}{6}$ $g=8$

1006. $\frac{a}{b}=\frac{7}{15}$ $g=9$

1007. $\frac{a}{b}=\frac{17}{24}$ $g=8$

1008. $\frac{a}{b}=\frac{17}{90}$ $g=6$

1009. $\frac{a}{b}=\frac{5}{14}$ $g=6$

1010. $\frac{a}{b}=\frac{13}{147}$ $g=7$

1011. $\frac{a}{b}=\frac{5}{18}$ $g=8$

1012. $\frac{a}{b}=\frac{7}{24}$ $g=8$

1013. $\frac{a}{b}=\frac{5}{12}$ $g=15$

1014. $\frac{a}{b}=\frac{11}{120}$ $g=6$

1015. $\frac{a}{b} = \frac{1}{48}$ $g = 8$

1016. $\frac{a}{b} = \frac{4}{15}$ $g = 5$

1017. $\frac{a}{b} = \frac{5}{24}$ $g = 8$

1018. $\frac{a}{b} = \frac{7}{15}$ $g = 5$

1019. $\frac{a}{b} = \frac{8}{15}$ $g = 5$

1020. $\frac{a}{b} = \frac{5}{14}$ $g = 6$

1021. $\frac{a}{b} = \frac{5}{14}$ $g = 22$

1022. $\frac{a}{b} = \frac{13}{15}$ $g = 9$

1023. $\frac{a}{b} = \frac{3}{20}$ $g = 6$

1024. $\frac{a}{b} = \frac{9}{10}$ $g = 4$

1025. $\frac{a}{b} = \frac{7}{20}$ $g = 6$.

ЛИТЕРАТУРА

1. Боревич З.И., Шафаревич И.Р. Теория чисел. – М.: Наука, 1972. –
2. 496 с.
3. Бухштаб А.А. Теория чисел. – М.: Просвещение, 1966. –384 с.
4. Вейль А. Основы теории чисел. – М.: Мир, 1972. – 408 с.
5. Вейль Г. Алгебраическая теория чисел. – М.: Гос. изд. иностр. литературы, 1947. – 226 с.
6. Виноградов И.М. Основы теории чисел. – М.: Наука, 1981.
7. Галочкин А.И., Нестеренко Ю.В., Шидловский А.Б. Введение в теорию чисел. – М.: МГУ, 1984. – 152 с.
8. Гекке Э., Лекции по теории алгебраических чисел. – ГТТИ, 1940.
9. Гельфонд А.О., Линник Ю.В. Элементарные методы аналитической теории чисел. – М.: Физматгиз, 1962. – 272 с.
10. Грибанов В.У., Титов П.И. Сборник упражнений по теории чисел. – М.: Просвещение, 1964. – 143 с.
11. Дэвенпорт Г. Мультипликативная теория чисел. – М.: Наука, 1971. – 200 с.
12. Карацуба А.А. Основы аналитической теории чисел. – М.: Наука, 1983. – 240 с.
13. Кострикин, А. И. Введение в алгебру: в 3 ч. / А.И. Кострикин. – М.: Физматлит, 2001.
14. Куликов Л.Я. Алгебра и теория чисел. – М.: Высш. шк., 1979. – 559 с.
15. Куликов, Л.Я., Москаленко А.И., Фомин А.А. Сборник задач по алгебре и теории чисел / – М.: Просвещение, 1993.
16. Лельчук, М.П. Полевченко И.И., Радьков А.М., Чеботаревский Б.Д. Практические занятия по алгебре и теории чисел. – Минск: Вышэйш. шк., 1986.
17. Ляпин Е.С., Евсеев А.Е. Алгебра и теория чисел. – М.: Просвещение. – 1974. – Ч. I. – 384 с.; 1976. – Ч. 2. – 448 с.
18. Михелович Ш.Х. Теория чисел. – М.: Высш. шк., 1967. – 335 с.
19. Монахов В.С. Числа и многочлены: тексты лекций по курсу «Алгебра и теория чтсел». – Гомель: ГГУ им. Ф. Скорины, 1992.
20. Окунев Л. Я. Высшая алгебра. – М.: Просвещение, 1966. – 336 с.
21. Сборник задач по алгебре / под ред. А.И. Кострикина. – М. Физматлит, 2001.
22. Серпинский В. 250 задач по элементарной теории чисел. – М.: Просвещение, 1968.
23. Серр Ж.-П. Курс арифметики; пер. с англ. – М.: Мир, 1972. – 184 с.
24. Сизый С.В. Лекции по теории чисел. – Екатеринбург: Уральский гос. ун-т, 1999.
25. Сушкевич А.К. Теория чисел. – Харьков: Издательство Харьковского государственного университета, 1956. – 204 с.

26. Фаддеев, Д.К. Лекции по алгебре / Д.К. Фаддеев. – М.: Наука, 1984.
27. Фаддеев, Д.К., Соминский И.С. Сборник задач по высшей алгебре – М.: Наука, 1977.
28. Хассе Г. Лекции по теории чисел. – М.: И.Л., 1953.
29. Чандрасекхаран К. Введение в аналитическую теорию чисел. – М.: Мир, 1974.
30. Чебышев П.Л. Теория сравнений. – С.-П.: Общественная польза, 1879.
31. Школа в «Кванте»: Арифметика и алгебра / под ред. А.А. Егорова. – М.: Бюро квантум, 1994. – 128 с. (приложение к журналу «Квант»).
32. Шнеперман, Л.Б. Курс алгебры и теории чисел в задачах и упражнениях: в 2 ч. / Л.Б. Шнеперман. – Минск: Вышэйш. шк., 1986–1987.
33. Шнеперман, Л.Б. Сборник задач по алгебре и теории чисел / Л.Б. Шнеперман. – Минск: Вышэйш. шк., 1982.

Учебное издание

ВОРОБЬЕВ Николай Николаевич
ВОРОБЬЕВ Сергей Николаевич
НАУМИК Михаил Иванович

ТЕОРИЯ ЧИСЕЛ: СРАВНЕНИЯ И ИХ ПРИЛОЖЕНИЯ

Сборник заданий

Технический редактор *Г.В. Разбоева*
Компьютерный дизайн *Т.Е. Сафранкова*

Подписано в печать .2017. Формат 60x84 $^{1}/_{16}$. Бумага офсетная.
Усл. печ. л. 3,89. Уч.-изд. л. 4,35. Тираж экз. Заказ .

Издатель и полиграфическое исполнение – учреждение образования
«Витебский государственный университет имени П.М. Машерова».

Свидетельство о государственной регистрации в качестве издателя,
изготовителя, распространителя печатных изданий
№ 1/255 от 31.03.2014 г.

Отпечатано на ризографе учреждения образования
«Витебский государственный университет имени П.М. Машерова».
210038, г. Витебск, Московский проспект, 33.