СБОРНИК ЗАДАЧ ПО ТЕОРИИ ЧИСЕЛ

Е. И. Деза
Л. В. Котова

112 задач с подробными решениями

URSS

Е. И. Деза, Л. В. Котова

СБОРНИК ЗАДАЧ ПО ТЕОРИИ ЧИСЕЛ

112 задач
с подробными решениями

Рекомендовано УМО по образованию
в области подготовки педагогических кадров
в качестве учебного пособия
для студентов высших учебных заведений,
обучающихся по специальности
050201.65 «Математика»,
направлению 050100 «Педагогическое образование»
(профиль «Математика»)

URSS
МОСКВА

ББК 22.1я73 22.131 22.132

Деза Елена Ивановна, Котова Лидия Владимировна

Сборник задач по теории чисел (112 задач с подробными решениями): Учебное пособие. — М.: Книжный дом «ЛИБРОКОМ», 2012. — 224 с.

Данное пособие содержит обширную коллекцию упражнений и задач по всем классическим разделам арифметики и теории чисел (теория делимости, простые и составные числа, арифметические функции, отношение сравнимости, малая теорема Ферма и теорема Эйлера, сравнения и системы сравнений с неизвестной величиной, квадратичные вычеты и символ Лежандра, показатели, первообразные корни и индексы, цепные дроби и др.). Каждый параграф содержит примеры решения задач, упражнения, аналогичные рассмотренным примерам, и задачи для самостоятельного решения. Кроме того, в пособии представлены циклы заданий для проведения контрольных и лабораторных работ, а также типовые задания для проверки усвоения обязательного минимума содержания дисциплины.

Пособие написано на основе лекций, которые в течение многих лет читаются студентам математического факультета Московского государственного педагогического университета, и может быть использовано для проведения семинарских занятий и организации самостоятельной работы студентов высших учебных заведений (прежде всего педагогических вузов) по дисциплине «Теория чисел», а также для проведения элективных курсов арифметической тематики и активизации учебно-исследовательской деятельности старшеклассников, выбравших естественно-математический профиль обучения; оно будет полезно для всех читателей, интересующихся арифметикой и элементарной теорией чисел.

Рецензенты:

доц. кафедры дифференциальных уравнений МАИ,
канд. физ.-мат. наук *Н. В. Александрова*;
проф. кафедры теории чисел МПГУ, канд. пед. наук *А. В. Жмулева*;
доц. факультета культурологии Государственного академического университета гуманитарных наук, канд. физ.-мат. наук *А. А. Привалов*

Издательство «Книжный дом "ЛИБРОКОМ"».
117335, Москва, Нахимовский пр-т, 56.
Формат 60×90/16. Печ. л. 14. Зак. № ЖТ-12.

Отпечатано в ООО «ЛЕНАНД».
117312, Москва, пр-т Шестидесятилетия Октября, 11А, стр. 11.

ISBN 978–5–397–02608–6

Содержание

Обозначения

- $\mathbb{N} = \{1, 2, 3, \ldots\}$ — множество натуральных чисел.
- $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ — множество целых чисел.
- $\text{rest}(a, b)$ — остаток от деления целого числа a на натуральное число b: $a = bq + \text{rest}(a, b)$, где $q, \text{rest}(a, b) \in \mathbb{Z}$, и $0 \leqslant \text{rest}(a, b) < b$.
- $\text{Rest}(a, b)$ — наименьшее по абсолютной величине число, получающееся при делении целого числа a на натуральное число b: $\text{Rest}(a, b) = \text{rest}(a, b)$ при $\text{rest}(a, b) \leqslant b/2$, и $\text{Rest}(a, b) = \text{rest}(a, b) - b$ при $\text{rest}(a, b) > b/2$.
- $b|a$ — целое число b, отличное от нуля, делит целое число a, то есть $a = bc$, где $c \in \mathbb{Z}$.
- $(a_1, \ldots, a_n)$ — *наибольший общий делитель* (НОД) целых чисел $a_1, \ldots, a_n$, хотя бы одно из которых не равно нулю, то есть наибольшее целое число, делящее каждое из чисел $a_1, \ldots, a_n$.
- $[a_1, \ldots, a_n]$ — *наименьшее общее кратное* (НОК) целых чисел $a_1, \ldots, a_n$, каждое из которых не равно нулю, то есть наименьшее натуральное число, делящееся на каждое из чисел $a_1, \ldots, a_n$.
- $P = \{2, 3, 5, 7, 11, 13, 17, 19, \ldots\}$ — множество *простых чисел*, то есть натуральных чисел, имеющих ровно два натуральных делителя; $p, q, p_1, \ldots, p_s, q_1, \ldots, q_t$ — простые числа; $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$, где $p_1, p_2, \ldots, p_s$ — различные простые числа, и $\alpha_1, \alpha_2, \ldots, \alpha_s \in \mathbb{N}$ — *каноническое представление* натурального числа $n > 1$, то есть представление n в виде произведения натуральных степеней различных простых чисел; $n = p_1 \cdot p_2 \cdot \ldots \cdot p_s$ — *бесквадратное число*.
- $S = \{4, 6, 8, 9, 10, 12, 14, 15, 16, 18, \ldots\}$ — множество *составных чисел*, то есть натуральных чисел, имеющих не менее трех натуральных делителей; $\mathbb{N} = P \cup S \cup \{1\}$.
- $\lfloor x \rfloor$ — *целая часть* действительного числа x, то есть наибольшее целое число, не превосходящее x.
- $\{x\}$ — *дробная часть* действительного числа x: $\{x\} = x - \lfloor x \rfloor$.

- $\lceil x \rceil$ — наименьшее целое число, большее или равное x.
- $\|x\| = \min\{\{x\}, 1 - \{x\}\}$ — расстояние от x до ближайшего целого числа.
- $\varphi(n)$ — *функция Эйлера*, дающая число натуральных чисел, не превосходящих n и взаимно простых с ним: $\varphi(n) = |\{x \in \mathbb{N} : x \leqslant n, (x, n) = 1\}|$.
- $\mu(n)$ — функция Мебиуса: $\mu(1) = 1$, $\mu(n) = (-1)^s$ для бесквадратного числа $n = p_1 \cdot \ldots \cdot p_s$, и $\mu(n) = 0$ в остальных случаях.
- $\nu(n)$ — число различных простых делителей натурального числа n.
- $\Omega(n)$ — число простых делителей n, считаемых с повторениями.
- $\pi(x) = \sum\limits_{p \leqslant x} 1$ — число простых чисел, не превосходящих положительное действительное число x.
- $\sum\limits_{d|n} f(d)$ — сумма значений комплекснозначной функции $f(x)$, определенной для всех $x \in \mathbb{N}$, по всем натуральным делителям d натурального числа n.
- $\tau(n) = \sum\limits_{d|n} 1$ — *число натуральных делителей* натурального числа n.
- $\sigma(n) = \sum\limits_{d|n} d$ — *сумма натуральных делителей* натурального числа n.
- $\sigma_s(n) = \sum\limits_{d|n} d^s$ — *s-функция делителей*, дающая сумму s-ых степеней натуральных делителей натурального числа n, где s — любое комплексное число; в частности, $\sigma_0(n) = \tau(n)$, и $\sigma_1(n) = \sigma(n)$.
- $\Lambda(n)$ — *функция Мангольдта*: $\Lambda(n) = \ln p$ для $n = p^k$, где $p \in P$, а $k \in \mathbb{N}$, и $\Lambda(n) = 0$ в остальных случаях.
- $\lambda(n)$ — *функция Кармайкла*: $\lambda(p^\alpha) = \varphi(p^\alpha)$ для простого $p \geqslant 3$ и натурального α; $\lambda(2^\alpha) = 2^{\alpha-2}$ для натурального $\alpha \geqslant 3$, в то время как $\lambda(2) = 1$, и $\lambda(4) = 2$; наконец, $\lambda(p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}) = [\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_s^{\alpha_s})]$, где $p_1, \ldots, p_s$ — различные простые числа, а $\alpha_1, \ldots, \alpha_s \in \mathbb{N}$.
- $a \equiv b (\mathrm{mod}\, n)$ — целые числа a и b *сравнимы по модулю* n, $n \in \mathbb{N}$, то есть a и b имеют одинаковые остатки при делении на n, или, что то же, $n | (a - b)$.
- $a \not\equiv b (\mathrm{mod}\, n)$ — целые числа a и b несравнимы по модулю n, $n \in \mathbb{N}$, то есть a и b имеют различные остатки при делении на n, или, что то же, $n \nmid (a - b)$.
- $\mathbf{a}_n = \{x \in \mathbb{Z} : x \equiv a (\mathrm{mod}\, n)\} = \{\ldots, a - 2n, a - n, a, a + n, a + 2n, a + 3n, \ldots\}$ — *класс вычетов* (числа a) по модулю n, то есть множество всех целых чисел, сравнимых с числом a по модулю n.

- $f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$, $a_n, a_{n-1}, \ldots, a_0 \in A$, $a_n \neq 0$ — *многочлен степени* n над кольцом $\langle A, +, \cdot\rangle$; $\deg f(x)$ — степень многочлена $f(x)$.
- (a/p) — *символ Лежандра*: $(a/p) = 1$, если целое число a, взаимно простое с нечетным простым числом p, является квадратичным вычетом по модулю p (то есть сравнение $x^2 \equiv a(\mathrm{mod}\, p)$ разрешимо), и $(a/p) = -1$, если целое число a, взаимно простое с нечетным простым числом p, является квадратичным невычетом по модулю p (то есть сравнение $x^2 \equiv a(\mathrm{mod}\, p)$ неразрешимо); если $a|p$, то $(a/p) = 0$.
- $(a/n) = \prod_{i=1}^{s}(a/p_i)^{\alpha_i}$ для нечетного $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$ — *символ Якоби*.
- $P_n(a)$ — *показатель* целого числа a (взаимно простого с n) по модулю n, то есть наименьшее натуральное число γ, такое что $a^\gamma \equiv 1(\mathrm{mod}\, n)$; если $P_n(g) = \varphi(n)$, то g — *первообразный корень* по модулю n.
- $\mathrm{ind}_g\, a$ — *индекс* числа a по модулю n с основанием g, то есть такое целое число $\beta \in [0, \varphi(n)-1]$, что $a \equiv g^\beta(\mathrm{mod}\, n)$. Здесь $n \in \{2, 4, p^\alpha, 2p^\alpha\}$ для нечетного простого p и натурального α, g — первообразный корень по модулю n, и a — целое число, взаимно простое с n.
- $[a_0, a_1, \ldots, a_n, \ldots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ldots \cfrac{1}{a_n + \ldots}}}$ — *цепная дробь*. Здесь a_0 — некоторое целое число, а все a_n, $n \in \mathbb{N}$ — натуральные числа, причем последнее, если оно существует, отлично от 1.
- $\delta_k = [a_0, a_1, \ldots, a_k] = P_k/Q_k$, $k = 0, 1, \ldots, n, \ldots$, — *подходящие дроби* для цепной дроби $[a_0, a_1, \ldots, a_n, \ldots]$; a_k, $k = 0, 1, \ldots, n, \ldots$ — *неполные частные* цепной дроби $[a_0, a_1, \ldots, a_n, \ldots]$; $\alpha_k = [a_k, a_{k+1}, \ldots, a_n, \ldots]$, $k = 0, 1, \ldots, n, \ldots$ — *полные частные* цепной дроби $[a_0, a_1, \ldots, a_n, \ldots]$.
- $n! = 1 \cdot 2 \cdot \ldots \cdot n$ — *факториал* натурального числа n; $0! = 1$.
- $\binom{n}{m} = \dfrac{n!}{m!(n-m)!}$, $n, m \in \mathbb{N}$, $n \geqslant m$ — *число сочетаний* из n элементов по m элементов; числа $\binom{n}{m}$ являются коэффициентами разложения *бинома Ньютона*: $(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n-2}a^2b^{n-2} + \binom{n}{1}ab^{n-1} + \binom{n}{n}b^n$.
- $F_n = 2^{2^n} + 1$, $n = 0, 1, 2, \ldots$ — *числа Ферма*.
- $M_n = 2^n - 1$ $n = 1, 2, 3, \ldots$ — *числа Мерсенна*.

Введение

Данное пособие содержит обширную коллекцию упражнений и задач по всем классическим разделам арифметики и теории чисел.

Пособие написано на основе лекций, читаемых в течение многих лет студентам математического факультета Московского государственного педагогического университета, и охватывает все вопросы, рассматриваемые в курсе теории чисел, предназначенном для будущих учителей математики, предлагая студентам системы упражнений и задач по следующим темам: теорема о делении с остатком, отношение делимости, простые и составные числа, НОД и НОК, алгоритм Евклида, взаимно простые числа, функции $[x]$ и $\{x\}$, мультипликативные функции, число и сумма делителей, функция Эйлера, функция Мебиуса, отношение сравнимости, классы вычетов, полная и приведенная системы вычетов, малая теорема Ферма и теорема Эйлера, линейные сравнения и системы сравнений, сравнения и системы сравнений по простому модулю, сравнения по степени простого и по составному модулю, квадратичные вычеты и символ Лежандра, показатели и первообразные корни, индексы, цепные дроби, применения цепных дробей, разные теоретико-числовые задачи.

Изложение каждой из вышеперечисленных тем проведено по единой схеме: основные определения и примеры; свойства рассматриваемых объектов, часть которых доказана, а остальные приведены без доказательства, но со ссылками на соответствующую литературу; примеры решения задач; упражнения, аналогичные рассмотренным выше примерам, решаемые по заданному алгоритму и предназначенные как для работы в аудитории, так и для выполнения домашней работы; задачи для самостоятельного решения, требующие от студентов активного поиска неизвестного им заранее алгоритма решения и зачастую представляющие собой частные случаи хорошо известных в теории чисел теорем.

Раздел **«Задачи для организации промежуточного и итогового контроля»** содержит цикл заданий для проведения контрольных работ (30 блоков заданий по 25 однотипных заданий в каждом блоке), задачи лабораторной

работы по теме **«Сравнения по составному модулю»** (90 заданий различного уровня сложности, от простейших, для решения которых достаточно лишь умения работать по заданному алгоритму, до творческих, решение которых требует от студента активного применения на практике всех основополагающих положений соответствующей теории), задачи лабораторной работы по теме **«Цепные дроби»** (25 вариантов по 8 заданий в каждом варианте), наконец, типовые задания для проверки усвоения обязательного минимума содержания дисциплины (30 блоков заданий по 18 однотипных заданий в каждом блоке).

Пособие предназначено для проведения семинарских занятий и организации самостоятельной работы студентов математических факультетов педвузов, для проведения элективных курсов арифметической тематики и активизации учебно-исследовательской деятельности старшеклассников, выбравших естественно-математический профиль обучения, для всех читателей, интересующихся арифметикой и элементарной теорией чисел.

Авторы благодарят за многолетнее плодотворное сотрудничество и совместную работу своих учителей и коллег, без помощи и поддержки которых было бы невозможно создание этой книги: Бухштаба А. А., Нечаева В. И., Митькина Д. А., Воронина С. М., Киселеву Л. В., Топунова В. Л., Степанову Л. Л., Чирского В. Г., Жмулеву А. В., Баулину Ю. Н., Иконникову Т. К., Юрченко А. Л., Александрову Н. В., Гладкову Е. Б.

Глава 1

Задачи по курсу теории чисел

Элементарная теория чисел имеет дело с *натуральными числами* $1, 2, 3, \ldots$ (множество натуральных чисел обозначается символом $\mathbb{N}$) и *целыми числами* $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$ (множество целых чисел обозначается символом $\mathbb{Z}$).

§ 1. Теорема о делении с остатком

Теорема о делении с остатком (см., например, [28]) утверждает, что *для любого* $a \in \mathbb{Z}$ *и любого* $b \in \mathbb{N}$ *существует единственная пара целых чисел* q *и* r, *таких что* $a = bq + r$ и $0 \leqslant r < b$. Действительно, для заданного целого числа a и заданного натурального числа b рассмотрим рациональное число a/b. Пусть q — наибольшее целое число, не превосходящее a/b, то есть $q \leqslant a/b < q+1$, $q \in \mathbb{Z}$. Тогда $bq \leqslant a < bq+b$, или, что то же, $0 \leqslant a - bq < b$. Вводя обозначение $r = a - bq$, мы можем утверждать, что для выбранных целых чисел q и r имеет место соотношение $a = bq + r$, причем $0 \leqslant r < b$. Для доказательства единственности указанного представления достаточно рассмотреть равенства $a = bq + r$, где $0 \leqslant r < b$, и $a = bq_1 + r_1$, где $0 \leqslant r_1 < b$. Тогда $b(q - q_1) = r_1 - r$, причем $-b < r_1 - r < b$. Поскольку $q, q_1 \in \mathbb{Z}$, то $q - q_1 = 0$, или $q - q_1 \geqslant 1$, или $q - q_1 \leqslant -1$. В первом случае мы получаем, что $r_1 - r = 0$, то есть $q = q_1$ и $r = r_1$, откуда следует, что представления $a = bq + r$ и $a = bq_1 + r_1$ совпадают. Во втором случае мы получаем, что $b(q - q_1) \geqslant b$, что дает противоречие с условием $r_1 - r < b$. В третьем случае мы получаем, что $b(q - q_1) \leqslant -b$, что дает противоречие с условием $r_1 - r > -b$.

Число q называется *целым частным*, а число r называется *остатком* от деления a на b. При решении задач обычно используют обозначение $r = \mathrm{rest}(a, b)$.

Например, $-10 = 3 \cdot (-4) + 2$, то есть $\mathrm{rest}(-10, 3) = 2$; $48 = 14 \cdot 3 + 6$, то есть $\mathrm{rest}(48, 14) = 6$; $100 = 20 \cdot 5 + 0$, то есть $\mathrm{rest}(100, 20) = 0$.

Примеры решения задач

1. Найдите целое частное и остаток от деления 19 на 3; -18 на 5; n^3+2n-1 на n, где $n \in \mathbb{N}$; $12n^5 + 10n^4 + 2$ на $2n$, где $n \in \mathbb{N}$.

Решение. Легко убедиться в том, что: $19 = 3 \cdot 6 + 1$, причем $6, 1 \in \mathbb{Z}$, и $0 \leqslant 1 < 3$; $-18 = 5 \cdot (-4) + 2$, причем $-4, 2 \in \mathbb{Z}$, и $0 \leqslant 2 < 5$; $n^3+2n-1 = n\cdot(n^2+1)+(n-1)$, причем $n^2+1, n-1 \in \mathbb{Z}$, и $0 \leqslant n-1 < n$. Аналогично, $12n^5 + 10n^2 + 2 = 2n \cdot (6n^4 + 5n) + 2$, где $6n^4 + 5n$, $2 \in \mathbb{Z}$, однако ограничение $0 \leqslant 2 < 2n$ *имеет место лишь для* $n \geqslant 2$. Для $n = 1$ искомое равенство принимает вид $12n^5 + 10n^4 + 2 = 2n \cdot (6n^4 + 5n^3 + 2) + 0$, то есть вид $24 = 2 \cdot 12 + 0$. ▷

2. Целые числа a, b и c дают при делении на 5 остатки 1, 2 и 4 соответственно. Какие остатки при делении на 5 дают числа $2a$; $-3b$; $5c$; $a + b + c$; $2a - 3b + 5c$; abc; a^2; b^3; c^4; $17a^2b^3c^4$?

Решение. Из условия задачи следует, что $a = 5q + 1$, $b = 5k + 2$, $c = 5m + 4$, где $q, k, m \in \mathbb{Z}$. Тогда $2a = 5 \cdot (2q) + 2$, причем $2q, 2 \in \mathbb{Z}$, и $0 \leqslant 2 < 5$. Следовательно, остаток числа $2a$ при делении на 5 равен 2: $\mathrm{rest}(2a, 5) = 2$. Далее, $-3b = 5 \cdot (-3k) - 6$; поскольку $-6 = 5 \cdot (-2) + 4$, то $-3b = 5 \cdot (-3k - 2) + 4$, причем $-3k - 2, 4 \in \mathbb{Z}$, и $0 \leqslant 4 < 5$. Следовательно, $\mathrm{rest}(-3b, 5) = 4$. Поскольку $5c = 5 \cdot c + 0$, причем $c, 0 \in \mathbb{Z}$, и $0 \leqslant 0 < 5$, то $\mathrm{rest}(5c, 5) = 0$. Аналогично, $a + b + c = 5(q + k + m) + (1 + 2 + 4)$, и $1 + 2 + 4 = 5 \cdot 1 + 2$, то есть $a + b + c = 5(q + k + m + 1) + 2$, причем $q + k + m + 1, 2 \in \mathbb{Z}$, и $0 \leqslant 2 < 5$. Таким образом, $\mathrm{rest}(a + b + c, 5) = 2$. Пользуясь полученными ранее соотношениями, можно утверждать, что $2a - 3b + 5c = 5 \cdot (2q - 3k - 2 + c) + (2 + 4 + 0)$, откуда, с учетом равенства $2 + 4 + 0 = 5 \cdot 1 + 1$, следует равенство $2a - 3b + 5c = 5 \cdot (2q - 3k + c - 1) + 1$, причем $2q - 3k + c - 1$, $1 \in \mathbb{Z}$, и $0 \leqslant 1 < 5$. Следовательно, $\mathrm{rest}(2a - 3b + 5c, 5) = 1$. Исследование произведения чисел a, b и c производится по той же схеме: поскольку $1 \cdot 2 \cdot 4 = 5 \cdot 1 + 3$, то $abc = (5q + 1)(5k + 2)(5m + 4) = 5(25qkm + 20qk + 10qm + 8q + 5km + 4k + 2m + 1) + 3$, то есть $\mathrm{rest}(abc, 5) = 3$. Далее, $a^2 = (5q + 1)^2 = 25q^2 + 10q + 1$, то есть $a^2 = 5(5q^2 + 2q) + 1$, откуда следует, что $\mathrm{rest}(a^2, 5) = 1$. Аналогично, $b^3 = (5k + 2)^3 = 125k^3 + 150k^2 + 60k + 8$, то есть, с учетом равенства $8 = 5 \cdot 1 + 3$, $b^3 = 5 \cdot (25k^3 + 30k^2 + 12k + 1) + 3$, откуда следует, что $\mathrm{rest}(b^3, 5) = 3$. Пользуясь формулой *бинома Ньютона* $(a + b)^4 = a^4+4a^3b+6a^2b^2+4ab^3+b^4$ и замечая, что $4^4 = 5 \cdot 51 + 1$, мы можем записать равенство $c^4 = 5 \cdot t + 1$ для некоторого целого числа t (найдите его самостоятельно!), откуда следует, что $\mathrm{rest}(c^4, 5) = 1$. Наконец, пользуясь предыдущими результатами и замечая, что $17 = 5 \cdot 3 + 2$,

мы можем утверждать, что $17a^2b^3c^4 = (5\cdot3+2)(5\cdot n+1)(5\cdot s+3)(5\cdot t+1)$, $n, s, t \in \mathbb{Z}$. Поскольку $2\cdot1\cdot3\cdot1 = 5\cdot1+1$, то $17a^2b^3c^4 = 5l+1$, $l \in \mathbb{Z}$, то есть $\mathrm{rest}(17a^2b^3c^4, 5) = 1$. ▷

Замечание. Анализ решения приведенной выше задачи позволяет утверждать, что для нахождения остатка суммы или произведения нескольких целых чисел a_1, a_2, ..., a_n (а также натуральной степени a^k целого числа a) при делении на данное натуральное число b достаточно оперировать известными остатками $\mathrm{rest}(a_i, b)$ чисел a_i, $i = 1, 2, \ldots, n$ при делении на b. Именно, *остаток суммы равен остатку суммы остатков, остаток произведения равен остатку произведения остатков, остаток степени равен остатку степени остатка*: $\mathrm{rest}(a_1 + \ldots + a_n, b) = \mathrm{rest}(\mathrm{rest}(a_1, b) + \ldots + \mathrm{rest}(a_n, b)$; $\mathrm{rest}(a_1 \cdot \ldots \cdot a_n, b) = \mathrm{rest}(\mathrm{rest}(a_1, b) \cdot \ldots \cdot \mathrm{rest}(a_n, b), b)$; $\mathrm{rest}(a^k, b) = \mathrm{rest}((\mathrm{rest}(a, b))^k, b)$.

3. Докажите, что любое целое число представимо в виде $5k$, или $5k \pm 1$, или $5k \pm 2$, $k \in \mathbb{Z}$, причем данное представление единственно.

Решение. Рассмотрим произвольное целое число z и разделим его с остатком на 5. По теореме о делении с остатком, имеет место соотношение $z = 5q + r$, где $q, r \in \mathbb{Z}$, и $0 \leqslant r < 5$. Другими словами, $r \in \{0, 1, 2, 3, 4\}$. Если $r = 0$, то $z = 5q + 0$, то есть, взяв $k = q$, мы можем представить z в виде $5k$, $k \in \mathbb{Z}$. Если $r = 1$, то $z = 5q + 1$, то есть, взяв $k = q$, мы можем представить z в виде $5k + 1$, $k \in \mathbb{Z}$. Если $r = 2$, то $z = 5q + 2$, то есть, взяв $k = q$, мы можем представить z в виде $5k + 2$, $k \in \mathbb{Z}$. Если $r = 3$, то $z = 5q + 3$, или, что то же, $z = 5(q + 1) - 2$, то есть, взяв $k = q + 1$, мы можем представить z в виде $5k - 2$, $k \in \mathbb{Z}$. Если $r = 4$, то $z = 5q + 4$, или, что то же, $z = 5(q + 1) - 1$, то есть, взяв $k = q + 1$, мы можем представить z в виде $5k - 1$, $k \in \mathbb{Z}$. Единственность полученного представления числа z следует из единственности представления числа z в виде $z = 5q + r$, где $q, r \in \mathbb{Z}$, и $0 \leqslant r < 5$. ▷

Замечание. В ходе рассуждений мы показали, что любое целое число представимо в виде $5k$, или $5k + 1$, или $5k + 2$, или $5k + 3$, или $5k + 4$, $k \in \mathbb{Z}$, причем указанное представление единственно. Этот факт немедленно следует из теоремы о делении с остатком.

4. Докажите, что квадрат целого числа не может иметь вид $4k+2$, $k \in \mathbb{Z}$.

Решение. Рассмотрим произвольное целое число z и поделим его с остатком на 4: $z = 4q + r$, $0 \leqslant r < 4$. Тогда $z^2 = (4q + r)^2 = 4(4q^2 + 2qr) + r^2$. Если $r = 0$ или $r = 2$, то z^2 имеет вид $4k$, $k \in \mathbb{Z}$; если $r = 1$ или $r = 3$, то z^2 меет вид $4k + 1$, $k \in \mathbb{Z}$. Таким образом, квадрат целого числа на может имет остаток два при делении на 4, то есть не может быть представлен в виде $4k + 2$, $k \in \mathbb{Z}$. Обычно приведенные вычисления принято оформлять в виде табл. 1*a*).

Таблица 1

а)

$\operatorname{rest}(z,4)$	0	1	2	3
$(\operatorname{rest}(z,4))^2$	0	1	4	9
$\operatorname{rest}((\operatorname{rest}(z,4))^2,4)$	0	1	0	1

б)

$\operatorname{Rest}(z,4)$	0	±1	2
$(\operatorname{Rest}(z,4))^2$	0	1	4
$\operatorname{rest}((\operatorname{Rest}(z,4))^2,4)$	0	1	0

Таблица станет еще компактнее (табл. 1*б*)), если воспользоваться идеей предыдущей задачи и представить произвольное целое число z в виде $4k$, или $4k \pm 1$, или $4k + 2$, $k \in \mathbb{Z}$, заменяя $\operatorname{rest}(z,4) \in \{0,1,2,3\}$ на $\operatorname{Rest}(z,4) \in \{0,\pm1,2\}$ по закону $\operatorname{Rest}(z,4) = \operatorname{rest}(z,4)$ при $\operatorname{rest}(z,4) \leqslant 2$, и $\operatorname{Rest}(z,4) = \operatorname{rest}(z,4) - 4$ при $\operatorname{rest}(z,4) > 2$. ▷

5. Докажите, что сумма четных степеней трех последовательных целых чисел не может равняться четной степени целого числа.

Решение. Прежде всего заметим, что четная степень любого целого числа на может иметь вид $3k + 2$, $k \in \mathbb{Z}$. Для доказательства этого факта достаточно представить произвольное целое число z в виде $3k$ или $3k \pm 1$, $k \in \mathbb{Z}$, и убедиться, что $\operatorname{rest}(0^{2m},3) = 0$, а $\operatorname{rest}((\pm1)^{2m},3) = 1$, то есть число z^{2m} имеет вид $3q$ или $3q + 1$, $q \in \mathbb{Z}$. Далее, рассмотрим три последовательных целых числа z, $z+1$ и $z + 2$. Легко убедиться в том, что они имеют различные остатки при делении на 3, то есть одно из указанных чисел имеет вид $3k$, второе — вид $3k + 1$, а третье — вид $3k - 1$, $k \in \mathbb{Z}$: действительно, если $z = 3t$, $t \in \mathbb{Z}$, то $z + 1 = 3t + 1$, а $z + 2 = 3(t + 1) - 1$; если $z = 3t + 1$, $t \in \mathbb{Z}$, то $z + 1 = 3(t + 1) - 1$, а $z + 2 = 3(t + 1)$; если $z = 3t - 1$, $t \in \mathbb{Z}$, то $z + 1 = 3t$, а $z + 2 = 3t + 1$. Следовательно, при возведении трех указанных чисел в четные степени мы получим три целых числа, одно из которых имеет вид $3l$, второе — вид $3q + 1$, а третье — вид $3s + 1$, $q, l, s \in \mathbb{Z}$. Сумма полученных целых чисел имеет вид $3(l + q + s) + 2$, то есть дает остаток два при делении на 3, и, следовательно, не может быть четной степенью целого числа. ▷

Упражнения

1. Найдите целое частное и остаток от деления:

а) 119 на 5;
б) -128 на 7;
в) 1000 на 11;
г) -666 на 13;
д) 12 345 на 6;
е) -144 на 7;
ж) 60 на 12;
з) -225 на 3;
и) 0 на 77.

2. Поделите с остатком при $n \in \mathbb{N}$:

а) $2n^2 + 4n + 1$ на 2;
б) $15n^4 + 9n^2 + 2$ на 3;
в) $8n^2 + 12n - 3$ на 4;
г) $25n^5 + 10n^4 - 2$ на 5;
д) $12n^2 - 24n + 29$ на 6;
е) $21n^8 - 35n^2 - 44$ на 7.

3. Поделите с остатком при $n \in \mathbb{N}$:

а) $4n^2 + 7n - 1$ на n;
б) $6n^7 + 3n - 2$ на n;
в) $6n^6 - 18n^5 + 3$ на $2n$;
г) $4n^9 + 14n^5 + 4$ на $2n$.

4. Целые числа a, b и c дают при делении на n остатки $n-1$, $n-2$ и $n-3$, соответственно. Какие остатки при делении на n дают числа:

а) $5a$;
б) $-7b$;
в) $9c$;
г) a^2;
д) b^3;
е) c^4;
ж) $4abc$;
з) $ab - 28c$;
и) $3a - 5b + 8c$;
к) $abc - 2a^2b^3c^4$?

Решите задачу для каждого $n \in \{3, 4, 5, 6, 7, 8, 9\}$.

5. Докажите, что любое целое число единственным образом представимо в виде:

а) $6k$, или $6k \pm 1$, или $6k \pm 2$, или $6k + 3$, $k \in \mathbb{Z}$;
б) $7k$, или $7k \pm 1$, или $7k \pm 2$, или $7k \pm 3$, $k \in \mathbb{Z}$;
в) $10k$, или $10k \pm 1$, или $10k \pm 2$, или $10k \pm 3$, или $10k \pm 4$, или $10k + 5$, $k \in \mathbb{Z}$;
г) $12k$, или $12k \pm 1$, или $12k \pm 2$, или $12k \pm 3$, или $12k \pm 4$, или $12k \pm 5$, или $12k + 6$, $k \in \mathbb{Z}$.

6. Докажите, что квадрат целого числа не может иметь вид:

а) $3k - 1$;
б) $4k - 1$;
в) $5k + 2$;
г) $5k - 2$;
д) $6k + 2$;
е) $6k - 1$.

7. Докажите, что сумма квадратов двух нечетных чисел не может быть квадратом целого числа.

8. Докажите, что сумма четных степеней двух нечетных чисел не может быть кубом целого числа.

Задачи

1. Для заданного четного натурального числа n, большего двух, докажите, что любое целое число представимо в виде nk, или $nk \pm 1$, ..., или $nk + n/2$, $k \in \mathbb{Z}$, причем данное представление единственно.

2. Для заданного нечетного натурального числа n, большего единицы, докажите, что любое целое число представимо в виде nk, или $nk \pm 1$, ..., или $nk \pm (n-1)/2$, $k \in \mathbb{Z}$, причем данное представление единственно.

3. Докажите, что четная степень целого числа не может иметь вид:

а) $5k \pm 2$; в) $7k - 2$; д) $8k \pm 2$; ж) $8k + 5$;

б) $7k + 3$; г) $7k - 1$; е) $8k \pm 3$; з) $8k - 1$.

4. Найдите остаток от деления суммы кубов первых n натуральных чисел на $n + 2$.

5. Докажите, что среди n последовательных целых чисел одно и только одно дает данный остаток r, $0 \leqslant r < n$, при делении на n, $n \in \mathbb{N}$.

6. На какие цифры не может оканчиваться квадрат целого числа; куб целого числа?

7. Докажите, что пятая степень любого целого числа оканчивается на ту же цифру, что и само число.

8. На какую цифру оканчивается сумма квадратов пяти последовательных целых чисел?

9. Докажите, что существует бесконечно много натуральных чисел, не представимых в виде суммы квадратов трех натуральных чисел.

§ 2. Отношение делимости

Говорят, что целое число a *делится* на целое число b, $b \neq 0$, и пишут $b|a$, если существует целое число c, такое что $a = b \cdot c$. В этом случае b называется *делителем* a.

1 и -1 делят любое целое число, любое целое число (кроме нуля) делит само себя, и любое целое число (кроме нуля) делит 0.

Числа, делящиеся на 2, называются *четными*, числа, не делящиеся на 2, называются *нечетными*.

Тривиальными делителями целого числа n называются числа 1, -1, n и $-n$. Делитель числа n, отличный от 1, -1, n или $-n$, называется *нетривиальным делителем* n. Положительный делитель числа n, отличный от n, называется *собственным делителем* n.

Например, тривиальными делителями числа 6 являются числа ± 1 и ± 6, нетривиальными делителями числа 6 являются числа ± 2 и ± 3, а собственными делителями числа 6 являются числа 1,2 и 3 [1].

[1] Легко видеть, что число 6 равно сумме своих собственных делителей: $6 = 1 + 2 + 3$. Натуральные числа, обладающие указанным свойством, называются *совершенными*. Таким образом, 6 — наименьшее совершенное число. Вторым совершенным числом является число 28, третьим — число 496 и четвертым — число 8128.

Свойства отношения делимости

1. Если $a|b$ и $a|c$, то $a|(b \pm c)$, более того, $a|(mb+nc)$ для любых целых m и n.
2. Если $a|b$ и $b|c$, то $a|c$.
3. Если $a|b$ и $b|a$, то $a = b$ или $a = -b$.
4. Если $a|b$, где $a, b \in \mathbb{N}$, то $b \geqslant a$.

Так, если $a|b$ и $a|c$, то $b = ak$, и $c = al$, $k, l \in \mathbb{Z}$. Тогда $mb = a(mk)$, $nc = a(nl)$, и $mb+nc=a(mk+nl)$, где $mk+nl \in \mathbb{Z}$, то есть $a|(mb+nc)$. Доказательства остальных свойств аналогичны. Их можно найти, например, в [28].

Примеры решения задач

1. Докажите, что произведение трех последовательных целых чисел делится на 3.

Решение. Рассмотрим произвольное целое число z и разделим его с остатком на 3: $z = 3q + r$, где $q, r \in \mathbb{Z}$, и $0 \leqslant r < 3$. Таким образом, $r \in \{0, 1, 2\}$. Если $r = 0$, то $z = 3q$, то есть z делится на 3. Если $r = 1$, то $z = 3q + 1$, то есть $z + 2 = 3(q + 1)$ делится на 3. Если $r = 2$, то $z = 3q + 2$, то есть $z + 1 = 3(q + 1)$ делится на 3. В каждом из рассмотренных случаев произведение $z(z + 1)(z + 2)$ имеет вид $3t$, $t \in \mathbb{Z}$, то есть делится на 3. ▷

2. Докажите, что число $a^5 + 9a$ делится на пять при любом целом a.

Решение. Легко убедиться в том, что остаток при делении на 5 пятой степени целого числа совпадает с остатком при делении на 5 самого числа: $\text{rest}(0^5, 5) = 0$, $\text{rest}(1^5, 5) = 1$, $\text{rest}(2^5, 5) = 2$, $\text{rest}(3^5, 5) = \text{rest}((-2)^5, 5) = 3$, $\text{rest}(4^5, 5) = \text{rest}((-1)^5, 5) = 4$. Поскольку остаток числа 9 при делении на 5 равен 4, то соответствующие остатки числа $9a$ равны, соответственно, 0, 4, 3, 2 и 1: $\text{rest}(4 \cdot 0, 5) = 0$, $\text{rest}(4 \cdot 1, 5) = 4$, $\text{rest}(4 \cdot 3, 5) = 2$, $\text{rest}(4 \cdot 4, 5) = 1$. Теперь становится очевидным, что остаток числа a^5+9a при делении на 5 всегда равен 0: $\text{rest}(0+0, 5) = 0$, $\text{rest}(1+4, 5) = 0$, $\text{rest}(2+3, 5) = 0$, $\text{rest}(3+2, 5) = 0$, $\text{rest}(4+1, 5) = 0$. Впрочем, убедиться в этом еще проще, заметив, что число 9 имеет вид $5q - 1$, то есть может быть заменено при проведении операций с остатками на число «-1», и, следовательно, вычисления с остатками сводятся к разности двух одинаковых чисел, что, очевидным образом, дает ноль. Обычно результаты вычислений принято оформлять в виде таблицы. В табл. 2 *а*) мы имеем дело с «классическими» остатками 0, 1, 2, 3, 4 при делении на 5, в табл. 2 *б*) — используем

Таблица 2

а)

$\operatorname{rest}(a, 5)$	0	1	2	3	4
$\operatorname{rest}(a^5, 5)$	0	1	2	3	4
$\operatorname{rest}(9a, 5)$	0	4	3	2	1
$\operatorname{rest}(a^5 + 9a, 5)$	0	0	0	0	0

б)

$\operatorname{rest}(a, 5)$	0	1	2	-2	-1
$\operatorname{rest}(a^5, 5)$	0	1	2	-2	-1
$\operatorname{rest}(9a, 5) = \operatorname{rest}(a, 5)$	0	-1	-2	2	1
$\operatorname{rest}(a^5 + 9a, 5) = \operatorname{rest}(a^5, 5)$	0	0	0	0	0

более удобные при промежуточных вычислениях величины $0, 1, 2, -2, -1$, соответственно.

Таким образом, мы доказали, что при любом целом a величина a^5+9a дает остаток ноль при делении на 5, то есть делится на 5. ▷

3. Докажите, что разность квадратов двух нечетных чисел делится на 8.

Решение. Замечая, что нечетные числа имеют вид $8k \pm 1$ или $8k \pm 3$, $k \in \mathbb{Z}$, мы легко убеждаемся в том, что квадраты нечетных чисел *всегда имеют вид* $8t + 1$, $t \in \mathbb{Z}$, то есть дают остаток 1 при делении на 8: $\operatorname{rest}((\pm 1)^2, 8) = 1$, и $\operatorname{rest}((\pm 3)^2, 8) = 1$. Очевидно, что разность двух чисел указанного вида имеет остаток 0 при делении на 8, то есть делится на 8. ▷

4. Докажите, что ab делится на 49, если $a^2 + b^2$ делится на 7.

Решение. Прежде всего выясним, какие остатки при делении на 7 могут давать квадраты натуральных чисел.

Из табл. 3 следует, что возможные остатки принадлежат множеству $\{0, 1, 2, 4\}$. Теперь выясним, какие остатки при делении на 7 может давать сумма квадратов двух целых чисел.

Из табл. 4 следует, что сумма квадратов двух целых чисел может давать при делении на 7 любой остаток, кроме остатка 3, однако остаток 0, то есть делимость на 7, имеет место только в случае, когда каждое из слагаемых имеет остаток ноль при делении на 7, то есть только тогда, когда и a^2, и b^2 делятся на 7. В свою очередь, квадрат целого числа делится на 7 только в том случае, когда само число делится на 7 (см. табл. 2 *а*), 2 *б*)). Таким образом, если величина $a^2 + b^2$ делится

Таблица 3

$\operatorname{Rest}(a, 7)$	0	1	2	3	-3	-2	-1
$\operatorname{rest}(a^2, 7)$	0	1	4	2	2	4	1

Таблица 4

$\text{rest}(a^2, 7)\backslash\text{rest}(b^2, 7)$	0	1	2	4
0	0	1	2	4
1	1	2	4	1
2	2	3	4	6
4	4	5	6	1

на 7, то $a = 7n$ и $b = 7k$, $n, k \in \mathbb{Z}$, и, следовательно, $ab = 49nk$, $nk \in \mathbb{Z}$, то есть ab делится на 49. ▷

Упражнения

1. Докажите, что:

а) произведение двух последовательных целых чисел делится на 2;

б) произведение четырех последовательных целых чисел делится на 4;

в) произведение пяти последовательных целых чисел делится на 5;

г) произведение n последовательных целых чисел делится на n, $n \in \mathbb{N}$.

2. Докажите, что для любого целого a:

а) $a^{10} - 9a + 8$ делится на 2;

б) $a^5 + 3a^3 - 12$ делится на 4;

в) $a^3 - 7a + 18$ делится на 6;

г) $a^7 - a - 56$ делится на 7;

д) $a^5 - 17a^3 + 24$ делится на 8;

е) $a^9 + 17a^3 - 18$ делится на 9.

3. Докажите, что:

а) разность четных степеней двух нечетных чисел делится на 4;

б) сумма кубов двух последовательных нечетных чисел делится на 4;

в) разность квадратов двух нечетных чисел делится на 8;

г) сумма кубов трех последовательных целых чисел делится на 3.

4. Докажите, что:

а) $5ab$ делится на 45, если $a^6 + b^6$ делится на 3;

б) $4ab$ делится на 100, если $a^8 + b^8$ делится на 5;

в) $2ab$ делится на 98, если $a^4 + b^4$ делится на 7;

г) $3ab$ делится на 363, если $a^2 + b^2$ делится на 11.

Задачи

1. Докажите, что $n \cdot (n^2 + 1) \cdot (n^2 + 4)$ делится на 5 при любом целом n.

2. Докажите, что целое число a не может быть квадратом целого числа, если число $a - 5$ делится на 9.

3. Докажите, что $(n-5)/15$ и $(n-6)/24$ не могут быть одновременно целыми числами.

4. Докажите, что abc делится на 3, если $a^3+b^3+c^3$ делится на 9.

5. Докажите, что $7^{n+2}+8^{2n+1}$ делится на 3 при любом целом неотрицательном n.

6. Докажите, что $5^{2n+1}\cdot 2^{n+2}+3^{n+2}\cdot 2^{2n+1}$ делится на 19 при любом целом неотрицательном n.

7. Докажите, что при любом натуральном n:

а) $2^{n+2}+2^{n+1}+2^n$ делится на 14; в) $5^{2n+1}+3^{n+2}\cdot 2^{n-1}$ делится на 19;

б) $7^{2n}-4^{2n}$ делится на 33; г) $12^{2n+1}+11^{n+1}$ делится на 133.

8. Докажите, что $(x-y)^5+(y-z)^5+(z-x)^5$ делится на 5, на $x-y$, на $y-z$ и на $z-x$, если x, y, z — попарно различные целые числа.

9. Докажите, что при любом целом a:

а) a^3-a делится на 3; б) a^5-a делится на 5; в) a^7-a делится на 7.

Нельзя ли обобщить эти результаты?

§ 3. Простые и составные числа

Натуральное число p называется *простым*, если оно имеет ровно два натуральных делителя (а именно, 1 и p).

Множество простых чисел принято обозначать символом $\mathbb{P}$. Первые 30 простых чисел: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109 и 113.

Натуральное число n называется *составным*, если оно имеет более двух натуральных делителей. Множество составных чисел принято обозначать символом $\mathbb{S}$. Первые 30 составных чисел: 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 25, 26, 27, 28, 30, 32, 33, 34, 35, 36, 38, 39, 40, 42, 44, 45.

Из определения следует, что *любое составное число n можно представить в виде $n=ab$*, где $1<a\leqslant b<n$: взяв наименьший натуральный делитель a числа n, отличный от самого n и от 1, мы получим, что $n=ab$, где, в силу выбора a, второй множитель b — натуральное число, меньшее n, но большее или равное a. (Для уточнения деталей см., например, [3].)

Таким образом, любое натуральное число либо простое, либо составное, либо равно 1. Другими словами, $\mathbb{N}=\mathbb{P}\cup\mathbb{S}\cup\{1\}$.

Хорошо известно, что *любое натуральное число n, большее* 1, *имеет простой делитель*. Для доказательства этого факта достаточно рассмотреть наименьший натуральный делитель n, отличный от 1. (см. [3], [28]).

Около двух тысяч лет назад Евклид доказал, что *множество простых чисел бесконечно*: предположив, что множество простых чисел конечно, и что $\mathbb{P} = \{p_1, p_2, \ldots, p_k\}$ — все простые числа, он построил число $E = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$ и рассмотрел простое число p, делящее E. Легко видеть, что число p не может совпадать ни с одним из чисел $p_1, p_2, \ldots, p_k$, так как иначе p должно делить разность $E - p_1 \cdot p_2 \cdot \ldots \cdot p_k = 1$, что невозможно. Таким образом, p — простое число, не попавшее в вышеприведенный список, то есть множество простых чисел не может исчерпываться числами $p_1, p_2, \ldots, p_k$.

Простейший метод нахождения всех простых чисел на данном интервале был предложен греческим математиком Эратосфеном. Он называется *решетом Эратосфена* и состоит в следующем. Рассмотрим последовательность 2, 3, 4, 5,... натуральных чисел, больших единицы. Так как 2 является первым простым числом, p_1, вычеркнем из нашей последовательности все числа, большие p_1 и делящиеся на p_1, то есть, начиная с 2, каждое второе число таблицы — они заведомо составные. Первое из оставшихся чисел 3 — второе простое число, p_2. Вычеркнем все числа, большие p_2 и делящиеся на p_2, то есть, начиная с 3, каждое третье число таблицы. Первое из оставшихся чисел 5 — третье простое число, p_3, и т. д. Следуя указанной схеме, мы получаем $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, ..., $p_{1000} = 7917$, ..., $p_{6000000} = 104\,395\,301$, ... Здесь символ p_n обозначает n-е простое число.

Существует много других возможностей определить, является ли данное натуральное число простым. Классический тест такого рода основывается на следующем утверждении: *если n является составным числом, то оно имеет простой делитель $p \leqslant \sqrt{n}$*. Действительно, составное n обладает нетривиальным натуральным делителем $a \notin \{1, n\}$, то есть представимо в виде $n = a \cdot b$, $1 < a \leqslant b < n$. При этом $a \leqslant \sqrt{n}$, так как в противном случае мы получаем противоречие: поскольку $a > \sqrt{n}$ и $b \geqslant a$, то $b > \sqrt{n}$, откуда следует, что $n = a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$, то есть $n > n$. Поскольку a — натуральное число, большее единицы, то оно обладает простым делителем p. При этом, с одной стороны, делитель p числа a является делителем n, и, с другой стороны, $p \leqslant a \leqslant \sqrt{n}$. Таким образом, мы нашли для составного числа n его простой делитель p, удовлетворяющий условию $p \leqslant \sqrt{n}$.

Представление $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$ натурального числа n, большего единицы, в виде произведения натуральных степеней различных простых чисел $p_1, \ldots, p_s$ называется *каноническим*.

Фундаментальная теорема арифметики утверждает, что *любое натуральное число, большее* 1, *можно, причем единственным образом* (*с точностью до порядка сомножителей*), *представить в виде произведения простых чисел.*

Доказательство существования такого разложения тривиально: любое натуральное число n, большее 1, обладает простым делителем p (рассмотрите наименьший натуральный делитель числа n, отличный от единицы). Таким образом, $n = pk$, где $k \in \mathbb{N}$, и $k < n$. Если $k = 1$, то искомое разложение получено: $n = p$. Если $k \geqslant 2$, то оно обладает простым делителем q: $k = qm$, где $m \in \mathbb{N}$, и $m < k$. Если $m = 1$, то искомое разложение получено: $n = pq$. Если нет, то мы продолжаем рассуждения. Поскольку убывающая последовательность натуральных чисел $n > k > m > \ldots$ конечна, то мы получим разложение числа n на простые множители после конечного числа шагов. Доказательство единственности указанного разложения несколько более сложно. Предположим, что существуют натуральные числа, обладающие несколькими разложениями на простые множители. Предположим, что n_0 — наименьшее натуральное число, обладающее несколькими разложениями на простые множители, и рассмотрим два таких разложения числа n_0: $n_0 = p_1 \cdot p_2 \cdot \ldots \cdot p_s = q_1 \cdot q_2 \cdot \ldots \cdot q_k$, где $p_i, q_j \in \mathbb{P}$, $1 \leqslant i \leqslant s$, $1 \leqslant j \leqslant k$. Не ограничивая общности рассуждений, будем считать, что p_1 — наименьшее из всех рассматриваемых простых чисел: $p_1 \leqslant p_i$ и $p_1 \leqslant q_j$ для всех $1 \leqslant i \leqslant s$, $1 \leqslant j \leqslant k$. Нетрудно убедиться и в том, что $p_1 \neq q_j$ для всех $1 \leqslant j \leqslant k$. Действительно, если, например, $p_1 = q_1$, то мы получим два различных разложения на простые множители числа n_0/p_1: $n_0/p_1 = p_2 \cdot \ldots \cdot p_s = q_2 \cdot \ldots \cdot q_k$. Поскольку $n_0/p_1 < n_0$, то мы получаем противоречие: число n_0 — минимальное натуральное число, обладающее несколькими разложениями на простые множители. Таким образом, $p_1 < q_1$, и, поделив простое число q_1 с остатком на простое число p_1, мы получим равенство $q_1 = p_1 \cdot q + r$, где $q, r \in \mathbb{Z}$, и $0 < r < p_1$. Заметим, что, в силу простоты чисел p_1 и q_1, остаток r не может быть равен нулю. Следовательно, мы получаем равенство $p_1 \cdot p_2 \cdot \ldots \cdot p_s = (p_1 \cdot q + r) \cdot q_2 \cdot \ldots \cdot q_k$ или, что то же, равенство $p_1 \cdot (p_2 \cdot \ldots \cdot p_s - q \cdot q_2 \cdot \ldots \cdot q_k) = r \cdot q_2 \cdot \ldots \cdot q_k$. Пусть $R = r \cdot q_2 \cdot \ldots \cdot q_k$. Поскольку $0 < r < q_1$, то R — натуральное число, меньшее n_0, и, следовательно, обладает единственным разложением на простые множители. Поскольку p_1 делит R, то p_1 должно входить в данное разложение на простые множители. Однако $p_1 \neq q_2$, $\ldots$, $p_1 \neq q_k$, откуда следует, что p_1 входит в разложение на простые множители числа r, то есть делит r. Поскольку p_1 и r — натуральные числа, то мы получаем соотношение $p_1 \leqslant r$, что приводит нас к противоречию с полученным ранее неравенством $r < p_1$. Таким образом, сделанное нами предположение о существовании натуральных чисел, обладающих несколькими разложениями на простые множители, привело нас к противоречию. Утверждение теоремы полностью доказано.

Эти и многие другие факты теории простых чисел можно найти, например, в [3], [12], [21], [25], [28], [37] и др.

Примеры решения задач

1. Разложите на простые множители число 495; число 101.

Решение. Для разложения числа 495 на простые множители проверим делимость данного числа на простые числа, не превосходящие $\sqrt{495}$: 2, 3, 5, 7, 11, 13, 17 и 19. Легко видеть, что число 495 не делится на 2, но делится на 3: $495 = 3 \cdot 165$. Далее, число 165 делится на 3: $165 = 3 \cdot 55$. В свою очередь, число 55 делится на 5: $55 = 5 \cdot 11$. Таким образом, мы получили разложение числа 495 на простые множители: $495 = 3^2 \cdot 5 \cdot 11$. Для разложения числа 101 на простые множители проверим делимость данного числа на простые числа, не превосходящие $\sqrt{101}$: 2, 3, 5 и 7. Легко видеть, что число 101 не делится ни на одно из указанных простых чисел, то есть само является простым. ▷

2. Докажите, что всякое простое число p, большее трех, представимо в виде $6q \pm 1$, $q \in \mathbb{N}$.

Решение. Пусть p — простое число. По теореме о делении с остатком, $p = 6k + r$, где $k, r \in \mathbb{Z}$, причем $0 \leqslant r < 6$. Таким образом, $r \in \{0, 1, 2, 3, 4, 5\}$. Если $r = 0$, то $p = 6k$, и, следовательно, p делится на 2 и на 3, что дает противоречие с определением простого числа. Если $r = 1$, то $p = 6k + 1$, причем k — число натуральное в силу того, что $p > 1$. Если $r = 2$, то $p = 6k + 2$, и, следовательно, p делится на 2, что возможно для простого p только в случае его совпадения с числом 2. Если $r = 3$, то $p = 6k + 3$, и, следовательно, p делится на 3, что возможно для простого p только в случае его совпадения с числом 3. Если $r = 4$, то $p = 6k + 4$, и, следовательно, p делится на 2 и не равно 2 (почему?), что дает противоречие с определением простого числа. Если $r = 5$, то $p = 6k + 5$ или, что то же, $p = 6(k + 1) - 1$, причем $k + 1$ — число натуральное в силу того, что $p > 1$. Таким образом, мы доказали, что любое простое число p, большее трех, представимо в виде $6q \pm 1$, $q \in \mathbb{N}$. ▷

Замечание. В процессе рассуждений мы доказали, что *любое простое число либо равно* 2, *либо равно* 3, *либо имеет вид* $6k + 1$, $k \in \mathbb{N}$, *либо имеет вид* $6q - 1$, $q \in \mathbb{N}$. Этот факт часто используется при решении задач.

3. Найдите все $p \in \mathbb{P}$, для которых $p + 10, p + 14 \in \mathbb{P}$.

Решение. Как было показано в ходе решения предыдущей задачи, любое простое число либо равно 2, либо равно 3, либо имеет вид $6k + 1$, $k \in \mathbb{N}$, либо имеет вид $6q - 1$, $q \in \mathbb{N}$. Если $p = 2$, то $p + 10 = 12$, то есть $p + 10 \notin \mathbb{P}$. Если $p = 3$, то $p + 10 = 13$, и $p + 14 = 17$, то есть $p + 10, p + 14 \in \mathbb{P}$. Если $p = 6k + 1$, $k \in \mathbb{Z}$, то $p + 14 = 6k + 15$, или, что то же, $p + 14 = 6(k + 2) + 3$, то есть $p + 14$ делится на 3 и не равно 3, а,

следовательно, является составным числом: $p+14 \notin \mathbb{P}$. Наконец, если $p = 6q-1$, $q \in \mathbb{Z}$, то $p+10 = 6q+9$, или, что то же, $p+10 = 6(k+1)+3$, то есть $p+10$ делится на 3 и не равно 3, а, следовательно, является составным числом: $p+10 \notin \mathbb{P}$. Таким образом, числа p, $p+10$ и $p+14$ являются простыми одновременно только при $p = 3$. ▷

4. Докажите, что сумма квадратов трех простых чисел, больших трех, есть число составное.

Решение. Как было показано ранее, любое простое число p, большее трех, имеет вид $6q \pm 1$, $q \in \mathbb{N}$. В каждом из этих случаев квадрат простого числа p имеет вид $6t+1$, $t \in \mathbb{N}$: $(6k \pm 1)^2 = 36k^2 \pm 12k + 1 = 6(6k^2 \pm 2k)+1$. Таким образом, сумма квадратов трех простых чисел, больших трех, имеет вид $6m+3$, $m \in \mathbb{N}$, и, следовательно, делится на три и не равно трем, то есть является составным числом. ▷

5. Найдите все натуральные n, для которых $8^n - 1$ — простое число.

Решение. Поскольку для любых целых чисел a и b и для любого натурального числа n имеет место тождество $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1})$, то $8^n - 1 = (8-1)\cdot(8^{n-1} + 8^{n-2} + \ldots + 8 + 1)$, или, что то же, $8^n - 1 = 7K$, где $K \in \mathbb{N}$. Следовательно, число $8^n - 1$ делится на 7 для любого натурального n. При этом если $n = 1$, то $8^n - 1 = 7$, то есть является простым числом. Если же $n > 1$, то $8^n - 1$ делится на 7 и не равно семи, то есть является числом составным. Таким образом, $8^n - 1 \in \mathbb{P}$ только при $n = 1$. ▷

6. Докажите, что для любого натурального n число $32^n + 1$ является составным.

Решение. Поскольку для любых целых чисел a и b и для любого нечетного натурального числа n имеет место тождество $a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + \ldots - ab^{n-2} + b^{n-1})$, то $32^n + 1 = (2^n)^5 + 1 = (2^n+1)\cdot(2^{4n} - 2^{3n} + 2^{2n} - 2^n + 1)$, или, что то же, $32^n + 1 = (2^n+1)L$, где $L \in \mathbb{N}$. Следовательно, число $32^n + 1$ делится на $2^n + 1$ для любого натурального n. При этом натуральное число $2^n + 1$ является нетривиальным делителем большего единицы натурального числа $32^n + 1$, поскольку $2^n + 1 \neq 1$ и $2^n + 1 \neq 32^n + 1$. Таким образом, для любого натурального n число $32^n + 1$ является составным. ▷

7. Может ли сумма пяти последовательных целых чисел быть простым числом?

Решение. Сумма пяти последовательных целых чисел z, $z+1$,..., $z+4$ имеет вид $5z + (0+1+2+3+4) = 5(z+2)$, или, что то же, вид $5q$, где $q \in \mathbb{Z}$. Следовательно, данная сумма делится на 5 и может быть простым числом только в случае совпадения с 5. Это возможно

только при $q = 1$, или, что то же, при $z = -1$, то есть искомыми последовательными целыми числами являются числа $-1, 0, 1, 2, 3$. ▷

8. При каких натуральных n число $n^4 + 4$ является простым числом?

Решение. Легко убедиться в том, что $n^4 + 4 = (n^4 + 4n^2 + 4) - 4n^2 = (n^2 + 2)^2 - (2n)^2 = (n^2 + 2 - 2n) \cdot (n^2 + 2 + 2n)$. Если $n = 1$, то данное разложение на множители тривиально: $5 = 1 \cdot 5$. Если $n > 1$, то $1 < n^2 + 2n + 2 < n^4 + 4$, откуда следует, что $n^4 + 4$ обладает нетривиальным натуральным делителем $n^2 + 2n + 2$ и, следовательно, является составным числом. Таким образом, *число $n^4 + 4$ является простым при $n = 1$ и представляет собой составное число при всех натуральных n, больших единицы.* Это утверждение называют *теоремой Софи Жермен.* ▷

9. Докажите, что любое натуральное число вида $6k - 1$, $k \in \mathbb{Z}$, имеет простой делитель того же вида. Верно ли аналогичное утверждение для натуральных чисел вида $6k + 1$, $k \in \mathbb{Z}$?

Решение. Пусть z — натуральное число вида $6k - 1$, $k \in \mathbb{Z}$. Пусть $z = p_1 \cdot p_2 \cdot \ldots \cdot p_s$ — разложение числа z на простые множители. Поскольку z нечетно, то среди его простых делителей $p_1, p_2, \ldots, p_s$ нет числа 2. Поскольку z не делится на 3, то среди его простых делителей $p_1, p_2, \ldots, p_s$ нет числа 3. Таким образом, каждое из простых чисел $p_1, p_2, \ldots, p_s$ имеет вид $6q \pm 1$, $q \in \mathbb{N}$. Если каждое из чисел $p_1, p_2, \ldots, p_s$ имеет вид $6q \pm 1$, $q \in \mathbb{N}$, то есть $p_1 = 6q_1 + 1$, $\ldots$, $p_s = 6q_s + 1$, то их произведение также имеет вид $6q + 1$: $(6q_1 + 1) \cdot \ldots \cdot (6q_s + 1) = 6q + 1$. Это приводит нас к противоречию — число z не может быть одновременно представимо как в виде $6k - 1$, $k \in \mathbb{Z}$, так и в виде $6q + 1$, $q \in \mathbb{N}$. Таким образом, хотя бы одно из чисел $p_1, \ldots, p_s$ должно иметь вид $6k - 1$, $k \in \mathbb{N}$, и, следовательно, натуральное число z вида $6k - 1$, $k \in \mathbb{Z}$, обязательно обладает простым делителем того же вида. Аналогичное утверждение не имеет места для натуральных чисел вида $6k + 1$, $k \in \mathbb{Z}$. Например, число 55 имеет вид $6k + 1$, $k \in \mathbb{Z}$, однако оба его простых делителя, 5 и 11, имеют вид $6q - 1$, $q \in \mathbb{N}$. ▷

10. Докажите, что существует бесконечно много простых чисел вида $6k - 1$, $k \in \mathbb{N}$.

Решение. Предположим, что множество простых чисел вида $6k - 1$ конечно, и что $\mathbb{P}_{6k-1} = \{p_1, p_2, \ldots, p_k\}$ — все простые числа указанного вида. Построим натуральное число $E = 6p_1 \cdot p_2 \cdot \ldots \cdot p_k - 1$. Поскольку оно имеет вид $6k - 1$, $k \in \mathbb{Z}$, то, в силу утверждения предыдущей задачи, оно обладает простым делителем p того же

вида. Легко видеть, что число p не может совпадать ни с одним из чисел $p_1, p_2, \ldots, p_k$, так как иначе p должно делить разность $E - 6p_1 \cdot p_2 \cdot \ldots \cdot p_k = 1$, что невозможно. Таким образом, p — простое число вида $6k - 1$, не попавшее в вышеприведенный список, то есть множество простых чисел вида $6k - 1$ не может исчерпываться числами $p_1, p_2, \ldots, p_k$. ▷

Упражнения

1. Разложите на простые множители числа:

а) 5472; в) 8250; д) 14 125; ж) 25 750;

б) 6624; г) 8775; е) 19 392; з) 34 800.

2. Докажите, что всякое простое число p, большее двух, представимо в виде $4q \pm 1$, $q \in \mathbb{N}$.

3. Докажите, что всякое простое число p, большее трех, представимо в виде $12q \pm 1$ или $12q \pm 5$, $q \in \mathbb{N}$.

4. Найдите все $p \in \mathbb{P}$, для которых $p + 5$, $p + 11 \in \mathbb{P}$.

5. Найдите все $p \in \mathbb{P}$, для которых $p^4 + 15 \in \mathbb{P}$.

6. Докажите, что сумма квадратов двух нечетных простых чисел есть число составное.

7. Докажите, что сумма квадратов четырех нечетных простых чисел есть число составное.

8. Найдите все натуральные n, для которых:

а) $3^n - 1 \in \mathbb{P}$; в) $12^n - 1 \in \mathbb{P}$;

б) $6^n - 1 \in \mathbb{P}$; г) $18^n - 1 \in \mathbb{P}$.

9. Докажите, что для любого натурального n:

а) $8^n + 1 \in \mathbb{S}$; в) $125^n + 8 \in \mathbb{S}$;

б) $64^n + 1 \in \mathbb{S}$; г) $32^n + 243 \in \mathbb{S}$.

10. Может ли быть простым числом сумма трех последовательных целых чисел; сумма четырех последовательных целых чисел; сумма шести последовательных целых чисел; сумма семи последовательных целых чисел?

11. При каких натуральных n число $n^4 + n^2 + 1$ является простым?

12. При каких натуральных n число $n^4 + 64$ является составным?

13. Докажите, что любое натуральное число вида $4k - 1$, $k \in \mathbb{Z}$, имеет простой делитель того же вида. Верно ли аналогичное утверждение для целых чисел вида $4k + 1$, $k \in \mathbb{Z}$?

14. Докажите, что существует бесконечно много простых чисел вида $4k - 1$, $k \in \mathbb{N}$.

Задачи

1. Составьте таблицу простых чисел p, $100 \leqslant p \leqslant 200$.
2. Составьте таблицу простых чисел p, $400 \leqslant p \leqslant 500$.
3. Найдите все тройки p, $p+2$, $p+4$ последовательных нечетных простых чисел.
4. Существуют ли четверки p, $p+2$, $p+4$, $p+6$ последовательных нечетных простых чисел?
5. Может ли сумма k последовательных нечетных чисел быть простым числом?
6. На какую цифру не может оканчиваться простое число в десятичной системе счисления?
7. Докажите, что всякое простое число p, не равное 2 и 5, представимо в виде $10k \pm 1$ или $10k \pm 3$, $k \in \mathbb{N}$.
8. Найдите все натуральные a и n, для которых $n^4 + 4a^4$ — составное число.
9. Найдите все натуральные n, для которых $2^{2n} - 1$ — простое число.
10. Найдите все простые p, для которых $7p^2 + 8$ — простое число.
11. Для каких простых p число $p+4$ является квадратом целого числа?
12. Найдите все простые числа p, для которых $2p+1$ является кубом целого числа.
13. Докажите, что если p и $2p-1$ — простые числа, большие трех, то $p-1$ делится на 6.
14. Найдите все числа p, для которых каждое из шести чисел p, $p+2$, $p+6$, $p+8$, $p+12$, $p+14$ является простым.
15. Докажите, что для любого натурального n число $(n+1)!+2$ является составным.
16. Докажите, что в натуральном ряду существуют сколь угодно длинные промежутки, не содержащие простых чисел.
17. Докажите, что $61!+1$ имеет простой делитель $p > 66$.
18. Докажите, что если простое число p является делителем числа $100!+101$, то $p \geqslant 103$.
19. Докажите, что разложение натурального числа n в произведение простых чисел содержит не более $\log_2 n$ множителей.
20. Пусть n — нечетное натуральное число. Докажите, что в разложении n на простые множители не более $\log_3 n$ множителей.
21. Докажите, что $p_n \leqslant 2^{2^{n-1}}$, где p_n — n-е простое число.
22. Если числа p и $p+2$ являются одновременно простыми, то пара $\langle p, p+2\rangle$ называется парой *простых-близнецов*. Укажите все пары $\langle p, p+2\rangle$ простых-близнецов, для которых:

а) $p \leqslant 100$; в) $100 \leqslant p \leqslant 150$;

б) $100 \leqslant p \leqslant 150$; г) $200 \leqslant p \leqslant 250$.

23. Какой остаток от деления на 12 дает сумма двух простых-близнецов, если меньшее из них больше 3?

24. Пусть $\langle p, q\rangle$ — пара простых-близнецов. Докажите, что либо $6|(q-1)$, либо $\langle p, q\rangle = \langle 3, 5\rangle$.

25. Найдите все пары простых-близнецов, в которых одно из чисел есть *число Мерсенна* $M_n = 2^n - 1$, $n \in \mathbb{N}$, а второе — *число Ферма* $F_n = 2^{2^n} + 1$, $n \in \mathbb{N} \cup \{0\}$.

§ 4. НОД и НОК

Наибольший общий делитель $(a_1, \ldots, a_n)$ целых чисел $a_1, \ldots, a_n$, хотя бы одно из которых не равно нулю, есть наибольшее целое число, делящее каждое из чисел $a_1, \ldots, a_n$.

Наименьшее общее кратное $[a_1, \ldots, a_n]$ целых чисел $a_1, \ldots, a_n$, каждое из которых не равно нулю, есть наименьшее натуральное число, делящееся на каждое из чисел $a_1, \ldots, a_n$.

Например, $(4, -6) = 2$, так как множество общих делителей чисел 4 и -6 имеет вид $\{-2, -1, 1, 2\}$, и его наибольший элемент равен 2. Аналогично, $[4, -6] = 12$, так как множество общих кратных чисел 4 и -6 имеет вид $\{\ldots, -36, -24, -12, 12, 24, 36, \ldots\}$, и его наименьший натуральный элемент равен 12.

Свойства НОД и НОК

1. $(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}, p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_s^{\beta_s}) = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \ldots \cdot p_s^{\gamma_s}$, $[p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}, p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_s^{\beta_s}] = p_1^{\delta_1} \cdot p_2^{\delta_2} \cdot \ldots \cdot p_s^{\delta_s}$, где $\alpha_i, \beta_i \geqslant 0$, $\gamma_i = \min\{\alpha_i, \beta_i\}$, и $\delta_i = \max\{\alpha_i, \beta_i\}$, $i = 1, 2, \ldots, s$.
2. Каждый общий делитель чисел a и b делит (a, b).
3. Каждое общее кратное чисел a и b делится на $[a, b]$.
4. Если $(a, b) = d$, то существуют целые числа x и y, такие что $ax + by = d$.
5. Если $a|bc$, и $(a, b) = d$, то $\dfrac{a}{d}|c$.
6. $(ma, mb) = m(a, b)$ для любого $m \in \mathbb{N}$.
7. Если $m|a$ и $m|b$, где $m \in \mathbb{N}$, то $(a/m,\ b/m) = (a, b)/m$.
8. Если $a \in \mathbb{Z}$, $b \in \mathbb{N}$, и $b|a$, то $(a, b) = b$.
9. Если целые числа a, b, c, k связаны соотношением $a = bk + c$, то $(a, b) = (b, c)$.

10. $(a + mb, b) = (a, b)$ для любого $m \in \mathbb{Z}$.
11. $(a, b) \cdot [a, b] = ab$ для любых $a, b \in \mathbb{N}$.

Доказательство первого утверждения основано на том, что любой общий делитель чисел $a = \prod_{i=1}^{s} p_i^{\alpha_i}$ и $b = \prod_{i=1}^{s} p_i^{\beta_i}$, где $\alpha_i, \beta_i \geqslant 0$, имеет вид $\pm \prod_{i=1}^{s} p_i^{\eta_i}$, где $0 \leqslant \eta_i \leqslant \min\{\alpha_i, \beta_i\}$, в то время как любое общее кратное этих чисел имеет вид $\pm \prod_{i=1}^{s} p_i^{\theta_i}$, где $\theta_i \geqslant \max\{\alpha_i, \beta_i\}$. Для доказательства свойства 9 рассмотрим множество $M_{a,b}$ общих делителей чисел a и b и множество $M_{b,c}$ общих делителей чисел b и c. Докажем, что эти множества совпадают. Действительно, если $x \in M_{a,b}$, то $x|a$ и $x|b$, а значит, $x|c$ в силу равенства $a = bk + c$, то есть $x \in M_{b,c}$. Аналогичные рассуждения позволяют утверждать: если $y \in M_{b,c}$, то $y \in M_{a,b}$. Итак, множества $M_{a,b}$ и $M_{b,c}$ совпадают, а, следовательно, совпадают и их наибольшие элементы, то есть $(a, b) = (b, c)$. Доказательства остальных свойств можно найти, например, в [3], [28].

Примеры решения задач

1. Найдите наибольший общий делитель и наименьшее общее кратное чисел: 15, −12, 3.

Решение. Рассматривая множества $\{\pm1, \pm3, \pm5, \pm15\}$, $\{\pm1, \pm2, \pm3, \pm4, \pm6, \pm12\}$ и $\{\pm1, \pm3\}$ делителей чисел 15, −12 и 3, соответственно, мы убеждаемся в том, что наибольший общий делитель указанных чисел равен 3. Рассматривая множества $\{\pm15, \pm30, \pm45, \pm60, \ldots\}$, $\{\pm12, \pm24, \pm36, \pm48, \pm60, \ldots\}$ и $\{\pm3, \pm6, \pm9, \ldots, \pm60, \ldots\}$ кратных чисел 15, −12 и 3, соответственно, мы убеждаемся в том, что наименьшее общее кратное указанных чисел равно 60. ▷

2. Найдите наибольший общий делитель и наименьшее общее кратное чисел 1500, −1224, −1440.

Решение. Для решения задачи разложим каждое из чисел 1500, 1224 и 1440 на простые множители. Легко убедиться в том, что $1500 = 2^2 \cdot 3 \cdot 5^3$, $1224 = 2^3 \cdot 3^2 \cdot 17$, и $1440 = 2^5 \cdot 3^2 \cdot 5$. Другими словами, $(1500, -1224, -1440) = (1500, 1224, 1440) = (2^2 \cdot 3^1 \cdot 5^3 \cdot 17^0, 2^3 \cdot 3^2 \cdot 5^0 \cdot 17^1, 2^5 \cdot 3^2 \cdot 5^1 \cdot 17^0)$. Выбирая минимальные значения показателей входящих в разложения простых чисел, мы получим, что $(1500, -1224, -1440) = 2^2 \cdot 3^1 \cdot 5^0 \cdot 17^0 = 2^2 \cdot 3 = 12$. Аналогично, $[1500, -1224, -1440] = [2^2 \cdot 3^1 \cdot 5^3 \cdot 17^0, 2^3 \cdot 3^2 \cdot 5^0 \cdot 17^1, 2^5 \cdot 3^2 \cdot 5^1 \cdot 17^0]$, и, выбирая минимальные значения показателей входящих в разложения простых чисел, мы получим, что $[1500, -1224, -1440] = 2^5 \cdot 3^2 \cdot 5^3 \cdot 17^1 = 612\,000$. ▷

3. Сократите дробь 1224/1440.

Решение. Для решения задачи найдем (1224, 1440). Как было показано ранее, $1224 = 2^3 \cdot 3^2 \cdot 17$, и $1440 = 2^5 \cdot 3^2 \cdot 5$. Другими словами, $(1224, 1440) = (2^3 \cdot 3^2 \cdot 5^0 \cdot 17^1, 2^5 \cdot 3^2 \cdot 5^1 \cdot 17^0) = 2^3 \cdot 3^2 = 72$. Тогда $1224/1440 = 17/2^2 \cdot 5 = 17/20$. ▷

4. Приведите дроби 1/1224, 7/1500 и $-13/1440$ к наименьшему общему знаменателю и найдите их сумму.

Решение. Для решения задачи вспомним, что

$$[1224, 1500, 1440] = 2^5 \cdot 3^2 \cdot 5^3 \cdot 17^1 = 612\,000.$$

Тогда

$$\frac{1}{1224} = \frac{2^2 \cdot 5^3}{2^5 \cdot 3^2 \cdot 5^3 \cdot 17} = \frac{600}{612000}, \quad \frac{7}{1500} = \frac{2^3 \cdot 3 \cdot 7 \cdot 17}{2^5 \cdot 3^2 \cdot 5^3 \cdot 17} = \frac{2856}{612000},$$
$$-\frac{11}{1440} = -\frac{3 \cdot 5^2 \cdot 13 \cdot 17}{2^5 \cdot 3^2 \cdot 5^3 \cdot 17} = -\frac{14025}{612000}.$$

Следовательно,

$$\frac{1}{1224} + \frac{7}{1500} - \frac{13}{1440} = \frac{600 + 2856 - 14025}{612000} = \frac{10569}{612000} =$$
$$= \frac{3 \cdot 13 \cdot 271}{2^5 \cdot 3^2 \cdot 5^3 \cdot 17} = \frac{13 \cdot 271}{2^5 \cdot 3 \cdot 5^3 \cdot 17} = \frac{3523}{204000}.$$ ▷

5. Докажите, что $(a, b) \cdot [a, b] = ab$ для любых $a, b \in \mathbb{N}$.

Решение. Пусть $a = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$, и $b = p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s}$, где $p_1, \ldots, p_s$ — различные простые числа, а $\alpha_1, \beta_1, \ldots, \alpha_s, \beta_s$ — целые неотрицательные числа. Тогда, с одной стороны, $a \cdot b = p_1^{\alpha_1+\beta_1} \cdot \ldots \cdot p_s^{\alpha_s+\beta_s}$. С другой стороны, $(a, b) = p_1^{\min\{\alpha_1,\beta_1\}} \cdot \ldots \cdot p_s^{\min\{\alpha_s,\beta_s\}}$, $[a, b] = p_1^{\max\{\alpha_1,\beta_1\}} \cdot \ldots \cdot p_s^{\max\{\alpha_s,\beta_s\}}$, и $(a, b) \cdot [a, b] = p_1^{\max\{\alpha_1,\beta_1\}+\min\{\alpha_1,\beta_1\}} \cdot \ldots \cdot p_s^{\max\{\alpha_s,\beta_s\}+\min\{\alpha_s,\beta_s\}}$. Поскольку имеет место очевидное соотношение $\max\{\alpha,\beta\}+\min\{\alpha,\beta\} = \alpha+\beta$, то $(a, b) \cdot [a, b] = ab$. ▷

Упражнения

1. Найдите наибольший общий делитель и наименьшее общее кратное чисел:

а) 10, 5 и −20;
б) 14, −21 и −7;
в) 1200 и −396;
г) 8888 и −666;
д) 288, 336 и −1220;
е) 48, 999 и 1580.

2. Сократите дроби:

а) 540/546; в) 1725/2295; д) 2002/1980;

б) $-1224/1440$; г) $-2431/3025$; е) $-819/1690$.

3. Приведите дроби к наименьшему общему знаменателю и найдите их сумму:

а) 1/210, 3/100, 13/294; в) 5/297, 13/396;

б) 1/1224, 7/1500, $-13/1440$; г) 7/1625, $-11/2925$.

4. Докажите, что $(ma, mb) = m(a, b)$ для любого $m \in \mathbb{N}$.

5. Докажите, что если $m|a$ и $m|b$, где $m \in \mathbb{N}$, то $(a/m,\ b/m) = (a, b)/m$.

Задачи

1. Сократите дроби:

а) 1200/3690; в) $-3267/65219$; д) 12348/1456;

б) $-9999/100002$; г) $-3042/1716$; е) $-6048/9072$.

2. Приведите дроби 1200/3690, 9/100002, 1/1224 и 7/1500 к общему знаменателю.

3. Найдите натуральное число c, если $c = (735, b)$, где $b = (1050, 80)$.

4. Найдите натуральные числа m и n, сумма которых равна 20, а $(m, n) = 5$.

5. Найдите НОД чисел 11 111 111 и $\underbrace{111\ldots\ldots111}_{\text{сто единиц}}$.

6. Докажите, что для любых целых чисел $a_1, a_2, \ldots, a_n$, хотя бы одно из которых отлично от нуля, существует наибольший общий делитель.

7. Докажите, что что для любых целых чисел $a_1, a_2, \ldots, a_n$, хотя бы одно из которых отлично от нуля, $(a_1, a_2, \ldots, a_k, 0, 0, \ldots, 0) = (a_1, a_2, \ldots, a_k)$.

8. При любом натуральном n найдите наименьшее общее кратное чисел:

а) $n^3 + 11n$ и 6; в) $n^5 + 4n$ и 10;

б) $(n^2 - 1) \cdot n^2 \cdot (n^2 + 1)$ и 60; г) $n^5 - 5n^4 + 4n$ и 10.

9. Докажите, что $[1, 2, \ldots, n, n + 1, \ldots, 2n] = [n + 1, \ldots, 2n]$.

10. Чему может быть равно наименьшее общее кратное трех последовательных натуральных чисел?

11. Найдите наименьшее натуральное число, которое делится на 2, 3, 4, 5, 6, 7, 8, 9 и 10.

12. Найдите наименьшее натуральное число, делящееся на 7 и дающее остаток 1 при делении на каждое из чисел 2, 3, 4, 5, 6.

13. Докажите, что $abc = [a, b, c](ab, ac, bc)$, если $a, b, c \in \mathbb{N}$.

14. Какое наименьшее число студентов могло сдавать экзамен при условии, что четырнадцатая часть из них получила оценку «неудовлетворительно», 75% — «удовлетворительно», 15% — «хорошо» и не менее пяти человек — «отлично» ?

15. В депо было сформировано 2 поезда из одинаковых вагонов: первый — на 456 пассажиров, второй — на 494 пассажира. Сколько вагонов в каждом поезде, если известно, что общее число вагонов не превышает 30?

§ 5. Алгоритм Евклида

Алгоритм Евклида — алгоритм для определения наибольшего общего делителя двух чисел путем последовательного применения теоремы о делении с остатком.

Именно, *для любого целого a и любого натурального b, не делящего a, наибольший общий делитель чисел a и b равен последнему ненулевому остатку r_s следующего алгоритма*:

$$a = bq_1 + r_1, \quad 0 < r_1 < b, \quad b = r_1q_2 + r_2, \quad 0 < r_2 < r_1,$$

$$\dots,$$

$$r_{s-2} = r_{s-1}q_s + r_s, \quad 0 < r_s < r_{s-1}, \quad r_{s-1} = r_sq_s + 0,$$

где $q_i, r_i \in \mathbb{Z}$, $i = 1, 2, \dots, s$. Другими словами, *наибольший общий делитель чисел a и b* ($a \in \mathbb{Z}, b \in \mathbb{N}$, $b \nmid a$) *равен последнему ненулевому остатку алгоритма Евклида, записанного для этих чисел.*

Действительно, пользуясь свойством 9 предыдущего параграфа, мы можем утверждать, что $(a, b) = (b, r_1) = (r_1, r_2) = (r_{s-2}, r_{s-1}) = (r_{s-1}, r_s)$, в то время как $(r_{s-1}, r_s) = r_s$ по свойству 8 предыдущего параграфа. При этом наличие хотя бы одного ненулевого остатка обеспечивается условием $b \nmid a$, в то время как существование последнего ненулевого остатка (то есть конечное число шагов алгоритма) следует из того факта, что числа $r_1, r_2, \dots, r_s$ образуют строго убывающую последовательность $b > r_1 > r_2 > \dots > r_s > 0$ *натуральных чисел, которая заведомо конечна.* (См., например, [3], [28].)

Например, алгоритм Евклида для чисел 1071 и 1029 имеет вид $1071 = 1029 \cdot 1 + 42$, $1029 = 42 \cdot 24 + 21$, $42 = 21 \cdot 2 + 0$, и мы получаем, что $(1071, 1029) = 21$.

Алгоритм Евклида является одним из старейших известных алгоритмов. Он встречается в «Началах» Евклида около 300 года до нашей эры. Евклид формулировал проблему геометрически, как задачу нахождения общей «меры» для двух отрезков, и его алгоритм состоял в последовательном вычитании меньшего отрезка из большего. Однако вероятно, что

алгоритм не был открыт Евклидом, а появился почти на 200 лет раньше. Он был, скорее всего, известен Евдоксу (около 375 года до нашей эры); Аристотель (около 330 года до нашей эры) упоминал о нем в своих трудах.

Этот алгоритм может быть использован на любом множестве, где возможно деление с остатком. Такие множества включают в себя кольца многочленов над полем, кольцо целых чисел Гаусса, наконец, Евклидовы области.

Примеры решения задач

1. Пользуясь алгоритмом Евклида, найдите (663, 126).

Решение. Следуя описанному выше алгоритму, получаем: $663 = 126 \cdot 5 + 33$, $126 = 33 \cdot 3 + 27$, $33 = 27 \cdot 1 + 6$, $27 = 6 \cdot 4 + 3$, $6 = 3 \cdot 2 + 0$, причем $0 < 3 < 22 < 27 < 49$. Таким образом, последний ненулевой остаток алгоритма Евклида равен 3, откуда следует, что $(213, 49) = 3$. Заметим, что в данном случае наибольший общий делитель можно найти и с помощью разложения каждого из чисел на простые множители: $(663, 126) = (3 \cdot 13 \cdot 17, 2 \cdot 3^2 \cdot 7) = 3$. ▷

2. Пользуясь алгоритмом Евклида, найдите наибольший общий делитель d чисел 232 и 44; укажите два целых числа x_0, y_0, таких что $d = 232x_0 + 44y_0$.

Решение. Поскольку $232 = 44 \cdot 5 + 12$, $44 = 12 \cdot 3 + 8$, $12 = 8 \cdot 1 + 4$, и $8 = 4 \cdot 2 + 0$, то последний ненулевой остаток алгоритма Евклида равен 4, откуда следует, что и $(232, 44) = 4$. Теперь нетрудно представить число 4 как линейную комбинацию исходных чисел 232 и 44, «поднимаясь по ступенькам» построенного алгоритма снизу вверх, начиная от предпоследней: $4 = 12 - 8 \cdot 1$, $4 = 12 - (44 - 12 \cdot 3) \cdot 1 = 44 \cdot (-1) + 12 \cdot 4$, $4 = 44 \cdot (-1) + (232 - 44 \cdot 5) \cdot 4 = 44 \cdot (-21) + 232 \cdot 4$. Таким образом, $4 = 232 \cdot 4 + 44 \cdot (-21)$, то есть $x_0 = 4$, и $y_0 = -21$. ▷

Замечание. Схема решения данной задачи позволяет доказать свойство 4 предыдущего параграфа: *если* $(a, b) = d$, *то существуют целые числа* x *и* y, *такие что* $d = ax + by$.

3. При любом натуральном n найдите наибольший общий делитель чисел: $6n^4 + n^2 + 3n$ и $2n^3 + 1$; $6n^6 + 10n^5 + 4n^3 + n$ и $3n^3 + 5n^2 + 2$.

Решение. В первом случае, следуя алгоритму Евклида, получаем: $6n^4 + n^2 + 3n = (2n^3 + 1) \cdot (3n) + n^2$, $2n^3 + 1 = n^2 \cdot (2n) + 1$, и $n^2 = 1 \cdot n^2 + 0$. таким образом, последний ненулевой остаток алгоритма Евклида равен 1, и $(6n^4 + n^2 + 3, 2n^3 + 1) = 1$ при любом натуральном n. Во втором случае, следуя алгоритму Евклида, получаем: $6n^6 + 10n^5 + 4n^3 + n = (3n^3 + 5n^2 + 2) \cdot (2n^3) + n$,

$3n^3+5n^2+2=n\cdot(3n^2+5n)+2$. Далее, $n=2\cdot k+r$, где $r\in\{0,1\}$. При $r=0$, то есть в случае $n=2k$, последний ненулевой остаток алгоритма Евклида равен 2, то есть $(6n^6+10n^5+4n^3+n,\ 3n^3+5n^2+2)=2$ при четных n. При $r=1$, то есть в случае $n=2k+1$, следующий шаг алгоритма имеет вид $2=1\cdot 2+0$, и последний ненулевой остаток алгоритма Евклида равен 1, то есть $(6n^6+10n^5+4n^3+n,\ 3n^3+5n^2+2)=1$ в случае нечетного n. ▷

4. Сократите дробь: $\dfrac{6n+4}{22n+15}$; $\dfrac{16n+60}{11n+41}$.

Решение. В первом случае, следуя алгоритму Евклида, получаем: $22n+15=(6n+4)\cdot 3+(4n+3)$, $6n+4=(4n+3)\cdot 1+(2n+1)$, $4n+3=(2n+1)\cdot 2+1$, и $2n+1=1\cdot(2n+1)+0$. Таким образом, последний ненулевой остаток алгоритма Евклида равен 1, и $(6n+4,\ 22n+15)=1$ при любом натуральном n, то есть дробь $\dfrac{6n+4}{22n+15}$ несократима. Во втором случае, следуя алгоритму Евклида, получаем: $16n+60=(11n+41)\cdot(5n+19)$, $11n+41=(5n+19)\cdot 2+(n+3)$, $5n+19=(n+3)\cdot 5+4$. Далее, $n+3=4\cdot k+r$, где $r\in\{0,1,2,3\}$. При $r=0$, то есть в случае $n+3=4k$, последний ненулевой остаток алгоритма Евклида равен 4, то есть $(16n+60,\ 11n+41)=4$ при $n=4k-3$ или, что то же, при $n=4t+1$, и дробь сократима на 4:

$$\frac{16n+60}{11n+41}=\frac{16(4t+1)+60}{11(4t+1)+41}=\frac{64t+76}{44t+52}=\frac{16t+19}{11t+12}.$$

При $r=1$, то есть в случае $n+3=4\cdot k+1$, следующий шаг алгоритма имеет вид $4=1\cdot 4+0$, и последний ненулевой остаток алгоритма Евклида равен 1, то есть $(16n+60,\ 11n+41)=1$ при $n=4k-2$ или, что то же, при $n=4t+2$, и дробь несократима. При $r=2$, то есть в случае $n+3=4\cdot k+2$, следующий шаг алгоритма имеет вид $4=2\cdot 2+0$, и последний ненулевой остаток алгоритма Евклида равен 2, то есть $(16n+60,\ 11n+41)=2$ при $n=4k-1$ или, что то же, при $n=4t+3$, и дробь сократима на 2:

$$\frac{16n+60}{11n+41}=\frac{16(4k-1)+60}{11(4k-1)+41}=\frac{64k+44}{44k+30}=\frac{32k+22}{22t+15}.$$

Наконец, при $r=3$, то есть в случае $n+3=4\cdot k+3$, следующие два шага алгоритма имеют вид $4=3\cdot 1+1$, $3=1\cdot 3+0$, и последний ненулевой остаток алгоритма Евклида равен 1, то есть $(16n+60,\ 11n+41)=1$ при $n=4k$, и дробь несократима. ▷

5. Для целых чисел a и b найдите наибольший общий делитель чисел $5a+3b$ и $3a+2b$, если $(a,b)=5$.

Решение. Записав цепочку равенств $5a+3b=(3a+2b)\cdot 1+(2a+b)$, $3a+2b=(2a+b)\cdot 1+(a+b)$, $2a+b=(a+b)\cdot 1+a$, $a+b=a\cdot 1+b$ и пользуясь тем, что $(a,b)=(b,c)$ в случае равенства $a=b\cdot k+c$, мы можем записать, что $(5a+3b,3a+2b)=(3a+2b,2a+b)=(2a+b,a+b)=$ $=(a+b,a)=(a,b)$, откуда следует, что $(5a+3b,3a+2b)=5$. ▷

Замечание. Алгоритм, использованный при решении данной задачи, не является алгоритмом Евклида, поскольку при целых a и b вторые слагаемые правых частей полученных равенств далеко не всегда являются «настоящими» остатками: например, при $a=-10$, $b=5$ величина $2a+b=-15$, в то время как остаток должен быть, по крайней мере, неотрицательным числом.

Упражнения

1. Пользуясь алгоритмом Евклида, найдите:

а) $(6238,445)$; в) $(-1836,-5292)$;

б) $(-872,236)$; г) $(-555,444)$.

2. Пользуясь алгоритмом Евклида, найдите наибольший общий делитель d чисел a и b и укажите два целых числа x_0, y_0, таких что $d=a\cdot x_0+b\cdot y_0$:

а) $a=12$, $b=28$; г) $a=-80$, $b=-1024$;

б) $a=-34$, $b=90$; д) $a=99$, $b=102$;

в) $a=91$, $b=-150$; е) $a=780$, $b=-45$.

3. При любом натуральном n найдите наибольший общий делитель чисел:

а) n^2+3n+1 и $n+3$; б) $3n^4+6n^2+1$ и n^3+2n.

4. Сократите дробь:

а) $\dfrac{3n+2}{4n+3}$; б) $\dfrac{6n+5}{8n+7}$; в) $\dfrac{5n+2}{3n+2}$; г) $\dfrac{9n+8}{7n+4}$.

5. Для целых чисел a и b найдите:

а) $(5a+7b,3a+4b)$, если $(a,b)=3$; в) $(7a+5b,3a+2b)$, если $(a,b)=2$;

б) $(13a+2b,20a+3b)$, если $(a,b)=1$; г) $(7a+2b,11a+3b)$, если $(a,b)=4$.

Задачи

1. Пользуясь алгоритмом Евклида, найдите:

а) $(1234,5678)$; д) $(1219,1357)$;

б) $(-765,-432)$; е) $(-667,580)$;

в) $(111,3333)$; ж) $(-1256,-8844)$;

г) $(2747,3149)$; з) $(7711,1122)$.

2. При любом натуральном n найдите наибольший общий делитель чисел:

а) n^2+1 и n^3+2n^2+2n+1;

б) n^3+3n^2+6n+2 и n^2+3n+5;

в) $n^4+2n^3+2n^2+3n+1$ и n^3+2n^2+2n+2.

3. При любом натуральном n найдите наибольший общий делитель чисел:

а) 4 и $2n+1$;

б) 3 и $3n+2$;

в) 25 и $5n+4$;

г) 10 и n^6-n^2+1.

4. Найдите наименьшее натуральное число n, при котором все дроби $7/(n+9)$, $8/(n+10)$, $9/(n+11)$, ..., $31/(n+33)$ несократимы.

5. Сократите дробь:

а) $\dfrac{6n+4}{22n+15}$; б) $\dfrac{16n+60}{11n+41}$; в) $\dfrac{6n+5}{3n+2}$; г) $\dfrac{21n+4}{14n+3}$.

6. Пользуясь алгоритмом Евклида, найдите наибольший общий делитель d чисел a и b и укажите два целых числа x_0, y_0, таких что $d = a\cdot x_0 + b\cdot y_0$:

а) $a=137$, $b=-31$;

б) $a=103$, $b=189$;

в) $a=41$, $b=47$;

г) $a=213$, $b=-321$;

д) $a=-56$, $b=44$;

е) $a=162$, $b=99$.

7. Пользуясь алгоритмом Евклида, найдите хотя бы одно целое решение уравнения:

а) $26x+91y=11$; в) $73x+85y=7$; д) $311x-28y=2$;

б) $33x+51y=21$; г) $44x+187y=22$; е) $253x-449y=3$.

8. Докажите, что для любого натурального n уравнение $7x-10y=n$ разрешимо в натуральных числах.

9. Докажите, что наибольший общий делитель чисел a и b делится на любой их общий делитель.

§ 6. Взаимно простые числа

Два целых числа a и b называются *взаимно простыми*, если их наибольший общий делитель равен 1. Другими словами, числа a и b взаимно просты, если они не имеют общих делителей, отличных от 1 и -1.

Например, 6 и 35 взаимно просты, так как $(6, 35) = 1$, но 6 и 27 не являются взаимно простыми, так как $(6, 27) = 3$.

Число 1 взаимно просто с любым целым числом; число 0 взаимно просто только с 1 и -1.

Свойства взаимно простых чисел

1. Целые числа a и b являются взаимно простыми тогда и только тогда, когда существуют целые числа x и y, такие что $ax+by=1$ (*критерий взаимной простоты*).
2. Если $b|ac$ и $(b,c)=1$, то $b|a$.
3. Если $b|a$, $c|a$ и $(b,c)=1$, то $bc|a$.
4. $(a,b)=1$ тогда и только тогда, когда $(a^n,b^m)=1$ для любых неотрицательных целых чисел m и n.

Например, доказательство критерия взаимной простоты опирается на следующие соображения: с одной стороны, если $(a,b)=1$, то, как было доказано ранее, существуют целые числа x и y, такие что $ax+by=1$; с другой стороны, если $ax+by=1$ и $(a,b)=d$, то $d|(ax+by)$, откуда следует, что $d|1$, то есть $d=1$. Для доказательства остальных свойств можно использовать общие соображения теории делимости (см., например, [28]). Однако рассуждения станут значительно проще, если воспользоваться следующим очевидным соображением: *натуральные числа a и b являются взаимно простыми тогда и только тогда, когда они не имеют общих простых делителей.*

Примеры решения задач

1. Докажите, что n^5-n делится на 30 при любом натуральном n.

Решение.

Конечно, можно решить данную задачу стандартным способом: рассмотрев все тридцать остатков 0, 1, ..., 29 при делении на 30, убедиться, что n^5 и n имеют одинаковые остатки при делении на 30, и, следовательно, число n^5-n дает остаток ноль при делении на 30, то есть делится на 30. Однако значительно проще решить данную задачу, пользуясь свойствами взаимно простых чисел. Именно, $30=2\cdot3\cdot5$, причем числа 2, 3 и 5 попарно взаимно просты. Если мы покажем, что число n^5-n делится одновременно на 2, на 3 и на 5, то тогда, в силу

Таблица 5

rest(n, 2)	0	1	Rest(n, 3)	0	1	-1	Rest(n, 5)	0	1	2	-2	-1
rest(n^5, 2)	0	1	Rest(n^5, 3)	0	1	-1	Rest(n^5, 5)	0	1	2	-2	-1
rest(n^5-n, 2)	0	0	rest(n^5-n, 3)	0	0	0	rest(n^5-n, 5)	0	0	0	0	0

свойств взаимно простых чисел, $n^5 - n$ будет делится и на произведение чисел 2, 3 и 5, то есть будет делиться на 30. Проверка делимости числа $n^5 - n$ на 2, 3 и 5 стандартна и отражена в табл. 5. ▷

2. Докажите, что $n^4 - 1$ делится на 10, если n — целое число, взаимно простое с 10.

Решение. Записывая число n в виде $n = 10k + R$, $R \in \{0, \pm 1, \pm 2, \pm 3, \pm 4, 5\}$, и пользуясь свойствами наибольшего общего делителя, легко убедиться в том, что $(n, 10) = (10, R)$, и, следовательно, для числа $n = 10k + R$, взаимно простого с 10, имеет место соотношение $(10, R) = 1$, откуда следует, что $R \in \{\pm 1, \pm 3\}$. Поскольку $(\pm 1)^4 = 1$ и $(\pm 3)^4 = 81$, то мы убедились в том, что для n, взаимно простого с 10, остаток числа n^4 при делении на 10 равен 1, то есть число $n^4 - 1$ делится на 10. ▷

3. Докажите, что натуральные числа n, $n + 1$ и $2n + 1$ попарно взаимно просты.

Решение. Проверку этого факта можно проводить различными способами. Например, предположив, что $(n, n + 1) = d$, мы получаем, что $d|n$ и $d|(n + 1)$, откуда следует, что $d|((n + 1) - n)$, то есть $d|1$, и, следовательно, $d = 1$, то есть числа n и $n + 1$ взаимно просты. Применив к числам n и $2n + 1$ алгоритм Евклида, мы получим, что $2n + 1 = n \cdot 2 + 1$ и $n = 1 \cdot n + 0$, откуда следует, что $(2n + 1, n) = 1$, то есть числа n и $2n + 1$ взаимно просты. Аналогично, алгоритм Евклида для чисел $n + 1$ и $2n + 1$ принимает вид $2n + 1 = (n + 1) \cdot 1 + n$, $n + 1 = n \cdot 1 + 1$ и $n = 1 \cdot n + 0$, откуда следует, что $(2n + 1, n + 1) = 1$, то есть числа $n + 1$ и $2n + 1$ взаимно просты. ▷

4. Докажите, что два натуральных числа a и b, больших единицы, взаимно просты тогда и только тогда, когда их разложения на простые множители состоят из различных простых чисел.

Решение. Пусть $a = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ и $b = q_1^{\beta_1} \cdot \ldots \cdot q_s^{\beta_s}$ — канонические разложения натуральных чисел a и b, больших единицы. Пусть $(a, b) = 1$. Предположим, что $p_i = q_j$ для некоторых $i \in \{1, \ldots, k\}$ и $j \in \{1, \ldots, s\}$. Тогда $p_i|a$, $p_i|b$, и, следовательно, $p_i|(a, b)$, то есть $p_i|1$, что дает противоречие. Обратно, пусть $p_i \neq q_j$ для всех $i \in \{1, \ldots, k\}$ и $j \in \{1, \ldots, s\}$. Кроме того, пусть $(a, b) = d > 1$. Тогда существует простое число p, делящее d, и, следовательно, делящее a и b, то есть входящее в каноническое разложение каждого из указанных чисел, что опять ведет к противоречию. ▷

Упражнения

1. Докажите, что при любом натуральном n:
   а) $n^6 - n^2$ делится на 60;
   б) $n^7 - n^3$ делится на 120;
   в) $10^n + 5$ делится на 15;
   г) $7^{6n} - 1$ делится на 18.
2. Докажите, что $n^6 + 17$ делится на 9, если n — целое число, взаимно простое с 9.
3. Докажите, что $n^2 - 1$ делится на 24, если n — целое число, взаимно простое с 6.
4. Докажите, что натуральные числа $4n + 3, 2n + 2$ и $2n + 1$ попарно взаимно просты.
5. Докажите, что натуральные числа $4n - 1, n$ и $2n - 1$ попарно взаимно просты.
6. Докажите, что два различных простых числа p и q взаимно просты: $(p, q) = 1$, если $p, q \in \mathbb{P}$, $p \neq q$.
7. Докажите, что взаимно просты целые неотрицательные степени двух различных простых чисел p и q: $(p^n, q^m) = 1$, если $p, q \in \mathbb{P}$, $p \neq q$, $n, m \in \mathbb{N} \cup \{0\}$.

Задачи

1. Докажите, что если $(a, b) = 1$, то $(ac, b) = (b, c)$, где $a, b, c \in \mathbb{Z}$.
2. Докажите, что $(a, b) = (a + b, [a, b])$, где $a, b \in \mathbb{Z}$.
3. Найдите натуральные числа a и b, такие, что:
   а) $a + b = 75$ и $[a, b] = 90$;
   б) $a - b = 18$ и $[a, b] = 165$;
   в) $a^2 - b^2 = 64$ и $[a, b] = 30$;
   г) $a^2 + b^2 = 13$ и $[a, b] = 6$.
4. Найдите $(a + b, a^2 + b^2)$, если $a, b \in \mathbb{Z}$, $(a, b) = 1$.
5. Пусть m — натуральное число, взаимно простое с 10. Докажите, что существует делящееся на m натуральное число, десятичная запись которого состоит из одних единиц.
6. Докажите, что при любом натуральном n произведение $n(n+1)\cdot$ $\cdot(n+2)(n+3)$ делится на 24.
7. Докажите, что при любом натуральном n:
   а) $n^2(n^2 - 1)$ делится на 12;
   б) $30^n + 5^{4n} - 4^{2n} - 1$ делится на 58;
   в) $n^5 - 5n^3 + 4n$ делится на 120;
   г) $n(n^4 - 125n^2 + 4)$ делится на 60.

8. Докажите, что при любых целых a и b число $ab(a^4 - b^4)$ делится на 30.

9. Докажите, что число $7a^3/3 + 3a^2/2 + a/6$ является целым при любом натуральном a.

10. Докажите, что $(n^7 - n^3 + 1, 30) = 1$ при любом натуральном n.

11. Докажите, что из равенства несократимых дробей следует равенство их числителей и знаменателей.

12. Пусть $m, n, a \in \mathbb{N}$, причем $(m, n) = 1$. Докажите, что если $d|(a^m - 1)$ и $d|a^n - 1$, то $d|(a^t - 1)$ при любом натуральном t.

§ 7. Функции $\lfloor x \rfloor$ и $\{x\}$

В теории чисел рассматриваются разнообразные функции, значения которых для натурального аргумента n связаны с арифметической природой числа n. Множество таких функций обычно ограничивают только одним требованием: каждая функция должна быть определена для всех натуральных значений аргумента. Таким образом, комплекснозначная функция $f(n)$ называется *арифметической функцией* (или *числовой функцией*), если значение $f(n)$ определено для любого натурального числа n. Обычно в теории чисел рассматриваются либо функции, которые вообще определены только при натуральных значениях аргумента, либо функции, для которых натуральные (целые) значения аргумента являются характеристическими точками, определяющими величину функции и в других точках.

Известными арифметическими функциями являются функции *целая часть числа* и *дробная часть числа*.

Функция *целая часть* x, обозначаемая $\lfloor x \rfloor$, есть наибольшее целое число, не превосходящее x. Например, $\lfloor 2.9 \rfloor = 2$, $\lfloor -2 \rfloor = -2$, и $\lfloor -2.3 \rfloor = -3$.

Функция *дробная часть* x, обозначаемая $\{x\}$, определяется как $\{x\} = x - \lfloor x \rfloor$. Например, $\{2.9\} = 0.9$, $\{-2\} = 0$, и $\{-2.3\} = 0.7$.

Часто используется и функция $||x|| = \min\{\{x\}, 1 - \{x\}\}$, дающая расстояние от x до ближайшего целого числа. Например, $||2.9|| = 0.1$, $|| - 2|| = 0$, и $|| - 2.3|| = 0.3$.

Менее известна функция $\lceil x \rceil$, определяемая как наименьшее целое число, большее или равное x. Например, $\lceil 2{,}9 \rceil = 3$, $\lceil -2 \rceil = -2$, и $\lceil -2{,}3 \rceil = -2$.

Свойства функций $\lfloor x \rfloor$ и $\{x\}$

1. $\lfloor x \rfloor \leqslant x < \lfloor x \rfloor + 1$ для любого действительного числа x с равенством слева, если и только если x — целое число.
2. $\lfloor k + x \rfloor = k + \lfloor x \rfloor$ для любого целого k и любого действительного x.
3. Если x — действительное число и n — целое число, то $n \leqslant x$, если и только если $n \leqslant \lfloor x \rfloor$.

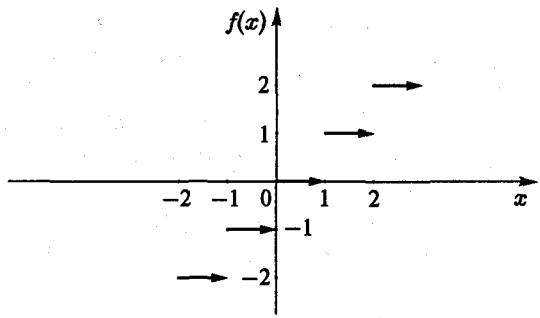

Рис. 1. $f(x) = \lfloor x \rfloor$

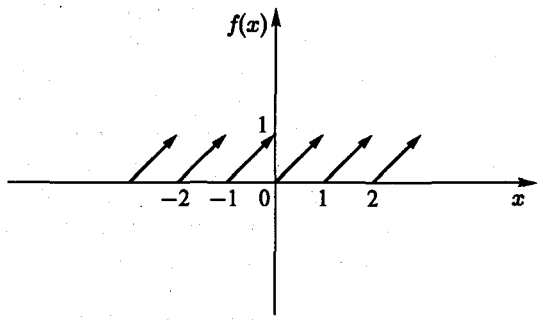

Рис. 2. $f(x) = \{x\}$

4. $|\{n \in \mathbb{N} : n \leqslant x, d|n\}| = \lfloor x/d \rfloor$ для любого положительного действительного числа x и любого натурального числа d.
5. $\lfloor \lfloor x \rfloor \rfloor = \lfloor x \rfloor$ для любого действительного числа x.
6. $\lfloor x/d \rfloor = \lfloor \lfloor x \rfloor / d \rfloor$ для любого положительного действительного числа x и любого натурального числа d.
7. $\lfloor x \rfloor - 2\lfloor x/2 \rfloor = 0$ или 1 для любого действительного числа x.
8. $n! = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, где p_i пробегает все простые числа, не превосходящие n, и $\alpha_i = \lfloor n/p_i \rfloor + \lfloor n/p_i^2 \rfloor + \lfloor n/p_i^3 \rfloor + \ldots$.
9. $0 \leqslant \{x\} < 1$ для любого действительного числа x с равенством слева, если и только если x — целое число.
10. $\{k + x\} = \{x\}$ для любого целого числа k и любого действительного числа x.

Например, для доказательства формулы $|\{n \in \mathbb{N} : n \leqslant x, d|n\}| = \lfloor x/d \rfloor$ достаточно рассмотреть числа $d, 2d, \ldots, kd \leqslant x < (k+1)d$. Тогда $|\{n \in \mathbb{N} :$

$n \leqslant x, d|n\}| = k$. С другой стороны, $k \leqslant x/d < k+1$, то есть, $k = \lfloor x/d \rfloor$. Доказательства остальных свойств можно найти, например, в [3].

Поскольку функция $f(x) = \lfloor x \rfloor$ обладает свойством $\lfloor x+k \rfloor = \lfloor x \rfloor + k$ для любого целого числа k, и для $x \in [0, 1)$ имеет место равенство $\lfloor x \rfloor = 0$, то для $x \in [1, 2)$ имеет место равенство $\lfloor x \rfloor = 1$, для $x \in [2, 3)$ имеет место равенство $\lfloor x \rfloor = 2, \ldots$, для $x \in [-1, 0)$ имеет место равенство $\lfloor x \rfloor = -1$, для $x \in [-2, -1)$ имеет место равенство $\lfloor x \rfloor = -2$, и график функции $f(x) = \lfloor x \rfloor$ изображен на рис. 1.

Поскольку функция $f(x) = \{x\}$ является периодической с периодом 1, и для $x \in [0, 1)$ имеет место равенство $\{x\} = x$, то график функции $f(x) = \{x\}$ изображен на рис. 2.

Примеры решения задач

1. Сколько натуральных n, не превосходящих 1000, не делится ни на 5, ни на 7?

Решение. Легко видеть, что $|\{n \in \mathbb{N} : n \leqslant 1000, 5|n\} = \lfloor 1000/5 \rfloor = 200$; $|\{n \in \mathbb{N} : n \leqslant 1000, 7|n\} = \lfloor 1000/7 \rfloor = 142$; $|\{n \in \mathbb{N} : n \leqslant 1000, 35|n\} = \lfloor 1000/35 \rfloor = 28$. Тогда $|\{n \in \mathbb{N} : n \leqslant 1000, 5 \nmid n, 7 \nmid n\} = 1000 - \lfloor 1000/5 \rfloor - \lfloor 1000/7 \rfloor + \lfloor 1000/35 \rfloor = 1000 - 200 - 142 + 28 = 686$. ▷

2. Запишите каноническое разложение числа 20!.

Решение. Для нахождения данного разложения мы выписываем все простые числа p, не превосхдящие 20, то есть числа 2, 3, 5, 7, 11, 13, 17 и 19. Для каждого такого p степень α, в которой p входит в разложение факториала, вычисляем по формуле $\alpha = \lfloor 20/p \rfloor + \lfloor 20/p^2 \rfloor + \lfloor 20/p^3 \rfloor + \ldots$ При этом поскольку $\lfloor 20/p^k \rfloor = \lfloor 20/p^{k-1}/p \rfloor = \lfloor \lfloor 20/p^{k-1} \rfloor /p \rfloor$, то вычисления упрощаются: на каждом следующем шаге мы делим на p предыдущее слагаемое и выписываем целую часть полученного числа. Именно, для числа 2 вычисления принимают вид $\alpha_1 = \lfloor 20/2 \rfloor + \lfloor 20/2^2 \rfloor + \lfloor 20/2^3 \rfloor + \lfloor 20/2^4 \rfloor + \lfloor 20/2^5 \rfloor + \ldots = 10 + \lfloor 10/2 \rfloor + \lfloor \lfloor 10/2 \rfloor /2 \rfloor + \ldots = 10 + 5 + 2 + 1 + 0 = 18$. Для числа 3 вычисления принимают вид $\alpha_2 = \lfloor 20/3 \rfloor + \lfloor 20/3^2 \rfloor + \lfloor 20/3^3 \rfloor + \ldots = 6 + 2 + 0 = 8$. Для числа 5 имеем $\alpha_3 = \lfloor 20/5 \rfloor + \lfloor 20/5^2 \rfloor + \ldots = 4 + 0 = 4$. Для числа 7 имеем $\alpha_4 = \lfloor 20/7 \rfloor + \lfloor 20/7^2 \rfloor + \ldots = 2 + 0 = 2$. Поскольку для числа 11 результат принимает вид $\alpha_5 = \lfloor 20/11 \rfloor + \lfloor 20/11^2 \rfloor + \ldots = 1 + 0 = 1$, то дальнейшие вычисления не требуются — оставшиеся простые числа 13, 17 и 19 также будут входить в разложение числа 20! в первой степени. Таким образом, $20! = 2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$. ▷

3. Сколькими нулями оканчивается число 2000! в пятнадцатиричной системе счисления?

Решение. Для нахождения числа нулей, на которые оканчивается 2000! в 15-й системе счисления, достаточно выяснить, сколько раз в каноническое разложение числа 2000! входит число 5: нуль на конце 15-й записи числа обеспечивается наличием в каноническом разложении данного числа множителя $15 = 3 \cdot 5$, а число $\lfloor 2000/5 \rfloor + \lfloor 2000/5^2 \rfloor + \ldots$ пятерок в каноническом разложении числа 2000! меньше, чем число $\lfloor 2000/3 \rfloor + \lfloor 20000/3^2 \rfloor + \ldots$ троек. Искомая величина равна $\lfloor 2000/5 \rfloor + \lfloor 2000/5^2 \rfloor + \lfloor 2000/5^3 \rfloor \ldots = 400 + 80 + 16 + 3 + 0 = 499$. Таким образом, число 2000! оканчивается в 15-й системе счисления 499 нулями. ▷

4. Решите уравнение $\lfloor x \rfloor = 1 + 2\{x\}$.

Решение. Достаточно заметить, что число $1 + 2\{x\}$ обязано быть целым и, следовательно, $\{x\} = 0$ или $\{x\} = 0{,}5$. В первом случае $\lfloor x \rfloor = 1$, то есть $x = \lfloor x \rfloor + \{x\} = 1 + 0 = 1$. Во втором случае $\lfloor x \rfloor = 2$, то есть $x = \lfloor x \rfloor + \{x\} = 2 + 0{,}5 = 2{,}5$.
Таким образом, решениями уравнения $\lfloor x \rfloor = 1 + 2\{x\}$ являются числа 1 и 2,5. ▷

5. Постройте графики функций $f(x) = \lfloor 2x - 1 \rfloor$; $f(x) = \{2x - 1\}$.

Решение. Для построения графиков функций $y = \lfloor f(x) \rfloor$ и $y = \{f(x)\}$ необходимо:

- построить график функции $y = f(x)$;
- построить систему горизонтальных прямых линий $y = a, a \in \mathbb{Z}$, проходящих через целые точки оси ординат;
- найти точки пересечения построенных горизонтальных прямых линий $y = a, a \in \mathbb{Z}$, с графиком функции $y = f(x)$; полученные этим путем точки $(x_i, f(x_i))$, $i = \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$, графика функции $y = f(x)$ соответствуют целым значениям функции $f(x)$: $f(x_i) = f_i \in \mathbb{Z}$, $i = \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$;
- построить систему вертикальных прямых линий $x = x_i$, $i = \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$, проходящих через построенные на предыдущем этапе точки $(x_i, f(x_i))$, $i = \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$, графика функции $y = f(x)$;
- рассмотреть сетку, полученную при наложении построенных горизонтальных и вертикальных прямых линий и состоящую из прямоугольников различного размера;
- для построения графика функции $y = \lfloor f(x) \rfloor$ спроецировать часть графика функции $y = f(x)$, находящуюся в том или ином прямоугольнике построенной сетки, на нижнюю сторону прямоугольника: внутри прямоугольника с вершинами $(x_i, f(x_i))$, $(x_i, f(x_{i+1}))$,

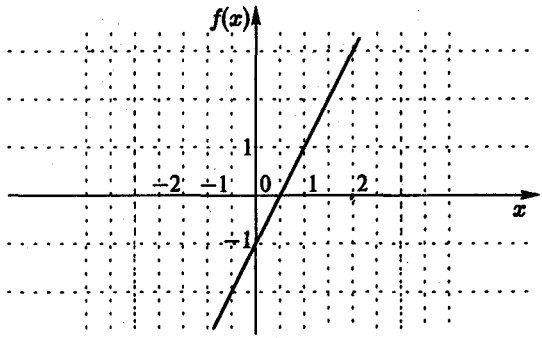

Рис. 3. $f(x) = 2x - 1$

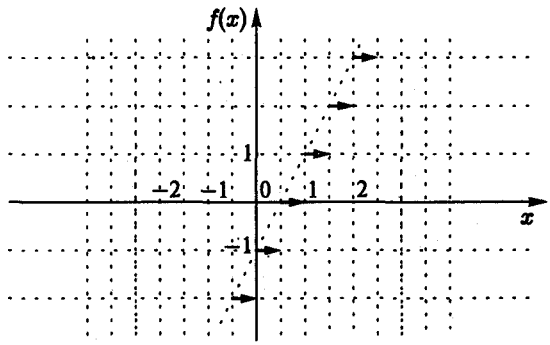

Рис. 4. $f(x) = [2x - 1]$

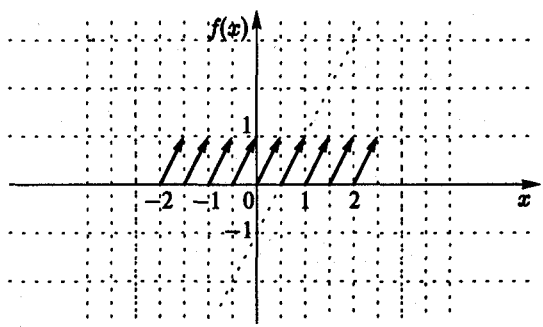

Рис. 5. $f(x) = \{2x - 1\}$

$(x_{i+1}, f(x_{i+1}))$, $(x_{i+1}, f(x_i))$ значения функции $f(x)$ располагаются между величинами f_i и f_{i+1}, то есть $\lfloor f(x) \rfloor = \min\{f_i, f_{i+1}\}$;

- для построения графика функции $y = \{f(x)\}$ поднять (или опустить) часть графика функции $y = f(x)$, находящуюся в том или ином прямоугольнике построенной сетки, на ось абсцисс: внутри прямоугольника с вершинами $(x_i, f(x_i))$, $(x_i, f(x_{i+1}))$, $(x_{i+1}, f(x_{i+1}))$, $(x_{i+1}, f(x_i))$ значения функции $f(x)$ располагаются между величинами f_i и f_{i+1}, то есть $\{f(x)\} = f(x) - \min\{f_i, f_{i+1}\}$.

На рис. 3 показана сетка, построенная для графика функции $f(x) = 2x - 1$, а также графики функций $f(x) = \lfloor 2x - 1 \rfloor$ и $f(x) = \{2x - 1\}$ (рис. 4, 5). ▷

Упражнения

1. Сколько натуральных чисел, не превосходящих 200, не делится ни на 2, ни на 5?
2. Сколько натуральных чисел, не превосходящих 6600, не делится ни на 3, ни на 11?
3. Сколько двузначных натуральных чисел не делится ни на 3, ни на 11?
4. Сколько натуральных чисел, не превосходящих 100, не делится ни на 2, ни на 3, ни на 5?
5. Сколько натуральных чисел, не превосходящих 4235, не делится ни на 5, ни на 7, ни на 11?
6. Сколько существует натуральных чисел, не превосходящих 300 и взаимно простых с 225?
7. Сколько существует натуральных чисел, не превосходящих 100 и взаимно простых с 36?
8. Сколько существует натуральных чисел, не превосходящих 300 и взаимно простых с 300?
9. Сколько существует трехзначных натуральных чисел, взаимно простых с 1000?
10. Запишите каноническое разложение чисел:

а) 14!; б) 16!; в) 18!; г) 20!; д) 26!; е) $\frac{20!}{10!10!}$; ж) $\frac{16!}{8!8!}$; з) $\frac{16!}{10!6!}$; и) $\frac{20!}{16!4!}$.

11. Сколькими нулями в g-ичной системе счисления оканчивается число:

а) 1994!, $g = 10$;

б) 200!, $g = 10$;

в) 2010!, $g = 6$;

г) 3000!, $g = 60$;

д) 2004!, $g = 12$;

е) 500!, $g = 12$;

ж) $\dfrac{100!}{80!20!}$, $g = 6$;

з) $\dfrac{200!}{100!100!}$, $g = 10$;

и) $\dfrac{666!}{660!6!}$, $g = 13$;

к) $\dfrac{100!}{50!50!}$, $g = 60$;

л) $\dfrac{30!}{10!10!}$, $g = 8$;

м) $\dfrac{200!}{50!150!}$, $g = 20$.

12. Делится ли:

а) 500! на 22^{50};

б) 100! на 30^{30};

в) $\dfrac{200!}{100!100!}$ на 100^{10};

г) $\dfrac{100!}{80!20!}$ на 20^{20}?

13. Решите уравнение:

а) $\lfloor x \rfloor = -3$;

б) $\lfloor 2x \rfloor = 2$;

в) $\lfloor x^2 - 4x + 7 \rfloor = 3$;

г) $\lfloor 3x^2 - x \rfloor = x + 1$;

д) $\{x\} = 0{,}2$;

е) $\{3x\} = 0{,}9$;

ж) $\{x^2 + 5\} = 0$;

з) $\{x\} = \lfloor x + 15 \rfloor$;

и) $\lfloor x \rfloor + 5 = 2\{x\}$;

к) $\{x\} = \lfloor x \rfloor$;

л) $\lfloor x \rfloor + 5 = \{x\}$;

м) $\dfrac{x-1}{3} = \{x\}$.

14. Постройте графики функций:

а) $f(x) = \lfloor x - 0{,}5 \rfloor$; $f(x) = \{x - 0{,}5\}$;

б) $f(x) = \lfloor \sin x \rfloor$; $f(x) = \{\sin x\}$;

в) $f(x) = \lfloor 2\cos x - 3 \rfloor$; $f(x) = \{2\cos x - 3\}$;

г) $f(x) = \lfloor x^3 - 1 \rfloor$; $f(x) = \{x^3 - 1\}$;

д) $f(x) = \lfloor \sqrt{x} + 1 \rfloor$; $f(x) = \{\sqrt{x} + 1\}$;

е) $f(x) = \lfloor x^2 - 4 \rfloor$; $f(x) = \{x^2 - 4\}$.

задачи

1. Сколько натуральных чисел, не превосходящих 120, делится на 7, но не делится на 6?

2. Найдите наибольшую степень числа 12, в которой оно делит число 120!.

3. Найдите максимальное α, такое что $\dfrac{101\cdot 102\cdot\ldots\cdot 200}{8^{\alpha}}\in\mathbb{Z}$.

4. Найдите максимальное α, такое что $3^{\alpha}|100!$.

5. Найдите наибольшую степень числа $2n$, в которой оно делит число 100^n, если $n=N-5\lfloor N/5\rfloor+5$, $N\in\{1,2,3,\ldots,25\}$.

6. Решите уравнение:

а) $\dfrac{x-3}{5}=2\{x\}$;

б) $\dfrac{x+5}{4}=3\{x\}$;

в) $\lfloor x\rfloor-3\{x\}=2x+1$;

г) $\lfloor x\rfloor+2\{x\}=2x-1$;

д) $\{x\}=0{,}4$;

е) $\{x+5\}=0{,}3$;

ж) $\lfloor x-3\rfloor=-3$;

з) $\lfloor x+3\rfloor=5$;

и) $\lfloor 1-x^2\rfloor=0$;

к) $\lfloor x^2-2\rfloor=-1$;

л) $\lfloor\sin x\rfloor=-1$;

м) $\lfloor\cos x\rfloor=0$;

н) $\lfloor\ln x+1\rfloor=-1$;

о) $\lfloor 2-\log_3 x\rfloor=4$.

7. Решите неравенство:

а) $\lfloor 1-x^2\rfloor>-4$;

б) $\{1-x^2\}>0{,}5$;

в) $\lfloor\sin 2x-4\rfloor\leqslant -3{,}5$;

г) $\{\sin 2x-4\}\leqslant 0{,}5$;

д) $\lfloor\log_5 x\rfloor\geqslant 0$;

е) $\{\log_5 x\}\geqslant 0{,}2$.

8. Постройте графики функций:

а) $f(x)=\lfloor 5\sin x+1\rfloor$; $f(x)=\{5\sin x+1\}$;

б) $f(x)=\lfloor 3\cos x-2\rfloor$; $f(x)=\{3\cos x-2\}$;

в) $f(x)=\lfloor 3\ln x+1\rfloor$; $f(x)=\{3\ln x+1\}$;

г) $f(x)=\lfloor 4\sin 2x\rfloor$; $f(x)=\{4\sin 2x\}$;

д) $f(x)=\lfloor|0{,}5x|-3\rfloor$; $f(x)=\{|0{,}5x|-3\}$;

е) $f(x)=\lfloor\ln|x|\rfloor$; $f(x)=\{\ln|x|\}$.

9. Вычислите:

а) $\left\lfloor\dfrac{\left\{\frac{\sqrt{2}}{2}\right\}-7}{\left\{\frac{\sqrt{2}+7}{2}\right\}}\right\rfloor$; б) $\left\lfloor\dfrac{2+\sqrt{7}}{3-\sqrt{7}}+\dfrac{1+\sqrt{3}}{2-\sqrt{3}}\right\rfloor$; в) $\left\lfloor\dfrac{3\sqrt{10}+2\sqrt{3}}{4}\right\rfloor$.

10. Для $n=N-5\lfloor N/5\rfloor+5$, $N\in\{1,2,\ldots,25\}$, вычислите:

а) $\left\lfloor-\dfrac{\left\lfloor\frac{3n-6}{n+2}\right\rfloor}{\left\{\frac{n+12}{n-1}-\frac{3}{14}\right\}}\right\rfloor$;

б) $\left\{\dfrac{\left\lfloor\frac{4-3n}{n}\right\rfloor}{\left\{\frac{5n+1}{3^n-2}+\frac{1}{17}\right\}}\right\}$.

11. Вычислите:

а) $\lfloor x \rfloor - 3\lfloor x/3 \rfloor$, где $x \in \mathbb{R}$;

б) $\lfloor x \rfloor - k\lfloor x/k \rfloor$, где $x \in \mathbb{R}$, $k \in \mathbb{N}$;

в) $\lfloor x \rfloor + \lfloor -x \rfloor$, где $x \in \mathbb{R}$;

г) $\lfloor \sqrt{1} \rfloor + \lfloor \sqrt{2} \rfloor + \ldots + \lfloor \sqrt{n^2+1} \rfloor$, где $n \in \mathbb{N}$.

12. Постройте графики функций $f(x) = \|x\|$ и $f(x) = \lceil x \rceil$.

13. Докажите:

а) $\lfloor x \rfloor + \lfloor x + 0{,}5 \rfloor = \lfloor 2x \rfloor$, где $x \in \mathbb{R}$;

б) $\|x\| = \lfloor x + 0{,}5 \rfloor$, где $x \in \mathbb{R}$;

в) $\lceil x \rceil = -\lfloor -x \rfloor$, где $x \in \mathbb{R}$;

г) $x \leqslant \lceil x \rceil < x + 1$, где $x \in \mathbb{R}$;

д) $\lfloor k/2 \rfloor + \lceil k/2 \rceil = k$, где $k \in \mathbb{Z}$;

е) $\lfloor x \rfloor + \lfloor y \rfloor \leqslant \lfloor x + y \rfloor \leqslant \lfloor x \rfloor + \lfloor y \rfloor + 1$, где $x, y \in \mathbb{R}$;

ж) $\lfloor x \rfloor + \lfloor x + 1/k \rfloor + \ldots + \lfloor x + (k-1)/k \rfloor = \lfloor kx \rfloor$, где $x \in \mathbb{R}$, $k \in \mathbb{N}$;

з) $\lfloor m/n \rfloor + \lfloor 2m/n \rfloor + \ldots + \lfloor (n-1)m/n \rfloor = (m-1)(n-1)/2$, где $m, n \in \mathbb{N}$, $(m, n) = 1$;

и) $\sum\limits_{n=1}^{q/2} \lfloor np/q \rfloor + \sum\limits_{m=1}^{p/2} \lfloor mq/p \rfloor = \dfrac{p-1}{2} \cdot (q-1)/2$, где $m, n \in \mathbb{N}$, $p, q \in P \setminus \{2\}$, $p \neq q$.

14. Докажите, что

$$\sum_{m \geqslant 1} \left(\left\lfloor \frac{n}{m} \right\rfloor - \left\lfloor \frac{n-1}{m} \right\rfloor \right) = 2 \Leftrightarrow n \in \mathbb{P}.$$

15. Докажите, что для действительного нецелого x имеет место следующее разложение в *ряд Фурье*:

$$\lfloor x \rfloor = x - \frac{1}{2} + \frac{1}{\pi} \sum_{k=1}^{\infty} \frac{\sin(2\pi k x)}{k}.$$

16. Докажите, что максимальное α, такое что $p^{\alpha} \left| \binom{2n}{n} \right.$, равно

$$\sum_{k=1}^{\infty} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2\left\lfloor \frac{n}{p^k} \right\rfloor \right).$$

17. Докажите, что для непрерывной функции $f(x)$, неотрицательной на отрезке $[a, b]$, число точек (x, y) с натуральными координатами x, y в криволинейной трапеции, ограниченной линиями $x = a$,

$x = b$, $y = 0$, $y = f(x)$, равно $\sum\limits_{a \leqslant x \leqslant b} \lfloor f(x) \rfloor$, где суммирование ведется по всем целым x из отрезка $[a, b]$.

18. Докажите, что число точек (x, y) с натуральными координатами x, y под гиперболой $xy = n$ равно $2 \sum\limits_{0 < x \leqslant \sqrt{n}} \lfloor n/x \rfloor - \lfloor \sqrt{n} \rfloor^2$, где суммирование ведется по всем натуральным x, не превосходящим n, $n \in \mathbb{N}$.

§ 8. Мультипликативные функции

Арифметическая функция f называется *мультипликативной*, если $f(1) = 1$ и $f(mn) = f(m)f(n)$ для любых взаимно простых натуральных чисел m и n.

Мультипликативная функция f называется *вполне мультипликативной*, если $f(mn) = f(m)f(n)$ для любых натуральных чисел m и n.

Например, функция $f(n) = n^\alpha$ является вполне мультипликативной для любого действительного α: $f(mn) = (mn)^\alpha = m^\alpha n^\alpha = f(m)f(n)$ для любых натуральных m и n.

Свойства мультипликативных функций

1. Произведение мультипликативных функций есть мультипликативная функция.
2. Если f — мультипликативная функция, то для данного

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s},$$

где $p_1, p_2, \ldots, p_s$ — различные простые числа, а $\alpha_1, \alpha_2, \ldots, \alpha_s \in \mathbb{N}$, имеет место равенство

$$\sum_{d|n} f(d) = \prod_{i=1}^{s} \left(1 + f(p_i) + f(p_i^2) + \ldots + f(p_i^{\alpha_i})\right).$$

3. Если f — мультипликативная функция, то $h(n) = \sum\limits_{d|n} f(d)$ — мультипликативная функция.
4. Мультипликативная функция f полностью определяется ее значениями на степенях простых чисел:

$$f(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}) = f(p_1^{\alpha_1}) \cdot f(p_2^{\alpha_2}) \cdot \ldots \cdot f(p_s^{\alpha_s}).$$

5. Если функция f мультипликативна, а m и n — произвольные натуральные числа, то $f(m)f(n) = f((m, n))f([m, n])$.

Так, поскольку любой натуральный делитель d числа $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$ имеет вид $d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_s^{\beta_s}$, где $0 \leqslant \beta_1 \leqslant \alpha_1$, $0 \leqslant \beta_2 \leqslant \alpha_2$, ..., $0 \leqslant \beta_s \leqslant \alpha_s$, то

$$\sum_{d|n} f(d) = \sum_{0 \leqslant \beta_i \leqslant \alpha_i, i=1,2,\ldots,s} f\Big(\prod_{i=1}^{s} p_i^{\beta_i}\Big) =$$

$$= \sum_{0 \leqslant \beta_i \leqslant \alpha_i, i=1,2,\ldots,s} \prod_{i=1}^{s} f(p_i^{\beta_i}) = \prod_{i=1}^{s} \sum_{0 \leqslant \beta_i \leqslant \alpha_i} f(p_i^{\beta_i}),$$

то есть

$$\sum_{d|n} f(d) = \prod_{i=1}^{s} \left(1 + f(p_i) + f(p_i^2) + \ldots + f(p_i^{\alpha_i})\right).$$

Аналогично, поскольку любой натуральный делитель d произведения mn взаимно простых чисел m и n имеет вид $d = d_1 d_2$, где $d_1 | m$, $d_2 | n$, и $(d_1, d_2) = 1$, то

$$h(mn) = \sum_{d|mn} f(d) = \sum_{d_1|m, d_2|n} f(d_1 d_2) = \sum_{d_1|m, d_2|n} f(d_1) f(d_2) =$$

$$= \Big(\sum_{d_1|m} f(d_1)\Big)\Big(\sum_{d_2|n} f(d_2)\Big) = h(m)h(n),$$

то есть функция $h(n) = \sum\limits_{d|n} f(d)$ мультипликативна. Доказательства других свойств можно найти, например, в [3].

Примеры решения задач

1. Проверьте, что функция $f(n) = 1/n^2$ является мультипликативной; вполне мультипликативной.

Решение. Функция $f(n) = 1/n^2$ является вполне мультипликативной, и, следовательно, мультипликативной, поскольку для любых натуральных чисел m и n имеет место равенство:

$$f(mn) = \frac{1}{(mn)^2} = \frac{1}{m^2} \cdot \frac{1}{n^2} = f(m) \cdot f(n).$$

▷

2. Проверьте формулу

$$\sum_{d|p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}} f(d) = \prod_{i=1}^{s} (1 + f(p_i) + f(p_i^2) + \ldots f(p_i^{\alpha_i}))$$

для функции $f(n) = n^2$ и всех натуральных $n \leqslant 20$.

Решение. Рассмотрим, например, $n = 20$. Каноническое разложение числа 20 имеет вид $2^2 \cdot 5$. Тогда выписанная выше формула принимает вид $\sum\limits_{d|20} d^2 = (1 + 2^2 + (2^2)^2)(1 + 5^2)$. Натуральными делителями числа 20 являются числа 1, 2, 4, 5, 10 и 20, поэтому мы получаем формулу $1^2 + 2^2 + 4^2 + 5^2 + 10^2 + 20^2 = (1 + 2^2 + 4^2)(1 + 5^2)$. Легко убедиться в том, что указанное равенство верно: $546 = 21 \cdot 26$. ▷

3. Определим функцию $\sigma_2(n)$ как сумму квадратов всех натуральных делителей натурального числа n: $\sigma_2(n) = \sum\limits_{d|n} d^2$. Докажите формулу

$$\sigma_2(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}) = \frac{p_1^{2(\alpha_1+1)} - 1}{p_1 - 1} \cdot \frac{p_2^{2(\alpha_2+1)} - 1}{p_1 - 1} \cdot \ldots \cdot \frac{p_s^{2(\alpha_s+1)} - 1}{p_s - 1}.$$

Решение. По определению, $\sigma_2(n) = \sum\limits_{d|n} d^2$. Как мы только что убедились, $\sum\limits_{d|p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}} d^2 = \prod_{i=1}^{s} \left(1 + (p_i)^2 + (p_i^2)^2 + \ldots + (p_i^{\alpha_i})^2\right)$. Поскольку

$$1 + (p_i)^2 + (p_i^2)^2 + \ldots + (p_i^{\alpha_i})^2 = 1 + p_i^2 + (p_i^2)^2 + \ldots + (p_i^2)^{\alpha_i} = \frac{(p_i^2)^{\alpha_i+1} - 1}{p_i^2 - 1}$$

как сумма $\alpha_i + 1$ членов геометрической прогрессии с начальным элементом 1 и знаменателем p_i^2, то мы доказали, что $\sigma_2(p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}) = \prod_{i=1}^{s} \frac{p_i^{2(\alpha_i+1)} - 1}{p_i^2 - 1}$. ▷

4. Найдите $\sigma_2(5)$, $\sigma_2(10)$, $\sigma_2(20)$.

Решение. Рассмотрим, например, $n = 20$. С одной стороны, действуя по определению, мы получим, что $\sigma_2(20) = 1^2 + 2^2 + 4^2 + 5^2 + 10^2 + 20^2$, то есть $\sigma_2(20) = 546$. С другой стороны, мы можем воспользоваться только что доказанной формулой: $\sigma_2(20) = \sigma_2(2^2 \cdot 5) = \frac{2^{2\cdot(2+1)} - 1}{2^2 - 1} \cdot \frac{5^{2\cdot(1+1)} - 1}{5^2 - 1} = \frac{2^6 - 1}{2^2 - 1} \cdot \frac{5^4 - 1}{5^2 - 1} = \frac{63}{3} \cdot \frac{624}{24} = 21 \cdot 26 = 546$. ▷

5. Докажите, что функция $\sigma_2(n)$ является мультипликативной. Является ли она вполне мультипликативной?

Решение. Покажем, что для любых взаимно простых натуральных чисел m и n имеет место равенство $\sigma_2(mn) = \sigma_2(m)\sigma_2(n)$. Не ограничивая общности можно считать, что каждое из чисел m и n больше единицы (для остальных случаев проведите рассуждения самостоятельно!). В этом случае каждое из чисел m и n обладает каноническим представлением: $m = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, и $n = q_1^{\beta_1} \cdot \ldots \cdot q_s^{\beta_s}$, причем, в силу того, что $(m, n) = 1$, $p_i \neq q_j$ для всех $i \in \{1, \ldots, k\}$ и $j \in \{1, \ldots, s\}$.

Тогда $mn = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} \cdot q_1^{\beta_1} \cdot \ldots \cdot q_s^{\beta_s}$ — каноническое представление числа mn, и мы имеем следующую цепочку равенств:

$$\sigma_2(mn) = \sigma_2(p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} \cdot q_1^{\beta_1} \cdot \ldots \cdot q_s^{\beta_s}) =$$
$$= \frac{p_1^{2(\alpha_1+1)} - 1}{p_1^2 - 1} \cdot \ldots \cdot \frac{p_k^{2(\alpha_k+1)} - 1}{p_k^2 - 1} \cdot \frac{q_1^{2(\beta_1+1)} - 1}{q_1^2 - 1} \cdot \ldots \cdot \frac{q_s^{2(\beta_s+1)} - 1}{q_s^2 - 1} =$$
$$= \left(\prod_{i=1}^{k} \frac{p_i^{2(\alpha_i+1)} - 1}{p_i^2 - 1} \right) \cdot \left(\prod_{j=1}^{s} \frac{q_j^{2(\beta_j+1)} - 1}{q_j^2 - 1} \right) = \sigma_2(m) \cdot \sigma_2(n).$$

Функция $\sigma_2(n)$ не является вполне мультипликативной, поскольку, например, $\sigma_2(4) = 1^2 + 2^2 + 4^2 = 21$, $\sigma_2(2) = 1^2 + 2^1 = 5$, и $\sigma_2(2 \cdot 2) \neq \sigma_2(2) \cdot \sigma_2(2)$. ▷

Упражнения

1. Проверьте, что функция $f(n) = n^\alpha$, $\alpha \in \{0, \pm 1, \pm 2, \pm 3, \pm 4\}$, является мультипликативной; вполне мультипликативной.
2. Проверьте формулу $\sum\limits_{d \mid p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}} f(d) = \prod_{i=1}^{s} (1 + f(p_i) + f(p_i^2) + \ldots + f(p_i^{\alpha_i}))$ для функции $f(n) = n^\alpha$ при $\alpha \in \{0, \pm 1, \pm 2, \pm 3, \pm 4\}$ и всех натуральных $n \leqslant 20$.
3. Докажите формулу $\sigma_3(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}) = \frac{p_1^{3(\alpha_1+1)} - 1}{p_1 - 1} \cdot \frac{p_2^{3(\alpha_2+1)} - 1}{p_1 - 1} \cdot \ldots \cdot \frac{p_s^{3(\alpha_s+1)} - 1}{p_s - 1}$ для функции $\sigma_3(n) = \sum\limits_{d \mid n} d^3$. Получите соответствующие формулы для функций $\sigma_\alpha = \sum\limits_{d \mid n} d^\alpha$ при всех $\alpha \in \{0, \pm 1, \pm 2, \pm 3, \pm 4\}$.
4. Найдите $\sigma_3(5)$, $\sigma_3(10)$, $\sigma_3(20)$, $\sigma_{-1}(5)$, $\sigma_{-1}(10)$, $\sigma_{-1}(20)$, $\sigma_4(5)$, $\sigma_4(10)$, $\sigma_4(20)$.
5. Докажите, что функция $\sigma_\alpha(n)$, $\alpha \in \{0, \pm 1, \pm 2, \pm 3, \pm 4\}$, является мультипликативной. Является ли она вполне мультипликативной?

Задачи

1. Является ли мультипликативной функция:

а) $f(n) = (n, 5)$;
б) $f(n) = [n, 5]$;
в) $f_k(n) = (n, k)$, где $k \in \mathbb{N}$;
г) $f_k(n) = [n, k]$, где $k \in \mathbb{N}$;
д) $f(n) = \sin \pi n$;
е) $f(n) = \cos \pi n$;
ж) $f(n) = \sin 2\pi n$;
з) $f(n) = \cos(\pi n/2)$?

2. Докажите, что функция $\sigma_\alpha(n) = \sum\limits_{d|n} d^\alpha$, где сумма берется по всем натуральным делителям d числа n, а α — любое комплексное число, является мультипликативной. При каких α она является вполне мультипликативной?
3. Является ли мультипликативной *характеристическая функция* $1_C(n)$ *множества* C, $C \subset \mathbb{N}$: $1_C(n) = 1$ для $n \in C$, и $1_C(n) = 0$ для $n \notin C$. Является ли она вполне мультипликативной?
4. Является ли мультипликативной *мультипликативная единица* $\varepsilon(n)$ *для конволюции Дирихле*: $\varepsilon(n) = 1$, если $n = 1$, и $\varepsilon(n) = 0$, если $n > 1$. Является ли она вполне мультипликативной?
5. Является ли мультипликативной *функция Кармайкла* $\lambda(n)$: $\lambda(p^\alpha) = \varphi(p^\alpha)$ для простого $p \geqslant 3$ и натурального α; $\lambda(2^\alpha) = 2^{\alpha-2}$ для натурального $\alpha \geqslant 3$, в то время как $\lambda(2) = 1$, и $\lambda(4) = 2$; наконец, $\lambda(p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}) = [\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_s^{\alpha_s})]$, где $p_1, \ldots, p_s$ — различные простые числа, а $\alpha_1, \ldots, \alpha_s \in \mathbb{N}$.
6. Докажите, что мультипликативной является *функция Лиувилля* $l(n)$, определяемая как $l(n) = (-1)^{\Omega(n)}$, где $\Omega(n)$ — число простых делителей n, считаемых с повторениями. Является ли она вполне мультипликативной?
7. Докажите, что мультипликативной является функция $\gamma(n)$, определяемая как $\gamma(n) = (-1)^{\nu(n)}$, где $\nu(n)$ — число различных простых делителей n. Является ли она вполне мультипликативной?
8. Постройте график функции $\pi(x) = \sum\limits_{p \leqslant x} 1$ для $0 \leqslant x \leqslant 20$. Докажите, что функция $\pi(x)$ не является мультипликативной.
9. Является ли мультипликативной *функция Мангольдта* $\Lambda(n)$: $\Lambda(n) = \ln p$ для $n = p^k$, где p — простое, а k — натуральное, и $\Lambda(n) = 0$ в остальных случаях.
10. Является ли мультипликативной функция $r_2(n)$, дающая число представлений n в виде суммы двух квадратов целых чисел? Является ли мультипликативной функция $r_2(n)/4$?

§ 9. Число и сумма делителей

Рассмотрим функцию $\tau(n) = \sum\limits_{d|n} 1$ дающую *число натуральных делителей натурального числа* n, и функцию $\sigma(n) = \sum\limits_{d|n} d$, дающую *сумму натуральных делителей натурального числа* n.

Например, $\tau(6) = 4$, так как натуральное число 6 имеет ровно 4 натуральных делителя 1, 2, 3 и 6, в то время как $\tau(13) = 2$, так как натуральное число 13 имеет ровно два натуральных делителя 1 и 13. При этом $\sigma(6) = 1 + 2 + 3 + 6 = 12$, и $\sigma(13) = 1 + 13 = 14$.

Свойства функций $\tau(n)$ и $\sigma(n)$

1. $\tau(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \ldots \cdot (\alpha_s + 1)$.
2. $\sigma(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}) = \dfrac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \dfrac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \dfrac{p_s^{\alpha_s+1} - 1}{p_s - 1}$.
3. Функция $\tau(n)$ мультипликативна.
4. Функция $\sigma(n)$ мультипликативна.

При доказательстве первого свойства можно воспользоваться, например, формулой $\sum\limits_{d|p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}} f(d) = \prod_{i=1}^{s}(1 + f(p_i) + f(p_i^2) + \ldots + f(p_i^{\alpha_i}))$ для мультипликативной функции $f(n) \equiv 1$. Именно, $\tau(p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}) = \sum\limits_{d|p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}} 1 = \prod_{i=1}^{s}(1 + f(p_i) + f(p_i^2) + \ldots + f(p_i^{\alpha_i})) = \prod_{i=1}^{s}(\alpha_i + 1)$. Второе свойство можно доказать аналогично при использовании мультипликативной функции $f(n) = n$. Мультипликативность функций $\tau(n)$ и $\sigma(n)$ становится при этом очевидна.

Примеры решения задач

1. Вычислите $\tau(\sigma(12))$.

Решение. Так как $120 = 2^3 \cdot 3 \cdot 5$, то $\sigma(120) = \sigma(2^3 \cdot 3 \cdot 5) = \dfrac{2^4 - 1}{2 - 1} \times \times \dfrac{3^2 - 1}{3 - 1} \cdot \dfrac{5^2 - 1}{5 - 1} = 15 \cdot 4 \cdot 6 = 2^3 \cdot 3^2 \cdot 5$. Тогда $\tau(\sigma(120)) = \tau(2^3 \cdot 3^2 \cdot 5) = (3 + 1) \cdot (2 + 1) \cdot (1 + 1) = 2^3 \cdot 3 = 24$. ▷

2. Решите уравнение $\tau(x) = 33$, $24|x$.

Решение. Поскольку число 33 может быть представлено в виде произведения отличных от единицы натуральных чисел ровно двумя способами, именно, как 33 (один множитель) или $3 \cdot 11$ (два множителя), то натуральное число x имеет либо один, либо два простых делителя. В первом случае $x = p^{\alpha}$, и $\tau(x) = \alpha + 1$. Таким образом, $\alpha + 1 = 33$, то есть $\alpha = 32$ и $x = p^{32}$. Во втором случае $x = p^{\alpha}q^{\beta}$, и $\tau(x) = (\alpha + 1)(\beta + 1)$. Таким образом, $(\alpha + 1)(\beta + 1) = 3 \cdot 11$, то есть $\alpha = 2$, $\beta = 10$, и $x = p^2q^{10}$. Таким образом, решениями уравнения $\tau(x) = 33$ являются числа p^{32}, $p \in \mathbb{P}$ и p^2q^{10}, $p, q \in P$, $p \neq q$.
Поскольку $24|x$, то в каноническое разложение x входят числа 2^3 и 3. Таким образом, $x = 3^2 \cdot 2^{10}$, то есть $x = 9216$. ▷

3. Решите уравнение $\tau(2x) = \tau(3x)$.

Решение. Запишем натуральное число x в виде $x = 2^\alpha 3^\beta y$, где α и β — целые неотрицательные числа, а натуральное число y не делится ни на 2, ни на 3, то есть $(2, y) = (3, y) = 1$. В этом случае $\tau(2x) = \tau(2^{\alpha+1})\tau(3^\beta)\tau(y)$, $\tau(3x) = \tau(2^\alpha)\tau(3^{\beta+1})\tau(y)$, и после сокращения на отличное от нуля число $\tau(y)$ уравнение $\tau(2x) = \tau(3x)$ принимает вид $\tau(2^{\alpha+1})\tau(3^\beta) = \tau(2^\alpha)\tau(3^{\beta+1})$. Отсюда следует равенство $(\alpha+2)(\beta+1) = (\alpha+1)(\beta+2)$, или, что то же, равенство $\alpha = \beta$. Таким образом, решениями уравнения $\tau(2x) = \tau(3x)$ являются все натуральные числа вида $2^\alpha 3^\alpha y$, где α — целое неотрицательное число, а натуральное число y не делится ни на 2, ни на 3. ▷

4. Решите уравнение $\sigma(x) = x + 3$.

Решение. Легко видеть, что $x \neq 1$. Тогда среди натуральных делителей числа x присутствуют по крайней мере два числа: 1 и x. Поскольку сумма делителей числа x равна $x + 3$, то помимо делителей 1 и x число x обладает ровно одним натуральным делителем 2. Это возможно лишь в случае $x = 4$.

Таким образом, единственным решением уравнения $\sigma(x) = x + 3$ является число 4. ▷

Упражнения

1. Вычислите:

а) $\tau(100)$;
б) $\tau(123)$;
в) $\tau(169)$;
г) $\sigma(50)$;
д) $\sigma(101)$;
е) $\sigma(200)$;
ж) $\tau(\sigma(12)!)$;
з) $\tau(\sigma(3!))$;
и) $\tau\left(\dfrac{10!}{5!5!}\right)$;
к) $\tau\left(\dfrac{12!}{4!8!}\right)$;
л) $\sigma\left(\dfrac{6!}{3!3!}\right)$;
м) $\sigma\left(\dfrac{10!}{5!5!}\right)$;
н) $\sigma(\tau(5!))$;
о) $\sigma(\tau(3!))$;
п) $\sigma(\tau(10)!)$;
р) $\sigma(\tau(16)!)$.

2. Делится ли:

а) $\tau(\sigma(37))!$ на $(\sigma(11))^7$;
б) $\tau(\sigma(41))!$ на $(\sigma(7))^6$;
в) $\sigma(\tau(12)!)$ на $(\tau(7))^{10}$;
г) $\sigma(\tau(24)!)$ на $(\tau(4))^{12}$?

3. Является ли целым число:

а) $\dfrac{\sigma(15)!}{\tau(\sigma(15))!}$; б) $\dfrac{\sigma(19)!}{\tau(19!)}$; в) $\dfrac{8!}{\tau(\sigma(15))!}$; г) $\dfrac{20!}{\tau(20!)}$?

4. Решите уравнение:

а) $\tau(x) = 14,\ 12|x$; д) $\tau(5x) = \tau(7x)$; и) $\sigma(x) = x$;
б) $\tau(x) = 22,\ 18|x$; е) $\tau(2x) = \tau(11x)$; к) $\sigma(x) = x + 1$;
в) $\tau(x) = 21,\ 24|x$; ж) $\tau(13x) = \tau(17x)$; л) $\sigma(x) = x + 2$;
г) $\tau(x) = 505,\ 75|x$; з) $\tau(3x) = \tau(37x)$; м) $\sigma(x) = x + 4$.

5. Найдите натуральное число n, если $n = p^\alpha q^\beta$, $\tau(n) = 6$, и $\sigma(n) = 28$.

6. Найдите натуральное число n, если $n = 32pq$, и $\sigma(n) = 3n$.

7. Докажите, что для $n = m^2$, $m \in \mathbb{Z}$, величина $\tau(n)$ нечетна. Верно ли обратное?

8. Докажите, что для бесквадратного числа n величина $\tau(n)$ является степенью двойки. Верно ли обратное?

Задачи

1. Вычислите при $n = N - 5\lfloor N/5 \rfloor + 5$, $N \in \{1, 2, 3, \ldots, 25\}$:

а) $\tau(100n)$; в) $\tau(2n + 100)$; д) $\tau(2n^3)$;
б) $\sigma(10n)$; г) $\sigma(2n + 1)$; е) $\sigma(3n^2)$.

2. Решите уравнение:

а) $\tau(x) = 2$; и) $\tau(x) = pq$; с) $\tau(3x) = \tau(5x)$;
б) $\tau(x) = 11$; к) $\tau(x) = 20$; т) $\tau(px) = \tau(qx)$;
в) $\tau(x) = 13$; л) $\tau(x) = 50$; у) $\sigma(x) = 3$;
г) $\tau(x) = 17$; м) $\tau(x) = pq^2$; ф) $\sigma(x) = 4$;
д) $\tau(x) = 101$; н) $\tau(3x) = \tau(13x)$; х) $\sigma(x) = 6$;
е) $\tau(x) = p$; о) $\tau(5x) = \tau(17x)$; ц) $\sigma(x) = x + 6$;
ж) $\tau(x) = 6$; п) $\tau(11x) = \tau(13x)$; ч) $\sigma(x) = x + 5$;
з) $\tau(x) = 10$; р) $\tau(3x) = \tau(7x)$; ш) $\sigma(x) = x + 7$.

3. Решите уравнение $\tau(x) = 2n$, если $n = N - 5\lfloor N/5 \rfloor + 5$, $N \in \{1, 2, 3, \ldots, 30\}$.

4. Найдите наименьшее натуральное число n, такое что:

а) $\tau(n) = 11$; б) $\tau(n) = 22$; в) $\tau(n) = 13$; г) $\tau(n) = 39$.

5. Найдите наименьшее натуральное число, имеющее 10 натуральных делителей; все двузначные натуральные числа, имеющие 10 натуральных делителей.

6. Найдите все натуральные n, для которых $\tau(n) = 9$, а $\sigma(n) = 91$.

7. Найдите натуральное число n, если $n = 32pq$, а $\sigma(n) = 27n/10$.

8. Найдите $\tau(n^3)$, если известно, что $\tau(n^2) = 15$.

9. Найдите сумму делителей числа 240, не делящихся на 3.

10. Найдите все натуральные числа $n \leqslant 100$, такие что $\sigma(n) = 2n$.

11. Докажите *теорему Евклида—Эйлера*: для любого четного натурального числа n равенство $\sigma(n) = 2n$ имеет место тогда и только тогда, когда $n = 2^{k-1}(2^k - 1)$, где $2^k - 1 \in \mathbb{P}$.

12. Докажите:

а) $\tau(1) + \tau(2) + \ldots + \tau(n) = \lfloor n/1 \rfloor + \lfloor n/2 \rfloor + \ldots + \lfloor n/n \rfloor$;

б) $\sigma(1) + \sigma(2) + \ldots + \sigma(n) = 1 \cdot \lfloor n/1 \rfloor + 2 \cdot \lfloor n/2 \rfloor + \ldots + n \cdot \lfloor n/n \rfloor$.

13. Докажите:

а) $2 | \tau(n) \Rightarrow n \neq a^2$;

б) $(\tau(m^n), n) = 1$;

в) $n > 2 \Rightarrow \tau(n) < n$;

г) $n \in \mathbb{S} \Rightarrow \sigma(n) > n + \sqrt{n}$;

д) $(a, b) > 1 \Rightarrow \tau(a)\tau(b) > \tau(ab)$;

е) $(a, b) > 1 \Rightarrow \sigma(a)\sigma(b) > \sigma(ab)$;

ж) $\prod_{d|n} d = n^{0{,}5\tau(n)}$.

§ 10. Функция Эйлера

Для данного натурального числа n функция Эйлера $\varphi(n)$ определяется как число натуральных чисел, не превосходящих n и взаимно простых с n:

$$\varphi(n) = |\{x \in \mathbb{N} : x \leqslant n, (x, n) = 1\}|.$$

Например, $\varphi(8) = 4$, так как ровно четыре натуральных числа, не превосходящих 8 (именно, числа 1, 3, 5 и 7), являются взаимно простыми с 8.

Свойства функции Эйлера

1. $\varphi(p) = p - 1$ для любого простого p.
2. $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ для любого простого p и любого натурального α.
3. Функция Эйлера мультипликативна.
4. $\varphi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}) = p_1^{\alpha_1 - 1} \cdot p_2^{\alpha_2 - 1} \cdot \ldots \cdot p_s^{\alpha_s - 1}(p_1 - 1) \cdot (p_2 - 1) \cdot \ldots \cdot (p_s - 1)$.
5. $\sum\limits_{d|n} \varphi(d) = n$ (*тождество Гаусса*).

Так, первое свойство очевидно, поскольку среди p натуральных чисел, не превосходящих простого числа p, только число p не является взаимно простым с p. Аналогично, среди p^α натуральных чисел $1, 2, \ldots, p^\alpha$ имеется ровно $p^{\alpha-1}$ чисел (именно, $p, p^2, p^3, \ldots, p^\alpha$), не являющихся взаимно простыми с p^α, что доказывает второе свойство. Доказательства остальных свойств можно найти, например, в [3]. Заметим, что свойство 4 может быть записано в следующем виде: $\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_s}\right)$ для $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$.

Примеры решения задач

1. Вычислите: $\varphi(12)$; $\varphi(63000)$.

Решение. Поскольку среди чисел 1, 2, 3, ..., 12 ровно 4 числа (именно, числа 1, 5, 7, 11) взаимно просты с 12, то, по определению, $\varphi(12) = 4$. Впрочем, мы можем и воспользоваться формулой: $\varphi(12) = \varphi(2^2 \cdot 3) = 2^1 \cdot 3^0(2-1)(3-1) = 2^2 = 4$. Поскольку $63\,000 = 2^3 \cdot 3^2 \cdot 5^3 \cdot 7$, то $\varphi(63000) = \varphi(2^3 \cdot 3^2 \cdot 5^3 \cdot 7) = 2^2 \cdot 3^1 \cdot 5^2 \cdot 7^0(2-1)(3-1)(5-1)(7-1) = 2^6 \cdot 3^3 \cdot 5 = 8640$. ▷

2. Сколько существует правильных несократимых дробей со знаменателем 150?

Решение. Дробь $a/150$ является правильной несократимой дробью тогда и только тогда, когда $a \in \mathbb{N}$, $a < 150$ и $(a, 150) = 1$. Легко видеть, что число таких дробей равно $\varphi(150)$. Поскольку $\varphi(150) = \varphi(2 \cdot 3 \cdot 5^2) = 5 \cdot (2-1)(3-1)(5-1) = 40$, то и число правильных несократимых дробей со знаменателем 150 равно 40. ▷

3. Найдите количество натуральных чисел n, не превосходящих 615, таких что $(n, 615) = 15$.

Решение. В этом случае натуральное число $n/15 \leqslant 41$, и $(n/15, 41) = 1$. Количество таких чисел равно $\varphi(41) = 40$. Таким образом, и количество натуральных чисел n, не превосходящих 615, таких что $(n, 615) = 15$, равно 40. ▷

4. Решите уравнение $\varphi(x) = x/3$.

Решение. Очевидно, что $x \neq 1$. В этом случае x обладает каноническим разложением $x = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, и $\varphi(x) = x(1 - 1/p_1) \ldots (1 - 1/p_k)$. После сокращения на x наше уравнение принимает вид $(1 - 1/p_1) \ldots \ldots (1 - 1/p_k) = 1/3$. Выписывая возможные множители левой части 1/2, 2/3, 4/5, 6/7,... , мы видим, что дробь 1/3 может быть получена только при перемножении дробей 1/2 и 2/3. Таким образом, $x = 2^\alpha \cdot 3^\beta$, где $\alpha, \beta \in \mathbb{N}$. ▷

5. Решите уравнение $\varphi(2x) = \varphi(3x)$.

Решение. Запишем натуральное число x в виде $x = 2^\alpha 3^\beta y$, где α и β — целые неотрицательные числа, а натуральное число y не делится ни на 2, ни на 3, то есть $(2, y) = (3, y) = 1$. В этом случае $\varphi(2x) = \varphi(2^{\alpha+1})\varphi(3^\beta)\varphi(y)$, $\varphi(3x) = \varphi(2^\alpha)\varphi(3^{\beta+1})\varphi(y)$, и после сокращения на отличное от нуля число $\varphi(y)$ уравнение $\varphi(2x) = \varphi(3x)$ принимает вид $\varphi(2^{\alpha+1})\varphi(3^\beta) = \varphi(2^\alpha)\varphi(3^{\beta+1})$.

Поскольку $\varphi(2^{\alpha+1}) = 2^\alpha$ и $\varphi(3^{\beta+1}) = 2\cdot 3^\beta$, то мы получаем уравнение $2^\alpha\varphi(3^\beta) = 2\cdot 3^\beta\varphi(2^\alpha)$.

Если $\alpha = 0$, $\beta = 0$, то уравнение принимает вид $1 = 2$, что дает противоречие.

Если $\alpha = 0$, $\beta \neq 0$, то уравнение принимает вид $2\cdot 3^{\beta-1} = 2\cdot 3^\beta$, что также дает противоречие.

Если $\alpha \neq 0$, $\beta = 0$, то уравнение превращается в тождество $2^\alpha = 2\cdot 2^{\alpha-1}$, верное при всех таких α и β.

Если $\alpha \neq 0$, $\beta \neq 0$, то уравнение принимает вид $2^\alpha\cdot 2\cdot 3^{\beta-1} = 2\cdot 3^\beta\cdot 2^{\alpha-1}$, что вновь ведет к противоречию.

Таким образом, множеству решений уравнения $\varphi(2x) = \varphi(3x)$ принадлежат все натуральные числа вида $2^\alpha y$, где $\alpha \in \mathbb{N}$, а натуральное число y не делится ни на 2, ни на 3. ▷

6. Решите уравнение $\varphi(x) = 2$.

Решение. Очевидно, что $x \neq 1$. В этом случае x обладает каноническим разложением $x = p_1^{\alpha_1}\cdot\ldots\cdot p_k^{\alpha_k}$, и $\varphi(x) = p_1^{\alpha_1-1}\cdot\ldots\cdot p_k^{\alpha_k-1}(p_1-1)\ldots(p_k-1)$. Пусть $\varphi(x) = 2^m l$, где l нечетно. Поскольку для нечетного простого числа p величина $p-1$ четна, то в каноническом разложении x имеется не более m нечетных простых множителей. Другими словами, $k \leqslant m+1$, причем если $k = m+1$, то $p_1 = 2$.

В нашем случае $m = 1$, то есть $k \leqslant 2$, причем если $k = 2$, то $p_1 = 2$.

Пусть $k = 1$, то есть $x = p^\alpha$.

Если $p = 2$, то $\varphi(x) = \varphi(2^\alpha) = 2^{\alpha-1}$, и наше уравнение принимает вид $2^{\alpha-1} = 2$, откуда следует, что $\alpha = 2$ и $x = 2^2 = 4$.

Если $p \neq 2$, то $\varphi(x) = \varphi(p^\alpha) = p^{\alpha-1}(p-1)$, и наше уравнение принимает вид $p^{\alpha-1}(p-1) = 2$, откуда следует, что $p-1 = 2$ и $p^{\alpha-1} = 1$. Таким образом, $p = 3$, $\alpha = 1$, и $x = 3$.

Пусть $k = 2$, то есть $x = 2^\alpha p^\beta$.

Тогда $\varphi(x) = \varphi(2^\alpha p^\beta) = 2^{\alpha-1}p^{\beta-1}(p-1)$, и наше уравнение принимает вид $2^{\alpha-1}p^{\beta-1}(p-1) = 2$, откуда следует, что $p-1 = 2$, $2^{\alpha-1} = 1$, и $p^{\beta-1} = 1$. Таким образом, $p = 3$, $\alpha = \beta = 1$, и $x = 2\cdot 3 = 6$.

Итак, решения уравнения $\varphi(x) = 2$ — это натуральные числа 3, 4 и 6. ▷

Упражнения

1. Вычислите:

а) $\varphi(13)$; г) $\varphi(1000000)$; ж) $\varphi(\varphi(12)!)$; к) $\varphi(\sigma(101))$;

б) $\varphi(125)$; д) $\varphi(\varphi(125))$; з) $\varphi(\varphi(20)!)$; л) $\varphi(\tau(100))$;

в) $\varphi(1000)$; е) $\varphi(\varphi(1000))$; и) $\varphi(\sigma(14))$; м) $\varphi(\tau(101))$.

2. Сколькими нулями в g-ичной системе счисления оканчивается число:

а) $\varphi(528)!$, $g = 15$; в) $\varphi(\sigma(13))!$, $g = 14$; д) $\varphi(\tau(144))!$, $g = 8$;
б) $\varphi(30)!$, $g = 12$; г) $\varphi(\sigma(17))!$, $g = 20$; е) $\varphi(\tau(196)!$, $g = 27$.

3. Сколько существует правильных несократимых дробей со знаменателем:

а) 180; б) 200; в) $\tau(1000)$; г) $\tau(10000)$?

4. Найдите количество натуральных чисел n, не превосходящих 200, таких что $(n, 200) = 4$.

5. Найдите количество натуральных чисел n, не превосходящих 500, таких что $(n, 500) = 10$.

6. Найдите количество натуральных чисел n, не превосходящих 50, таких что $(n, 10) = 2$.

7. Найдите количество натуральных чисел n, не превосходящих 1000, таких что $(n, 200) = 8$.

8. Решите уравнение:

а) $\varphi(x) = 2x/3$; ж) $7\varphi(x) = 2x$; н) $\varphi(x) = 6$;
б) $\varphi(x) = 4x/11$; з) $15\varphi(x) = 4x$; о) $\varphi(x) = 10$;
в) $\varphi(x) = x/6$; и) $\varphi(2x) = \varphi(5x)$; п) $\varphi(x) = 3$;
г) $\varphi(x) = x/12$; к) $\varphi(3x) = \varphi(5x)$; р) $\varphi(x) = 4$.
д) $7\varphi(x) = 4x$; л) $\varphi(13x) = \varphi(17x)$;
е) $7\varphi(x) = 3x$; м) $\varphi(2x) = \varphi(31x)$;

Задачи

1. Вычислите:

а) $\varphi(\varphi(27)!)$;
б) $\tau(\sigma(\varphi(20)))!$;
в) $\dfrac{\varphi(\sigma(12))}{\tau(\sigma(12))}$;
г) $\dfrac{\varphi(120)}{\tau(120)}$.

2. Запишите каноническое разложение числа:

а) $(\varphi(\varphi(21))!)$; б) $(\varphi(\varphi(27))!)$; в) $\varphi(275)^{\tau(275)}$; г) $\varphi(405)^{\tau(405)}$.

3. Являются ли целыми числа:

а) $\dfrac{\varphi(19!)}{\tau(19!)}$; б) $\dfrac{\varphi(22!)}{\tau(22!)}$; в) $\dfrac{\varphi(\tau(100)!)}{\varphi(10)}$; г) $\dfrac{\varphi(\tau(200)!)}{\tau(22)}$?

4. Делится ли:

а) $\varphi(506)!$ на $\tau(506)!$;
б) $\varphi(200)!$ на $\tau(200)!$;
в) $\varphi(100)!$ на $(\tau(100))^{\tau(100)}$;
г) $\varphi(50)!$ на $(\tau(50))^{\tau(50)}$?

5. Найдите число правильных несократимых дробей со знаменателем:
а) 90; б) 114; в) 12!; г) 15!; д) p, где $p \in P$.

6. Сколько существует правильных несократимых дробей со знаменателем, делящим 2002?

7. Сколькими нулями оканчивается число:
а) $\varphi(528)!$ в 12-й системе счисления;
б) $\varphi(506)!$ в 48-й системе счисления;
в) $\varphi(400)!$ в 48-й системе счисления;
г) $\varphi(396)!$ в 48-й системе счисления?

8. Найдите число натуральных чисел, не превосходящих 1000 и взаимно простых с 77.

9. Найдите число натуральных чисел, не превосходящих 875 и взаимно простых с 175.

10. Найдите число натуральных чисел, не превосходящих $2^{30} - 1$ и взаимно простых с $2^{10} - 1$.

11. Найдите число натуральных чисел, не превосходящих 8! и взаимно простых с 6!.

12. Найдите число натуральных чисел n, не превосходящих 1665 и удовлетворяющих условию $(1665, n) = 15$.

13. Решите уравнение:
а) $\varphi(x) = 8$; в) $\varphi(x) = 14$; д) $\varphi(x) = 20$; ж) $\varphi(x) = 40$;
б) $\varphi(x) = 12$; г) $\varphi(x) = 16$; е) $\varphi(x) = 24$; з) $\varphi(x) = 50$.

14. Найдите все четные натуральные $n \leqslant 50$, для которых уравнение $\varphi(x) = n$ не имеет решений.

15. Решите уравнение:
а) $\varphi(x) = \tau(1519)$; в) $\varphi(x) = \sigma(5)$;
б) $\varphi(0{,}5x) = \tau(70)$; г) $\varphi(0{,}5x) = \sigma(3)$.

16. Решите уравнение:
а) $\varphi(2x) = \varphi(7x)$; в) $\varphi(5x) = \varphi(7x)$; д) $\varphi(3x) = \varphi(5x)$;
б) $\varphi(11x) = \varphi(2x)$; г) $\varphi(11x) = \varphi(7x)$; е) $\varphi(31x) = \varphi(101x)$.

17. Решите уравнение $\varphi(px) = \varphi(qx)$, если p и q — различные простые числа.

18. Решите уравнение:
а) $\varphi(x) = x/4$; г) $\varphi(x) = 8x/13$; ж) $\varphi(x) = 64x/129$;
б) $\varphi(x) = 8x/11$; д) $\varphi(x) = 9x/19$; з) $\varphi(x) = 7x/5$.
в) $\varphi(x) = 4x/5$; е) $\varphi(x) = 16x/33$;

19. Решите уравнение $\varphi(x) = (p-1)x/p$, если p — простое число.

20. Найдите натуральное число n, если $n = 3^{\alpha} \cdot 5^{\beta}$, и $\varphi(n) = 600$.

21. Найдите натуральное число n, если $\varphi(7^n) = 705\,894$.

22. Найдите натуральное число n, если $\varphi(3^n) = 162$.

23. При каких натуральных x имеет место равенство:

а) $\varphi(6x-3) = \varphi(2x-1)$;

б) $\varphi(3x+1) = \varphi(6x+2)$;

в) $\varphi(3x-1) = \varphi(9x-3)$.

24. При каких натуральных n имеет место соотношение $2|\varphi(n)$?

25. Вычислите $\sum\limits_{k=0}^{\infty} \dfrac{\varphi(p^k)}{p^{ks}}$, где $s \in \mathbb{R}$, $s > 1$.

26. Докажите:

а) $\varphi(4n) = 2\varphi(2n)$;

б) $\varphi(4n+2) = \varphi(2n+1)$;

в) $n > 1 \Rightarrow 4|\varphi(n^2+1)$;

г) $a|b \;\Rightarrow\; \varphi(a)|\varphi(b)$;

д) $(a,b) = d \Rightarrow \dfrac{\varphi(ab)}{\varphi(a)\varphi(b)} = \dfrac{d}{\varphi(d)}$;

е) $(a,b) > 1 \Rightarrow \varphi(a)\varphi(b) < \varphi(ab)$;

ж) $s \geqslant t \geqslant 1 \;\Rightarrow\; \dfrac{\varphi(a^s)}{\varphi(a^t)} = a^{s-t}$;

з) $\varphi(n) + \tau(n) = \sigma(n) \;\Leftrightarrow\; n \in P$;

и) $\varphi(n) + \sigma(n) = n\tau(n) \;\Leftrightarrow\; n \in P$;

к) $p, 2p+1 \in P \;\Rightarrow\; \varphi(4p+2) = \varphi(4p) + 2$.

27. Докажите, что $|\{x \in \mathbb{N} : x \leqslant km, (x,m) = 1\}| = km \prod_{p|m}(1 - 1/p)$, где $k, m \in \mathbb{N}$.

28. Что больше: $\varphi(m^2)$ или $\varphi^2(m)$?

29. Докажите:

а) $\sum\limits_{k=1}^{n} \varphi(k)\lfloor n/k \rfloor = n(n+1)/2$;

б) $\sum\limits_{d|n} \tau(d)\varphi(n/d) = \sigma(n)$;

в) $\sum\limits_{k=1}^{n} \lfloor 1/(n,k) \rfloor = \varphi(n)$;

г) $\sum\limits_{k=1}^{n} (n,k) = \sum\limits_{d|n} d\varphi(n/d)$.

§ 11. Функция Мебиуса

Рассмотрим *функцию Мебиуса* $\mu(n)$, определенную для всех натуральных n и принимающую значения из множества $\{-1, 0, 1\}$ в зависимости от разложения n на простые множители: $\mu(n) = 1$, если n — бесквад-

ратное число с четным числом простых делителей; $\mu(n) = -1$, если n — бесквадратное число с нечетным числом простых делителей; $\mu(n) = 0$, если n не является бесквадратным. Другими словами,

$$\mu(n) = \begin{cases} 1, \text{ если } n = 1, \\ (-1)^s, \text{ если } n = p_1 \cdot \ldots \cdot p_s, \text{ где } p_i \in P, \text{ и } p_i \neq p_j \text{ при } i \neq j, \\ 0, \text{ если } \exists\, p \in P : p^2 | n. \end{cases}$$

Например, $\mu(6) = 1$, поскольку $6 = 2 \cdot 3$ — бесквадратное число, имеющее два простых делителя; $\mu(70) = -1$, поскольку $70 = 2 \cdot 5 \cdot 7$ — бесквадратное число, имеющее три простых делителя; $\mu(50) = 0$, поскольку $50 = 2 \cdot 5^2$ делится на квадрат простого числа 5, и, следовательно, не является бесквадратным.

Свойства функции Мебиуса

1. Функция Мебиуса мультипликативна.
2. $\sum\limits_{d|n} \mu(d) = 1$ для $n = 1$, и $\sum\limits_{d|n} \mu(d) = 0$ для $n > 1$.
3. $F(n) = \sum\limits_{d|n} f(d)$, если и только если $f(n) = \sum\limits_{d|n} \mu(d) F(n/d)$ (*формула обращения Мебиуса*).
4. $\sum\limits_{d|n} \mu(d) \tau(n/d) = 1$.
5. $\sum\limits_{d|n} \mu(d) n/d = \varphi(n)$.
6. $\sum\limits_{d|n} \mu(d) \sigma(n/d) = n$.

Так, первое свойство можно доказать непосредственной проверкой. Для доказательства второго свойства прежде всего убедимся в том, что $\sum\limits_{d|1} \mu(d) = \mu(1) = 1$. Если же $n \neq 1$, то $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$, и $\sum\limits_{d|n} \mu(d) = \prod_{i=1}^{s} (1 + \mu(p_i) + \mu(p_i^2) + \ldots + \mu(p_i^{\alpha_i})) = \prod_{i=1}^{s} (1 - 1 + 0 + \ldots + 0) = 0$. Доказательство формулы обращения Мебиуса основано, с одной стороны, на цепочке равенств

$$\sum_{d|n} \mu(d) F(n/d) = \sum_{d|n} \mu(d) \sum_{c|n/d} f(c) = \sum_{cd|n} \mu(d) f(c) = \sum_{c|n} f(c) \sum_{d|n/c} \mu(d) = f(n).$$

С другой стороны,

$$\sum_{d|n} f(d) = \sum_{d|n} \sum_{c|d} \mu(c) F(d/c) = \sum_{k|n} F(k) \sum_{c} n/k \cdot \mu(c) = F(n).$$

Более детальные рассуждения можно найти, например, в [3].

Примеры решения задач

1. Вычислите: $\mu(30)$; $\mu(101)$; $\mu(210)$; $\mu(300)$.

Решение. Поскольку $30 = 2\cdot 3\cdot 5$, то $\mu(30) = \mu(2\cdot 3\cdot 5) = (-1)^3 = -1$. Поскольку $101 \in P$, то $\mu(101) = (-1)^1 = -1$. Поскольку $210 = 2\cdot 3\cdot 5\cdot 7$, то $\mu(210) = \mu(2\cdot 3\cdot 5\cdot 7) = (-1)^4 = 1$. Поскольку $300 = 2^2\cdot 3\cdot 5^2$, то $\mu(300) = \mu(2^2\cdot 3\cdot 5^2) = 0$. ▷

2. Решите уравнение $\mu(2x) = \mu(3x)$, $x \in [1, 20]$.

Решение. Запишем натуральное число x в виде $x = 2^\alpha 3^\beta y$, где α и β — целые неотрицательные числа, а натуральное число y не делится ни на 2, ни на 3, то есть $(2, y) = (3, y) = 1$. В этом случае $\mu(2x) = \mu(2^{\alpha+1})\mu(3^\beta)\mu(y)$, $\mu(3x) = \mu(2^\alpha)\mu(3^{\beta+1})\mu(y)$. Если $\mu(y) = 0$, то есть в случае делимости числа y на квадрат некоторого простого числа, равенство выполнено. Если $\mu(y) \neq 0$, то есть в том случае, когда y — бесквадратное число, после сокращения на отличное от нуля число $\mu(y)$ уравнение $\mu(2x) = \mu(3x)$ принимает вид $\mu(2^{\alpha+1})\mu(3^\beta) = \mu(2^\alpha)\mu(3^{\beta+1})$.

Если $\alpha > 1$ или $\beta > 1$, то уравнение превращается в тождество $0 = 0$.

Если $\alpha = 0$ и $\beta = 0$, то уравнение принимает вид $\mu(2) = \mu(3)$, то есть превращается в тождество $-1 = -1$.

Если $\alpha = 0$, $\beta = 1$, то уравнение принимает вид $1 = 0$, что дает противоречие.

Если $\alpha = 1$, $\beta = 0$, то уравнение принимает вид $0 = 1$, что дает противоречие.

Если $\alpha = 1$ и $\beta = 1$, то уравнение превращается в тождество $0 = 0$.

Таким образом, множеству решений уравнения $\mu(2x) = \mu(3x)$ принадлежат все натуральные числа, кроме бесквадратных чисел вида $2y$ или $3y$, где $(y, 2) = (y, 3) = 1$. Среди натуральных чисел от 1 до 20 такими числами будут 2, 3, 10, 14 и 15. Таким образом, решениями нашего уравнения на отрезке $[1, 20]$ будут числа 1, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 16, 17, 18, 19 и 20. ▷

3. Проверьте тождество $\sum\limits_{d|n} \mu(d)\tau(n/d) = 1$ для $n \in \{1, 5, 10, 20\}$; докажите его для любого натурального n.

Решение. При $n = 1$ утверждение тривиально: $\sum\limits_{d|1} \mu(d)\tau(1/d) = \mu(1)\tau(1/1) = 1\cdot 1 = 1$. При $n = 20$ мы получаем следующую цепочку равенств: $\sum\limits_{d|20} \mu(d)\tau(1/d) = \mu(1)\tau(20/1) + \mu(2)\tau(20/2) + \mu(4)\tau(20/4) +$

$+ \mu(5)\tau(20/5) + \mu(10)\tau(20/10) + \mu(20)\tau(20/20) = 1\cdot 6 + (-1)\cdot 4 +$

$+0\cdot 2+(-1)\cdot 3+(-1)^2\cdot 2+0\cdot 1=6-4-3+2=1$. Доказать тождество можно, пользуясь формулой обращения Мебиуса: поскольку $\tau(n)=\sum\limits_{d|n}1$, то, взяв $F(n)=\tau(n)$ и $f(n)\equiv 1$, мы получим, что $\sum\limits_{d|n}\mu(d)F(n/d)=f(n)$, или, что то же, $\sum\limits_{d|n}\mu(d)\tau(n/d)=1$. Впрочем, доказательство можно получить и непосредственно: $\sum\limits_{d|n}\mu(d)\tau(n/d)=$

$$=\sum_{d|n}\mu(d)\sum_{c|n/d}1=\sum_{cd|n}\mu(d)=\sum_{c|n}1\sum_{d|n/c}\mu(d)=1. \qquad \triangleright$$

4. Запишите сумму $\sum\limits_{d|n}\mu(d)/d$ в виде произведения.

Решение. Поскольку функции $f_1(n)=\mu(n)$ и $f_2(n)=1/n$ мультипликативны, то мультипликативна и функция $f(n)=\mu(n)/n$, являющаяся произведением функций $f_1(n)$ и $f_2(n)$. Тогда $\sum\limits_{d|n}f(d)=$ $=\prod_{i=1}^{s}(1+f(p_i)+f(p_i^2)+\ldots+f(p_i^{\alpha_i}))$ для $n=p_1^{\alpha_1}\cdot\ldots\cdot p_s^{\alpha_s}$. Другими словами,

$$\sum_{d|n}\frac{\mu(d)}{d}=\prod_{i=1}^{s}\left(1+\frac{\mu(p_i)}{p_i}+\frac{\mu(p_i^2)}{p_i^2}+\ldots+\frac{\mu(p_i^{\alpha_i})}{p_i^{\alpha_i}}\right)=$$

$$=\prod_{i=1}^{s}\left(1-\frac{1}{p_i}+0+\ldots+0\right).$$

Таким образом, для $n=p_1^{\alpha_1}\cdot\ldots\cdot p_s^{\alpha_s}$ имеет место формула

$$\sum_{d|n}\frac{\mu(d)}{d}=\left(1-\frac{1}{p_1}\right)\cdot\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_s}\right). \qquad \triangleright$$

Замечание. Поскольку $(1-1/p_2)\cdot\ldots\cdot(1-1/p_s)=\varphi(n)/n$ для $n=$ $=p_1^{\alpha_1}\cdot\ldots\cdot p_s^{\alpha_s}$, то мы доказали формулу $\sum\limits_{d|n}\mu(d)/d=\varphi(n)/n$, или, что то же, свойство 4 функции Мебиуса: $\sum\limits_{d|n}\mu(d)n/d=\varphi(n)$.

Упражнения

1. Вычислите:

а) $\mu(65)$; в) $\mu(91)$; д) $\mu(68)$; ж) $\mu(242)$;
б) $\mu(66)$; г) $\mu(330)$; е) $\mu(135)$; з) $\mu(250)$.

2. Вычислите:

а) $\mu(\sigma(14))$; б) $\mu(\tau(10)!)$. в) $\mu(\varphi(15))$; г) $\mu(10!/(5!5!))$.

3. Решите уравнение:

а) $\mu(5x) = \mu(3x)$, $x \in [5, 25]$; в) $\mu(3x) = \mu(7x)$, $x \in [40, 70]$;
б) $\mu(2x) = \mu(7x)$, $x \in [10, 30]$; г) $\mu(5x) = \mu(7x)$, $x \in [40, 60]$.

4. Проверьте тождество $\sum\limits_{d|n} \mu(d)\sigma(n/d) = n$ для $n \in \{1, 5, 10, 20\}$; докажите его для любого натурального n.

5. Запишите сумму в виде произведения:

а) $\sum\limits_{d|n} \mu(d)\varphi(d)$; б) $\sum\limits_{d|n} \mu(d)d^k$; в) $\sum\limits_{d|n} \dfrac{\mu(d)}{\varphi(d)}$; г) $\sum\limits_{d|n} \dfrac{\mu^2(d)}{\varphi^2(d)}$.

Задачи

1. Пусть $\nu(n)$ — число различных простых делителей натурального числа n, и $\Omega(n)$ — число всех возможных простых делителей натурального числа n, считаемых с повторениями. Докажите, что $\mu(n) = (-1)^{\nu(n)} = (-1)^{\Omega(n)}$, если $\nu(n) = \Omega(n)$, и $\mu(n) = 0$ в остальных случаях.

2. Найдите значения *функции Мертенса* $M(n) = \sum\limits_{i=1}^{n} \mu(i)$ для всех $n \in \{1, 2, \ldots, 20\}$.

3. Найдите сумму:

а) $\sum\limits_{d|n} \mu(d)/d$;
б) $\sum\limits_{d|n} \mu(d)/\tau(d)$;
в) $\sum\limits_{d|n} \mu(d)\tau^3(d)$;
г) $\sum\limits_{d|n} \mu(n/d)(-7)^{\nu(d)}$;
д) $\sum\limits_{d|n} \mu(d)3^{\nu(d)}$;
е) $\sum\limits_{d|n} \mu(n/d)(-3)^{\nu(d)}$;
ж) $\sum\limits_{d|n} \mu^2(d)/\varphi(d)$;
з) $\sum\limits_{d|n} \mu(n/d)d/\varphi(d)$;
и) $\sum\limits_{d|n} \mu(d)2^{\nu(d)}$;
к) $\sum\limits_{d|n} \mu(n/d)(-1)^{\nu(d)}$.

4. Докажите, что $\sum\limits_{\varphi(d)=n} \mu(d) = 0$, где $n \in \mathbb{N}$

5. Докажите, что $\sum\limits_{d|n} |\mu(d)| = 2^{\nu(n)}$.

6. Докажите, что $\mu(n) = \sum\limits_{1 \leqslant k \leqslant n, (k,n)=1} e^{2\pi i k/n}$.

7. Докажите, что $\sum\limits_{i=1}^{\infty} \dfrac{\mu(n)}{n^s} = \prod\limits_{p \in P}(1 - p^{-s})$, где $s \in \mathbb{R}$, $s > 1$.

8. Докажите, что $\sum\limits_{n=1}^{\infty} \dfrac{\mu(n)x^n}{1 - x^n} = x$, где $x \in \mathbb{R}$, $|x| < 1$.

§ 12. Отношение сравнимости

Два целых числа a и b называются *сравнимыми* по модулю n, $n \in \mathbb{N}$, если a и b имеют одинаковые остатки при делении на n, или, что то же, если $n|(a - b)$. В этом случае пишут $a \equiv b (\mathrm{mod}\, n)$.

Например, $-27 \equiv 15 (\mathrm{mod}\, 7)$, так как $-27 = 7 \cdot (-4) + 1$, и $15 = 7 \cdot 2 + 1$; другими словами, $15 - (-27) = 42$, и $7|42$. С другой стороны, $5 \not\equiv -4 (\mathrm{mod}\, 7)$, так как $5 = 7 \cdot 0 + 5$, но $-4 = 7 \cdot (-1) + 3$; другими словами, $5 - (-4) = 9$, и $7 \nmid 9$.

Свойства отношения сравнимости

1. Отношение сравнимости $\equiv$ является *отношением эквивалентности*, то есть:
   - $a \equiv a (\mathrm{mod}\, n)$ для любого целого a;
   - если $a \equiv b (\mathrm{mod}\, n)$, то $b \equiv a (\mathrm{mod}\, n)$;
   - если $a \equiv b (\mathrm{mod}\, n)$ и $b \equiv c (\mathrm{mod}\, n)$, то $a \equiv c (\mathrm{mod}\, n)$.
2. Если $a \equiv b (\mathrm{mod}\, n)$, то $f(a) \equiv f(b) (\mathrm{mod}\, n)$ для любого многочлена $f(x)$ с целыми коэффициентами.
3. $a \equiv b (\mathrm{mod}\, n) \Leftrightarrow ka \equiv kb (\mathrm{mod}\, kn)$, где $k \in \mathbb{N}$.
4. $a \equiv b (\mathrm{mod}\, n) \Leftrightarrow ka \equiv kb (\mathrm{mod}\, n)$, где $k \in \mathbb{Z}$, $(k, n) = 1$.
5. $$\begin{cases} a \equiv b \pmod{n_1} \\ a \equiv b \pmod{n_2} \\ \dots \\ a \equiv b \pmod{n_k} \end{cases} \Leftrightarrow \quad a \equiv b (\mathrm{mod}\, M), \text{ где } M = [n_1, n_2, \dots, n_k].$$

Так, доказательство первого свойства следует из определения: $a \equiv a (\mathrm{mod}\, n)$, поскольку $a - a = 0$, и $n|0$; если $a \equiv b (\mathrm{mod}\, n)$, то $n|(a - b)$, и, следовательно, $n|(b - a)$, то есть $b \equiv a (\mathrm{mod}\, n)$; если $a \equiv b (\mathrm{mod}\, n)$ и $b \equiv c (\mathrm{mod}\, n)$, то $n|(a - b)$, $n|(b - c)$ и, следовательно, $n|(a - b) + (b - c)$, то есть $n|(a - c)$, и $a \equiv c (\mathrm{mod}\, n)$. Таким образом, отношение сравнимости обладает свойствами рефлекстивности, симметричности и транзитивности, то есть

является отношением эквивалентности. Доказательства остальных свойств аналогичны; их можно найти, например, в [3].

Примеры решения задач

1. Найдите остаток от деления $f(86)$ на 11, если $f(x) = 15x^3 - 33x^2 + 7$.

Решение. Для решения задачи заменим все числа на «первом» этаже сравнения остатками от деления на 11 или, что еще удобнее, наименьшими по абсолютной величине числами, сравнимыми с ними по модулю 11: $86 \equiv -2 (\mathrm{mod}\ 11)$; $15 \equiv 4 (\mathrm{mod}\ 11)$; $33 \equiv 0 (\mathrm{mod}\ 11)$, и $7 \equiv -4 (\mathrm{mod}\ 11)$. Тогда $f(86) \equiv f(-2) (\mathrm{mod}\ 11)$, и мы получаем цепочку сравнений $f(-2) \equiv 4(-2)^3 - 0 \cdot (-2)^2 - 4 \equiv -32 - 4 \equiv -36 \equiv -3 \equiv 8 (\mathrm{mod}\ 11)$. Таким образом, остаток от деления $f(86)$ на 11 равен 8. ▷

2. Верно ли, что $10! \equiv 7! (\mathrm{mod}\ 1000)$?

Решение. Разложив числа 11!, 7! и 1000 на простые множители, мы получим сравнение $2^8 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 11 \equiv 2^4 \cdot 3^2 \cdot 5 \cdot 7 (\mathrm{mod}\ 2^3 \cdot 5^3)$. Сокращая все три части сравнения на число $2^3 \cdot 5$, мы получим сравнение $2^5 \cdot 3^4 \cdot 5 \cdot 7 \cdot 11 \equiv 2 \cdot 3^2 \cdot 7 (\mathrm{mod}\ 25)$. Сокращая две части сравнения на число $2 \cdot 3^2 \cdot 7$, *взаимно простое с модулем 25, мы получим сравнение* $2^4 \cdot 3^2 \cdot 5 \cdot 11 \equiv 1 (\mathrm{mod}\ 25)$. Поскольку $2^3 \cdot 3 \equiv -1 (\mathrm{mod}\ 25)$, и $2 \cdot 11 \equiv -3 (\mathrm{mod}\ 25)$, то $2^4 \cdot 3^2 \cdot 5 \cdot 11 \equiv (-1) \cdot (-3) \cdot 3 \cdot 5 \equiv 9 \cdot 5 \equiv 20 (\mathrm{mod}\ 25)$. Таким образом, первоначальное сравнение неверно. ▷

3. Найдите наименьшее натуральное четырехзначное число, сравнимое с 23 по модулю 101.

Решение. Задача сводится к нахождению наименьшего целого неотрицательного числа t, такого что $1000 + t \equiv 23 (\mathrm{mod}\ 101)$. В этом случае $t \equiv 23 - 1000 \equiv 23 + 10 \equiv 33 (\mathrm{mod}\ 101)$, то есть $t = 33$. Таким образом, наименьшее натуральное четырехзначное число, сравнимое с 23 по модулю 101, равно 1033. ▷

4. Докажите, что $9^{2n+1} + 8^{n+2} \equiv 0 (\mathrm{mod}\ 73)$ для любого целого неотрицательного числа n.

Решение. Легко видеть, что $9^{2n+1} + 8^{n+2} \equiv 9 \cdot 81^n + 64 \cdot 8^n \equiv 9 \cdot 8^n - 9 \cdot 8^n \equiv 0 (\mathrm{mod}\ 73)$. ▷

Упражнения

1. Заполните табл. 6 для $n = 5$, если x — наименьшее неотрицательное число, сравнимое с a по модулю n, y — наибольшее отрицательное число, сравнимое с a по модулю n, и z — наименьшее по абсолютной величине число, сравнимое с a по модулю n.

Таблица 6

a	3	17	35	−21	21
$x \equiv a (\mathrm{mod}\, n)$					
$y \equiv a (\mathrm{mod}\, n)$					
$z \equiv a (\mathrm{mod}\, n)$					

Таблица 7

n	3	7	12	100	121
$x \equiv a (\mathrm{mod}\, n)$					
$y \equiv a (\mathrm{mod}\, n)$					
$z \equiv a (\mathrm{mod}\, n)$					

2. Заполните табл. 7 для $a = 200$, если x — наименьшее неотрицательное число, сравнимое с a по модулю n, y — наибольшее отрицательное число, сравнимое с a по модулю n, и z — наименьшее по абсолютной величине число, сравнимое с a по модулю n.

3. Найдите остаток от деления числа a на 17, если $a = 1 - 4 \cdot 121^2 + 121^4 - 4 \cdot 121^6 + 121^8 - 4 \cdot 121^{10} + 121^{12} - 4 \cdot 121^{14}$.

4. Найдите остаток от деления числа a на 21, если $a = 256^3 \cdot 374 - 321 \cdot 58^2 + 129^2 \cdot 53^2$.

5. Найдите остаток от деления $f(75)$ на 11, если $f(x) = x^{10} + 4x^7 - 22x^4 + 101$.

6. Найдите остаток от деления $f(55)$ на 17, если $f(x) = 35x^5 - 50x^4 + 87x + 177$.

7. Верно ли, что:

а) $28^2 \equiv 55^2 (\mathrm{mod}\, 60)$;

б) $11! \equiv 8! (\mathrm{mod}\, 16560)$;

в) $\tau(175) \equiv 175 (\mathrm{mod}\, 27)$;

г) $\sigma(115) \equiv 115 (\mathrm{mod}\, 115)$?

8. Докажите, что $2^{4n+1} + 2^{4n} - 3^{n+1} \equiv 0 (\mathrm{mod}\, 13)$ для любого натурального числа n.

9. Докажите, что $3^{3n+2} + 2^{n+4} \equiv 0 (\mathrm{mod}\, 25)$ для любого натурального числа n.

10. Найдите наименьшее натуральное пятизначное число, сравнимое с 60 по модулю 109.

11. Найдите наибольшее натуральное четырехзначное число, сравнимое с 14 по модулю 180.

Задачи

1. Найдите остаток от деления $f(24)$ на 13, если $f(x) = 12x^6 - 15x^4 - 34x^3 + 39x - 54$.

2. Найдите остаток от деления $f(24)$ на 19, если $f(x) = 5x^4 - 22x^3 - 38x^2 + 25x - 18$.

3. Верно ли, что:

а) $336^2 \equiv 114^2 \pmod{90}$;

б) $11! \equiv 8! \pmod{23 \cdot 8!}$;

в) $\binom{14}{7} \equiv \binom{10}{5} \pmod{5710}$;

г) $\binom{14}{7} \equiv \binom{10}{5} \pmod{636}$?

4. Верно ли, что $(3299^5 + 6)^{18} \equiv 1 \pmod{112}$?

5. При каких n имеет место сравнение:

а) $3^5 \equiv 5^3 \pmod{n}$;

б) $5! \equiv 4! \pmod{n}$?

6. Докажите, что для любого целого a имеет место соотношение:

а) $a^5 \equiv a \pmod{10}$;

б) $a^7 \equiv a \pmod{7}$;

в) $a^2 \not\equiv 2 \pmod{3}$;

г) $a^3 \not\equiv 4 \pmod{8}$.

7. При каких натуральных m имеет место сравнение:

а) $m^2 + 7m + 8 \equiv 0 \pmod{3}$;

б) $(m+1)^2 + m + 1024 \equiv 0 \pmod{5}$;

в) $m^3 + 300m + 500 \equiv 0 \pmod{5}$;

г) $2m^4 + 3m^2 + 4m + 50 \equiv 0 \pmod{7}$;

д) $2^5 \equiv 5^2 \pmod{m}$;

е) $10! \equiv 5! \pmod{m}$;

ж) $\varphi(13!) \equiv \varphi(15!) \pmod{m}$;

з) $\varphi(18!) \equiv 0 \pmod{2^m}$?

8. При каких натуральных n имеет место сравнение:

а) $51 \cdot 52 \cdot \ldots \cdot 300 \equiv 0 \pmod{11^n}$;

б) $51 \cdot 52 \cdot \ldots \cdot 300 \equiv 0 \pmod{15^n}$;

в) $31 \cdot 32 \cdot \ldots \cdot 400 \equiv 0 \pmod{7^n}$;

г) $31 \cdot 32 \cdot \ldots \cdot 400 \equiv 0 \pmod{33^n}$?

9. Докажите:

а) $a \equiv b \pmod{n} \Leftrightarrow a = b + mt$, где $t \in \mathbb{Z}$;

б) $a \equiv b \pmod{n} \Leftrightarrow (2n-1)a \equiv (2n-1)b \pmod{d}$, где $d \in \mathbb{N}$, $d \mid n$;

в) $a \equiv b \pmod{n} \Leftrightarrow (4n-1)a^k \equiv (4n-1)b^k \pmod{d}$, где $k, d \in \mathbb{N}$, $d \mid n$;

г) $a \equiv b \pmod{n} \Leftrightarrow f(a) \equiv f(b) \pmod{d}$, где $f(x) = x^{4n} + x^{2n} + 1$, $d \in \mathbb{N}$, $d \mid n$.

10. Докажите, что $(mn)! \equiv 0 \pmod{(m!)^n \cdot n!}$, где $m, n \in \mathbb{N}$.

11. Верно ли, что для любого нечетного числа a имеет место сравнение $a^{2^n} \equiv 1 \pmod{2^{n+2}}$?

§ 13. Классы вычетов

Множество $\mathbf{a_n}=\{x\in\mathbb{Z}: x\equiv a(\mathrm{mod}n)\}=\{\ldots,a-2n,a-n,a,a+n,a+2n,a+3n,\ldots\}$ всех целых чисел, сравнимых с данным числом a по модулю n, называется *классом вычетов* (числа a) по модулю n. При работе с конкретным модулем n вместо символа $\mathbf{a_n}$ обычно используется символ $\mathbf{a}$.

Например, $\mathbf{2_5}=\{x\in\mathbb{Z}: x\equiv 2(\mathrm{mod}\,5)\}=\{\ldots,2-3\cdot5,2-2\cdot5,2-5,2,2+5,2+2\cdot5,2+3\cdot5,\ldots\}=\{\ldots,-13,-8,-3,2,7,12,17,\ldots\}$.

Сложение и умножение на множестве $\mathbb{Z}/n\mathbb{Z}=\{\mathbf{0_n},\mathbf{1_n},\mathbf{2_n},\ldots,\mathbf{(n-1)_n}\}$ всех классов вычетов определяются следующим образом: $\mathbf{a_n}+\mathbf{b_n}=\mathbf{(a+b)_n}$, и $\mathbf{a_n}\cdot\mathbf{b_n}=\mathbf{(ab)_n}$. В этом случае $\mathbb{Z}/n\mathbb{Z}$ превращается в коммутативное кольцо, содержащее n элементов. Для простого числа p множество $\mathbb{Z}/p\mathbb{Z}$ образует поле (см., например, [3], [18]).

Свойства классов вычетов

1. $\mathbf{a_n}=\{a+mt: t\in\mathbb{Z}\}$.
2. $\mathbf{a_n}=\mathbf{b_n}$ тогда и только тогда, когда $a\equiv b(\mathrm{mod}\,n)$.
3. Число классов вычетов по модулю n равно n.
4. Все числа одного класса вычетов по модулю n имеют с модулем n один и тот же наибольший общий делитель: если $x\in\mathbf{a_n}$, то $(x,n)=(a,n)$.
5. Число классов вычетов по модулю n, взаимно простых с n, равно $\varphi(n)$, где $\varphi(n)$ — функция Эйлера.
6. Число классов вычетов по модулю n, являющихся делителями нуля, равно $n-\varphi(n)-1$.
7. Один класс вычетов $\mathbf{a_n}$ по модулю n разбивается на k классов вычетов $\mathbf{a_{kn}}$, $\mathbf{(a+n)_{kn}}$, $\mathbf{(a+2n)_{kn}}$, $\ldots$, $\mathbf{(a+(k-1)n)_{kn}}$ по модулю kn, $k\in\mathbb{N}$.

Так, если $x\in\mathbf{a_n}$, то $x\equiv a(\mathrm{mod}\,n)$, и, следовательно, $x=a+nt$, $t\in\mathbb{Z}$, что доказывает первое свойство. Теперь для доказательства свойства 7 достаточно заметить, что, по теореме о делении с остатком, $t=kq+r$, $q,r\in\mathbb{Z}$, $r\in\{0,1,\ldots,k-1\}$, и, следовательно, $x=a+nt=a+n(kq+r)=(a+nr)+(kn)q$. Другими словами, $x\equiv a+nr(\mathrm{mod}\,kn)$, где $r\in\{0,1,\ldots,k-1\}$, то есть x принадлежит одному из классов вычетов $\mathbf{a_{kn}}$, $\mathbf{(a+n)_{kn}}$, $\mathbf{(a+2n)_{kn}}$, $\ldots$, $\mathbf{(a+(k-1)n)_{kn}}$ по модулю kn. Доказательства остальных свойств можно найти, например, в [3].

Примеры решения задач

1. Составьте таблицы сложения и умножения в кольце классов вычетов по модулю 3. Проверьте, что система $\langle\mathbb{Z}/3\mathbb{Z},+,\cdot\rangle$ образует поле. Решите в $\mathbb{Z}/3\mathbb{Z}$ уравнения $\mathbf{2+x=1}$; $\mathbf{2\cdot x=1}$; $\mathbf{2\cdot x^2-1=0}$.

Таблица 8

а)

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

б)

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Решение. Рассмотрим множество $\mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$. Легко убедиться в том, что таблицы сложения и умножения имеют представленный табл. 8 вид.

Пользуясь табл. 8*а*), можно утверждать, что нулевым элементом системы $\langle \mathbb{Z}/3\mathbb{Z}, +, \cdot \rangle$ является класс $\mathbf{0}$, и всякий элемент множества $\mathbb{Z}/3\mathbb{Z}$ имеет противоположный: $-\mathbf{0} = \mathbf{0}$ (так как $\mathbf{0} + \mathbf{0} = \mathbf{0}$), $-\mathbf{1} = \mathbf{2}$ (так как $\mathbf{1} + \mathbf{2} = \mathbf{0}$), и $-\mathbf{2} = \mathbf{1}$ (так как $\mathbf{2} + \mathbf{1} = \mathbf{0}$).

Пользуясь табл. 8*б*), можно утверждать, что единичным элементом системы $\langle \mathbb{Z}/3\mathbb{Z}, +, \cdot \rangle$ является класс $\mathbf{1}$, и всякий ненулевой элемент множества $\mathbb{Z}/3\mathbb{Z}$ имеет обратный: $\mathbf{1}^{-1} = \mathbf{1}$ (так как $\mathbf{1} \cdot \mathbf{1} = \mathbf{1}$), и $\mathbf{2}^{-1} = \mathbf{2}$ (так как $\mathbf{2} \cdot \mathbf{2} = \mathbf{1}$). Учитывая, что операции сложения и умножения классов вычетов по модулю n обладают свойствами ассоциативности, коммутативности и дистрибутивности, мы можем утверждать, что система $\langle \mathbb{Z}/3\mathbb{Z}, +, \cdot \rangle$ образует поле.

Для решения первого уравнения $\mathbf{2}+\mathbf{x} = \mathbf{1}$ заметим, что $\mathbf{x} = \mathbf{1}-\mathbf{2} = -\mathbf{1} = \mathbf{2}$. Впрочем, тот же результат можно получить, переходя к сравнениям по модулю 3: $\mathbf{2} + \mathbf{x} = \mathbf{1} \Leftrightarrow 2 + x \equiv 1 (\mathrm{mod}\, 3) \Leftrightarrow x \equiv 1 - 2 \equiv -1 \equiv \equiv 2 (\mathrm{mod}\, 3)$. Таким образом, единственным решением уравнения $\mathbf{2} + \mathbf{x} = \mathbf{1}$ *является класс* $\mathbf{2}$.

Для решения второго уравнения $\mathbf{2} \cdot \mathbf{x} = \mathbf{1}$ домножим обе части уравнения на класс $\mathbf{2}^{-1} = \mathbf{2}$: $\mathbf{2} \cdot \mathbf{2} \cdot \mathbf{x} = \mathbf{2} \cdot \mathbf{1}$, или $\mathbf{4} \cdot \mathbf{x} = \mathbf{2}$, или $\mathbf{x} = \mathbf{2}$. Впрочем, тот же результат можно получить, переходя к сравнениям по модулю 3: $\mathbf{2} \cdot \mathbf{x} = \mathbf{1} \Leftrightarrow 2x \equiv 1 (\mathrm{mod}\, 3) \Leftrightarrow 4x \equiv 2 (\mathrm{mod}\, 3) \Leftrightarrow x \equiv 2 (\mathrm{mod}\, 3)$. Таким образом, единственным решением уравнения $\mathbf{2} \cdot \mathbf{x} = \mathbf{1}$ является класс $\mathbf{2}$.

Проделывая аналогичные преобразования для третьего уравнения, записанного в виде $\mathbf{2} \cdot \mathbf{x}^2 = \mathbf{1}$, мы получим, что $\mathbf{2} \cdot \mathbf{2} \cdot \mathbf{x}^2 = \mathbf{2} \cdot \mathbf{1}$, или $\mathbf{4} \cdot \mathbf{x}^2 = \mathbf{2}$, или $\mathbf{x}^2 = \mathbf{2}$. Однако таблица умножения свидетельствует о том, что таких классов нет. Таким образом, уравнение $\mathbf{2} \cdot \mathbf{x}^2 - \mathbf{1} = \mathbf{0}$ не имеет решений. ▷

Таблица 9

а)

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

б)

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

2. Составьте таблицы сложения и умножения в кольце классов вычетов по модулю 4. Проверьте, что система $\langle \mathbb{Z}/4\mathbb{Z}, +, \cdot \rangle$ образует кольцо, но не является полем. Укажите все делители нуля кольца $\langle \mathbb{Z}/4\mathbb{Z}, +, \cdot \rangle$. Решите в $\mathbb{Z}/4\mathbb{Z}$ уравнения $3 + x = 2$; $3 \cdot x = 2$; $3 \cdot x^2 + 1 = 0$.

Решение. Рассмотрим множество $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$. Легко убедиться в том, что таблицы сложения и умножения имеют представленный табл. 9 вид.

Пользуясь табл. 9*а*), можно утверждать, что нулевым элементом системы $\langle \mathbb{Z}/4\mathbb{Z}, +, \cdot \rangle$ является класс 0, и всякий элемент множества $\mathbb{Z}/4\mathbb{Z}$ имеет противоположный: $-0 = 0$, $-1 = 3$, $-2 = 2$ и $-3 = 1$. Учитывая, что операции сложения и умножения классов вычетов по модулю n обладают свойствами ассоциативности, коммутативности и дистрибутивности, мы можем утверждать, что система $\langle \mathbb{Z}/4\mathbb{Z}, +, \cdot \rangle$ образует коммутативное кольцо с единицей.

Пользуясь табл. 9*б*), можно утверждать, что единичным элементом системы $\langle \mathbb{Z}/4\mathbb{Z}, +, \cdot \rangle$ является класс 1, однако не всякий ненулевой элемент множества $\mathbb{Z}/4\mathbb{Z}$ имеет обратный: $1^{-1} = 1$ (так как $1 \cdot 1 = 1$), $3^{-1} = 3$ (так как $3 \cdot 3 = 1$), но класс 2 не имеет обратного, поскольку $2 \cdot a \neq 1$ для $a \in \{1, 2, 3\}$. Таким образом, поля система $\langle \mathbb{Z}/4\mathbb{Z}, +, \cdot \rangle$ не образует.

Напомним, что *делителем нуля* кольца $\langle A, +, \cdot \rangle$ называется такой ненулевой элемент $a \in A$, для которого существует ненулевой элемент $b \in A$, такой что $a \cdot b = 0$.

Таблица умножения позволяет утверждать, что единственным делителем нуля кольца $\langle \mathbb{Z}/4\mathbb{Z}, +, \cdot \rangle$ является класс 2: $2 \cdot 2 = 0$. Заметим что класс 2 — единственный ненулевой класс, не взаимно простой с модулем 4.

Для решения первого уравнения $3 + x = 2$ заметим, что $x = 2 - 3 = -1 = 3$. Впрочем, тот же результат можно получить, переходя

к сравнениям по модулю 4: $3 + x = 2 \Leftrightarrow \quad 3 + x \equiv 2 (\mathrm{mod}\, 4) \Leftrightarrow x \equiv 2 - 3 \equiv -1 \equiv 3 (\mathrm{mod}\, 4)$. Таким образом, единственным решением уравнения $3 + x = 2$ является класс 3.

Для решения второго уравнения $3 \cdot x = 2$ домножим обе части уравнения на класс $3^{-1} = 3$: $3 \cdot 3 \cdot x = 3 \cdot 2$, или $9 \cdot x = 2$, или $x = 2$. Впрочем, тот же результат можно получить, переходя к сравнениям по модулю 4: $3 \cdot x = 2 \Leftrightarrow \quad 3x \equiv 2 (\mathrm{mod}\, 4) \Leftrightarrow \quad 9x \equiv 6 (\mathrm{mod}\, 4) \Leftrightarrow \quad x \equiv 2 (\mathrm{mod}\, 4)$. Таким образом, единственным решением уравнения $3 \cdot x = 2$ является класс 2.

Проделывая аналогичные преобразования для третьего уравнения $3 \cdot x^2 + 1 = 0$, мы получим, что $3 \cdot 3 \cdot x^2 + 3 \cdot 1 = 3 \cdot 0$, или $9 \cdot x^2 + 3 = 0$, или $x^2 = -3$, или $x^2 = 1$. Таблица умножения свидетельствует о том, что существует ровно два класса вычетов по модулю 4, квадрат которых равен 1: 1 и 3. Таким образом, уравнение $3 \cdot x^2 + 1 = 0$ имеет два решения: классы 1 и 3. ▷

3. *Выпишите натуральные числа, не превосходящие 20 и принадлежащие классу вычетов* 2_5.

Решение. По определению, $2_5 = \{\ldots, -13, -8, -3, 2, 7, 12, 17, 22, \ldots\}$. Следовательно, искомыми числами являются числа 2, 7, 12 и 17. ▷

4. Каким классам вычетов по модулю 15 принадлежат элементы класса вычетов 2_5?

Решение. Класс $2_5 = \{\ldots, -13, -8, -3, 2, 7, 12, 17, 22, \ldots\}$ разбивается на три класса по модулю 15: 2_{15}, $(2+5)_{15} = 7_{15}$, и $(2 + 2 \cdot 5)_{15} = 12_{15}$. При этом $2_{15} = \{\ldots, -43, -28, -13, 2, 17, 32, 47, 52, \ldots\}$, $7_{15} = \{\ldots, -23, -8, 7, 22, 37, 62, \ldots\}$, и $12_{15} = \{\ldots, -33, -18, -3, 12, 27, 42, 57, 72, \ldots\}$. ▷

Упражнения

1. Составьте таблицы сложения и умножения в кольце классов вычетов по модулю n, $n \in \{5, 6, 7, 8, 9, 10, 11, 12\}$. Образует ли система $\langle \mathbb{Z}/n\mathbb{Z}, +, \cdot \rangle$ кольцо; поле? Укажите все делители нуля кольца $\langle \mathbb{Z}/n\mathbb{Z}, +, \cdot \rangle$. Решите в $\mathbb{Z}/n\mathbb{Z}$ уравнения $4_n + x_n = 2_n$; $(n-1)_n \cdot x_n = 3_n$; $(n-1)_n \cdot x_n{}^2 + 1 = 0$.

2. Выпишите натуральные числа, не превосходящие 40, принадлежащие классу вычетов 3_7.

3. Выпишите отрицательные числа, большие -25, принадлежащие классу вычетов 33_9.

4. Выпишите нечетные двузначные натуральные числа, принадлежащие классу 11_{25}.

5. Выпишите четные двузначные натуральные числа, принадлежащие классу 70_{15}.
6. Запишите класс 3_7 в виде двух классов вычетов по модулю 14.
7. Запишите класс 4_6 в виде трех классов вычетов по модулю 18.
8. Каким классам вычетов по модулю 24 принадлежат элементы класса вычетов 34_8?
9. Каким классам вычетов по модулю 20 принадлежат элементы класса вычетов 123_5?

Задачи

1. Найдите наименьший неотрицательный вычет класса 100_4; наименьший положительный вычет класса 100_4; наибольший отрицательный вычет класса 100_4.
2. Найдите наименьший неотрицательный вычет класса $(\varphi(20)!)_{11}$; наименьший положительный вычет класса $(\varphi(20)!)_{11}$; наибольший отрицательный вычет класса $(\varphi(20)!)_{11}$.
3. Найдите наименьшее трехзначное число, принадлежащее классу вычетов 1_4.
4. Найдите наибольшее двузначное число, принадлежащее классу вычетов 2_{40}.
5. Докажите, что:

   а) $73_5 = -92_5$; б) $99_6 = -87_6$; в) $3!_8 = -2!_8$; г) $12!_9 = 15!_9$.
6. Докажите, что:

   а) $2_6 \cup 4_6 = 2_3$;

   б) $5_{12} \cup -1_{12} = 5_6$;

   в) $5_{16} \cup -3_{16} \cup 21_{32} = 5_8$;

   г) $11_{18} \cup 20_{18} \cup 74_{36} = 2_9$.
7. Выполните действия:

   а) $2_{12} \cdot 9_{12} + 25_{12}$;

   б) $34_{14} \cdot 4_{14} - 79_{14}$;

   в) $344_{17} \div 2_{17} + 5 \cdot (4_{17})^2$;

   г) $2 \cdot (5_{23})^3 - 18_{23} - 69 \cdot 5_{23} \div 3_{23}$.
8. В кольце классов вычетов по модулю 21 укажите все делители нуля и решите уравнение $7_{21} \cdot x_{21} = 0_{21}$.
9. В кольце классов вычетов по модулю 22 укажите все делители нуля и решите уравнение $4_{22} \cdot x_{22} = 10_{22}$.
10. В кольце классов вычетов по модулю 24 укажите все делители нуля и решите уравнение $3_{24} \cdot x_{24} = 6_{24}$.
11. В кольце классов вычетов по модулю 25 укажите все делители нуля и решите уравнение $5_{25} \cdot x_{25} = 0_{25}$.

12. В кольце классов вычетов по модулю $6n$ укажите все делители нуля и решите уравнение $\mathbf{n}_{6n} \cdot \mathbf{x}_{6n} = \mathbf{0}_{6n}$, если $n = N - 4[N/4] + 5$, $N \in \{1, 2, 3, \ldots, 25\}$.

13. Найдите все делители нуля в кольце $\mathbb{Z}/n\mathbb{Z}$, где $n \in \{8, 9, 10, 14, 15, 26, 28\}$.

§ 14. Полная и приведенная системы вычетов

Полной системой вычетов по модулю n называется система чисел, взятых по одному из каждого класса вычетов по модулю n.

Приведенной системой вычетов по модулю n называется система чисел, взятых по одному из каждого класса вычетов, взаимно простого с модулем n.

Введем для полной и приведенной системы вычетов по модулю n обозначения ПСВ_n и ПрСВ_n соответственно.

Например, полными системами вычетов по модулю 5 являются множества $\{0, 1, 2, 3, 4\}$ (система наименьших неотрицательных вычетов), $\{-2, -1, 0, 1, 2\}$ (система абсолютно наименьших вычетов) и $\{-50, 41, -3, 3, -441\}$, в то время как множества $\{1, 2, 3, 4\}$, $\{-2, -1, 1, 2\}$ и $\{41, -3, 3, -441\}$ образуют приведенные системы вычетов по модулю 5. Полной системой вычетов по модулю 10 является, например, множество $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ (система наименьших неотрицательных вычетов), а соответствующая приведенная система вычетов по модулю 10 имеет вид $\{1, 3, 7, 9\}$.

Свойства полной и приведенной систем вычетов

1. $|\text{ПСВ}_n| = n$.
2. $|\text{ПрСВ}_n| = \varphi(n)$, где $\varphi(n)$ — функция Эйлера.
3. Если x пробегает полную систему вычетов по модулю n, то и $ax + b$ пробегает полную систему вычетов по модулю n для любого целого b и любого целого a, взаимно простого с n.
4. Если x пробегает приведенную систему вычетов по модулю n, то и ax пробегает полную систему вычетов по модулю n для любого целого a, взаимно простого с n.

Так, для любого целого a, взаимно простого с n, сравнение $x_i \equiv x_j (\mathrm{mod}\, n)$ имеет место тогда и только тогда, когда имеет место сравнение $ax_i \equiv ax_j (\mathrm{mod}\, n)$, и, для любого целого b, сравнение $ax_i \equiv ax_j (\mathrm{mod}\, n)$ выполнено тогда и только тогда, когда выполнено сравнение $ax_i + b \equiv ax_j + b (\mathrm{mod}\, n)$, что доказывает третье свойство. Для доказательства четвертого свойства необходимо только добавить, что домножение числа x, взаимно простого с n, на число a, взаимно простое с n,

дает число ax, взаимно простое с n. Доказательства остальных свойств очевидны; их можно найти, например, в [3].

Примеры решения задач

1. По модулю 15 выпишите:

а) полную систему вычетов;

б) приведенную систему вычетов;

в) полную систему вычетов, состоящую из чисел, делящихся на 4;

г) полную систему вычетов, состоящую из чисел, делящихся на 3;

д) полную систему вычетов, состоящую из чисел, сравнимых с 2 по модулю 14;

е) полную систему вычетов, состоящую из значений линейной формы $3x + 5y$.

Решение. Простейшая полная система вычетов по модулю 15 имеет вид $\{0, 1, 2, 3, \ldots, 13, 14\}$. Полными системами вычетов по модулю 15 являются множества $\{0, \pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm7\}$ и $\{30, -13, 3, 4, 20, -9, 37, 68, 9, -5, 41, 12, -2, 14\}$.

Простейшая приведенная система вычетов по модулю 15 имеет вид $\{1, 2, 4, 7, 8, 11, 13, 14\}$. Приведенными системами вычетов по модулю 15 являются множества $\{\pm1, \pm2, \pm4, \pm7\}$ и $\{-13, 4, 37, 68, 41, -2, 14\}$.

Полная система вычетов по модулю 15, состоящая из чисел, делящихся на 4, имеет, например, вид $\{4x : x = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\} = \{0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56\}$.

Полной системы вычетов по модулю 15, состоящей из чисел, делящихся на 3, не существует, поскольку $(3, 15) \neq 1$.

Полная система вычетов по модулю 15, состоящая из чисел, сравнимых с 2 по модулю 14, имеет вид $\{14x+2 : x = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\} = \{2, 16, 30, 44, 58, 72, 86, 100, 114, 128, 142, 156, 170, 184, 198\}$.

Полная система вычетов по модулю 15, состоящая из значений линейной формы $3x+5y$, имеет вид $\{3x+5y : x = 0, 1, 2; y = 0, 1, 2, 3, 4\} = \{0, 3, 6, 5, 8, 11, 10, 13, 16, 15, 18, 21, 20, 23, 26\}$. ▷

2. При каких n имеют место соотношения: $|\text{ПрСВ}_n| = 2$; $|\text{ПСВ}_n| = 3|\text{ПрСВ}_n|$?

Решение. Поскольку $|\text{ПрСВ}_n| = \varphi(n)$, а $|\text{ПСВ}_n| = n$, то первое соотношение эквивалентно уравнению $\varphi(x) = 2$, решениями которого являются числа 3, 4 и 6. Второе соотношение эквивалентно уравнению $\varphi(x) = x/3$, решениями которого являются числа вида $2^\alpha 3^\beta$, $\alpha, \beta \in \mathbb{N}$. ▷

Упражнения

1. По модулю 10 выпишите:
   а) полную систему вычетов;
   б) приведенную систему вычетов;
   в) полную систему вычетов, состоящую из чисел, делящихся на 3;
   г) полную систему вычетов, состоящую из чисел, делящихся на 4;
   д) полную систему вычетов, состоящую из чисел, сравнимых с 6 по модулю 21;
   е) полную систему вычетов, состоящую из значений линейной формы $2x + 5y$.
2. По модулю 18 выпишите:
   а) полную систему вычетов;
   б) приведенную систему вычетов;
   в) полную систему вычетов, состоящую из чисел, делящихся на 2;
   г) полную систему вычетов, состоящую из чисел, делящихся на 3;
   д) полную систему вычетов, состоящую из чисел, делящихся на 5;
   е) полную систему вычетов, состоящую из чисел, делящихся на 7;
   ж) полную систему вычетов, состоящую из чисел, сравнимых с 3 по модулю 13;
   з) полную систему вычетов, состоящую из значений линейной формы $2x + 9y$.
3. Выпишите полную систему вычетов по модулю 13 с помощью чисел, сравнимых с тремя по модулю 22.
4. Выпишите полную систему вычетов по модулю 13 с помощью чисел, сравнимых с 6 по модулю 22, и расположите ее в порядке возрастания наименьших по абсолютной величине вычетов.
5. Выпишите полную систему вычетов по модулю 18 с помощью чисел, сравнимых с 4 по модулю 11.
6. Для каких модулей полная система вычетов в семь раз длиннее, чем приведенная?
7. Для каких модулей полная система вычетов в шесть раз длиннее, чем приведенная?
8. Для каких модулей число чисел в приведенной системе вычетов составляет 2/3 от числа чисел полной системы вычетов?
9. Для каких модулей число чисел в приведенной системе вычетов составляет 4/5 от числа чисел полной системы вычетов?

Задачи

1. Является ли система чисел $\{1, -10, 2, 30, 8\}$ полной системой вычетов по какому-либо модулю?
2. Является ли система чисел $\{1, 3, 7, -1, -2\}$ приведенной системой вычетов по какому-либо модулю?
3. Выпишите полную (приведенную) систему наименьших неотрицательных вычетов по модулю n, $n \in \{2, 3, \ldots, 25\}$.
4. Выпишите полную (приведенную) систему наименьших по абсолютной величине вычетов по модулю n, $n \in \{2, 3, \ldots, 25\}$.
5. Выпишите полную (приведенную) систему наименьших двузначных вычетов по модулю n, $n \in \{2, 3, \ldots, 25\}$.
6. Для каких модулей число чисел в приведенной системе вычетов равно 30?
7. Выпишите полную систему вычетов по модулю n, $n \in \{2, 3, \ldots, 25\}$, с помощью чисел, сравнимых с 3 по модулю $2n + 1$.
8. Выпишите полную систему вычетов по модулю n, $n \in \{2, 3, \ldots, 25\}$, с помощью чисел, сравнимых с 6 по модулю $2n - 1$, и расположите ее в порядке возрастания наименьших по абсолютной величине вычетов.
9. Выпишите приведенную систему вычетов по модулю n, $n \in \{2, 3, \ldots, 25\}$, с помощью чисел, делящихся на $n - 1$.
10. Выпишите приведенную систему вычетов по модулю n, $n \in \{2, 3, \ldots, 25\}$, с помощью чисел, делящихся на $n + 1$, и расположите ее в порядке возрастания наименьших неотрицательных вычетов.
11. Выпишите полную систему вычетов по модулю 28, состоящую из чисел, являющихся значениями линейной формы $7x + 4y$.
12. Выпишите полную систему вычетов по модулю 30, состоящую из чисел, являющихся значениями линейной формы $10x + 3y$.
13. Выпишите полную систему вычетов по модулю pq, состоящую из чисел, являющихся значениями линейной формы $px + qy$, если $p, q \in \{2, 3, 5, 7, 11, 13, 17, 19\}$, $p \neq q$.
14. Для каких модулей приведенная система вычетов в три раза короче полной?
15. Для каких модулей приведенная система вычетов в пять раз короче полной?
16. Для каких модулей число чисел в приведенной системе вычетов составляет 2/5 от числа чисел полной системы вычетов?

17. При каких натуральных n имеет место соотношение:

а) $|\text{ПрСВ}_{2n}| = |\text{ПрСВ}_{3n}|$;
б) $|\text{ПрСВ}_{2n}| = |\text{ПрСВ}_{7n}|$;
в) $1/4|\text{ПСВ}_n| = |\text{ПрСВ}_n|$;
г) $17|\text{ПрСВ}_n| = 8|\text{ПСВ}_n|$;
д) $17|\text{ПрСВ}_n| = 16|\text{ПСВ}_n|$;
е) $10|\text{ПСВ}_n| = 11|\text{ПрСВ}_n|$;
ж) $11|\text{ПрСВ}_n| = 5|\text{ПСВ}_n|$;
з) $13|\text{ПрСВ}_n| = 6|\text{ПСВ}_n|$;
и) $8|\text{ПСВ}_n| = 13|\text{ПрСВ}_n|$?

18. При каких натуральных n имеет место соотношение:

а) $|\text{ПрСВ}_n| = 3$;
б) $|\text{ПрСВ}_n| = 4$;
в) $|\text{ПрСВ}_n| = 5$;
г) $|\text{ПрСВ}_n| = 6$;
д) $|\text{ПрСВ}_n| = 10$;
е) $|\text{ПрСВ}_n| = 12$?

§ 15. Малая теорема Ферма и теорема Эйлера

Малая теорема Ферма утверждает, что *для любого простого p и любого целого a имеет место сравнение* $a^p \equiv a (\mathrm{mod}\, p)$.

Часто используется и такая формулировка: *если p — простое число, и a — целое число, взаимно простое с p, то* $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$.

Теорема Эйлера утверждает, что *для любого натурального числа n и любого целого a, взаимно простого с n, имеет место сравнение* $a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$, *где $\varphi(n)$ — функция Эйлера.*

Теорема Эйлера является обобщением малой теоремы Ферма и, в свою очередь, обобщается теоремой Кармайкла.

Теорема Кармайкла утверждает, что для взаимно простых чисел a и n имеет место сравнение $a^{\lambda(n)} \equiv 1 (\mathrm{mod}\, n)$, где $\lambda(n)$ — *функция Кармайкла*: $\lambda(p^\alpha) = \varphi(p^\alpha)$ для простого $p \geqslant 3$ и натурального α; $\lambda(2^\alpha) = 2^{\alpha-2}$ для натурального $\alpha \geqslant 3$, в то время как $\lambda(2) = 1$, и $\lambda(4) = 2$; наконец, $\lambda(p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}) = [\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_s^{\alpha_s})]$, где $p_1, \ldots, p_s$ — различные простые числа, а $\alpha_1, \ldots, \alpha_s \in \mathbb{N}$.

Для доказательства теоремы Эйлера достаточно рассмотреть приведенную систему вычетов $\{x_1, x_2, \ldots, x_{\varphi(n)}\}$ по модулю n. Поскольку $(a, n) = 1$, то система $\{ax_1, ax_2, \ldots, ax_{\varphi(n)}\}$ также образует приведенную систему вычетов по модулю n и, следовательно, для любого $i \in \{1, 2, \ldots, \varphi(n)\}$ найдется $j \in \{1, 2, \ldots, \varphi(n)\}$, такое что $x_i \equiv ax_j (\mathrm{mod}\, n)$. Перемножая почленно все эти сравнения, мы получим соотношение $x_1 \cdot x_2 \cdot \ldots \cdot x_{\varphi(n)} \equiv$ $\equiv a^{\varphi(n)} \cdot x_1 \cdot x_2 \cdot \ldots \cdot x_{\varphi(n)} (\mathrm{mod}\, n)$ и, сокращая две части полученного сравнения на число $x_1 \cdot x_2 \cdot \ldots \cdot x_{\varphi(n)}$, взаимно простое с модулем n, мы получим соотношение $a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$.

Теорема Ферма является частным случаем теоремы Эйлера, поскольку $\varphi(p) = p - 1$ для простого числа p. Доказательство теоремы Кармайкла можно найти, например, в [3].

Примеры решения задач

1. Найдите остаток от деления 13^{26} на 10.

Решение. Прежде всего заменим число 13 наименьшим по абсолютной величине вычетом по модулю 10: $13 \equiv 3 (\mathrm{mod}\, 10)$. Поскольку $(3, 10) = 1$, то $3^{\varphi(10)} \equiv 1 (\mathrm{mod}\, 10)$. Поскольку $\varphi(10) = 4$, то $3^{26} \equiv (3^4)^6 \cdot 3^2 \equiv 3^2 \equiv 9 (\mathrm{mod}\, 10)$. Таким образом, остаток от деления 13^{26} на 10 равен 9. ▷

2. Найдите остаток от деления $2^{7^{2002}}$ на 352.

Решение. Прежде всего заметим, что остатком от деления $2^{7^{2002}}$ на 352 является такое целое число x, что $2^{7^{2002}} \equiv x (\mathrm{mod}\, 352)$, и $0 \leqslant x < 352$. Поскольку $352 = 2^5 \cdot 11$, то $(2^{7^{2002}}, 352) = 2^5$, откуда следует, что $x = 2^5 \cdot x_1$. Разделив все три части выписанного выше сравнения на 2^5, мы получим сравнение $2^{7^{2002}-5} \equiv x_1 (\mathrm{mod}\, 11)$.

Поскольку $(2, 11) = 1$, и $\varphi(11) = 10$, то $2^{10} \equiv 1 (\mathrm{mod}\, 11)$. Найдем остаток от деления числа $7^{2002} - 5$ на 10, то есть такое целое число y, что $7^{2002} - 5 \equiv y (\mathrm{mod}\, 10)$, и $0 \leqslant y < 10$. В этом случае $2^{7^{2002}} \equiv 2^y (\mathrm{mod}\, 11)$, то есть $2^y \equiv x_1 (\mathrm{mod}\, 11)$.

Поскольку $(7, 10) = 1$ и $\varphi(10) = 4$, то $7^4 \equiv 1 (\mathrm{mod}\, 10)$. Поскольку $2002 = 4 \cdot 500 + 2$, то $7^{2002} - 5 \equiv (7^4)^{500} \cdot 7^2 - 5 \equiv 7^2 - 5 \equiv 9 - 5 \equiv 4 (\mathrm{mod}\, 10)$. Таким образом, $y = 4$, и мы получаем сравнение $2^4 \equiv x_1 (\mathrm{mod}\, 11)$.

Поскольку $2^4 \equiv 5 (\mathrm{mod}\, 11)$, то $x_1 = 5$, и $x = 2^5 \cdot x_1 = 32 \cdot 5 = 160$. ▷

Упражнения

1. Найдите остаток от деления:

а) 5^{14} на 7; в) 5^{100} на 11; д) 3^{100} на 16; ж) 3^{20} на 28;

б) 24^{16} на 7; г) 15^{175} на 11; е) 37^{100} на 16; з) 31^{200} на 28.

2. Найдите наибольший отрицательный вычет, с которым сравнимо число:

а) 100^{345} по модулю 14; в) 99^{345} по модулю 54;

б) 30^{1000} по модулю 22; г) 1000^{99} по модулю 45.

3. Верно ли, что для $f(x) = 292x^{181} - 121x^{133} + 252x^{122} - 171x^{121} - 133x^{62} + 3$ имеет место сравнение:

а) $f(24) \equiv -2 (\mathrm{mod}\ 13)$; в) $f(-55) \equiv -4 (\mathrm{mod}\ 13)$;

б) $f(-24) \equiv 2 (\mathrm{mod}\ 11)$; г) $f(55) \equiv 4 (\mathrm{mod}\ 11)$?

4. Найдите остаток от деления:

а) $\tau(265)^{\sigma(265)}$ на $\varphi(625)$; г) $(5!)^{\sigma(25)}$ на $\varphi(7!)$;

б) $\varphi(2011)^{\varphi(2011)}$ на 1 000 000; д) $\sigma(10)^{\varphi(100)}$ на $\tau(1000)$;

в) $(6!)^{\varphi(25)}$ на 9!; е) $\varphi(1000)^{\varphi(1000)}$ на 17 000 000.

5. На какую цифру оканчивается число:

а) $32^{101} + 35^{301}$ в пятнадцатиричной системе счисления;

б) $(87^{78} + 78^{87})(432^{234} - 501^{501})$ в восемнадцатиричной системе счисления?

6. Найдите две последние цифры десятичной записи числа:

а) 2^{999}; в) 5^{2011}; д) 123^{2010}; ж) 200^{100};

б) 3^{999}; г) 7^{2011}; е) 557^{2012}; з) 55^{550}.

7. Найдите остаток от деления:

а) $5^{5^{1000}}$ на 325; б) $4^{5^{3000}}$ на 208; в) $5^{3^{1000}}$ на 275; г) $3^{3^{1000}}$ на 297.

8. На какую цифру оканчивается число:

а) $27^{23^{76}}$ в 37-ой системе счисления;

б) $37^{87^{107}}$ в 34-ой системе счисления?

9. Какому классу вычетов по модулю 351 принадлежит число $3^{5^{202}}$?

10. Найдите наибольший отрицательный вычет, с которым сравнимо число $10^{100^{100}}$ по модулю 71.

Задачи

1. Верно ли сравнение:

а) $2^{2145} + 3^{2145} \equiv 0 (\mathrm{mod}\ 11)$; в) $50^{151} + 616^{666} \equiv -93 (\mathrm{mod}\ 99)$;

б) $15^{2011} + 28^{2011} \equiv 0 (\mathrm{mod}\ 13)$; г) $29^{464} + 220^{330} \equiv -14 (\mathrm{mod}\ 45)$?

2. Найдите остаток от деления:

а) 177^{1000} на 10; е) 315^{487} на 85; л) 3^{1985} на 135;

б) 3^{49} на 15; ж) 2^{1000} на 100; м) 2^{10000} на 176;

в) 2^{6000} на 24; з) 15^{1000} на 108; н) 15^{1000} на 189;

г) 714^{3043} на 52; и) 145^{541} на 108; о) 2^{2000} на 208;

д) 714^{3034} на 58; к) 21^{10000} на 108; п) 21^{1000} на 297;

р) 3^{6000} на 297; т) 21^{1073} на 693;
с) 3^{13000} на 351; у) 3^{5000} на 891.

3. Найдите остаток от деления:

а) $(12371^{56}+34)^{28}$ на 11; в) $38^{30}\cdot 20^{23}\cdot 17^{31}$ на 215;
б) $(37^{73}+73^{37})\cdot 105^{26}$ на 13; г) $38^{30}\cdot 2^{22}\cdot 18^{31}$ на 215.

4. Найдите остатки от деления числа $(87^{78}+78^{87})(432^{234}-501^{501})$ на $3n$ и на $2(n+1)$, если $n=N-4[N/4]+5$, $N\in\{1,2,3,\ldots,25\}$.

5. Найдите остаток от деления:

а) $f(100)$ на 30, если $f(x)=2x^{100}+3x^{50}+4x+5$;
б) $f(200)$ на 90, если $f(x)=2x^{100}+3x^{50}+4x+5$.

6. Верно ли сравнение:

а) $f(47)\equiv -14(\mathrm{mod}\,7)$,
если $f(x)=88x^{122}+121x^{121}-99x^{110}+131x^{66}-100x^{55}-3$;
б) $f(24)\equiv -8(\mathrm{mod}\,13)$,
если $f(x)=292x^{181}-121x^{133}+252x^{122}171x^{121}-133x^{62}-3$;

7. Делится ли:

а) $f(75)$ на 11, если $f(x)=88x^{10}+4x^7-22x^4+101$;
б) $f(33)$ на 7, если $f(x)=55x^{99}+111x^{66}-141x^{45}-100x^{33}-99$;
в) $f(41)$ на 11, если $f(x)=171x^{101}+555x^{62}+202x^{51}-121x^{22}-90x-3$?

8. Найдите наименьшее по абсолютной величине число, с которым $201^{131}\cdot 302^{251}\cdot 17$ сравнимо по модулю 233.

9. Найдите две последние цифры десятичной записи числа:

а) 2^{2011}; б) 3^{2011}; в) 4^{2011}; г) 7^{2011}; д) 9^{2011}.

10. Найдите две последние цифры числа:

а) 88^{1986} в пятеричной системе счисления;
б) 50^{1990} в троичной системе счисления;
в) 55^{2000} в четверичной системе счисления.
г) 77^{2011} в шестеричной системе счисления.

11. Найдите четыре последние цифры троичной записи числа 28^{1000}.

12. Найдите пять последних цифр двоичной записи числа 28^{2000}.

13. Найдите остаток от деления:

а) $9^{99^{999}}$ на 14; д) $714^{30^{43}}$ на 52; и) $2^{5^{1000}}$ на 208;
б) $31^{57^{7}}$ на 17; е) $3^{2^{100}}$ на 73; к) $5^{3^{1000}}$ на 275;
в) $3^{33^{40}}$ на 29; ж) $2^{3^{1000}}$ на 176; л) $3^{3^{3000}}$ на 297;
г) $10^{100^{100}}$ на 49; з) $198^{5^{2000}}$ на 200; м) $2^{3^{400}}$ на 324;

н) $5^{5^{1000}}$ на 325; п) $6^{6^{6000}}$ на 396;

о) $3^{5^{1000}}$ на 351; р) $3^{3^{300}}$ на 420.

14. Найдите:

а) $\mathrm{rest}(2^{7^{91}-2}, 70)$; в) $\mathrm{rest}(5^{3^{73}}+29, 77)$; д) $\mathrm{rest}(14^{3^{1000}}, 80)$;

б) $\mathrm{rest}(3^{5^{602}-3}, 50)$; г) $\mathrm{rest}(11^{2^{666}-14}, 78)$; е) $\mathrm{rest}(7^{3^{207}}, 63)$.

15. В какой класс вычетов по модулю 79 попадает число $81^{9^{99}}$?

16. Найдите наибольший отрицательный вычет числа $280^{3^{1002}}$ по модулю 275.

17. Найдите наименьшее по абсолютной величине число, с которым $8^{747^{606}}$ сравнимо по модулю 43.

18. Найдите абсолютно наименьший вычет числа $300^{3^{3000}}$ по модулю 297.

19. Найдите последнюю цифру числа:

а) 20^{48} в двенадцатеричной системе счисления;

б) 20^{48^5} в двенадцатеричной системе счисления;

в) 13^{7^5} в десятичной системе счисления;

г) $13^{7^{5^3}}$ в десятичной системе счисления.

20. Найдите две последние цифры десятичной записи числа:

а) $17^{17^{100}}$; б) $13^{13^{100}}$; в) $19^{19^{100}}$; г) $27^{57^{67}}$.

21. Найдите наибольший отрицательный вычет, с которым сравнимо число $201^{131^{333}\cdot 302^{252}\cdot 17}$ по модулю 233.

22. Для любого натурального числа n найдите остаток от деления 5^{21^n} на 37.

23. Найдите остаток от деления:

а) $7^{7^{7^7}}$ на 37; б) $2^{2^{2^{2^2}}}$ на 324.

24. На какую цифру оканчивается число $7^{7^{7^7}} - 7^{7^7}$ в десятичной системе счисления?

25. Найдите две последние цифры десятичной записи числа $7^{7^{7^{\cdots^7}}}$, если в конструкции участвует 1001 семерка.

26. Найдите остаток от деления числа $2^{2^{2^{\cdots^2}}}$ на 7, если в конструкции участвуют n двоек.

27. Найдите остаток от деления числа $5^{5^{5^{\cdots^5}}}$ на 35, если в конструкции участвуют n пятерок.

28. Найдите остаток от деления числа $5^{5^{5^{\cdots^5}}}$ на 100, если в конструкции участвуют n пятерок.

29. При каких m имеет место сравнение:

а) $m^5 + 7m + 8 \equiv 0 (\mathrm{mod}\ 3)$;

б) $(m+1)^m + m^{m+1} \equiv 0 (\mathrm{mod}\ 3)$;

в) $2m^{100} + 3m^{50} + 4m + 5 \equiv 0 (\mathrm{mod}\ 20)$?

30. Докажите:

а) $p \in P,\ p > 3 \Rightarrow a^p \equiv a (\mathrm{mod}\ 6p)$;

б) $a \equiv b (\mathrm{mod}\ p),\ p \in P \Rightarrow a^{p-1} + a^{p-2}b + a^{p-3}b^2 + \ldots + b^{p-1} \equiv 0 (\mathrm{mod}\ p)$.

§ 16. Линейные сравнения и системы сравнений

Пусть $f(x) = a_m x^m + \ldots + a_1 x + a_0$ — многочлен с целыми коэффициентами, и $a_m \not\equiv 0 (\mathrm{mod}\ n)$. Если $f(b) \equiv 0 (\mathrm{mod}\ n)$ для некоторого $b \in \mathbb{Z}$, то $f(x) \equiv 0 (\mathrm{mod}\ n)$ для любого $x \equiv b (\mathrm{mod}\ n)$. В этом случае говорят, что класс вычетов $\mathbf{b}_n = \{x \in \mathbb{Z} : x \equiv b (\mathrm{mod}\ n)\}$ является *решением* сравнения $f(x) \equiv 0 (\mathrm{mod}\ n)$, которое называется *сравнением степени m по модулю n*.

Так, решением сравнения третьей степени $2x^3 + 1 \equiv 0 (\mathrm{mod}\ 5)$ по модулю 5 является класс $\mathbf{3}_5 = \{x \in \mathbb{Z} : x \equiv 3 (\mathrm{mod}\ 5)\}$, поскольку $2 \cdot 3^3 + 1 \equiv 55 \equiv 0 (\mathrm{mod}\ 5)$. Кроме того, данное решение будет единственным, поскольку $2 \cdot 0^3 + 1 \not\equiv 0 (\mathrm{mod}\ 5)$, $2 \cdot 1^3 + 1 \not\equiv 0 (\mathrm{mod}\ 5)$, $2 \cdot 2^3 + 1 \not\equiv 0 (\mathrm{mod}\ 5)$, и $2 \cdot 4^3 + 1 \not\equiv 0 (\mathrm{mod}\ 5)$.

Теорема о линейных сравнениях (см. [3]) утверждает, что *линейное сравнение $ax \equiv b (\mathrm{mod}\ n)$ имеет ровно одно решение, если $(a, n) = 1$, ровно d решений, если $(a, n) = d$, $d | n$, и не имеет решений в остальных случаях.*

При этом единственное решение $x \equiv \alpha (\mathrm{mod}\ n)$ для случая $(a, n) = 1$ может быть найдено различными способами.

Простейший способ — перебор представителей всех классов вычетов по модулю n до первого «подходящего» класса. Этот способ применим лишь для малых n.

Второй способ связан с рассмотрением сравнений $ax \equiv b (\mathrm{mod}\ n)$, $ax \equiv b + n (\mathrm{mod}\ n)$, $ax \equiv b + 2n (\mathrm{mod}\ n)$, $\ldots$, $ax \equiv b + nk (\mathrm{mod}\ n)$,... с целью получения в правой части числа $b + nk$, делящегося на a. Поскольку $(a, n) = 1$, то числа k и $nk + b$ пробегают полную систему вычетов по модулю $|a|$ одновременно, то есть найдется единственное число $k \in \{0, 1, \ldots, |a| - 1\}$, такое что $nk + b \equiv 0 (\mathrm{mod}\ |a|)$. Следовательно, искомое решение принимает вид $x \equiv \dfrac{b + nk}{a} (\mathrm{mod}\ n)$, где $k \in \{0, 1, \ldots, |a| - 1\}$.

Третий способ основан на теореме Эйлера: поскольку $a^{\varphi(n)} \equiv 1 (\mathrm{mod}\ n)$, то искомое решение принимает вид $x \equiv b a^{\varphi(n)-1} (\mathrm{mod}\ n)$.

Четвертый способ основан на свойствах цепных дробей: искомое решение имеет вид $x \equiv (-1)^s P_{s-1} (\mathrm{mod}\, n)$, где

$$P_0/Q_0, \frac{P_1}{Q_1}, \ldots, \frac{P_{s-1}}{Q_{s-1}}, \frac{P_s}{Q_s} = \frac{n}{a}$$

— система подходящих дробей для разложения обыкновенной дроби n/a в цепную дробь. Мы подробнее остановимся на этом способе в разделе, посвященном цепным дробям.

Если же $(a, n) = d$, где $d > 1$ и $d|b$, то, разделив все три части сравнения $ax \equiv b (\mathrm{mod}\, n)$ на число d, мы получим новое сравнение первой степени $a/dx \equiv b/d (\mathrm{mod}\, n/d)$. Поскольку $(a/d, n/d) = 1$, то указанное сравнение имеет единственное решение $x \equiv \alpha (\mathrm{mod}\, n/d)$ по модулю n/d. Найдя это решение одним из указанных выше способов, мы запишем d решений первоначального сравнения по модулю n в виде $x \equiv \alpha + m/d \cdot k (\mathrm{mod}\, n)$, где $k = 0, 1, \ldots, d - 1$.

Китайская теорема об остатках (см. [5]) утверждает, что система линейных сравнений

$$\begin{cases} x & \equiv & c_1 (\mathrm{mod}\, n_1) \\ \ldots & & \\ x & \equiv & c_k (\mathrm{mod}\, n_k) \end{cases}$$

с попарно взаимно простыми модулями $n_1, \ldots, n_k$ имеет ровно одно решение, представляющее собой класс вычетов по модулю $N = [n_1, \ldots, n_k] = n_1 \cdot \ldots \cdot n_k$, которое имеет вид

$$x \equiv \frac{N}{n_1} c_1 y_1 + \ldots + \frac{N}{n_k} c_k y_k (\mathrm{mod}\, N),$$

где y_i — решение линейного сравнения $N/(n_i) \cdot y \equiv 1 (\mathrm{mod}\, n_i)$, $i = 1, \ldots, k$.

В общем случае решением системы линейных сравнений

$$\begin{cases} x & \equiv & c_1 (\mathrm{mod}\, n_1) \\ \ldots & & \\ x & \equiv & c_k (\mathrm{mod}\, n_k) \end{cases}$$

является класс вычетов по модулю $N = [n_1, \ldots, n_k]$: $x \equiv \alpha (\mathrm{mod}\, N)$.

Примеры решения задач

1. Решите сравнение $11x \equiv 5 (\mathrm{mod}\, 7)$ всеми возможными способами.

Решение. Прежде всего перепишем сравнение в виде $4x \equiv -2 (\mathrm{mod}\, 7)$. Поскольку $(4, 7) = 1$, то сравнение имеет единственное решение — класс вычетов по модулю 7.

Последовательно перебирая числа 0, 1, 2, ..., 6, являющиеся представителями всех классов вычетов по модулю 7, мы получим, что $4 \cdot 3 \equiv -2 (\mathrm{mod}\, 7)$, то есть решением сравнения $4x \equiv -2 (\mathrm{mod}\, 7)$ является класс вычетов $x \equiv 3 (\mathrm{mod}\, 7)$.

Последовательно добавляя к правой части модуль 7, мы получим сравнения $4x \equiv -2 (\mathrm{mod}\, 7)$, $4x \equiv 5 (\mathrm{mod}\, 7)$, $4x \equiv 12 (\mathrm{mod}\, 7)$. Деля две части последнего сравнения на 4, мы получим, что $x \equiv 3 (\mathrm{mod}\, 7)$.

Наконец, домножая обе части сравнения $4x \equiv -2 (\mathrm{mod}\, 7)$ на $4^{\varphi(7)-1} = 4^5$, мы получаем, что $x \equiv -2 \cdot 4^5 (\mathrm{mod}\, 7)$. Поскольку $4^5 \equiv (-3)^5 \equiv 9 \cdot (-27) \equiv 2 \cdot 1 \equiv 2 (\mathrm{mod}\, 7)$, то $x \equiv -2 \cdot 2 \equiv -4 \equiv 3 (\mathrm{mod}\, 7)$. ▷

2. Решите систему сравнений первой степени

$$\begin{cases} x \equiv 4 & (\mathrm{mod}\, 5) \\ x \equiv 1 & (\mathrm{mod}\, 12) \\ x \equiv 0 & (\mathrm{mod}\, 7). \end{cases}$$

Решение. Легко видеть, что $[5, 12, 7] = [5, 2^2 \cdot 3, 7] = 2^2 \cdot 3 \cdot 5 \cdot 7 = 420$. Поскольку $x \equiv 1 (\mathrm{mod}\, 12)$, то $x = 12t + 1$, где $t \in \mathbb{Z}$. Подставляя в сравнение $x \equiv 0 (\mathrm{mod}\, 7)$ полученное выше выражение для x, мы получим сравнение $12t + 1 \equiv 0 (\mathrm{mod}\, 7)$. Решая его относительно t, мы получим, что $-2t \equiv -1 (\mathrm{mod}\, 7)$, или $-2t \equiv 6 (\mathrm{mod}\, 7)$, или $t \equiv -3 (\mathrm{mod}\, 7)$. Таким образом, $t = 7t_1 - 3$, $t_1 \in \mathbb{Z}$, то есть $x = 12(7t_1 - 3) + 1 = 84t_1 - 35$, $t_1 \in \mathbb{Z}$. Подставляя в сравнение $x \equiv 4 (\mathrm{mod}\, 5)$ полученное выше выражение для x, мы получим сравнение $84t_1 - 35 \equiv 4 (\mathrm{mod}\, 5)$. Решая его относительно t_1, мы получим, что $4t_1 \equiv 4 (\mathrm{mod}\, 5)$, или $t_1 \equiv 1 (\mathrm{mod}\, 5)$. Таким образом, $t_1 = 5t_2 + 1$, $t_2 \in \mathbb{Z}$, то есть $x = 84(5t_2 + 1) - 35 = 420t_2 + 49$, $t_2 \in \mathbb{Z}$. Следовательно, единственное решение первоначальной системы — класс вычетов $x \equiv 49 (\mathrm{mod}\, 420)$. ▷

3. Решите систему сравнений первой степени

$$\begin{cases} 2x \equiv 14 & (\mathrm{mod}\, 10) \\ 15x \equiv 6 & (\mathrm{mod}\, 12). \end{cases}$$

Решение. Легко видеть, что $[10, 12] = [2 \cdot 5, 2^2 \cdot 3] = 2^2 \cdot 3 \cdot 5 = 60$. Поскольку $15x \equiv 6 (\mathrm{mod}\, 12)$, то $3x \equiv 6 (\mathrm{mod}\, 12)$, и $x \equiv 2 (\mathrm{mod}\, 4)$. Поскольку $2x \equiv 14 (\mathrm{mod}\, 10)$, то $2x \equiv 4 (\mathrm{mod}\, 10)$, и $x \equiv 2 (\mathrm{mod}\, 5)$. Таким образом, наша система эквивалентна системе

$$\begin{cases} x \equiv 2 & (\mathrm{mod}\, 5) \\ x \equiv 2 & (\mathrm{mod}\, 4). \end{cases}$$

Поскольку $x \equiv 2(\mathrm{mod}\,5)$, то $x = 5t + 2$, где $t \in \mathbb{Z}$. Подставляя в сравнение $x \equiv 2(\mathrm{mod}\,4)$ полученое выше выражение для x, мы получим сравнение $5t + 2 \equiv 2(\mathrm{mod}\,4)$. Решая его относительно t, мы получим, что $t \equiv 0(\mathrm{mod}\,4)$. Таким образом, $t = 4t_1$, $t_1 \in \mathbb{Z}$, то есть $x = 5(4t_1) + 2 = 20t_1 + 2$. Следовательно, $x \equiv 2(\mathrm{mod}\,20)$. Поскольку один класс $x \equiv 2(\mathrm{mod}\,20)$ по модулю 20 разбивается на три класса $x \equiv 2(\mathrm{mod}\,60)$, $x \equiv 2 + 20(\mathrm{mod}\,20)$, $x \equiv 2 + 2 \cdot 20(\mathrm{mod}\,20)$, то мы получаем три решения $x \equiv 2(\mathrm{mod}\,60)$, $x \equiv 22(\mathrm{mod}\,60)$, $x \equiv 42(\mathrm{mod}\,60)$ первоначальной системы сравнений. ▷

Упражнения

1. Решите сравнение $8x \equiv 6(\mathrm{mod}\,5)$ всеми возможными способами.

2. Решите сравнение $5x \equiv 6(\mathrm{mod}\,7)$ всеми возможными способами.

3. Решите сравнение:

а) $3x \equiv 1(\mathrm{mod}\,7)$;
б) $100x \equiv 21(\mathrm{mod}\,23)$;
в) $42x \equiv 33(\mathrm{mod}\,90)$;
г) $20x \equiv 12(\mathrm{mod}\,48)$;
д) $20x - 50 \equiv 0(\mathrm{mod}\,35)$;
е) $78x \equiv 102(\mathrm{mod}\,273)$;
ж) $315x \equiv -10(\mathrm{mod}\,275)$;
з) $76x \equiv 232(\mathrm{mod}\,220)$;
и) $45x \equiv 75(\mathrm{mod}\,100)$.

4. Решите систему сравнений первой степени:

а) $\begin{cases} x \equiv 1(\mathrm{mod}\,5) \\ x \equiv 2(\mathrm{mod}\,6) \\ x \equiv 3(\mathrm{mod}\,7) \end{cases}$;

б) $\begin{cases} 3x \equiv 7(\mathrm{mod}\,10) \\ 2x \equiv 5(\mathrm{mod}\,15) \\ 7x \equiv 5(\mathrm{mod}\,12) \end{cases}$;

в) $\begin{cases} 5x + 7 \equiv 0(\mathrm{mod}\,12) \\ 3x \equiv 7(\mathrm{mod}\,8) \end{cases}$;

г) $\begin{cases} 4x \equiv 3(\mathrm{mod}\,7) \\ 5x \equiv 4(\mathrm{mod}\,11) \\ 11x \equiv 8(\mathrm{mod}\,13) \end{cases}$;

д) $\begin{cases} 18x \equiv 226(\mathrm{mod}\,10) \\ 30x \equiv 232(\mathrm{mod}\,24) \end{cases}$;

е) $\begin{cases} 3x \equiv 1(\mathrm{mod}\,10) \\ 4x \equiv 3(\mathrm{mod}\,5) \\ 2x \equiv 7(\mathrm{mod}\,9) \end{cases}$;

ж) $\begin{cases} 5x \equiv 1(\mathrm{mod}\,12) \\ 5x \equiv 2(\mathrm{mod}\,8) \\ 7x \equiv 3(\mathrm{mod}\,11) \end{cases}$;

з) $\begin{cases} 3x \equiv 5(\mathrm{mod}\,2) \\ x \equiv -3(\mathrm{mod}\,5) \\ 4x \equiv 7(\mathrm{mod}\,9) \end{cases}$;

и) $\begin{cases} 20x \equiv -10(\mathrm{mod}\,15) \\ 2x \equiv -12(\mathrm{mod}\,10) \end{cases}$

5. Для любых целых чисел a, b и c решите систему сравнений первой степени:

а) $\begin{cases} x \equiv a \pmod{13} \\ x \equiv b \pmod{5} \end{cases}$;

б) $\begin{cases} x \equiv a \pmod{3} \\ x \equiv b \pmod{5} \\ x \equiv c \pmod{7} \end{cases}$;

в) $\begin{cases} x \equiv a \pmod{7} \\ x \equiv b \pmod{81} \end{cases}$.

Задачи

1. Сколько решений имеет сравнение:

а) $14x \equiv 28 \pmod{77}$;
б) $15x \equiv 25 \pmod{35}$;
в) $12x \equiv 18 \pmod{42}$;
г) $18x \equiv 27 \pmod{45}$;
д) $11x \equiv 33 \pmod{55}$;
е) $24x \equiv 40 \pmod{80}$;
ж) $13x \equiv 26 \pmod{65}$;
з) $21x \equiv 56 \pmod{70}$;
и) $25x \equiv 50 \pmod{100}$?

2. Решите сравнение:

а) $10x \equiv 15 \pmod{65}$;
б) $15x \equiv 9 \pmod{39}$;
в) $12x \equiv 8 \pmod{52}$;
г) $48x \equiv 171 \pmod{111}$;
д) $114x \equiv 6 \pmod{186}$;
е) $92x \equiv 8 \pmod{164}$;
ж) $47x \equiv 2 \pmod{127}$;
з) $212x \equiv -44 \pmod{20}$;
и) $155x \equiv -55 \pmod{15}$;
к) $295x \equiv 15 \pmod{415}$;
л) $1000x \equiv 200 \pmod{300}$;
м) $3650x \equiv 1450 \pmod{5350}$.

3. При каких целых a сравнение $ax \equiv 3 \pmod{30}$ разрешимо?

4. Для любого натурального a решите сравнение:

а) $(a^2+1)x \equiv a^2 \pmod{a^3+2a}$; б) $(a^2+2a)x \equiv 1 \pmod{a^2+3a+1}$.

5. Решите систему сравнений первой степени:

а) $\begin{cases} 5x \equiv 9 \pmod{12} \\ 3x \equiv 15 \pmod{30} \end{cases}$;

б) $\begin{cases} 4x \equiv 8 \pmod{14} \\ 15x \equiv 12 \pmod{27} \end{cases}$;

в) $\begin{cases} 6x \equiv 12 \pmod{30} \\ 12x \equiv 36 \pmod{42} \end{cases}$;

г) $\begin{cases} 4x \equiv 4 \pmod{15} \\ 3x \equiv 8 \pmod{10} \end{cases}$;

д) $\begin{cases} 4x \equiv 2 \pmod{10} \\ 3x \equiv 3 \pmod{6} \end{cases}$;

з) $\begin{cases} 12x \equiv 6 \pmod{27} \\ 10x \equiv 8 \pmod{12} \end{cases}$;

е) $\begin{cases} 5x \equiv 10 \pmod{25} \\ 10x \equiv 15 \pmod{35} \end{cases}$;

и) $\begin{cases} 600x \equiv 150 \pmod{375} \\ 810x \equiv 420 \pmod{210} \end{cases}$;

ж) $\begin{cases} 14x \equiv 2 \pmod{16} \\ 6x \equiv 18 \pmod{21} \end{cases}$;

к) $\begin{cases} 1000x \equiv 20 \pmod{300} \\ 625x \equiv 400 \pmod{175} \end{cases}$.

6. Решите систему сравнений первой степени:

а) $\begin{cases} x \equiv 3 \pmod{8} \\ x \equiv 11 \pmod{20} \\ x \equiv 1 \pmod{5} \end{cases}$;

ж) $\begin{cases} 5x \equiv 11 \pmod{18} \\ 3x \equiv 9 \pmod{16} \\ 8x \equiv 4 \pmod{25} \end{cases}$;

б) $\begin{cases} 5x \equiv 8 \pmod{14} \\ 3x \equiv 72 \pmod{15} \\ 2x \equiv -2 \pmod{10} \end{cases}$;

з) $\begin{cases} 6x \equiv 2 \pmod{7} \\ 15x \equiv 3 \pmod{36} \\ 2x \equiv 2 \pmod{20} \end{cases}$;

в) $\begin{cases} 6x \equiv 2 \pmod{20} \\ x \equiv -2 \pmod{5} \\ 4x \equiv 11 \pmod{29} \end{cases}$;

и) $\begin{cases} 2x \equiv 2 \pmod{16} \\ x \equiv 15 \pmod{37} \\ 16x \equiv 0 \pmod{4} \end{cases}$;

г) $\begin{cases} 10x \equiv 20 \pmod{30} \\ 4x \equiv 2 \pmod{10} \\ 8x \equiv 16 \pmod{4} \end{cases}$;

к) $\begin{cases} 6x \equiv -8 \pmod{15} \\ 8x \equiv -4 \pmod{12} \\ 4x \equiv 5 \pmod{7} \end{cases}$;

д) $\begin{cases} 9x \equiv 9 \pmod{21} \\ 27x \equiv 9 \pmod{45} \\ 3x \equiv 1 \pmod{4} \end{cases}$;

л) $\begin{cases} 10x \equiv 5 \pmod{15} \\ 6x \equiv 6 \pmod{21} \\ 4x \equiv -6 \pmod{10} \end{cases}$;

е) $\begin{cases} 8x \equiv 2 \pmod{14} \\ 10x \equiv 10 \pmod{22} \\ 8x \equiv 4 \pmod{12} \end{cases}$;

м) $\begin{cases} 1000x \equiv 20 \pmod{300} \\ 625x \equiv 400 \pmod{175} \\ 8x \equiv 16 \pmod{4} \end{cases}$.

7. Решите систему сравнений первой степени:

а) $\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 4 \pmod{5} \\ x \equiv 2 \pmod{7} \\ x \equiv 9 \pmod{11} \\ x \equiv 3 \pmod{13} \end{cases}$;

б) $\begin{cases} x \equiv 0 \pmod{2} \\ x \equiv -2 \pmod{3} \\ x \equiv -3 \pmod{5} \\ x \equiv 4 \pmod{6} \\ x \equiv 7 \pmod{15} \end{cases}$;

в) $\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{4} \\ x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{6} \\ x \equiv 5 \pmod{7} \end{cases}$.

8. Для натурального числа $n = N - 4\lfloor N/4 \rfloor + 5$, где $N \in \{1, 2, 3, \ldots, 25\}$, решите систему сравнений первой степени $\begin{cases} nx \equiv 1 (\mathrm{mod}\ 11) \\ x \equiv -2 (\mathrm{mod}\ n) \\ 31x \equiv 8 (\mathrm{mod}\ 13) \end{cases}$.

9. Для нечетного простого числа p решите систему сравнений первой степени:

а) $\begin{cases} x \equiv 1 (\mathrm{mod}\ p-1) \\ x \equiv 2 (\mathrm{mod}\ p) \\ x \equiv 3 (\mathrm{mod}\ p+1) \end{cases}$; б) $\begin{cases} x \equiv p-2 (\mathrm{mod}\ p+1) \\ x \equiv p+2 (\mathrm{mod}\ p-1) \end{cases}$.

10. При каких целых a совместна система сравнений первой степени:

а) $\begin{cases} x \equiv a (\mathrm{mod}\ 42) \\ x \equiv 11 (\mathrm{mod}\ 70) \end{cases}$; б) $\begin{cases} x \equiv a (\mathrm{mod}\ 28) \\ x \equiv a^2 (\mathrm{mod}\ 77) \end{cases}$?

11. Определите все целые значения параметра a, при которых разрешима система сравнений:

а) $\begin{cases} 8x \equiv 20 (\mathrm{mod}\ 36) \\ 75x + 30a \equiv 0 (\mathrm{mod}\ 36) \end{cases}$; в) $\begin{cases} 9x \equiv 15 (\mathrm{mod}\ 30) \\ 8x + 12a \equiv 0 (\mathrm{mod}\ 30) \end{cases}$;

б) $\begin{cases} 9x \equiv 12 (\mathrm{mod}\ 24) \\ 50x + 70a \equiv 0 (\mathrm{mod}\ 24) \end{cases}$; г) $\begin{cases} 18x \equiv 90 (\mathrm{mod}\ 60) \\ 46x - 5a \equiv 0 (\mathrm{mod}\ 60) \end{cases}$.

Решите систему при найденных значениях параметра a.

12. Трехзначное число при делении на 12 дает в остатке 5. Удвоение этого числа дает число, которое при делении на 35 дает в остатке 4. Найдите первоначальное число.

13. Найдите все натуральные числа между 200 и 500, которые при делении на 4, 5 и 7 дают в остатке 3, 4 и 5, соответственно.

14. Найдите все натуральные числа, которые при делении на 2, 3, 4, 5, 6, 7 дают остатки 0, 1, 2, 3, 4, 5, соответственно.

§ 17. Сравнения и системы сравнений по простому модулю

Для данного простого числа p сравнение $f(x) \equiv 0 (\mathrm{mod}\ p)$ степени m по модулю p эквивалентно сравнению $x^s + b_{s-1}x^{s-1} + \ldots + b_1 x + b_0 \equiv 0 (\mathrm{mod} p)$ степени $s \leqslant p-1$ по модулю p и имеет не более s решений. Их можно

найти перебором представителей $0, \ldots, p-1$ всех классов вычетов по модулю p.

Для бесквадратного числа $n = p_1 \cdot \ldots \cdot p_k$, являющегося произведением различных простых чисел, все решения сравнения $f(x) \equiv 0 (\mathrm{mod}\, n)$ степени m по модулю n могут быть найдены, используя приведенные выше аргументы и следующее свойство: $f(x) \equiv 0 (\mathrm{mod}\, n)$ тогда и только тогда, когда

$$\begin{cases} f(x) \equiv 0 (\mathrm{mod}\, p_1) \\ \ldots \\ f(x) \equiv 0 (\mathrm{mod}\, p_k). \end{cases}$$

В этом случае число R решений сравнения $f(x) \equiv 0 (\mathrm{mod}\, n)$ по модулю $n = p_1 \cdot \ldots \cdot p_k$ равно произведению $R_1 \cdot R_2 \cdot \ldots \cdot R_k$, где R_i — число решений сравнения $f(x) \equiv 0 (\mathrm{mod}\, p_i)$, $i = 1, 2, \ldots, k$.

Подробные доказательства этих и других фактов можно найти, например, в [3].

Примеры решения задач

1. Решите сравнение $133x^{40} - 148x^{39} + 85x^{38} - 98x^2 + x + 6 \equiv 0 (\mathrm{mod}\, 7)$.

Решение. Прежде всего заменим коэффициенты многочлена $133x^{40} - 148x^{39} + 85x^{38} - 98x^2 + x + 6$, то есть числа, стоящие на «первом этаже» нашего сравнения, их остатками от деления на 7 (или их наименьшими по абсолютной величине вычетами по модулю 7). Поскольку $133 \equiv 0 (\mathrm{mod}\, 7)$, $-148 \equiv -1 (\mathrm{mod}\, 7)$, $85 \equiv 1 (\mathrm{mod}\, 7)$, $-98 \equiv 0 (\mathrm{mod}\, 7)$ и $6 \equiv -1 (\mathrm{mod}\, 7)$, то наше сравнение эквивалентно сравнению $-x^{39} + x^{38} + x - 1 \equiv 0 (\mathrm{mod}\, 7)$.

Проверим, является ли решением сравнения нулевой класс по модулю 7. Поскольку $-1 \not\equiv 0 (\mathrm{mod}\, 7)$, то нулевой класс $x \equiv 0 (\mathrm{mod}\, 7)$ решением нашего сравнения не является.

Если $x \not\equiv 0 (\mathrm{mod}\, 7)$, то $(x, 7) = 1$, и $x^6 \equiv 1 (\mathrm{mod}\, 7)$. Для таких x мы можем заменить показатели степеней в записи многочлена $-x^{39} + x^{38} + x - 1$, то есть числа, стоящие на «втором этаже» нашего сравнения, их остатками от деления на 6. Поскольку $39 \equiv 3 (\mathrm{mod}\, 6)$ и $38 \equiv 2 (\mathrm{mod}\, 6)$, то для $x \not\equiv 0 (\mathrm{mod}\, 7)$ сравнение $-x^{39} + x^{38} + x - 1 \equiv 0 (\mathrm{mod}\, 7)$ эквивалентно сравнению $-x^3 + x^2 + x - 1 \equiv 0 (\mathrm{mod}\, 7)$. Перебирая представители 1, 2, 3, -3, -2, -1 ненулевых классов вычетов по модулю 7, мы получаем, что $-1^3 + 1^2 + 1 - 1 \equiv 0 (\mathrm{mod}\, 7)$; $-2^3 + 2^2 + 2 - 1 \equiv 4 \not\equiv 0 (\mathrm{mod}\, 7)$; $-3^3 + 3^2 + 3 - 1 \equiv 5 \not\equiv 0 (\mathrm{mod}\, 7)$; $-(-3)^3 + (-3)^2 - 3 - 1 \equiv -3 \not\equiv 0 (\mathrm{mod}\, 7)$; $-(-2)^3 + (-2)^2 - 2 - 1 \equiv 2 \not\equiv 0 (\mathrm{mod}\, 7)$; $-(-1)^3 + (-1)^2 - 1 - 1 \equiv 0 (\mathrm{mod}\, 7)$. Таким образом, решениями сравнения $133x^{40} - 148x^{39} + 85x^{38} - 98x^2 +$

$+x+6 \equiv 0 (\mathrm{mod}\, 7)$ являются следующие классы вычетов по модулю 7: $x \equiv 1 (\mathrm{mod}\, 7)$ и $x \equiv -1 (\mathrm{mod}\, 7)$.

Впрочем, в данной задаче этот результат мог быть получен и более простым способом: поскольку $-x^3+x^2+x-1 = -x^2(x-1)+(x-1) = -(x-1)(x^2-1) = -(x-1)^2(x+1)$, то сравнение $-x^3+x^2+x-1 \equiv 0 (\mathrm{mod}\, 7)$ выполняется либо при $x \equiv 1 (\mathrm{mod}\, 7)$, либо при $x \equiv -1 (\mathrm{mod}\, 7)$. ▷

2. Решите сравнение $76x^{244} - 353x^{123} + 43x^{121} + 359 \equiv 0 (\mathrm{mod}\, 35)$.

Решение. Поскольку $35 = 5 \cdot 7$, то сравнение $76x^{244} - 353x^{123} + 43x^{121} + 359 \equiv 0 (\mathrm{mod}\, 35)$ эквивалентно системе сравнений

$$\begin{cases} 76x^{244} - 353x^{123} + 43x^{121} + 359 \equiv 0 (\mathrm{mod}\, 5) \\ 76x^{244} - 353x^{123} + 43x^{121} + 359 \equiv 0 (\mathrm{mod}\, 7). \end{cases}$$

Решим каждое из сравнений выписанной выше системы.

Для решения сравнения $76x^{244} - 353x^{123} + 43x^{121} + 359 \equiv 0 (\mathrm{mod}\, 5)$ заменим коэффициенты многочлена $76x^{244} - 343x^{123} + 43x^{121} + 359$ их наименьшими по абсолютной величине вычетами по модулю 5. Поскольку $76 \equiv 1 (\mathrm{mod}\, 5)$, $-343 \equiv 2 (\mathrm{mod}\, 5)$, $43 \equiv -2 (\mathrm{mod}\, 5)$, и $359 \equiv -1 (\mathrm{mod}\, 5)$, то наше сравнение эквивалентно сравнению $x^{244} + 2x^{123} - 2x^{121} - 1 \equiv 0 (\mathrm{mod}\, 5)$.

Поскольку $-1 \not\equiv 0 (\mathrm{mod}\, 5)$, то нулевой класс $x \equiv 0 (\mathrm{mod}\, 5)$ не является *решением нашего сравнения.*

Если $x \not\equiv 0 (\mathrm{mod}\, 5)$, то $(x, 5) = 1$, и $x^4 \equiv 1 (\mathrm{mod}\, 5)$. Для таких x заменим показатели степеней в записи многочлена $x^{244} + 2x^{123} - 2x^{121} - 1$ их остатками от деления на 4. Поскольку $244 \equiv 0 (\mathrm{mod}\, 4)$, $123 \equiv 3 (\mathrm{mod}\, 4)$ и $121 \equiv 1 (\mathrm{mod}\, 4)$, то для $x \not\equiv 0 (\mathrm{mod}\, 5)$ сравнение $x^{244} + 2x^{123} - 2x^{121} - 1 \equiv 0 (\mathrm{mod}\, 5)$ эквивалентно сравнению $x^0 + 2x^3 - 2x - 1 \equiv 0 (\mathrm{mod}\, 5)$ или, что то же, сравнению $2x^3 - 2x \equiv 0 (\mathrm{mod}\, 5)$. Перебирая представители 1, 2, -2, -1 ненулевых классов вычетов по модулю 7, мы получаем следующие классы вычетов по модулю 5: $x \equiv 1 (\mathrm{mod}\, 5)$, и $x \equiv -1 (\mathrm{mod}\, 5)$.

Тот же результат можно получить и более простым способом: поскольку $2x^3 - 2x = 2x(x^2-1) = 2x(x-1)(x+1)$, то, сокращая сравнение $2x(x-1)(x+1) 2x(x-1)(x+1) 0 (\mathrm{mod}\, 5)$ на число $2x$, взаимно простое с модулем (напомним, что все преобразования выполняются при условии $x \not\equiv 0 (\mathrm{mod}\, 5)$), мы получим сравнение $(x-1)(x+1) \equiv 0 (\mathrm{mod}\, 5)$, которое выполняется либо при $x \equiv 1 (\mathrm{mod}\, 5)$, либо при $x \equiv -1 (\mathrm{mod}\, 5)$.

Для решения сравнения $76x^{244} - 353x^{123} + 43x^{121} + 359 \equiv 0 (\mathrm{mod}\, 7)$ заменим коэффициенты многочлена $76x^{244} - 353x^{123} + 43x^{121} + 359$ их

наименьшими по абсолютной величине вычетами по модулю 7. Поскольку $76 \equiv -1 (\mathrm{mod}\, 7)$, $-353 \equiv -3 (\mathrm{mod}\, 7)$, $43 \equiv 1 (\mathrm{mod}\, 7)$, и $359 \equiv 2 (\mathrm{mod}\, 7)$, то наше сравнение эквивалентно сравнению $-x^{244} - 3x^{123} + x^{121} + 2 \equiv 0 (\mathrm{mod}\, 7)$.

Поскольку $2 \not\equiv 0 (\mathrm{mod}\, 7)$, то нулевой класс $x \equiv 0 (\mathrm{mod}\, 7)$ не является решением нашего сравнения.

Если $x \not\equiv 0 (\mathrm{mod}\, 7)$, то $(x, 7) = 1$, и $x^6 \equiv 1 (\mathrm{mod}\, 7)$. Для таких x заменим показатели степеней в записи многочлена $-x^{244} - 3x^{123} + x^{121} + 2$ их остатками от деления на 6. Поскольку $244 \equiv 4 (\mathrm{mod}\, 6)$, $123 \equiv 3 (\mathrm{mod}\, 6)$ и $121 \equiv 1 (\mathrm{mod}\, 6)$, то для $x \not\equiv 0 (\mathrm{mod}\, 7)$ сравнение $x^{244} - 3x^{123} + x^{121} + 2 \equiv 0 (\mathrm{mod}\, 7)$ эквивалентно сравнению $x^4 - 3x^3 + x + 2 \equiv 0 (\mathrm{mod}\, 7)$. Перебирая представители 1, 2, 3, -3, -2, -1 ненулевых классов вычетов по модулю 7, мы получаем единственный класс вычетов по модулю 7: $x \equiv -3 (\mathrm{mod}\, 7)$.

Решим теперь систему сравнений $\begin{cases} x \equiv a (\mathrm{mod}\, 5) \\ x \equiv b (\mathrm{mod}\, 7) \end{cases}$, где $a \in \{1, -1\}$, и $b = -3$.

Если $x \equiv a (\mathrm{mod}\, 5)$, то $x = 5t + a$, где $t \in \mathbb{Z}$. Подставляя полученное выражение для x во второе сравнение системы, мы получим сравнение $5t + a \equiv b (\mathrm{mod}\, 7)$, или, что то же, сравнение $5t \equiv b - a (\mathrm{mod}\, 7)$. Домножая обе части сравнения на число 3, взаимно простое с модулем, мы получим сравнение $15t \equiv 3(b - a) (\mathrm{mod}\, 7)$, или, что то же, сравнение $t \equiv 3(b - a) (\mathrm{mod}\, 7)$. Таким образом, $t = 7t_1 + 3(b - a)$, где $t_1 \in \mathbb{Z}$, и $x = 5t + a = 5(7t_1 + 3(b - a)) + a = 35t_1 + 15b - 14a$, где $t_1 \in \mathbb{Z}$.

Следовательно, решениями сравнения $76x^{244} - 353x^{123} + 43x^{121} + 359 \equiv 0 (\mathrm{mod}\, 35)$ являются следующие классы вычетов по модулю 35: $x \equiv 15b - 14a (\mathrm{mod}\, 35)$, где $a \in \{1, -1\}$, и $b = -3$. Подстановка дает окончательный результат: $x \equiv 11 (\mathrm{mod}\, 35)$, и $x \equiv 14 (\mathrm{mod}\, 35)$. ▷

Упражнения

1. Решите сравнение по простому модулю:

а) $x^3 + x^2 - 2x + 1 \equiv 0 (\mathrm{mod}\, 5)$;

б) $133x^5 - 148x^4 + 85x^3 - 98x^2 + x + 6 \equiv 0 (\mathrm{mod}\, 7)$;

в) $12x^{18} + 3x^{16} + 7x^{14} + 8x^{13} + 7x^{12} + 11x^{11} + 13x^{10} + 6x^7 + 31x^5 + 5x^4 + 11x^3 + 7x^2 \equiv 0 (\mathrm{mod}\, 7)$;

г) $232x^{484} + 852x^{252} - 124x^{202} - x^{200} + 78 \equiv 0 (\mathrm{mod}\, 11)$;

д) $292x^{181} - 121x^{133} + 252x^{122} - 171x^{121} - 133x^{62} + 5 \equiv 0 (\mathrm{mod}\, 13)$;

е) $357x^{427} - 811x^{403} - 127x^{311} + 45 \equiv 0 (\mathrm{mod}\, 7)$;

ж) $883x^{693} - 106x^{484} + 59x^{241} + 87x^{233} + 84 \equiv 0 (\mathrm{mod}\, 5)$;

з) $4015x^{10892} + 605x^{9999} + 365x^{1002} + 888x^{1001} - 24 \equiv 0 (\mathrm{mod}\, 11)$.

2. Решите сравнение:

а) $x^4 + 2x^3 + 8x + 9 \equiv 0 (\mathrm{mod}\, 35)$;

б) $103x^{103} + 88x^{73} + 210x^{13} + 100 \equiv 0 (\mathrm{mod}\, 105)$;

в) $725x^{603} - 507x^{407} - 311x^{126} + 85 \equiv 0 (\mathrm{mod}\, 77)$;

г) $1051x^{77} + 841x^{52} + 631x^{39} + 421x^{26} + 211x^{13} + 1 \equiv 0 (\mathrm{mod}\, 42)$.

Задачи

1. Решите сравнение по простому модулю:

а) $803x^{396} - 601x^{484} + 55x^{211} - 83x^{105} + 34 \equiv 0 (\mathrm{mod}\, 7)$;

б) $62x^{359} + 77x^{209} - 47x^{71} + 33x^{33} - 145 \equiv 0 (\mathrm{mod}\, 3)$;

в) $883x^{963} - 101x^{404} + 52x^{211} + 88x^{323} + 119 \equiv 0 (\mathrm{mod}\, 11)$;

г) $198x^{550} + 47x^{382} - 346x^{799} + 164x^{841} - 15 \equiv 0 (\mathrm{mod}\, 7)$;

д) $521x^{893} - 29x^{104} + 79x^{185} + 68x^{93} + 5x^9 - 2 \equiv 0 (\mathrm{mod}\, 7)$;

е) $x^{22} + x^{12} + 7x^{11} - 2x^2 + 6 \equiv 0 (\mathrm{mod}\, 11)$;

ж) $6x^{20} - 19x^{19} - 7x^2 + 6 \equiv 0 (\mathrm{mod}\, 11)$.

2. Решите систему сравнений

$$\begin{cases} 4x^{21} + 9x^{13} + 3x^{11} + 2x^3 - 2 \equiv 0 (\mathrm{mod}\, 11) \\ x^{13} + x^7 + x^5 - x^3 + 7 \equiv 0 (\mathrm{mod}\, 5) \end{cases}$$

3. Решите сравнение:

а) $6x^3 + 27x^2 + 17x + 20 \equiv 0 (\mathrm{mod}\, 30)$;

б) $46x^{35} + 357x^{82} + 13x + 620 \equiv 0 (\mathrm{mod}\, 30)$.

4. Решите сравнение $x^{p-1} + x^{p-2} + \ldots + x^2 + x + 1 \equiv 0 (\mathrm{mod}\, p)$, где $p \in P$.

5. Решите сравнение $x^{p-2} + x^{p-3} + \ldots + x^2 + x + 1 \equiv 0 (\mathrm{mod}\, p)$, где $p \in P$.

6. Решите сравнение $(p-1)x^{p-2} - (p-2)x^{p-3} + \ldots - 3x^2 + 2x - 1 \equiv 0 (\mathrm{mod}\, p)$, где $p \in P$.

7. Решите сравнение $(p-2)x^{p-3} + (p-3)x^{p-4} + \ldots + 3x^2 + 2x + 1 \equiv 0 (\mathrm{mod}\, p)$, где $p \in P$.

8. Придумайте сравнение 5 степени по модулю 13, не имеющее решений.

9. Придумайте сравнение 5 степени по модулю 11, имеющее два решения.

§ 18. Сравнения по степени простого и по составному модулю

Для данного простого числа p и данного натурального $\alpha > 1$ рассмотрим сравнение $f(x) \equiv 0(\mathrm{mod}\, p^\alpha)$ степени m по модулю p^α. Для нахождения всех решений данного сравнения можно использовать нижеследующий алгоритм.

- Рассмотрим сравнение $f(x) \equiv 0(\mathrm{mod}\, p)$ и найдем все его решения; пусть $x \equiv x_1(\mathrm{mod}\, p)$ — одно из этих решений, то есть $f(x_1) \equiv 0(\mathrm{mod}\, p)$, и $x = x_1 + pt_1$, $t_1 \in \mathbb{Z}$.
- Рассмотрим линейное сравнение $f(x_1)/p + f'(x_1)t_1 \equiv 0(\mathrm{mod}\, p)$ и найдем все его решения; пусть $t_1 \equiv t'(\mathrm{mod}\, p)$ — одно из этих решений, то есть $t_1 = t' + pt_2$, и $x = x_1 + pt_1 = x_1 + p(t' + pt_2) = (x_1 + pt') + p^2t_2 = x_2 + p^2t_2$, $t_2 \in \mathbb{Z}$.
- Рассмотрим линейное сравнение $f(x_2)/p^2 + f'(x_2)t_2 \equiv 0(\mathrm{mod}\, p)$ и найдем все его решения; пусть $t_2 \equiv t''(\mathrm{mod}\, p)$ — одно из этих решений, то есть $t_2 = t'' + pt_3$, и $x = x_3 + p^3t_3$, $t_3 \in \mathbb{Z}$.

...

- Рассмотрим линейное сравнение $f(x_{\alpha-1})/p^{\alpha-1} + f'(x_{\alpha-1})t_{\alpha-1} \equiv 0(\mathrm{mod}\, p)$ и найдем все его решения; пусть $t_{\alpha-1} \equiv t''\cdots'(\mathrm{mod}\, p)$ — одно из этих решений, то есть $t_{\alpha-1} = t''\cdots' + pt_\alpha$, и $x = x_\alpha + p^\alpha t_\alpha$, $t_\alpha \in \mathbb{Z}$.

Следовательно, $x \equiv x_\alpha(\mathrm{mod}\, p^\alpha)$ — одно из решений первоначального сравнения, и все его решения могут быть найдены этим способом.

Наконец, для данного составного числа $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ все решения сравнения $f(x) \equiv 0(\mathrm{mod}\, n)$ степени m по модулю n могут быть найдены с использованием приведенных выше аргументов и следующего свойства: $f(x) \equiv 0(\mathrm{mod}\, n)$ тогда и только тогда, когда

$$\begin{cases} f(x) \equiv 0(\mathrm{mod}\, p^{\alpha_1}) \\ \ldots \\ f(x) \equiv 0(\mathrm{mod}\, p_k^{\alpha_k}). \end{cases}$$

В этом случае число R решений сравнения $f(x) \equiv 0(\mathrm{mod}\, n)$ по модулю $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ равно произведению $R_1 \cdot R_2 \cdot \ldots \cdot R_k$, где R_i — число решений сравнения $f(x) \equiv 0(\mathrm{mod}\, p_i^{\alpha_i})$, $i = 1, 2, \ldots, k$.

В свою очередь, подсчет числа решений сравнения $f(x) \equiv 0(\mathrm{mod}\, p^\alpha)$, где $p \in P$, а $\alpha > 1$, основан на следующей теореме, позволяющей определить, сколько решений по модулю p^{k+1} можно получить, используя данное решение по модулю p^k: *если* $f(x_k) \equiv 0(\mathrm{mod}\, p^k)$, *причем* $p \nmid f'(x_k)$, *то сравнение* $f(x) \equiv 0(\mathrm{mod}\, p^{k+1})$ *имеет ровно одно решение, принадлежащее классу*

$x \equiv x_k (\mathrm{mod}\, p^k)$; *если* $f(x_k) \equiv 0 (\mathrm{mod}\, p^k)$, *причем* $p | f'(x_k)$ *и* $p^{k+1} | f(x_k)$, *то сравнение* $f(x) \equiv 0 (\mathrm{mod}\, p^{k+1})$ *имеет ровно* p *решений, принадлежащих классу* $x \equiv x_k (\mathrm{mod}\, p^k)$; *если* $f(x_k) \equiv 0 (\mathrm{mod}\, p^k)$, *причем* $p | f'(x_k)$ *и* $p^{k+1} \nmid f(x_k)$, *то сравнение* $f(x) \equiv 0 (\mathrm{mod}\, p^{k+1})$ *не имеет решений, принадлежащих классу* $x \equiv x_k (\mathrm{mod}\, p^k)$.

Таким образом, двигаясь «по ступенькам» приведенного выше алгоритма, на $k+1$-ой ступеньке мы получаем из каждого решения, полученного на k-ой ступеньке, либо одно, либо p, либо ни одного решения.

Подробные обоснования приведенного выше алгоритма и детальное изложение всех аспектов соответствующей теории можно найти, например, в [3].

Примеры решения задач

1. Решите сравнение $9x^2 + 29x + 62 \equiv 0 (\mathrm{mod}\, 32)$.

Решение. Пусть $f(x) = 9x^2 + 29x + 62$. Поскольку $32 = 2^5$, то мы получаем сравнение $f(x) \equiv 0 (\mathrm{mod}\, 2^5)$, для решения которого рассмотрим сначала сравнение $f(x) \equiv 0 (\mathrm{mod}\, 2)$. Заменив коэффициенты многочлена $9x^2 + 29x + 62$ их остатками от деления на 2, мы получим сравнение $x^2 + x \equiv 0 (\mathrm{mod}\, 2)$. Легко видеть, что оно выполняется для любого целого x, то есть его решениями являются классы $x \equiv 0 (\mathrm{mod}\, 2)$ и $x \equiv 1 (\mathrm{mod}\, 2)$.

A. Мы доказали, что $x \equiv 0 (\mathrm{mod}\, 2)$ — решение сравнения $f(x) \equiv 0 (\mathrm{mod}\, 2)$. Следовательно, $f(0) \equiv 0 (\mathrm{mod}\, 2)$ и $x = 2t_1 + 0$, где $t_1 \in \mathbb{Z}$.

Рассмотрим сравнение $f(x) \equiv 0 (\mathrm{mod}\, 2^2)$, где $x = 2t_1 + 0$, $t_1 \in \mathbb{Z}$. Для его решения перейдем к линейному сравнению $f(0)/2 + f'(0) \cdot t_1 \equiv 0 (\mathrm{mod}\, 2)$.

Легко видеть, что $f(0) = 62$. Поскольку $f'(x) = 18x + 29$, то $f'(0) = 29$. Таким образом, мы получаем сравнение $62/2 + 29 \cdot t_1 \equiv 0 (\mathrm{mod}\, 2)$, или, что то же, сравнение $31 + 29 \cdot t_1 \equiv 0 (\mathrm{mod}\, 2)$. Поскольку $31 \equiv 1 (\mathrm{mod}\, 2)$ и $29 \equiv 1 (\mathrm{mod}\, 2)$, то мы получаем сравнение $1 + t_1 \equiv 0 (\mathrm{mod}\, 2)$, выполняющееся для $t_1 \equiv 1 (\mathrm{mod}\, 2)$. Таким образом, $t_1 = 2t_2 + 1$, где $t_2 \in \mathbb{Z}$, и $x = 2t_1 + 0 = 2(2t_2 + 1) + 0 = 2^2 t_2 + 2$, $t_2 \in \mathbb{Z}$.

Рассмотрим сравнение $f(x) \equiv 0 (\mathrm{mod}\, 2^3)$, где $x = 2^2 t_2 + 2$, $t_2 \in \mathbb{Z}$. Для его решения перейдем к линейному сравнению $f(2)/2^2 + f'(2) \cdot t_2 \equiv 0 (\mathrm{mod}\, 2)$.

Легко видеть, что $f(2) = 156$ и $f'(2) = 65$. Таким образом, мы получаем сравнение $156/(2^2) + 65 \cdot t_2 \equiv 0 (\mathrm{mod}\, 2)$, или, что то же, сравнение $39 + 65 \cdot t_2 \equiv 0 (\mathrm{mod}\, 2)$. Поскольку $39 \equiv 1 (\mathrm{mod}\, 2)$ и $65 \equiv 1 (\mathrm{mod}\, 2)$, то мы получаем сравнение $1 + t_2 \equiv 0 (\mathrm{mod}\, 2)$, выполняющееся для

$t_2 \equiv 1 (\mathrm{mod}\ 2)$. Таким образом, $t_2 = 2t_3 + 1$, где $t_3 \in \mathbb{Z}$, и $x = 2^2 t_2 + 2 = 2^2(2t_3 + 1) + 2 = 2^3 t_3 + 6$, $t_3 \in \mathbb{Z}$.

Рассмотрим сравнение $f(x) \equiv 0 (\mathrm{mod}\ 2^4)$, где $x = 2^3 t_3 + 6$, $t_3 \in \mathbb{Z}$. Для его решения перейдем к линейному сравнению $f(6)/2^3 + f'(6) \cdot t_3 \equiv 0 (\mathrm{mod}\ 2)$.

Легко видеть, что $f(6) = 560$ и $f'(6) = 137$. Таким образом, мы получаем сравнение $560/(2^3) + 137 \cdot t_3 \equiv 0 (\mathrm{mod}\ 2)$, или, что то же, сравнение $70 + 137 \cdot t_1 \equiv 0 (\mathrm{mod}\ 2)$. Поскольку $70 \equiv 0 (\mathrm{mod}\ 2)$ и $137 \equiv 1 (\mathrm{mod}\ 2)$, то мы получаем сравнение $t_3 \equiv 0 (\mathrm{mod}\ 2)$. Таким образом, $t_3 = 2t_4$, где $t_4 \in \mathbb{Z}$, и $x = 2^3 t_3 + 6 = 2^3(2t_4) + 6 = 2^4 t_4 + 6$, $t_4 \in \mathbb{Z}$.

Рассмотрим сравнение $f(x) \equiv 0 (\mathrm{mod}\ 2^5)$, где $x = 2^4 t_4 + 6$, $t_4 \in \mathbb{Z}$. Для его решения перейдем к линейному сравнению $f(6)/2^4 + f'(6) \cdot t_4 \equiv 0 (\mathrm{mod}\ 2)$.

Поскольку $f(6) = 560$ и $f'(6) = 137$, то мы получаем сравнение $560/(2^4) + 137 \cdot t_4 \equiv 0 (\mathrm{mod}\ 2)$, или, что то же, сравнение $35 + 137 \cdot t_4 \equiv 0 (\mathrm{mod}\ 2)$. Поскольку $35 \equiv 1 (\mathrm{mod}\ 2)$ и $137 \equiv 1 (\mathrm{mod}\ 2)$, то мы получаем сравнение $1 + t_4 \equiv 0 (\mathrm{mod}\ 2)$, выполняющееся для $t_4 \equiv 1 (\mathrm{mod}\ 2)$. Таким образом, $t_4 = 2t_5 + 1$, где $t_5 \in \mathbb{Z}$, и $x = 2^4 t_4 + 6 = 2^4(2t_5 + 1) + 6 = 2^5 t_5 + 22$, $t_5 \in \mathbb{Z}$.

Следовательно, решением сравнения $f(x) \equiv 0 (\mathrm{mod}\ 32)$ является класс $x \equiv 22 (\mathrm{mod}\ 32)$.

В. Мы доказали, что $x \equiv 1 (\mathrm{mod}\ 2)$ — решение сравнения $f(x) \equiv 0 (\mathrm{mod}\ 2)$. Следовательно, $f(1) \equiv 0 (\mathrm{mod}\ 2)$ и $x = 2t_1 + 1$, где $t_1 \in \mathbb{Z}$.

Рассмотрим сравнение $f(x) \equiv 0 (\mathrm{mod}\ 2^2)$, где $x = 2t_1 + 1$, $t_1 \in \mathbb{Z}$. Для его решения перейдем к линейному сравнению $f(1)/2 + f'(1) \cdot t_1 \equiv 0 (\mathrm{mod}\ 2)$.

Легко видеть, что $f(1) = 100$ и $f'(1) = 47$. Таким образом, мы получаем сравнение $100/2 + 47 \cdot t_1 \equiv 0 (\mathrm{mod}\ 2)$, или, что то же, сравнение $50 + 47 \cdot t_1 \equiv 0 (\mathrm{mod}\ 2)$. Поскольку $50 \equiv 0 (\mathrm{mod}\ 2)$ и $47 \equiv 1 (\mathrm{mod}\ 2)$, то мы получаем сравнение $t_1 \equiv 0 (\mathrm{mod}\ 2)$. Таким образом, $t_1 = 2t_2$, где $t_2 \in \mathbb{Z}$, и $x = 2t_1 + 1 = 2(2t_2) + 1 = 2^2 t_2 + 1$, $t_2 \in \mathbb{Z}$.

Рассмотрим сравнение $f(x) \equiv 0 (\mathrm{mod}\ 2^3)$, где $x = 2^2 t_2 + 1$, $t_2 \in \mathbb{Z}$. Для его решения перейдем к линейному сравнению $f(1)/2^2 + f'(1) \cdot t_2 \equiv 0 (\mathrm{mod}\ 2)$.

Поскольку $f(1) = 100$ и $f'(1) = 47$, то мы получаем сравнение $100/(2^2) + 47 \cdot t_2 \equiv 0 (\mathrm{mod}\ 2)$, или, что то же, сравнение $25 + 65 \cdot t_2 \equiv 0 (\mathrm{mod}\ 2)$. Поскольку $25 \equiv 1 (\mathrm{mod}\ 2)$ и $47 \equiv 1 (\mathrm{mod}\ 2)$, то мы получаем сравнение $1 + t_2 \equiv 0 (\mathrm{mod}\ 2)$, выполняющееся для $t_2 \equiv 1 (\mathrm{mod}\ 2)$. Таким образом, $t_2 = 2t_3 + 1$, где $t_3 \in \mathbb{Z}$, и $x = 2^2 t_2 + 1 = 2^2(2t_3 + 1) + 1 = 2^3 t_3 + 5$, $t_3 \in \mathbb{Z}$.

Рассмотрим сравнение $f(x) \equiv 0 (\mathrm{mod}\, 2^4)$, где $x = 2^3 t_3 + 5$, $t_3 \in \mathbb{Z}$. Для его решения перейдем к линейному сравнению $f(5)/2^3 + f'(5) \cdot t_3 \equiv \equiv 0 (\mathrm{mod}\, 2)$.

Легко видеть, что $f(5) = 432$ и $f'(5) = 119$. Таким образом, мы получаем сравнение $432/(2^3) + 119 \cdot t_3 \equiv 0 (\mathrm{mod}\, 2)$, или, что то же, сравнение $54 + 119 \cdot t_3 \equiv 0 (\mathrm{mod}\, 2)$. Поскольку $54 \equiv 0 (\mathrm{mod}\, 2)$ и $119 \equiv \equiv 1 (\mathrm{mod}\, 2)$, то мы получаем сравнение $t_3 \equiv 0 (\mathrm{mod}\, 2)$. Таким образом, $t_3 = 2t_4$, где $t_4 \in \mathbb{Z}$, и $x = 2^3 t_3 + 5 = 2^3 (2t_4) + 5 = 2^4 t_4 + 5$, $t_4 \in \mathbb{Z}$.

Рассмотрим сравнение $f(x) \equiv 0 (\mathrm{mod}\, 2^5)$, где $x = 2^4 t_4 + 5$, $t_4 \in \mathbb{Z}$. Для его решения перейдем к линейному сравнению $f(5)/2^4 + f'(5) \cdot t_4 \equiv \equiv 0 (\mathrm{mod}\, 2)$.

Поскольку $f(5) = 432$ и $f'(5) = 119$, то мы получаем сравнение $432/(2^4) + 119 \cdot t_4 \equiv 0 (\mathrm{mod}\, 2)$, или, что то же, сравнение $27 + 119 \cdot t_4 \equiv \equiv 0 (\mathrm{mod}\, 2)$. Поскольку $27 \equiv 1 (\mathrm{mod}\, 2)$ и $119 \equiv 1 (\mathrm{mod}\, 2)$, то мы получаем сравнение $1 + t_4 \equiv 0 (\mathrm{mod}\, 2)$, выполняющееся для $t_4 \equiv 1 (\mathrm{mod}\, 2)$. Таким образом, $t_4 = 2t_5 + 1$, где $t_5 \in \mathbb{Z}$, и $x = 2^4 t_4 + 5 = 2^4 (2t_5 + 1) + 5 = = 2^2 t_5 + 21$, $t_5 \in \mathbb{Z}$.

Следовательно, решением сравнения $f(x) \equiv 0 (\mathrm{mod}\, 32)$ является класс $x \equiv 21 (\mathrm{mod}\, 32)$. Таким образом, мы доказали, что решениями сравнения $9x^2 + 29x + 62 \equiv 0 (\mathrm{mod}\, 32)$ являются классы $x \equiv 21 (\mathrm{mod}\, 32)$ и $x \equiv 22 (\mathrm{mod}\, 32)$. ▷

Замечание. Значения функции $f(x)$ удобно вычислять, пользуясь *схемой Горнера* (см. [18]).

	9	29	62
0	9	29	62
2	9	$18 + 29 = 47$	$94 + 62 = 156$
6	9	$54 + 29 = 83$	$498 + 62 = 560$
1	9	$9 + 29 = 38$	$38 + 62 = 100$
5	9	$45 + 29 = 74$	$370 + 62 = 432$

2. Решите сравнение $x^5 - x^4 + 6x^2 + 15x + 45 \equiv 0 (\mathrm{mod}\, 675)$.

Решение. Пусть $f(x) = x^5 - x^4 + 6x^2 + 15x + 45$. Поскольку $675 = = 3^3 \cdot 5^2$, то мы получаем сравнение $f(x) \equiv 0 (\mathrm{mod}\, 3^3 \cdot 5^2)$, эквивалентное системе сравнений

$$\begin{cases} f(x) \equiv 0 (\mathrm{mod}\, 3^3) \\ f(x) \equiv 0 (\mathrm{mod}\, 5^2). \end{cases}$$

I. Решим сравнение $f(x) \equiv 0 (\mathrm{mod}\, 3^3)$.

Для этого рассмотрим сначала сравнение $f(x) \equiv 0 (\mathrm{mod}\, 3)$. Заменив коэффициенты многочлена $x^5 - x^4 + 6x^2 + 15x + 45$ их наименьшими по абсолютной величине вычетами по модулю 3, мы получим сравнение $x^5 - x^4 \equiv 0 (\mathrm{mod}\, 3)$.

Легко видеть, что нулевой класс $x \equiv 0 (\mathrm{mod}\, 3)$ является решением нашего сравнения.

Если $x \not\equiv 0 (\mathrm{mod}\, 3)$, то $(x, 3) = 1$, и $x^2 \equiv 1 (\mathrm{mod}\, 3)$. Для таких x заменим показатели степеней в записи многочлена $x^5 - x^4$ их остатками от деления на 2, и перейдем к сравнению $x - 1 \equiv 0 (\mathrm{mod}\, 3)$. Отсюда следует, что $x \equiv 1 (\mathrm{mod}\, 3)$.

Таким образом, решениями сравнения $f(x) \equiv 0 (\mathrm{mod}\, 3)$ являются классы $x \equiv 0 (\mathrm{mod}\, 3)$ и $x \equiv 1 (\mathrm{mod}\, 3)$.

Впрочем, тот же результат можно получить, записав многочлен $x^5 - x^4$ в виде $x^4(x - 1)$ и перейдя к сравнению $x^4(x - 1) \equiv 0 (\mathrm{mod}\, 3)$, решениями которого очевидным образом являются классы $x \equiv 0 (\mathrm{mod}\, 3)$ и $x \equiv 1 (\mathrm{mod}\, 3)$.

A. Мы доказали, что $x \equiv 0 (\mathrm{mod}\, 3)$ — решение сравнения $f(x) \equiv 0 (\mathrm{mod}\, 3)$. Следовательно, $f(0) \equiv 0 (\mathrm{mod}\, 3)$ и $x = 3t_1 + 0$, где $t_1 \in \mathbb{Z}$.

Рассмотрим сравнение $f(x) \equiv 0 (\mathrm{mod}\, 3^2)$, где $x = 3t_1 + 0$, $t_1 \in \mathbb{Z}$. Для его решения перейдем к линейному сравнению $f(0)/3 + f'(0) \cdot t_1 \equiv 0 (\mathrm{mod}\, 3)$.

Легко видеть, что $f(0) = 45$. Поскольку $f'(x) = 5x^4 - 4x^3 + 12x + 15$, то $f'(0) = 15$. Таким образом, мы получаем сравнение $45/3 + 15 \cdot t_1 \equiv 0 (\mathrm{mod}\, 3)$, или, что то же, сравнение $15 + 15 \cdot t_1 \equiv 0 (\mathrm{mod}\, 3)$. Поскольку $15 \equiv 0 (\mathrm{mod}\, 3)$, то мы получаем сравнение $0 + 0 \cdot t_1 \equiv 0 (\mathrm{mod}\, 3)$, выполняющееся для любого целого t_1. Таким образом, мы получаем три решения выписанного выше линейного сравнения: $t_1 \equiv 0 (\mathrm{mod}\, 3)$, $t_1 \equiv 1 (\mathrm{mod}\, 3)$ и $t_1 \equiv -1 (\mathrm{mod}\, 3)$.

В первом случае $t_1 = 3t_2$, где $t_2 \in \mathbb{Z}$, и $x = 3t_1 + 0 = 3(3t_2) + 0 = 3^2 \cdot t_2 + 0$. Во втором случае $t_1 = 3t_2 + 1$, где $t_2 \in \mathbb{Z}$, и $x = 3t_1 + 0 = 3(3t_2 + 1) + 0 = 3^2 \cdot t_2 + 3$. В третьем случае $t_1 = 3t_2 - 1$, где $t_2 \in \mathbb{Z}$, и $x = 3t_1 + 0 = 3(3t_2 - 1) + 0 = 3^2 \cdot t_2 - 3$.

1. Рассмотрим сравнение $f(x) \equiv 0 (\mathrm{mod}\, 3^3)$, где $x = 3^2 t_2 + 0$, $t_2 \in \mathbb{Z}$. Для его решения перейдем к линейному сравнению $f(0)/3^2 + f'(0) \cdot t_2 \equiv 0 (\mathrm{mod}\, 3)$.

Поскольку $f(0) = 45$ и $f'(0) = 15$, то мы получаем сравнение $45/9 + 15 \cdot t_2 \equiv 0 (\mathrm{mod}\, 3)$, или, что то же, сравнение $5 + 15 \cdot t_2 \equiv 0 (\mathrm{mod}\, 3)$. Поскольку $5 \equiv -1 (\mathrm{mod}\, 3)$ и $15 \equiv 0 (\mathrm{mod}\, 3)$, то мы получаем сравнение $-1 + 0 \cdot t_2 \equiv 0 (\mathrm{mod}\, 3)$, не выполняющееся ни для какого целого t_2. Таким образом, в данном случае решения по модулю 3^3 не существует.

2. Рассмотрим сравнение $f(x) \equiv 0 (\mathrm{mod}\, 3^3)$, где $x = 3^2 t_2 + 3$, $t_2 \in \mathbb{Z}$. Для его решения перейдем к линейному сравнению $f(3)/3^2 + f'(3) \cdot t_2 \equiv \equiv 0 (\mathrm{mod}\, 3)$.

Поскольку $f(3) = 306$ и $f'(3) = 348$, то мы получаем сравнение $306/9 + 348 \cdot t_2 \equiv 0 (\mathrm{mod}\, 3)$, или, что то же, сравнение $34 + 348 \cdot t_2 \equiv \equiv 0 (\mathrm{mod}\, 3)$. Поскольку $34 \equiv 1 (\mathrm{mod}\, 3)$ и $348 \equiv 0 (\mathrm{mod}\, 3)$, то мы получаем сравнение $1 + 0 \cdot t_2 \equiv 0 (\mathrm{mod}\, 3)$, не выполняющееся ни для какого целого t_2. Таким образом, и в данном случае решения по модулю 3^3 не существует.

3. Рассмотрим сравнение $f(x) \equiv 0 (\mathrm{mod}\, 3^3)$, где $x = 3^2 t_2 - 3$, $t_2 \in \mathbb{Z}$. Для его решения перейдем к линейному сравнению $f(-3)/3^2 + f'(-3) \cdot t_2 \equiv \equiv 0 (\mathrm{mod}\, 3)$.

Поскольку $f(-3) = 270$ и $f'(-3) = 492$, то мы получаем сравнение $270/9 + 492 \cdot t_2 \equiv 0 (\mathrm{mod}\, 3)$, или, что то же, сравнение $30 + 492 \cdot t_2 \equiv \equiv 0 (\mathrm{mod}\, 3)$. Поскольку $30 \equiv 0 (\mathrm{mod}\, 3)$ и $492 \equiv 0 (\mathrm{mod}\, 3)$, то мы получаем сравнение $0 + 0 \cdot t_2 \equiv 0 (\mathrm{mod}\, 3)$, выполняющееся для любого целого t_2. Таким образом, мы получаем три решения выписанного выше линейного сравнения: $t_2 \equiv 0 (\mathrm{mod}\, 3)$, $t_2 \equiv 1 (\mathrm{mod}\, 3)$ и $t_2 \equiv -1 (\mathrm{mod}\, 3)$. В первом случае $t_2 = 3t_3$, где $t_3 \in \mathbb{Z}$, и $x = 3^2 t_2 - 3 = 3^2 (3t_3) - 3 = = 3^3 \cdot t_3 - 3$. Во втором случае $t_2 = 3t_3 + 1$, где $t_3 \in \mathbb{Z}$, и $x = 3^2 t_2 - 3 = = 3^2 (3t_3 + 1) - 3 = 3^3 \cdot t_3 + 6$. В третьем случае $t_2 = 3t_3 - 1$, где $t_3 \in \mathbb{Z}$, и $x = 3^2 t_2 - 3 = 3^2 (3t_3 - 1) - 3 = 3^2 \cdot t_3 - 12$.

Итак, решениями сравнения $f(x) \equiv 0 (\mathrm{mod}\, 3^3)$ являются классы $x \equiv -3 (\mathrm{mod}\, 3^3)$, $x \equiv -6 (\mathrm{mod}\, 3^3)$ и $x \equiv -12 (\mathrm{mod}\, 3^3)$.

Замечание. В этой ситуации можно избежать кропотливого перебора всех возможных случаев.

Именно, убедившись, что сравнение $f(x) \equiv 0 (\mathrm{mod}\, 3^2)$, где $x = 3t_1 + 0$, выполняется для любого целого t_1, не будем переходить к трем возможным представлениям x по модулю 3^2, оставив имеющееся представление $x = 3t_1 + 0$.

Рассмотрим сравнение $f(x) \equiv 0 (\mathrm{mod}\, 3^3)$, где $x = 3t_1 + 0$, $t_1 \in \mathbb{Z}$. Для его решения разложим $f(x)$ в ряд Тейлора по степеням x:

$$f(x) = f(0) + f'(0) \cdot x + \frac{f''(0)}{2!} x^2 + \frac{f'''(0)}{3!} x^3 + \ldots = $$

$$= f(0) + f'(0) \cdot 3t_1 + \frac{f''(0)}{2!} 9t_1^2 + \frac{f'''(0)}{3!} 27t_1^3 + \ldots .$$

Замечая, что все слагаемые, начиная с третьего, делятся на 27, то есть сравнимы с 0 по модулю 3^3, мы перейдем от сравнения $f(x) \equiv 0 (\mathrm{mod}\, 3^3)$ к сравнению $f(0) + f'(0) \cdot 3t_1 + f''(0)/2! 9t_1^2 \equiv 0 (\mathrm{mod}\, 3^3)$. Замечая, что $f(0)$ делится на 9 и $f'(0)$ делится на 3, мы разделим все три части последнего сравнения

на 9, получив сравнение

$$\frac{f(0)}{3^2} + \frac{f'(0)}{3} \cdot t_1 + \frac{f''(0)}{2!} t_1^2 \equiv 0 (\mathrm{mod}\, 3).$$

Поскольку

$$f''(x) = 20x^3 - 12x^2 + 12,$$

то

$$f''(0) = 12.$$

Подставляя значения $f(0) = 45$, $f'(0) = 15$ и $f''(0) = 12$ в сравнение

$$\frac{f(0)}{3^2} + \frac{f'(0)}{3} \cdot t_1 + \frac{f''(0)}{2!} \cdot t_1^2 \equiv 0 (\mathrm{mod}\, 3),$$

мы получаем сравнение

$$\frac{45}{9} + \frac{15}{3} \cdot t_1 + \frac{12}{2!} t_1^2 \equiv 0 (\mathrm{mod}\, 3),$$

или, что то же, сравнение $5 + 5 \cdot t_1 + 6 \cdot t_1^2 \equiv 0 (\mathrm{mod}\, 3)$. Поскольку $5 \equiv$ $\equiv -1 (\mathrm{mod}\, 3)$, и $6 \equiv 0 (\mathrm{mod}\, 3)$, то мы получаем сравнение $-1 - t_1 \equiv 0 (\mathrm{mod}\, 3)$, выполняющееся для $t_1 \equiv -1 (\mathrm{mod}\, 3)$. Таким образом, $t_1 = 3t_2 - 1$, где $t_2 \in \mathbb{Z}$, и $x = 3t_1 + 0 = 3(3t_2 - 1) + 0 = 3^2 t_2 - 3$.

Разбивая один класс $x \equiv -3 (\mathrm{mod}\, 3^2)$ по модулю 9 на три класса по модулю 27, мы получим решения $x \equiv -3 (\mathrm{mod}\, 3^3)$, $x \equiv -6 (\mathrm{mod}\, 3^3)$, $x \equiv -12 (\mathrm{mod}\, 3^3)$.

В. Мы доказали, что $x \equiv 1 (\mathrm{mod}\, 3)$ — решение сравнения $f(x) \equiv 0 (\mathrm{mod}\, 3)$. Следовательно, $f(1) \equiv 0 (\mathrm{mod}\, 3)$ и $x = 3t_1 + 1$, где $t_1 \in \mathbb{Z}$.

Рассмотрим сравнение $f(x) \equiv 0 (\mathrm{mod}\, 3^2)$, где $x = 3t_1 + 1$, $t_1 \in \mathbb{Z}$. Для его решения перейдем к линейному сравнению $f(1)/3 + f'(1) \cdot t_1 \equiv 0 (\mathrm{mod}\, 3)$.

Легко видеть, что $f(1) = 66$ и $f'(1) = 28$. Таким образом, мы получаем сравнение $66/3 + 28 \cdot t_1 \equiv 0 (\mathrm{mod}\, 3)$, или, что то же, сравнение $22 +$ $+ 28 \cdot t_1 \equiv 0 (\mathrm{mod}\, 3)$. Поскольку $22 \equiv 1 (\mathrm{mod}\, 3)$ и $28 \equiv 1 (\mathrm{mod}\, 3)$, то мы получаем сравнение $1 + t_1 \equiv 0 (\mathrm{mod}\, 3)$, выполняющееся для целого $t_1 \equiv -1 (\mathrm{mod}\, 3)$. Таким образом, $t_1 = 3t_2 - 1$, где $t_2 \in \mathbb{Z}$, и $x = 3t_1 + 1 = 3(3t_2 - 1) + 1 = 3^2 \cdot t_2 - 2$.

Рассмотрим сравнение $f(x) \equiv 0 (\mathrm{mod}\, 3^3)$, где $x = 3^2 t_2 - 2$, $t_2 \in \mathbb{Z}$. Для его решения перейдем к линейному сравнению

$$\frac{f(-2)}{3^2} + f'(-2) \cdot t_2 \equiv 0 (\mathrm{mod}\, 3).$$

Поскольку $f(-2) = -9$ и $f'(-2) = 103$, то мы получаем сравнение $-9/9 + 103 \cdot t_2 \equiv 0 (\mathrm{mod}\, 3)$, или, что то же, сравнение $-1 + 103 \cdot t_2 \equiv$ $\equiv 0 (\mathrm{mod}\, 3)$. Поскольку $103 \equiv 1 (\mathrm{mod}\, 3)$, то мы получаем сравнение $-1 + t_2 \equiv 0 (\mathrm{mod}\, 3)$, выполняющееся для $t_2 \equiv 1 (\mathrm{mod}\, 3)$. Таким образом, $t_2 = 3t_3 + 1$, где $t_3 \in \mathbb{Z}$, и $x = 3^2 t_2 - 2 = 3^2(3t_3 + 1) - 2 = 3^3 \cdot t_3 + 7$.

Следовательно, решением сравнения $f(x) \equiv 0 (\mathrm{mod}\, 3^3)$ является класс $x \equiv 7 (\mathrm{mod}\, 3^3)$.

Таким образом, мы нашли все решения сравнения $f(x) \equiv 0 (\mathrm{mod}\, 3^3)$: $x \equiv -3 (\mathrm{mod}\, 3^3)$, $x \equiv -6 (\mathrm{mod}\, 3^3)$, $x \equiv -12 (\mathrm{mod}\, 3^3)$ и $x \equiv -7 (\mathrm{mod}\, 3^3)$.

II. Решим сравнение $f(x) \equiv 0 (\mathrm{mod}\, 5^2)$.

Для этого рассмотрим сначала сравнение $f(x) \equiv 0 (\mathrm{mod}\, 5)$. Заменив коэффициенты многочлена $x^5 - x^4 + 6x^2 + 15x + 45$ их наименьшими по абсолютной величине вычетами по модулю 5, мы получим сравнение $x^5 - x^4 + x^2 \equiv 0 (\mathrm{mod}\, 5)$.

Легко видеть, что нулевой класс $x \equiv 0 (\mathrm{mod}\, 5)$ является решением нашего сравнения.

Если $x \not\equiv 0 (\mathrm{mod}\, 5)$, то $(x, 5) = 1$, и $x^4 \equiv 1 (\mathrm{mod}\, 5)$. Для таких x заменим показатели степеней в записи многочлена $x^5 - x^4 + x^2$ их остатками от деления на 4, и перейдем к сравнению $x - x^0 + x^2 \equiv 0 (\mathrm{mod}\, 5)$, или, что то же, к сравнению $x^2 + x - 1 \equiv 0 (\mathrm{mod}\, 5)$. Перебирая представители 1, -1, 2, -2 всех классов вычетов по модулю 5, взаимно простых с модулем, мы убедимся, что сравнению удовлетворяет ровно один класс: $x \equiv 2 (\mathrm{mod}\, 5)$.

Таким образом, решениями сравнения $f(x) \equiv 0 (\mathrm{mod}\, 5)$ являются классы $x \equiv 0 (\mathrm{mod}\, 5)$ и $x \equiv 2 (\mathrm{mod}\, 5)$.

A. Мы доказали, что $x \equiv 0 (\mathrm{mod}\, 5)$ — решение сравнения $f(x) \equiv 0 (\mathrm{mod}\, 5)$. Следовательно, $f(0) \equiv 0 (\mathrm{mod}\, 5)$ и $x = 5t_1 + 0$, где $t_1 \in \mathbb{Z}$.

Рассмотрим сравнение $f(x) \equiv 0 (\mathrm{mod}\, 5^2)$, где $x = 5t_1 + 0$, $t_1 \in \mathbb{Z}$. Для его решения перейдем к линейному сравнению

$$\frac{f(0)}{5} + f'(0) \cdot t_1 \equiv 0 (\mathrm{mod}\, 5).$$

Поскольку $f(0) = 45$ и $f'(0) = 15$, то мы получаем сравнение $45/5 + 15 \cdot t_1 \equiv 0 (\mathrm{mod}\, 5)$, или, что то же, сравнение $9 + 15 \cdot t_1 \equiv 0 (\mathrm{mod}\, 5)$. Поскольку $9 \equiv -1 (\mathrm{mod}\, 5)$ и $15 \equiv 0 (\mathrm{mod}\, 5)$, то мы получаем сравнение $-1 + 0 \cdot t_1 \equiv 0 (\mathrm{mod}\, 5)$, не выполняющееся ни для какого целого t_1. Таким образом, в данном случае решения по модулю 5^2 не существует.

B. Мы доказали, что $x \equiv 2 (\mathrm{mod}\, 5)$ — решение сравнения $f(x) \equiv 0 (\mathrm{mod}\, 5)$. Следовательно, $f(2) \equiv 0 (\mathrm{mod}\, 5)$ и $x = 5t_1 + 2$, где $t_1 \in \mathbb{Z}$.

Рассмотрим сравнение $f(x) \equiv 0 (\mathrm{mod}\, 5^2)$, где $x = 5t_1 + 2$, $t_1 \in \mathbb{Z}$. Для его решения перейдем к линейному сравнению

$$\frac{f(2)}{5} + f'(2) \cdot t_1 \equiv 0 (\mathrm{mod}\, 5).$$

Легко видеть, что $f(2) = 115$ и $f'(2) = 87$. Таким образом, мы получаем сравнение $115/5 + 87 \cdot t_1 \equiv 0 (\mathrm{mod}\, 5)$, или, что то же, сравнение

$23 + 87 \cdot t_1 \equiv 0 (\mathrm{mod}\, 5)$. Поскольку $23 \equiv -2 (\mathrm{mod}\, 5)$ и $87 \equiv 2 (\mathrm{mod}\, 3)$, то мы получаем сравнение $-2 + 2t_1 \equiv 0 (\mathrm{mod}\, 5)$, выполняющееся для целого $t_1 \equiv 1 (\mathrm{mod}\, 5)$. Таким образом, $t_1 = 5t_2 + 1$, где $t_2 \in \mathbb{Z}$, и $x = 5t_1 + 2 = 5(5t_2 + 1) + 2 = 5^2 \cdot t_2 + 7$.

Таким образом, мы доказали, что единственным решением сравнения $f(x) \equiv 0 (\mathrm{mod}\, 5^2)$ является класс $x \equiv 7 (\mathrm{mod}\, 5^2)$.

III. Решим теперь систему сравнений $\begin{cases} x \equiv a (\mathrm{mod}\, 5^2) \\ x \equiv b (\mathrm{mod}\, 3^3) \end{cases}$, где $a = 7$, и $b \in \{-3, 6, 15, 7\}$.

Если $x \equiv a (\mathrm{mod}\, 25)$, то $x = 25t + a$, где $t \in \mathbb{Z}$. Подставляя полученное выражение для x во второе сравнение системы, мы получим сравнение $25t + a \equiv b (\mathrm{mod}\, 27)$, или, что то же, сравнение $-2t \equiv b - a (\mathrm{mod}\, 27)$. Домножая обе части сравнения на число 13, взаимно простое с модулем, мы получим сравнение $-26t \equiv 13(b - a) (\mathrm{mod}\, 27)$, или, что то же, сравнение $t \equiv 13(b - a) (\mathrm{mod}\, 27)$. Таким образом, $t = 27t_1 + 13(b - a)$, где $t_1 \in \mathbb{Z}$, и $x = 25t + a = 25(27t_1 + 13(b - a)) + a = 675t_1 + 325b - 324a$, где $t_1 \in \mathbb{Z}$.

Следовательно, решениями сравнения $x^5 - x^4 + 6x^2 = 15x + 45 \equiv$ $\equiv 0 (\mathrm{mod}\, 675)$ являются следующие классы вычетов по модулю 675: $x \equiv 325b - 324a (\mathrm{mod}\, 675)$, где $a = 7$, а $b \in \{-3, 6, 15, 7\}$. Подстановка дает окончательный результат: $x \equiv 7 (\mathrm{mod}\, 675)$, $x \equiv 132 (\mathrm{mod}\, 675)$, $x \equiv 357 (\mathrm{mod}\, 675)$, и $x \equiv 582 (\mathrm{mod}\, 675)$.

Замечание. Значения функции $f(x)$ удобно вычислять, пользуясь схемой Горнера. При этом, найдя значения функции $f(x)$ в точках $0, 1, -1, 2, -2$, соответствующих наименьшим по абсолютной величине представителям всех классов вычетов по модулям 3 (числа 0, 1, -1) и 5 (числа $0, 1, -1, 2, -2$), мы немедленно получим решения соответствующих сравнений по модулям 3 и 5: на три делятся значения $f(0) = 45$ и $f(1) = 66$; на 5 делятся значения $f(0) = 45$ и $f(2) = 115$.

	1	−1	0	6	15	45
0	1	−1	0	6	15	45
1	1	0	0	6	21	66
−1	1	−2	2	4	11	34
2	1	1	2	10	35	115
−2	1	−3	6	−6	27	−9

Оставив в построенной таблице несколько пустых строк, мы используем их в процессе решения, в нашем случае — для вычисления значений $f(3)$ и $f(-3)$.

	1	−1	0	6	15	45
3	1	2	6	24	87	306
−3	1	−4	12	−30	−75	270

Тот же прием можно использовать и для вычисления значений функции $f'(x) = 5x^4 - 4x^3 + 12x + 15$ в нужных точках.

	5	−4	0	12	15
0	5	−4	0	12	15
1	5	1	1	13	28
2	5	6	12	36	87
−2	5	−14	28	−44	103
3	5	11	33	111	348
−3	5	−19	57	−159	492

▷

Упражнения

1. Решите сравнение:

а) $x^4 + 7x + 4 \equiv 0 (\mathrm{mod}\, 27)$;

б) $x^5 + 3x^4 - 7x^3 + 4x^2 + 4x - 10 \equiv 0 (\mathrm{mod}\, 25)$;

в) $x^4 + 4x^3 + 2x^2 + x + 12 \equiv 0 (\mathrm{mod}\, 625)$.

2. Решите сравнение:

а) $3x^4 + 4x^3 + 2x^2 + x + 3 \equiv 0 (\mathrm{mod}\, 3375)$;

б) $x^4 - 2x^2 - 2x + 16 \equiv 0 (\mathrm{mod}\, 416)$.

Задачи

1. Решите сравнение:

а) $9x^2 + 29x + 62 \equiv 0 (\mathrm{mod}\, 64)$;

б) $x^3 + 2x + 2 \equiv 0 (\mathrm{mod}\, 125)$;

в) $4x^3 + 6x^2 + 7x \equiv 0 (\mathrm{mod}\, 125)$.

2. Решите систему сравнений

$$\begin{cases} f(x) \equiv 0 (\mathrm{mod}\, 7), \\ f(x) \equiv 0 (\mathrm{mod}\, 44), \end{cases}$$

если $f(x) = 2x^{100} + 3x^{50} + 4x + 5$.

3. Для любых целых a и b решите систему сравнений:

а) $\begin{cases} x \equiv a(\mathrm{mod}\, 5^2) \\ x \equiv b(\mathrm{mod}\, 3^2) \end{cases}$; б) $\begin{cases} x \equiv a(\mathrm{mod}\, 5^3) \\ x \equiv b(\mathrm{mod}\, 3^3) \end{cases}$; в) $\begin{cases} x \equiv a(\mathrm{mod}\, 3^3) \\ x \equiv b(\mathrm{mod}\, 2^2) \end{cases}$.

4. Решите сравнение:

а) $31x^4 + 57x^3 + 96x + 191 \equiv 0(\mathrm{mod}\, 675)$;

б) $3x^4 - 8x^3 + 8x^2 - 3x + 3 \equiv 0(\mathrm{mod}\, 225)$;

в) $x^3 + 6x + 7 \equiv 0(\mathrm{mod}\, 675)$;

г) $x^3 + 2x^2 + 2x + 4 \equiv 0(\mathrm{mod}\, 675)$;

д) $x^3 - x^2 + x + 3 \equiv 0(\mathrm{mod}\, 108)$;

е) $x^3 + 5x^2 + 9x + 9 \equiv 0(\mathrm{mod}\, 108)$.

5. Найдите число решений сравнения:

а) $x^4 - 4x^3 + 12x^2 - 16x + 2 \equiv 0(\mathrm{mod}\, 175)$;

б) $x^5 + x^4 - x^3 + 5x^2 + 30x - 45 \equiv 0(\mathrm{mod}\, 225)$;

в) $x^5 - 4x^4 + 5x^3 + 4x^2 + 18x - 69 \equiv 0(\mathrm{mod}\, 225)$;

г) $2x^3 - 6x^2 + 5x - 2 \equiv 0(\mathrm{mod}\, 675)$.

6. Сколько решений может иметь сравнение третьей степени по модулю 8?

7. Может ли сравнение второй степени по модулю p^2, где $p \in P\backslash\{2\}$, иметь: p решений; $p+1$ решение; $p+2$ решения; $2p-1$ решение?

8. Придумайте и решите сравнение $f(x) \equiv 0(\mathrm{mod}\, p_1^{\alpha_1} p_2^{\alpha_2})$, имеющее t решений, если

а) $p_1 = 2$, $p_2 = 3$, $\alpha_1 = 3$, $\alpha_2 = 2$, $t = 6$;

б) $p_1 = 3$, $p_2 = 5$, $\alpha_1 = 2$, $\alpha_2 = 2$, $t = 10$;

в) $p_1 = 2$, $p_2 = 5$, $\alpha_1 = 3$, $\alpha_2 = 2$, $t = 3$.

9. Придумайте и решите сравнение с использованием не менее двух случаев теоремы: $f(x) \equiv 0(\mathrm{mod}\, p_1^{\alpha_1} p_2^{\alpha_2})$, $\alpha_1 \geqslant 2, \alpha_2 \geqslant 2, p_2 > p_1 \geqslant 2$.

10. Придумайте и решите сравнение с использованием всех трех случаев теоремы: $f(x) \equiv 0(\mathrm{mod}\, p_1^{\alpha_1} p_2^{\alpha_2})$, $\alpha_1 \geqslant 2, \alpha_2 \geqslant 1, p_2 > p_1 > 2$.

§ 19. Квадратичные вычеты и символ Лежандра

Для данного нечетного простого числа p, целое число a, взаимно простое с p, называется *квадратичным вычетом* по модулю p, если $x_0^2 \equiv a(\mathrm{mod}\, p)$ для некоторого целого x_0. В противном случае a называется *квадратичным невычетом* по модулю p.

Например, числа 1 и 4 являются квадратичными вычетами по модулю 5, поскольку сравнения $x^2 \equiv 1(\mathrm{mod}\,5)$ и $x^2 \equiv 4(\mathrm{mod}\,5)$ разрешимы: достаточно взять $x_0 = 1$ и $x_0 = 2$, соответственно. С другой стороны, числа 2 и 3 являются квадратичными невычетами по модулю 5, поскольку сравнения $x^2 \equiv 2(\mathrm{mod}\,5)$ и $x^2 \equiv 3(\mathrm{mod}\,5)$ неразрешимы: действительно, $1^2 \equiv 1(\mathrm{mod}\,5)$, $2^2 \equiv 4(\mathrm{mod}\,5)$, $3^2 \equiv 4(\mathrm{mod}\,5)$, и $4^2 \equiv 1(\mathrm{mod}\,5)$, то есть $x^2 \not\equiv 2(\mathrm{mod}\,5)$ и $x^2 \not\equiv 3(\mathrm{mod}\,5)$ для любого целого x.

Среди чисел $1, 2, \ldots, p-1$ (более того, в любой приведенной системе вычетов по модулю p) имеется ровно $(p-1)/2$ квадратичных вычетов и ровно $(p-1)/2$ квадратичных невычетов по модулю p; при этом все квадратичные вычеты принадлежат классам $\mathbf{1}_p^2$, $\mathbf{2}_p^2$, $\ldots$, $(\mathbf{(p-1)/2})_p^2$. Например, для нахождения всех квадратичных вычетов и невычетов по модулю 7, принадлежащих множеству $\{1, 2, 3, 4, 5, 6\}$, достаточно найти наименьшие неотрицательные вычеты по модулю 7 для чисел 1^2, 2^3 и 3^2: поскольку $1^2 \equiv 1(\mathrm{mod}\,7)$, $2^2 \equiv 4(\mathrm{mod}\,7)$ и $3^2 \equiv 2(\mathrm{mod}\,7)$, то квадратичными вычетами по модулю 7 являются числа 1, 2 и 4 (более того, все числа, принадлежащие классам $\mathbf{1}_7$, $\mathbf{2}_7$ и $\mathbf{4}_7$), в то время как квадратичными невычетами по модулю 7 являются числа 3, 5 и 6 (более того, все числа, принадлежащие классам $\mathbf{3}_7$, $\mathbf{5}_7$ и $\mathbf{6}_7$).

Для любого целого a, взаимно простого с нечетным простым числом p, *символ Лежандра* (a/p) определяется следующим образом: $(a/p) = 1$, если a является квадратичным вычетом по модулю p, и $(a/p) = -1$, если a является квадратичным невычетом по модулю p. Если $p|a$, то мы считаем, что $(a/p) = 0$.

Таким образом, с помощью символа Лежандра легко выяснить, сколько решений имеет сравнение $x^2 \equiv a(\mathrm{mod}\,p)$, где $p \in P\backslash\{2\}$: *если* $(a/p) = 1$, *то сравнение* $x^2 \equiv a(\mathrm{mod}\,p)$ *имеет два решения*: $x \equiv \pm x_0(\mathrm{mod}\,p)$; *если* $(a/p) = -1$, *то сравнение* $x^2 \equiv a(\mathrm{mod}\,p)$ *не имеет решений*; *если* $(a/p) = 0$, *то сравнение* $x^2 \equiv a(\mathrm{mod}\,p)$ *имеет одно решение*: $x \equiv 0(\mathrm{mod}\,p)$.

Символ Лежандра является специальным случаем *символа Якоби*, определяемого как $(a/n) = (a/p_1)^{\alpha_1} \cdot \ldots \cdot (a/p_k)^{\alpha_k}$ для любого нечетного $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$.

С помощью символа Якоби можно получить подтверждение неразрешимости сравнения $x^2 \equiv a(\mathrm{mod}\,n)$: *если* $(a/n) = -1$, *то сравнение* $x^2 \equiv a(\mathrm{mod}\,n)$ *не имеет решений.*

Свойства символа Лежандра

1. $(a/p) \equiv a^{(p-1)/2}(\mathrm{mod}\,p)$ (*критерий Эйлера*).
2. Если $a \equiv b(\mathrm{mod}\,p)$, то $(a/p) = (b/p)$.
3. $(ab/p) = (a/p)(b/p)$.
4. $(a^2/p) = 1$; в частности, $(1/p) = 1$.

5. $(-1/p) = (-1)^{(p-1)/2}$, то есть $(-1/p) = 1$, если $p \equiv 1 (\mathrm{mod}\, 4)$, и $(-1/p) = -1$, если $p \equiv -1 (\mathrm{mod}\, 4)$.
6. $(2/p) = (-1)^{(p^2-1)/8}$, то есть $(2/p) = 1$, если $p \equiv \pm 1 (\mathrm{mod}\, 8)$, и $(2/p) = -1$, если $p \equiv \pm 3 (\mathrm{mod}\, 8)$.
7. Для различных нечетных простых чисел p и q имеет место равенство $(p/q) = (-1)^{(p-1)/2 q-1/2}(q/p)$ (*квадратичный закон взаимности*).
8. Число решений сравнения $x^2 \equiv a (\mathrm{mod}\, p)$ равно $(a/p) + 1$.

Так, теорема Ферма позволяет утверждать, что $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$, откуда следует, что $(a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) \equiv 1 (\mathrm{mod}\, p)$; поскольку $p \in P \backslash \{2\}$, то $a^{(p-1)/2} \equiv 1 (\mathrm{mod}\, p)$ или $a^{(p-1)/2} \equiv -1 (\mathrm{mod}\, p)$ для любого целого a, взаимно простого с p, причем имеет место ровно одно из указанных сравнений. Если a — квадратичный вычет по модулю p, то для некоторого целого числа x_0 имеет место сравнение $x_0^2 \equiv a (\mathrm{mod}\, p)$, и, следовательно, выполняется сравнение $x_0^{p-1} \equiv a^{(p-1)/2} (\mathrm{mod}\, p)$. Легко видеть, что число x_0 взаимно просто с p. Следовательно, теорема Ферма позволяет утверждать, что $x_0^{p-1} \equiv 1 (\mathrm{mod}\, p)$, то есть для квадратичного вычета a по модулю p имеет место сравнение $a^{(p-1)/2} \equiv 1 (\mathrm{mod}\, p)$. Тогда для квадратичного невычета a по модулю p имеет место сравнение $a^{(p-1)/2} \equiv -1 (\mathrm{mod}\, p)$, что доказывает первое свойство. Опираясь на критерий Эйлера, нетрудно доказать и свойства 2–5 символа Лежандра. Для доказательства квадратичного закона взаимности воспользуемся классическим методом Гаусса.

• Прежде всего, докажем *лемму Гаусса*: $(a/p) = (-1)^n$, *где* n *— число чисел системы* $\{1 \cdot a, 2 \cdot a, \ldots, (p-1)/2 \cdot a\}$, *имеющих отрицательный абсолютно наименьший вычет по модулю* p.

Именно, рассмотрев числа $1 \cdot a, \ldots, (p-1)/2 \cdot a$, мы убедимся, что все они взаимно просты с числом p. Действительно, каждое из чисел $i \in \{1, \ldots, (p-1)/2\}$ взаимно просто с p, число a взаимно просто с p, и, следовательно, каждое произведение ia взаимно просто с p.

Кроме того, числа $1 \cdot a, \ldots, (p-1)/2 \cdot a$ принадлежат разным классам вычетов по модулю p. Действительно, если $ia \equiv ka (\mathrm{mod}\, p)$, то $i \equiv k (\mathrm{mod}\, p)$; так как $i, k \in \{1, \ldots, (p-1)/2\}$, то $i = k$. Следовательно, каждое из чисел $1 \cdot a, \ldots, (p-1)/2 \cdot a$ сравнимо ровно с одним элементом приведенной системы вычетов $\{\pm 1, \ldots, \pm(p-1)/2\}$ по модулю p: $ia \equiv (-1)^{n_i} r_i$, $i \in \{1, \ldots, (p-1)/2\}$, $r_i \in \{1, \ldots, (p-1)/2\}$, $n_i \in \{0, 1\}$. При этом если $i \neq k$, то и $r_i \neq r_k$: иначе $ia \equiv \pm ka (\mathrm{mod}\, p)$, и следовательно $i = k$, что дает противоречие. Таким образом,

$$1 \cdot \ldots \cdot \frac{(p-1)}{2} a^{(p-1)/2} \equiv (-1)^{n_1 + \ldots + n_{(p-1)/2}} r_1 \ldots r_{(p-1)/2} (\mathrm{mod}\, p).$$

Сокращение на одно и то же число $1 \cdot \ldots \cdot (p-1)/2 = r_1 \cdot \ldots \cdot r_{(p-1)/2}$ позволяет получить соотношение $a^{(p-1)/2} \equiv (-1)^n$, где $n = n_1 + \ldots + n_{(p-1)/2}$ равно

числу элементов ia, для которых $n_i = 1$, то есть тех элементов, которые имеют отрицательные абсолютно наименьшие вычеты.

• Докажем теперь, что $(a/p) = (-1)^t$, *где* $t = \sum\limits_{i=1}^{(p-1)/2} \lfloor 2ia/p \rfloor$.

Действительно, рассмотрев числа ia из доказательства предыдущего пункта, мы получим, что $ia = pq_i + r_i$, $0 < r_i < p$, при этом ia имеет положительный абсолютно наименьший вычет (равный r_i) тогда и только тогда, когда $0 < r_i \leqslant (p-1)/2$. Таким образом, $n_i = 0$, если $r_i \in \{1, \ldots, (p-1)/2\}$, и $n_i = 1$, иначе.

Рассмотрим число $2ia/p = 2q_i + 2r_i/p$. Если $r_i \in \{1, \ldots, (p-1)/2\}$, то $0 < 2r_i/p < 1$, и, так как $2q_i \in \mathbb{Z}$, мы получим, что $\lfloor 2ia/p \rfloor = 2q_i + \lfloor 2r_i/p \rfloor = 2q_i$. В остальных случаях $(p-1)/2 < r_i \leqslant p$, $1 < 2r_i/p < 2$, и $\lfloor 2ia/p \rfloor = 2q_i + \lfloor 2r_i/p \rfloor = 2q_i + 1$.

Таким образом, $\lfloor 2ia/p \rfloor$ есть число четное тогда и только тогда, когда $n_i = 0$, и число нечетное тогда и только тогда, когда $n_i = 1$, откуда следует, что суммы $t = \sum\limits_{i=1}^{(p-1)/2} \lfloor ia/p \rfloor$ и $n = \sum\limits_{i=1}^{(p-1)/2} n_i$ имеют одинаковую четность, то есть, $(-1)^t = (-1)^n$, что и доказывает наше утверждение.

• Докажем, что *для нечетного* a *имеет место равенство* $(a/p) = (-1)^s$, *где* $s = \sum\limits_{i=1}^{(p-1)/2} \lfloor ia/p \rfloor$.

Действительно, если a нечетно, то $a + p$ четно. Тогда

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{2a}{p}\right) = \left(\frac{4\dfrac{a+p}{2}}{p}\right) = \left(\frac{\dfrac{a+p}{2}}{p}\right) = (-1)^t,$$

$$t = \sum_{i=1}^{(p-1)/2} \left\lfloor \frac{i(a+p)}{p} \right\rfloor = \sum_{i=1}^{(p-1)/2} \left(\left\lfloor \frac{ia}{p} \right\rfloor + i \right) = \frac{p^2-1}{8} + \sum_{i=1}^{(p-1)/2} \left\lfloor \frac{ia}{p} \right\rfloor.$$

Беря $a = 1$, получим, что $\sum\limits_{i=1}^{(p-1)/2} \lfloor ia/p \rfloor = 0$, и $(a/p) = 1$, то есть $(2/p) = (-1)^{(p^2-1)/8}$. Сокращая теперь обе части равенства на одинаковую величину, получим искомый результат. (Заметим, что в процессе рассуждений мы получили доказательство свойства 6 символа Лежандра.)

• Пусть $p, q \in P \backslash \{2\}$ и $p \neq q$. Пользуясь утверждением предыдущего пункта, можно утверждать, что $(p/q)(q/p) = (-1)^{s+f}$, где $s = \sum\limits_{i=1}^{(p-1)/2} \lfloor iq/p \rfloor$, $f = \sum\limits_{i=1}^{q-1/2} \lfloor ip/q \rfloor$.

Рассмотрим на плоскости прямоугольник с вершинами $(0,0)$, $(0,(p-1)/2)$, $((q-1)/2,0)$, $((q-1)/2,(p-1)/2)$. Очевидно, что число точек с натуральными координатами в этом прямоугольнике равно

$$\frac{(p-1)}{2}\cdot\frac{(q-1)}{2}.$$

Подсчитаем число данных точек другим способом. Для этого проведем прямую $y=px/q$. Она не содержит ни одной точки вида (x_0,y_0), $x_0,y_0\in\mathbb{N}$: в противном случае $qy_0=px_0$, то есть $q|x_0$ и $p|y_0$, что невозможно для натуральных x_0 и y_0, если $0<x_0\leqslant(q-1)/2$, $0<y_0\leqslant(p-1)/2$. Легко видеть, что число точек с натуральными координатами, расположенных в нашем прямоугольнике под этой прямой, равно $\sum\limits_{i=1}^{(q-1)/2}\lfloor ip/q\rfloor$. Аналогично, число точек с натуральными координатами, лежащих в нашем прямоугольнике над данной прямой, равно $\sum\limits_{i=1}^{(p-1)/2}\lfloor iq/p\rfloor$ («переверните» оси координат и рассмотрите нашу прямую как прямую $x=q/py$). Таким образом, $(p-1)/2\cdot(q-1)/2=s+f$, и $(p/q)(q/p)=(-1)^{(p-1)/2(q-1)/2}$.

Доказательства остальных свойств можно найти, например, в [3].

Примеры решения задач

1. Вычислите: $(-125/47)$.

Решение. $(-125/47)=(-5\cdot25/47)=(-5/47)\cdot(5^2/47)=(-5/47)=$ $=(-1/47)(5/47)=(-1)\cdot(5/47)=(-1)\cdot(47/5)=(-1)\cdot(2/5)=(-1)\cdot$ $\cdot(-1)=1$. ▷

2. *Укажите число решений сравнения* $x^2-503\equiv0(\mathrm{mod}\,409)$.

Решение. Убедившись, что 409 — простое число и переписав сравнение в виде $x^2\equiv503(\mathrm{mod}\,409)$, рассмотрим символ Лежандра $(503/409)$: $(503/409)=(94/409)=(2\cdot47/409)=(2/409)\cdot(47/409)=1\cdot(47/409)=$ $(409/47)=(33/47)=(3/47)(11/47)=(-(47/3))\cdot(-(47/11))=(47/3)\cdot$ $(47/11)=(-1/3)(3/11)=(-1)\cdot(-(11/3))=(11/3)=(-1/3)=-1$. Следовательно, сравнение не имеет решений. ▷

3. Докажите, что сравнение $ax^2+bx+c\equiv0(\mathrm{mod}\,p)$, $p\in P\backslash\{2\}$, $(a,p)=1$, имеет два решения, если $(D/p)=1$, одно решение, если $(D/p)=0$, и не имеет решений, если $(D/p)=-1$, где $D=b^2-4ac$.

Решение. Так как p — нечетно, то можно провести ряд равносильных преобразований: $ax^2+bx+c\equiv0(\mathrm{mod}\,p)\Leftrightarrow4a^2x^2+4abx+$ $4ac\equiv0(\mathrm{mod}\,p)\Leftrightarrow(2ax+b)^2-b^2+4ac\equiv0(\mathrm{mod}\,p)\Leftrightarrow(2ax+b)^2\equiv$

$b^2 - 4ac (\mathrm{mod}\, p)$. В итоге сравнение $ax^2 + bx + c \equiv 0 (\mathrm{mod}\, p)$ равносильно сравнению $y^2 \equiv b^2 - 4ac (\mathrm{mod}\, p)$, или, что то же, сравнению $y^2 \equiv D (\mathrm{mod}\, p)$. Таким образом, если $(D/p) = 1$, то сравнение $y^2 \equiv D (\mathrm{mod}\, p)$ имеет два решения, и им соответствуют два решения сравнения $ax^2 + bx + c \equiv 0 (\mathrm{mod}\, p)$; если $(D/p) = -1$, то сравнение $y^2 \equiv D (\mathrm{mod}\, p)$ не имеет решений, и равносильное ему сравнение $ax^2 + bx + c \equiv 0 (\mathrm{mod}\, p)$ также неразрешимо; наконец, если $(D/p) = 0$, то сравнение $y^2 \equiv D (\mathrm{mod}\, p)$ имеет единственное нулевое решение и ему соответствует единственное решение сравнения $ax^2 + bx + c \equiv 0 (\mathrm{mod}\, p)$. ▷

4. Укажите число решений сравнения $x^2 - 6x + 7 \equiv 0 (\mathrm{mod}\, 31)$.

Решение. Поскольку $D = 36 - 28 = 8$ и $(8/31) = (2/31) = 1$,то сравнение $x^2 - 6x + 7 \equiv 0 (\mathrm{mod}\, 31)$ имеет два решения.

Впрочем, убедиться в этом можно и непосредственно: домножив наше сравнение на число 4, взаимно простое с модулем 31, мы получим сравнение $4x^2 - 24x + 28 \equiv 0 (\mathrm{mod}\, 31)$, равносильное исходному. Выделим в левой части полный квадрат: $4x^2 - 24x + 28 \equiv 4x^2 - 2 \cdot 2x \cdot 6 + 36 - 36 + 28 \equiv (2x-6)^2 - 36 + 28 \equiv (2x-6)^2 - 8 \equiv 0 (\mathrm{mod}\, 31)$. Таким образом, сравнение $x^2 - 6x + 7 \equiv 0 (\mathrm{mod}\, 31)$ равносильно сравнению $(2x - 6)^2 \equiv 8 (\mathrm{mod}\, 31)$.

Простой перебор показывает, что решениями сравнения $y^2 \equiv 8 (\mathrm{mod}\, 31)$ являются классы $y \equiv \pm 16 (\mathrm{mod}\, 31)$. Если $2x - 6 \equiv 16 (\mathrm{mod}\, 31)$, то $2x \equiv 22 (\mathrm{mod}\, 31)$, и $x \equiv 11 (\mathrm{mod}\, 31)$; Если $2x - 6 \equiv -16 (\mathrm{mod}\, 31)$, то $2x \equiv -10 (\mathrm{mod}\, 31)$, и $x \equiv -5 (\mathrm{mod}\, 31)$. Итак, сравнение $x^2 - 6x + 7 \equiv 0 (\mathrm{mod}\, 31)$ имеет два решения: $x \equiv 11 (\mathrm{mod}\, 31)$, и $x \equiv -5 (\mathrm{mod}\, 31)$. ▷

5. Укажите число решений сравнения $168x^2 + 169x + 84 \equiv 0 (\mathrm{mod}\, 503)$.

Решение. Убедившись, что число 503 — простое, домножим обе части сравнения на число 3, взаимно простое с модулем, и получим эквивалентное первоначальному сравнение $504x^2 + 507x + 252 \equiv 0 (\mathrm{mod}\, 503)$, или, что то же, сравнение $x^2 + 4x + 252 \equiv 0 (\mathrm{mod}\, 503)$. Домножив обе части последнего сравнения на число 2, взаимно простое с модулем, мы получим эквивалентное первоначальному сравнение $2x^2 + 8x + 504 \equiv 0 (\mathrm{mod}\, 503)$, или, что то же, сравнение $2x^2 + 8x + 1 \equiv 0 (\mathrm{mod}\, 503)$. Поскольку $D = 64 - 8 = 56$ и $(56/503) = (7 \cdot 2^3/503) = (7/503)(2/503) = (7/503) \cdot 1 = (7/503) = -(503/7) = -(-1/7) = -(-1) = 1$, то сравнение $2x^2 + 8x + 1 \equiv 0 (\mathrm{mod}\, 503)$ имеет два решения и, следовательно, сравнение $168x^2 + 169x + 84 \equiv 0 (\mathrm{mod}\, 503)$ имеет два решения. ▷

6. Укажите число решений сравнения $x^2 \equiv -1 (\mathrm{mod}\, 221)$.

Решение. Заметив, что число $221 = 13 \cdot 17$ — составное, перейдем от сравнения $x^2 \equiv -1 (\mathrm{mod}\, 221)$ к эквивалентной ему системе сравнений $\begin{cases} x^2 \equiv -1 \pmod{13} \\ x^2 \equiv -1 \pmod{17} \end{cases}$. Поскольку $(-1/13) = 1$ и $(-1/17) = 1$, то каждое из сравнений системы имеет ровно два решения, откуда следует, что сравнение $x^2 \equiv -1 (\mathrm{mod}\, 221)$ имеет четыре решения. ▷

7. Для каких простых p число 5 является квадратичным невычетом?

Решение. Очевидно, что $p \neq 2$ и $p \neq 5$. Далее, для $p \in P \backslash \{2, 5\}$ имеет место соотношение $(5/p) = ((p-1)/5)$. Если $p \equiv 1 (\mathrm{mod}\, 5)$, то $((p-1)/5) = (1/5) = 1$. Если $p \equiv -1 (\mathrm{mod}\, 5)$, то $((p-1)/5) = (-1/5) = 1$. Если $p \equiv 2 (\mathrm{mod}\, 5)$, то $((p-1)/5) = (2/5) = -1$. Если $p \equiv -2 (\mathrm{mod}\, 5)$, то $((p-1)/5) = (-2/5) = (-1/5)(2/5) = 1 \cdot (-1) = -1$. Таким образом, $((p-1)/5) = -1$ и, следовательно, 5 является квадратичным невычетом по модулю p, для нечетных простых $p \equiv \pm 2 (\mathrm{mod}\, 5)$, то есть для $p = \{3, 7, 13, 17, 23, 37, 43, 47, \ldots\}$. ▷

8. Укажите все простые делители квадратичной формы $x^2 + 6$.

Решение. Если p — простой делитель квадратичной формы $x^2 + 6$, то сравнение $x^2 + 6 \equiv 0 (\mathrm{mod}\, p)$ разрешимо. Это верно для $p = 2$: сравнение принимает вид $x^2 \equiv 0 (\mathrm{mod}\, 2)$, и его решением является класс $x \equiv 0 (\mathrm{mod}\, 2)$. Это верно для $p = 3$: сравнение принимает вид $x^2 \equiv 0 (\mathrm{mod}\, 3)$, и его решением является класс $x \equiv 0 (\mathrm{mod}\, 3)$. Если $p \in P \backslash \{2, 3\}$, то вопрос о разрешимости сравнения $x^2 \equiv -6 (\mathrm{mod}\, p)$ можно решить, найдя значение символа Лежандра $(-6/p)$. В этом случае $(-6/p) = (-1/p)(2/p)(3/p) = (-1)^{p-1/2}(2/p)(-1)^{p-1/2 \cdot 3-1/2}((p-1)/3) = (2/p)((p-1)/3)$. При этом $(2/p) = 1$, если $p \equiv \pm 1 (\mathrm{mod}\, 8)$, и $(2/p) = -1$, если $p \equiv \pm 3 (\mathrm{mod}\, 8)$, $((p-1)/3) = 1$, если $p \equiv 1 (\mathrm{mod}\, 3)$, и $((p-1)/3) = -1$, если $p \equiv -1 (\mathrm{mod}\, 3)$. Таким образом $(-6/p) = 1$, если $p \equiv \pm 1 (\mathrm{mod}\, 8)$ и $p \equiv 1 (\mathrm{mod}\, 3)$, или если $p \equiv \pm 3 (\mathrm{mod}\, 8)$ и $p \equiv -1 (\mathrm{mod}\, 3)$. Решая систему сравнений $\begin{cases} p \equiv a \pmod{3} \\ p \equiv b \pmod{8} \end{cases}$, мы получим, что $p = 8t + b$, и $8t + b \equiv a (\mathrm{mod}\, 3)$, откуда следует, что $-t \equiv a - b (\mathrm{mod}\, 3)$, или $t \equiv b - a (\mathrm{mod}\, 3)$, то есть $t = 3t_1 + (b - a)$, и $p = 8t + b = 8(3t_1 + (b - a)) + b = 24t_1 + (9b - 8a)$, или, что то же, $p \equiv 9b - 8a (\mathrm{mod}\, 24)$. Таким образом, для $a = 1, b = 1$ имеем $p \equiv 1 (\mathrm{mod}\, 24)$, для $a = 1, b = -1$ имеем $p \equiv 7 (\mathrm{mod}\, 24)$, для $a = -1, b = 3$ имеем $p \equiv 11 (\mathrm{mod}\, 24)$, для $a = -1, b = -3$ имеем $p \equiv 5 (\mathrm{mod}\, 24)$.

Итак, все простые делители квадратичной формы x^2+6 имеют вид $\{2, 3, 24t+1, 24t+5, 24t+7, 24t+11, t \in \mathbb{Z}\}$. ▷

Упражнения

1. Вычислите:

а) $(102/17)$; г) $(5000/101)$; ж) $(204/311)$;
б) $(-88/23)$; д) $(-5000/103)$; з) $(219/383)$.
в) $(125/47)$; е) $(-1116/73)$;

2. Существует ли целое число x, для которого x^2+5 делится на 61?

3. Существует ли целое число x, для которого x^2-40 делится на 71?

4. Укажите число решений сравнения:

а) $x^2-200 \equiv 0 (\mathrm{mod}\ 79)$; е) $x^2 \equiv 304 (\mathrm{mod}\ 299)$;
б) $x^2 \equiv 56 (\mathrm{mod}\ 87)$; ж) $x^2-990 \equiv 0 (\mathrm{mod}\ 1787)$;
в) $x^2 \equiv 555 (\mathrm{mod}\ 101)$; з) $x^2 \equiv 500 (\mathrm{mod}\ 1777)$;
г) $x^2 \equiv 15 (\mathrm{mod}\ 209)$; и) $x^2-270 \equiv (\mathrm{mod}\ 2803)$.
д) $x^2+27 \equiv 0 (\mathrm{mod}\ 91)$;

5. Укажите число решений сравнения:

а) $2x^2+7x+5 \equiv 0 (\mathrm{mod}\ 37)$;
б) $3x^2+5x+7 \equiv 0 (\mathrm{mod}\ 87)$.
в) $2x^2-3x+4 \equiv 0 (\mathrm{mod}\ 151)$;
г) $3x^2-x+7 \equiv 0 (\mathrm{mod}\ 151)$;
д) $5x^2+2x-5 \equiv 0 (\mathrm{mod}\ 71)$;
е) $4x^2-2x+9 \equiv 0 (\mathrm{mod}\ 137)$;
ж) $5x^2+3x+25 \equiv 0 (\mathrm{mod}\ 167)$;
з) $76x^2-77x+36 \equiv 0 (\mathrm{mod}\ 227)$.

6. Укажите число решений сравнения:

а) $5x^2+x+8 \equiv 0 (\mathrm{mod}\ 289)$;
б) $3x^2-11x+17 \equiv 0 (\mathrm{mod}\ 329)$.
в) $30x^2-x+14 \equiv 0 (\mathrm{mod}\ 494)$;
г) $204x^2+103x+1 \equiv 0 (\mathrm{mod}\ 818)$.

7. Для каких простых p число 3 является квадратичным невычетом?

8. Для каких простых p число 7 является квадратичным вычетом?

9. Укажите все простые делители квадратичной формы $2y^2+10$.

10. Укажите все простые делители квадратичной формы $3x^2+15$.

Задачи

1. Является ли число 71 квадратичным вычетом по модулю 93?

2. Найдите все классы квадратичных вычетов (невычетов) по модулю p, если $p \in \{11, 13, 15, 17\}$. Какой вывод можно сделать о их количестве?

3. Найдите наименьший натуральный двузначный квадратичный вычет по модулю 31.

4. Найдите наименьшее натуральное число, для которого сравнение $x^2 \equiv a \pmod{101}$ неразрешимо.

5. Вычислите:

а) $(1001/61)$; е) $(514/727)$; л) $(342/677)$;
б) $(2741/97)$; ж) $(438/593)$; м) $(2741/97)$;
в) $(342/667)$; з) $(232/367)$; н) $(1001/61)$;
г) $(342/677)$; и) $(157/379)$; о) $(514/727)$;
д) $(514/327)$; к) $(438/593)$; п) $(-88/263)$.

6. Разрешимо ли сравнение:

а) $x^2 + 67 \equiv 0 \pmod{1357}$; г) $x^2 \equiv 215 \pmod{47}$;
б) $x^2 - 69 \equiv 0 \pmod{307}$; д) $x^2 + 53 \equiv 0 \pmod{253}$;
в) $x^2 - 200 \equiv 0 \pmod{61}$; е) $x^2 - 300 \equiv 0 \pmod{151}$?

7. Сколько решений имеет сравнение:

а) $x^2 + 170x - 142 \equiv 0 \pmod{167}$;
б) $x^2 - 137x + 125 \equiv 0 \pmod{167}$;
в) $x^2 + 147x - 1 \equiv 0 \pmod{167}$;
г) $x^2 + 81x + 15 \equiv 0 \pmod{101}$;
д) $x^2 - 71x + 29 \equiv 0 \pmod{101}$;
е) $x^2 - 77x + 93 \equiv 0 \pmod{101}$;
ж) $x^2 + 83x + 56 \equiv 0 \pmod{103}$;
з) $x^2 - 73x + 67 \equiv 0 \pmod{103}$;
и) $x^2 - 83x + 15 \equiv 0 \pmod{103}$.

8. Укажите число решений сравнения:

а) $-196x^2 + 261x + 35 \equiv 0 \pmod{262}$;
б) $526x^2 + 50x - 44 \equiv 0 \pmod{214}$.

9. Для каких простых p число 13 является квадратичным невычетом?

10. Укажите все простые делители квадратичной формы $x^2 + 10y^2$.

11. Найдите сумму: $\sum\limits_{x=0}^{p-1} \left(\frac{x}{p}\right)$; $\sum\limits_{x=0}^{p-1} \left(\frac{x^2}{p}\right)$.

12. Докажите, что функция $f(n) = (n/p)$ является мультипликативной для любого фиксированного $p \in P\backslash\{2\}$. Является ли она вполне мультипликативной?

13. Убедитесь в том, что символ Якоби обладает свойствами, аналогичными свойствам 2–8 символа Лежандра.

14. Вычислите:

а) (75/363); б) (160/693); в) (250/351); г) (343/585).

15. Верно ли, что $(a/n) \equiv a^{(n-1)/2} (\mathrm{mod}\, n)$ для любого нечетного $n > 1$? Используя полученный результат, докажите, что число 21 является составным.

§ 20. Показатели и первообразные корни

Для данного натурального числа n и данного целого числа a, взаимно-простого с n, *показателем* $P_n(a)$ *числа* a *по модулю* n называется наименьшее натуральное число γ, такое что $a^\gamma \equiv 1 (\mathrm{mod}\, n)$. Целое число g называют *первообразным корнем* по модулю n, если $P_n(g) = \varphi(n)$.

Например, $P_5(4) = 2$, поскольку $4^2 \equiv 1 (\mathrm{mod}\, 5)$, но $4^1 \not\equiv 1 (\mathrm{mod}\, 5)$. С другой стороны, $P_5(3) = 4$, поскольку $3^4 \equiv 1 (\mathrm{mod}\, 5)$, и $3^1 \not\equiv 1 (\mathrm{mod}\, 5)$, $3^2 \not\equiv 1 (\mathrm{mod}\, 5)$, $3^3 \not\equiv 1 (\mathrm{mod}\, 5)$. Так как $\varphi(5) = 4$, то число 3 является первообразным корнем по модулю 5, а число 4 первообразным корнем по модулю 5 не является.

Аналогично, $P_9(2) = 6$, поскольку $2^6 \equiv 1 (\mathrm{mod}\, 9)$, но $2^1 \not\equiv 1 (\mathrm{mod}\, 9)$, $2^2 \not\equiv 1 (\mathrm{mod}\, 9)$, $\ldots$, $2^5 \not\equiv 1 (\mathrm{mod}\, 9)$. С другой стороны, $P_9(7) = 3$, поскольку $7^3 \equiv 1 (\mathrm{mod}\, 9)$, и $7^1 \not\equiv 1 (\mathrm{mod}\, 5)$, $7^2 \not\equiv 1 (\mathrm{mod}\, 9)$. Так как $\varphi(9) = 6$, то число 2 является первообразным корнем по модулю 9, а число 7 первообразным корнем по модулю 9 не является.

Известно (см. [3], [5]), что первообразные корни существуют только по модулю $2, 4, p^\alpha$ и $2p^\alpha$, где $p \in P\backslash\{2\}$, а $\alpha \in \mathbb{N}$.

Свойства показателей

1. Если $a \equiv b (\mathrm{mod}\, n)$, то $P_n(a) = P_n(b)$.
2. $a^\delta \equiv 1 (\mathrm{mod}\, n)$ тогда и только тогда, когда $P_n(a) | \delta$.
3. $P_n(a) | \varphi(n)$; в частности, $1 \leqslant P_n(a) \leqslant \varphi(n)$.
4. $a^\delta \equiv a^\eta (\mathrm{mod}\, n)$ тогда и только тогда, когда $\delta \equiv \eta (\mathrm{mod}\, P_n(a))$.
5. Числа $a^0, a^1, a^2, \ldots, a^{P_n(a)-1}$ принадлежат различным классам вычетов по модулю n.
6. Для первообразного корня g по модулю n числа $g^0, g^1, g^2, \ldots, g^{\varphi(n)-1}$ образуют приведенную систему вычетов по модулю n.

7. Количество натуральных чисел, не превосходящих n, показатель которых равен k, равно 0 или $\varphi(k)$; в частности, количество классов вычетов по простому модулю p, показатель которых равен k, $k|p-1$, равно $\varphi(k)$.
8. $P_{p_1^{\alpha_1}\cdot\ldots\cdot p_s^{\alpha_s}}(a) = [P_{p_1^{\alpha_1}}(a), \ldots, P_{p_s^{\alpha_s}}(a)]$.
9. $P_m(a^n) = \dfrac{P_m(a)}{(n, P_m(a))}$.
10. Если $P_m(a) = \gamma_1 \cdot \gamma_2$, то $P_m(a^{\gamma_1}) = \gamma_2$.
11. Если $P_{p^k}(a) = \gamma$, то $P_{p^{k+1}}(a) \in \{\gamma, \gamma \cdot p\}$; если $P_{p^k}(a) = \gamma$, $P_{p^{k+1}}(a) = \gamma \cdot p$ и $p^k > 2$, то $P_{p^{k+2}}(a) = \gamma \cdot p^2$.
12. Длина периода g-ной записи правильной несократимой дроби $a/(b_1 \cdot b_2)$, где $(b_1, g) = 1$, и b_2 состоит только из простых чисел, входящих в каноническое разложение g, равна $P_{b_1}(g)$; в частности, правильная несократимая дробь a/b, где $(b, 10) = 1$, разложима в чистопериодическую десятичную дробь, длина периода которой равна $P_b(10)$.

Первое свойство очевидным образом следует из определения показателя. Доказательство первой части свойства 2 тривиально: если $P_n(a)|\delta$, то $\delta = P_n(a)q$, и $a^\delta \equiv (a^{P_n(a)})^q \equiv 1 (\mathrm{mod}\, n)$. Для доказательства второй части свойства 2 достаточно поделить δ на $P_n(a)$ с остатком: $\delta = P_n(a)q + r$, где $0 \leqslant r < P_n(a)$. Поскольку $a^\delta \equiv 1 (\mathrm{mod}\, n)$, то $(a^{P_n(a)})^q \cdot a^r \equiv 1 (\mathrm{mod}\, n)$. С учетом того, что $a^{P_n(a)} \equiv 1 (\mathrm{mod}\, n)$, мы получаем сравнение $a^r \equiv 1 (\mathrm{mod}\, n)$. Так как $0 \leqslant r < P_n(a)$, то последнее сравнение возможно только при $r = 0$. Следовательно, $P_n(a)|\delta$. Третье свойство немедленно следует из свойства 2 и теоремы Эйлера: $a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$.

Для доказательства свойства 12 при $g = 10$ и $(b, 10) = 1$ введем обозначение $P_b(10) = s$ и рассмотрим следующую цепочку равенств:

$$10a = bq_1 + r_1, \quad 10r_1 = bq_2 + r_2, \quad \ldots, \quad 10r_{s-1} = bq_s + r_s,$$

где $0 \leqslant r_1 < b$, $0 \leqslant r_2 < b$, $\ldots$, $0 \leqslant r_s < b$. Деля первое равенство на $10b$, второе равенство — на $10^2 b$, $\ldots$, s-е равенство — на $10^s b$, мы получим, что

$$a/b = \frac{q_1}{10} + \frac{q_2}{10^2} + \ldots + \frac{q_s}{10^s} + \frac{r_s}{10^s b}.$$

Тогда $10^s a = b(q_1 10^{s-1} + q_2 10^{s-2} + \ldots + q_s) + r_s$, то есть $r_s \equiv 10^s a (\mathrm{mod}\, b)$, и, так как $10^s \equiv 1 (\mathrm{mod}\, b)$, то $r_s \equiv a (\mathrm{mod}\, b)$. Поскольку дробь a/b несократима, то числа a и b взаимно просты, и, с учетом условия $(10, b) = 1$, мы получаем, что $(10a, b) = 1$, откуда следует, что и $(b, r_1) = 1$. Аналогичные рассуждения позволяют утверждать, что $(b, r_2) = 1$, $\ldots$, $(b, r_s) = 1$. Таким образом, $0 < r_1 < b$, $0 < r_2 < b$, $\ldots$, $0 < r_s < b$. Поскольку дробь a/b правильная, то $0 < a < b$. Так как $r_s \equiv a (\mathrm{mod}\, b)$, то ограничения

$0 < r_s < b$ и $0 < a < b$ позволяют утверждать, что $r_s = a$. Отсюда следует, что $q_k = q_{s+k}$ для любого натурального k. Кроме того, мы можем легко убедиться в том, что $0 \leqslant q_1 < 10$, $0 \leqslant q_2 < 10$, ..., $0 \leqslant q_s < 10$. Наконец, $r_n/10^n b \to 0$ при $n \to \infty$, и мы получаем периодическое разложение

$$a/b = \frac{q_1}{10} + \frac{q_2}{10^2} + \ldots \frac{q_s}{10^s} + \frac{q_1}{10^{s+1}} + \ldots + \frac{q_s}{10^{2s}} + \ldots,$$

или, в сокращенной записи, $a/b = 0,(q_1 q_2 \ldots q_s)$, где $s = P_b(10)$.

Доказательства остальных свойств можно найти, например, в [3], [5].

Примеры решения задач

1. Найдите: $P_{11}(27)$; $P_{13}(15)$; $P_{12}(-53)$; $P_{10}(-225)$.

Решение. Поскольку $27 \equiv 5 (\mathrm{mod}\ 11)$, то $P_{11}(27) = P_{11}(5)$. Поскольку $\varphi(11) = 10$, то $P_{11}(5) | 10$, то есть $P_{11}(5) \in \{1, 2, 5, 10\}$. При этом $5^1 \equiv 5 \neq 1 (\mathrm{mod}\ 11)$, $5^2 \equiv 4 \neq 1 (\mathrm{mod}\ 11)$, $5^5 \equiv 5^2 \cdot 5^2 \cdot 5 \equiv 3 \cdot 3 \cdot 5 \equiv$ $\equiv (-2) \cdot 5 \equiv 1 (\mathrm{mod}\ 11)$. Таким образом, $P_{11}(27) = 5$.

Поскольку $15 \equiv 2 (\mathrm{mod}\ 13)$, то $P_{13}(15) = P_{13}(2)$. Поскольку $\varphi(13) = 12$, то $P_{13}(2) | 12$, то есть $P_{13}(2) \in \{1, 2, 3, 4, 6, 12\}$. При этом $2^1 \equiv 2 \neq$ $\neq 1 (\mathrm{mod}\ 13)$, $2^2 \equiv 4 \neq 1 (\mathrm{mod}\ 13)$, $2^3 \equiv 8 \neq 1 (\mathrm{mod}\ 13)$, $2^4 \equiv 16 \equiv 3 \neq$ $\neq 1 (\mathrm{mod}\ 13)$, $2^6 \equiv 2^4 \cdot 2^2 \equiv 3 \cdot 4 \equiv -1 \neq 1 (\mathrm{mod}\ 13)$, а по теореме Эйлера $2^{12} \equiv 1 (\mathrm{mod}\ 13)$. Таким образом, $P_{13}(2) = 12$, то есть число 2 является первообразным корнем по модулю 13.

Поскольку $-53 \equiv 7 (\mathrm{mod}\ 12)$, то $P_{12}(-53) = P_{12}(7)$. Поскольку $\varphi(12) = 4$, то $P_{12}(7) | 4$, то есть $P_{12}(7) \in \{1, 2, 4\}$. При этом $7^1 \equiv 7 \neq 1 (\mathrm{mod}\ 12)$, и $7^2 \equiv 49 \equiv 1 (\mathrm{mod}\ 12)$. Таким образом, $P_{12}(7) = P_{12}(-53) = 2$.

Поскольку $(10, -225) = 5 \neq 1$, то $P_{10}(-225)$ не существует. ▷

2. Вычислите $P_{4000}(81)$.

Решение. Прежде всего заметим, что

$$P_{4000}(81) = P_{4000}(3^4) = \frac{P_{4000}(3)}{(4, P_{4000}(3))}.$$

Перейдем к нахождению $P_{4000}(3)$. Легко видеть, что

$$P_{4000}(3) = P_{2^5 \cdot 5^3}(3) = [P_{2^5}(3), P_{5^3}(3)].$$

Найдем $P_{2^5}(3)$. Начнем вычисления с нахождения $P_2(3) = 1$. Тогда $P_{2^2}(3) \in \{1, 1 \cdot 2\}$. Поскольку $3^1 \neq 1 (\mathrm{mod}\ 2^2)$, то $P_{2^2}(3) = 2$. Тогда $P_{2^3}(3) \in \{2, 2 \cdot 2\}$. Поскольку $3^2 \equiv 1 (\mathrm{mod}\ 2^3)$, то $P_{2^3}(3) = 2$. Тогда $P_{2^4}(3) \in \{2, 2 \cdot 2\}$. Поскольку $3^2 \neq 1 (\mathrm{mod}\ 2^4)$, то $P_{2^4}(3) = 2^2$. Тогда $P_{2^5}(3) = 2^3$.

Найдем $P_{5^3}(3)$. Начнем вычисления с нахождения $P_5(3)$. Легко убедиться, что $P_5(3) = 4$. Тогда $P_{5^2}(3) \in \{4, 4 \cdot 5\}$. Поскольку $3^4 \not\equiv 1 (\mathrm{mod}\, 5^2)$, то $P_{5^2}(3) = 4 \cdot 5$. Тогда $P_{5^3}(3) = 4 \cdot 5^2$.

Теперь мы получим, что

$$P_{4000}(3) = [P_{2^5}(3), P_{5^3}(3)] = [2^3, 4 \cdot 5^2] = 2^3 \cdot 5^2 = 200.$$

Тогда

$$P_{4000}(81) = \frac{P_{4000}(3)}{(4, P_{4000}(3))} = \frac{200}{(4, 200)} = \frac{200}{4} = 50. \qquad \triangleright$$

3. Найдите все классы вычетов $\mathbf{x}_{11}$, для которых $P_{11}(x) = 3$; $P_{11}(x) = 5$.

Решение. Поскольку $\varphi(11) = 10$, и $3 \nmid 10$, то классов вычетов $\mathbf{x}_{11}$, для которых $P_{11}(x) = 3$, не существует.

Для нахождения всех классов вычетов $\mathbf{x}_{11}$, для которых $P_{11}(x) = 5$, найдем подбором один такой класс, например $\mathbf{3}_{11}$: именно, $3^1 \not\equiv 1 (\mathrm{mod}\, 11)$, $3^2 \not\equiv 1 (\mathrm{mod}\, 11)$, но $3^5 \equiv 27 \cdot 9 \equiv 5 \cdot (-2) \equiv -10 \equiv 1 (\mathrm{mod}\, 11)$.

Если $P_{11}(x) = 5$, то $x^5 \equiv 1 (\mathrm{mod}\, 11)$. С одной стороны, сравнение $x^5 \equiv 1 (\mathrm{mod}\, 11)$ по простому модулю 11 имеет не более пяти решений. С другой стороны, поскольку $3^5 \equiv 1 (\mathrm{mod}\, 11)$, то для любого целого неотрицательного числа k имеет место сравнение $(3^k)^5 \equiv 1 (\mathrm{mod}\, 11)$. Поскольку числа $3^0, 3^1, 3^2, 3^3, 3^4$ принадлежат различным классам вычетов по модулю 11, то классы $\mathbf{3}^0_{11}, \mathbf{3}^1_{11}, \mathbf{3}^2_{11}, \mathbf{3}^3_{11}, \mathbf{3}^4_{11}$ дают все решения сравнения $x^5 \equiv 1 (\mathrm{mod}\, 11)$. Поскольку

$$P_{11}(3^k) = \frac{P_{11}(3)}{(k, P_{11}(3))} = \frac{5}{(k, 5)},$$

то $P_{11}(3^k) = 5$ в том и только в том случае, когда $(k, 5) = 1$, то есть для $k \in \{1, 2, 3, 4\}$. Таким образом, $\mathbf{x}_{11} \in \{\mathbf{3}^1_{11}, \mathbf{3}^2_{11}, \mathbf{3}^3_{11}, \mathbf{3}^4_{11}\}$, или, что то же, $\mathbf{x}_{11} \in \{\mathbf{3}_{11}, \mathbf{9}_{11}, \mathbf{5}_{11}, \mathbf{4}_{11}\}$. $\triangleright$

4. Зная, что 7 — первообразный корень по модулю 11, запишите приведенную систему вычетов по модулю 11; найдите все первообразные корни по модулю 11.

Решение. Поскольку $P_{11}(7) = 10$, то числа $7^0, 7^1, 7^2, \ldots, 7^8, 7^9$ принадлежат различным классам по модулю 11 и, следовательно, образуют приведенную систему вычетов по модулю 11.

Для нахождения всех первообразных корней по модулю 11, то есть всех классов вычетов $\mathbf{x}_{11}$, для которых $P_{11}(x) = 10$, заметим, что если $P_{11}(x) = 10$, то $x^{10} \equiv 1 (\mathrm{mod}\, 11)$. С одной стороны, сравнение $x^{10} \equiv 1 (\mathrm{mod}\, 11)$ по простому модулю 11 имеет не более десяти решений. С другой стороны, для любого целого неотрицательного числа k имеет место сравнение $(7^k)^{10} \equiv 1 (\mathrm{mod}\, 11)$. Так как числа

$7^0, 7^1, 7^2, \ldots, 7^8, 7^9$ принадлежат различным классам вычетов по модулю 11, то классы 7^0_{11}, 7^1_{11}, 7^2_{11}, $\ldots$, 7^8_{11}, 7^9_{11} дают все решения сравнения $x^{10} \equiv 1 (\mathrm{mod}\ 11)$. Поскольку

$$P_{11}(7^k) = \frac{P_{11}(7)}{(k, P_{11}(7))} = \frac{10}{(k, 10)},$$

то $P_{11}(7^k) = 10$ в том и только в том случае, когда $(k, 10) = 1$, то есть для $k \in \{1, 3, 7, 9\}$. Таким образом, $\mathbf{x}_{11} \in \{7^1_{11}, 7^3_{11}, 7^7_{11}, 7^9_{11}\}$, или, что то же, $\mathbf{x}_{11} \in \{\mathbf{7}_{11}, \mathbf{2}_{11}, \mathbf{6}_{11}, \mathbf{8}_{11}\}$. ▷

5. Найдите длину периода g-ной записи дроби: $25/65$, $g = 10$; $663/(294 \cdot 10^7)$, $g = 7$.

Решение. Длина периода g-ной записи несократимой дроби $a/(b_1 \cdot b_2)$, где $(b_1, g) = 1$, и b_2 состоит только из простых чисел, входящих в каноническое разложение g, равна $P_g(10)$.

Таким образом, длина периода десятичной записи дроби $25/65 = 5/13$ равна $P_{13}(10)$. Поскольку $\varphi(13) = 12$, то $P_{13}(10) | 12$, то есть $P_{13}(10) \in \{1, 2, 3, 4, 6, 12\}$. При этом $10^1 \equiv -3 \neq 1 (\mathrm{mod}\ 13)$, $10^2 \equiv 9 \neq 1 (\mathrm{mod}\ 13)$, $10^4 \equiv (-4)^2 \equiv 16 \equiv 3 \neq 1 (\mathrm{mod}\ 13)$, $10^6 \equiv 10^4 \cdot 10^2 \equiv 3 \cdot 9 \equiv 1 (\mathrm{mod}\ 13)$. Таким образом, $P_{13}(10) = 6$, то есть длина периода десятичной записи дроби $25/65$ равна 6.

Для нахождения длины периода семиричной записи дроби $663/(294 \cdot 10^7)$ разложим числитель и знаменатель дроби на простые множители: $663 = 3 \cdot 13 \cdot 17$, и $294 \cdot 10^7 = 2^8 \cdot 3 \cdot 5^7 \cdot 7^2$. Таким образом, $663/(294 \cdot 10^7) = 13 \cdot 17/(2^8 \cdot 5^7 \cdot 7^2)$, и длина периода семиричной записи дроби $663/(294 \cdot 10^7)$ равна $P_{2^8 \cdot 5^7}(7)$.

При этом $P_{2^8 \cdot 5^7}(7) = [P_{2^8}(7), P_{5^7}(7)]$.

Найдем $P_{2^8}(7)$. Начнем вычисления с нахождения $P_2(7) = 1$. Тогда $P_{2^2}(7) \in \{1, 1 \cdot 2\}$. Поскольку $7^1 \neq 1 (\mathrm{mod}\ 2^2)$, то $P_{2^2}(7) = 2$. Тогда $P_{2^3}(7) \in \{2, 2 \cdot 2\}$. Поскольку $7^2 \equiv 1 (\mathrm{mod}\ 2^3)$, то $P_{2^3}(7) = 2$. Тогда $P_{2^4}(7) \in \{2, 2 \cdot 2\}$. Поскольку $7^2 \equiv 1 (\mathrm{mod}\ 2^4)$, то $P_{2^4}(7) = 2$. Тогда $P_{2^5}(7) \in \{2, 2 \cdot 2\}$. Поскольку $7^2 \neq 1 (\mathrm{mod}\ 2^5)$, то $P_{2^5}(7) = 2^2$. Тогда $P_{2^6}(7) = 2^3$, $P_{2^7}(7) = 2^4$, и $P_{2^8}(7) = 2^5$.

Найдем $P_{5^7}(7)$. Начнем вычисления с нахождения $P_5(7)$. Легко убедиться, что $P_5(7) = 4$. Тогда $P_{5^2}(7) \in \{4, 4 \cdot 5\}$. Поскольку $7^4 \equiv 7^2 \cdot 7^2 \equiv (-1)^2 \equiv 1 (\mathrm{mod}\ 5^2)$, то $P_{5^2}(7) = 4$. Тогда $P_{5^3}(7) \in \{4, 4 \cdot 5\}$. Поскольку $7^4 \equiv 7^3 \cdot (-33) \cdot 7 \equiv -231 \neq 11 (\mathrm{mod}\ 5^3)$, то $P_{5^3}(7) = 4 \cdot 5$. Тогда $P_{5^4}(7) = 4 \cdot 5^2$, $P_{5^5}(7) = 4 \cdot 5^3$, $P_{5^6}(7) = 4 \cdot 5^4$, и $P_{5^7}(7) = 4 \cdot 5^5$.

Теперь мы получим, что $[P_{2^8}(7), P_{5^7}(7)] = [2^5, 4 \cdot 5^5] = 2^5 \cdot 5^5 = 10^5$. Таким образом, длина периода семиричной записи дроби $663/(294 \cdot 10^7)$ равна 100 000. ▷

Замечание. Известно, что длина предпериода g-ной записи правильной несократимой дроби $a/(b_1 \cdot b_2)$, где $(b_1, g) = 1$, и b_2 состоит только из простых чисел, входящих в каноническое разложение g, равна n, где n — наименьшее натуральное число, такое что $g^n | b_2$ (см. [28]). В нашем случае $g = 7$ и $b_2 = 7^2$, то есть $g^2 | b_2$, откуда следует, что длина предпериода семиричной записи дроби $663/(294 \cdot 10^7)$ равна двум.

6. Найдите число всех правильных несократимых дробей, обращающихся в чистопериодическую десятичную дробь с длиной периода, равной 3.

Решение. Нас интересует число дробей вида a/b, где $0 < a < b$, $(a, b) = 1$, $(b, 10) = 1$, и $P_b(10) = 3$. В этом случае $10 \not\equiv 1 (\mathrm{mod}\, b)$, $10^2 \not\equiv 1 (\mathrm{mod}\, b)$, и $10^3 \equiv 1 (\mathrm{mod}\, b)$. Следовательно, $999 \equiv 0 (\mathrm{mod}\, b)$, то есть $b | 999$.

При этом имеется ровно $\tau(999) = \tau(3^3 \cdot 37) = 8$ натуральных делителей числа 999: $1, 3, 3^2, 3^3, 37, 3 \cdot 37, 3^2 \cdot 37, 3^3 \cdot 37$. Непосредственная проверка показывает, что $b \in \{3^3, 37, 3 \cdot 37, 3^2 \cdot 37, 3^3 \cdot 37\}$. При этом число правильных несократимых дробей со знаменателем 3^3 равно $\varphi(3^3) = 18$, число правильных несократимых дробей со знаменателем 37 равно $\varphi(37) = 36$, число правильных несократимых дробей со знаменателем $3 \cdot 37$ равно $\varphi(3 \cdot 37) = 2 \cdot 36$, число правильных несократимых дробей со знаменателем $3^2 \cdot 37$ равно $\varphi(3^2 \cdot 37)) = 6 \cdot 36$, число правильных несократимых дробей со знаменателем $3^3 \cdot 37$ равно $\varphi(3^3 \cdot 37)) = 18 \cdot 36$. Следовательно, число всех правильных несократимых дробей, обращающихся в чистопериодическую десятичную дробь с длиной периода, равной 3, равно $18 + 36 + 2 \cdot 36 + 6 \cdot 36 + 18 \cdot 36 = 990$. ▷

Упражнения

1. Найдите:

а) $P_{11}(13)$; г) $P_{12}(-55)$; ж) $P_{10}(-115)$;
б) $P_7(80)$; д) $P_{13}(-128)$; з) $P_{12}(245)$.
в) $P_{15}(9)$; е) $P_{21}(430)$.

2. Вычислите:

а) $P_{5000}(3)$; д) $P_{1000}(27)$; и) $P_{7^5 3^5}(2)$;
б) $P_{81000}(11)$; е) $P_{6075}(8)$; к) $P_7(5^{2010})$;
в) $P_{50048}(7)$; ж) $P_{7000}(625)$; л) $P_{187}(3^{80n+4})$;
г) $P_{39375}(2)$; з) $P_{1100}(169)$; м) $P_{75 \cdot 3^5}(2^{30n+5})$.

3. Найдите все классы вычетов x_7, для которых: $P_7(x) = 3$; $P_7(x) = 5$; $P_7(x) = 6$.

4. Найдите все классы вычетов $\mathbf{x}_{15}$, для которых: $P_{15}(x) = 2$; $P_{15}(x) = 8$; $P_{15}(x) = 4$.
5. Зная, что 2 — первообразный корень по модулю 13, запишите приведенную систему вычетов по модулю 13; найдите все первообразные корни по модулю 13.
6. Зная, что 3 — первообразный корень по модулю 17, запишите приведенную систему вычетов по модулю 17; найдите все первообразные корни по модулю 17.
7. Найдите все первообразные корни по модулю n, $n \in \{2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 15\}$.
8. Найдите длину периода g-ной записи дроби:
   а) $20/132$, $g = 11$;
   б) $12/41$, $g = 10$;
   в) $15/2870$, $g = 10$;
   г) $2/77^9$, $g = 12$;
   д) $5/33^7$, $g = 10$;
   е) $7/65^8$, $g = 11$.
9. Найдите число всех правильных несократимых дробей, обращающихся в чистопериодическую десятичную дробь с длиной периода, равной s, где $s \in \{2, 4, 5\}$.

Задачи

1. Вычислите:
   а) $P_{35424}(17)$;
   б) $P_{334368}(-17)$;
   в) $P_{6075}(8)$;
   г) $P_{864}(625)$;
   д) $P_{46575}(64)$;
   е) $P_{48608}(125)$;
   ж) $P_{28768}(81)$;
   з) $P_{203056}(125)$;
   и) $P_{20000}(81)$;
   к) $P_{99225}(16)$;
   л) $P_{11^{50}}(5^{50})$;
   м) $P_{2^{2009}}(3)$;
   н) $P_{2000}(343)$;
   о) $P_{63072}(49)$;
   п) $P_{253}(3^{55n+2})$.
2. Какие значения могут принимать показатели целого числа a по модулю n, если $n = N - 5\lfloor N/5 \rfloor + 5$, $N \in \{1, 2, 3, \ldots, 25\}$?
3. Сколько классов вычетов по модулю 17 имеют показатель:
   а) 2; б) 3; в) 4; г) 8; д) 16?
4. Скольким классам вычетов по модулю 17 принадлежат натуральные степени числа 7?
5. Сколько классов первообразных корней существует по модулю:
   а) 81; б) 98; в) 242; г) 338; д) 1250?
6. Найдите все классы вычетов $\mathbf{x}_{43}$, для которых: $P_{43}(x) = 14$; $P_{43}(x) = 7$.

7. Определите число цифр периода десятичной дроби, в которую обращается данное рациональное число, не обращая его в десятичную дробь:

а) 1000/1001; б) 26/1001; в) 19/77; г) 15/91; д) 23/143; е) 7/99; ж) 1/51; з) 17/57; и) 50/297; к) 14/539.

8. Найдите длину периода g-ичной записи дроби

а) $\frac{221}{30\,000\,000}$, $g = 7$; б) $\frac{225}{70000}$, $g = 4$; в) $\frac{28}{99 \cdot 10^{12}}$, $g = 3$; г) $\frac{405}{242 \cdot 30^{10}}$, $g = 8$.

9. Найдите число всех правильных несократимых дробей с длиной периода, равной s, где $s \in \{6, 7, 8\}$.

10. Докажите, что если $P_p(a) = 2\alpha$, то $a^\alpha \equiv -1 (\mathrm{mod}\, p)$, где $p \in P$.

11. Докажите, что если g — первообразный корень по простому модулю p и $g^{p^{\alpha-2}\cdot(p-1)} \not\equiv 1 (\mathrm{mod}\, p^\alpha)$, то g — первообразный корень по модулю p^α для $\alpha \geqslant 2$.

12. Докажите, что если g — первообразный корень по нечетному простому модулю p, то либо g, либо g^2 — первообразный корень по модулю p^2.

13. Докажите, что если g — первообразный корень по модулю p^2, $p \in P \setminus \{2\}$, то g — первообразный корень по модулю p^α для любого $\alpha \geqslant 2$.

14. Докажите, что если g — нечетный первообразный корень по модулю p^α, $p \in P \setminus \{2\}$, то g — первообразный корень по модулю $2p^\alpha$; если же g — четный первообразный корень по модулю p^α, $p \in P \setminus \{2\}$, то $g + p^\alpha$ - нечетный первообразный корень по модулю $2p^\alpha$.

15. Докажите, что число 2 является первообразным корнем по модулю 3^n для любого натурального n.

16. Найдите все первообразные корни по модулю:

а) 12; б) 14; в) 50; г) 81; д) 98; е) 242; ж) 250; з) 338; и) 625; к) 1250.

§ 21. Индексы

Если g является первообразным корнем по модулю n, то для любого целого числа a, взаимно простого с n, имеет место сравнение $a \equiv g^\beta (\mathrm{mod}\, n)$, где $\beta \in \{0, 1, \ldots, \varphi(n) - 1\}$. Число β называется *индексом*

числа a по модулю n с основанием g. В этом случае мы пишем $\beta = \operatorname{ind}_g a$, или, короче, $\beta = \operatorname{ind} a$.

Например, число 3 является первообразным корнем по модулю 5, и индекс числа 4 по модулю 5 с основанием 3 равен 2, поскольку $4 \equiv 3^2 (\mathrm{mod}\, 5)$. Более того, так как $3^0 \equiv 1 (\mathrm{mod}\, 5)$, $3^1 \equiv 3 (\mathrm{mod}\, 5)$, $3^2 \equiv 4 (\mathrm{mod}\, 5)$ и $3^3 \equiv 2 (\mathrm{mod}\, 5)$, то мы можем утверждать, что $\operatorname{ind} 1 = 0$, $\operatorname{ind} 2 = 3$, $\operatorname{ind} 3 = 1$ и $\operatorname{ind} 4 = 2$.

Поскольку первообразные корни существуют только по модулю $n \in \{2, 4, p^\alpha, 2p^\alpha\}$, где $p \in \mathbb{P}\backslash\{2\}$, и $\alpha \in \mathbb{N}$, то и индексы существуют только по модулю n из указанного списка. В частности, мы всегда можем говорить об индексах по простому модулю p.

Свойства индексов

1. Если $a \equiv b (\mathrm{mod}\, n)$, то $\operatorname{ind} a \equiv \operatorname{ind} b (\mathrm{mod}\, \varphi(n))$.
2. $\operatorname{ind} ab \equiv \operatorname{ind} a + \operatorname{ind} b (\mathrm{mod}\, \varphi(n))$.
3. $\operatorname{ind} a^k \equiv k \operatorname{ind} a (\mathrm{mod}\, \varphi(n))$ для любого целого неотрицательного числа k.
4. $P_n(a) = \dfrac{\varphi(n)}{(\operatorname{ind} a, \varphi(n))}$.

Так, первое свойство немедленно следует из определения. Для доказательства второго свойства достаточно заметить, что из сравнений $a \equiv g^\beta (\mathrm{mod}\, n)$ и $b \equiv g^\gamma (\mathrm{mod}\, n)$ следует сравнение $ab \equiv g^{\beta+\gamma} (\mathrm{mod}\, n)$. Доказательства остальных свойств аналогичны; их можно найти, например, в [3], [5].

Целое число a, взаимно простое с простым числом p, называется *вычетом степени n по модулю p*, если сравнение $x^n \equiv a (\mathrm{mod}\, p)$ разрешимо. В противном случае a называется *невычетом степени n по модулю p*.

Нетрудно убедиться в том, что при $(a, p) = 1$ и $(n, p-1) = \delta$ сравнение $x^n \equiv a (\mathrm{mod}\, p)$ имеет δ решений, если $\delta | \operatorname{ind} a$, и не имеет решений, если $\delta \nmid \operatorname{ind} a$ (см. [3]).

Примеры решения задач

1. Составьте таблицу индексов по модулю 11, используя наименьший натуральной первообразной корень по модулю 11.

Решение. В процессе решения задач предыдущего параграфа мы доказали, что 2 является первообразным корнем по модулю 11: $2^{10} \equiv 1 (\mathrm{mod}\, 11)$, но $2^5 \not\equiv 1 (\mathrm{mod}\, 11)$, $2^2 \not\equiv (\mathrm{mod}\, 11)$, и $2^1 \not\equiv 1 (\mathrm{mod}\, 11)$. Тогда числа $2^0, 2^1, 2^2, \ldots, 2^9$ образуют приведенную систему вычетов по модулю 11. Именно, $2^0 \equiv 1 (\mathrm{mod}\, 11)$, $2^1 \equiv 2 (\mathrm{mod}\, 11)$, $2^3 \equiv 8 (\mathrm{mod}\, 11)$, $2^4 \equiv 5 (\mathrm{mod}\, 11)$, $2^5 \equiv 10 (\mathrm{mod}\, 11)$, $2^6 \equiv 9 (\mathrm{mod}\, 11)$, $2^7 \equiv 7 (\mathrm{mod}\, 11)$, $2^8 \equiv 3 (\mathrm{mod}\, 11)$, $2^9 \equiv 6 (\mathrm{mod}\, 11)$. Таким образом, $\operatorname{ind} 1 = 0$, $\operatorname{ind} 2 = 1$,

Таблица 10

a	1	2	3	4	5	6	7	8	9	10
ind a	0	1	8	2	4	9	7	3	6	5

ind 3 = 8, ind 4 = 2, ind 5 = 4, ind 6 = 9, ind 7 = 7, ind 8 = 3, ind 9 = 6, ind 10 = 5, имеем искомую табл. 10 ▷

2. Пользуясь табл. 10, найдите:

- первообразный корень, по которому составлена таблица;
- все первообразные корни по модулю 11;
- все квадратичные вычеты по модулю 11;
- все квадратичные невычеты по модулю 11;
- все классы $\mathbf{x}_{11}$, такие что $P_{11}(x) = 5$.

Решение. Поскольку $\beta \equiv \beta^1 (\mathrm{mod}\, p)$, то первообразный корень, по которому составлена таблица, всегда имеет индекс, равный 1. Следовательно, в нашем случае $\beta = 2$.

Поскольку

$$P_p(a) = (p-1)/(\mathrm{ind}\, a, p-1),$$

то число a является первообразным корнем по модулю p, то есть обладает свойством $P_p(a) = p-1$, тогда и только тогда, когда $(\mathrm{ind}\ a, p-1) = 1$. Таким образом, индексами первообразных корней по модулю 11 будут числа, взаимно простые с 10, то есть числа 1, 3, 5 и 7. Следовательно, первообразными корнями по модулю 11 являются числа 2, 6, 7 и 8, точнее, все числа, принадлежащие классам вычетов $\mathbf{2}_{11}$, $\mathbf{6}_{11}$, $\mathbf{7}_{11}$ и $\mathbf{8}_{11}$.

Поскольку сравнение $x^2 \equiv a (\mathrm{mod}\, p)$ эквивалентно сравнению

$$2\mathrm{ind}\ x \equiv \mathrm{ind}\ a (\mathrm{mod}\, p-1),$$

а последнее сравнение разрешимо в том и только в том случае, когда $(2, p-1) | \mathrm{ind}\ a$, то есть тогда и только тогда, когда ind a — четное число, то квадратичными вычетами по модулю 11 являются числа, обладающие четными индексами, именно, числа 1, 4, 5, 9 и 3, точнее, все числа, принадлежащие классам вычетов $\mathbf{1}_{11}$, $\mathbf{4}_{11}$, $\mathbf{5}_{11}$ $\mathbf{9}_{11}$ и $\mathbf{3}_{11}$.

Квадратичными невычетами по модулю 11 являются числа, обладающие нечетными индексами, именно, числа 2, 6, 7, 8 и 10, точнее, все числа, принадлежащие классам вычетов $\mathbf{2}_{11}$, $\mathbf{6}_{11}$, $\mathbf{7}_{11}$ $\mathbf{8}_{11}$ и $\mathbf{10}_{11}$.

Поскольку

$$P_{11}(a) = \frac{10}{(\mathrm{ind}\ a, 10)},$$

то $P_{11}(a) = 5$ тогда и только тогда, когда $(\text{ind}\ a, 10) = 2$. Такими индексами являются 2, 4, 6 и 8. Им соответствуют числа 4, 5, 9 и 3, точнее, все числа, принадлежащие классам вычетов $\mathbf{4}_{11}$, $\mathbf{5}_{11}$, $\mathbf{9}_{11}$ и $\mathbf{3}_{11}$. ▷

3. Решите сравнение $7x \equiv 9(\text{mod}\ 11)$.

Решение. Пользуясь свойствами индексов, мы получим, что

$$7x \equiv 9(\text{mod}\ 11) \Leftrightarrow \text{ind}\ 7x \equiv \text{ind}\ 9(\text{mod}\ 10) \Leftrightarrow$$
$$\Leftrightarrow \text{ind}\ 7 + \text{ind}\ x \equiv \text{ind}\ 9(\text{mod}\ 10) \Leftrightarrow$$
$$\Leftrightarrow 7 + \text{ind}\ x \equiv 6(\text{mod}\ 10) \Leftrightarrow \text{ind}\ x \equiv 9(\text{mod}\ 10) \Leftrightarrow x \equiv 6(\text{mod}\ 11).$$

Таким образом, сравнение $7x \equiv 9(\text{mod}\ 11)$ имеет единственное решение: класс $x \equiv 6(\text{mod}\ 11)$. ▷

4. Решите сравнение $24x \equiv 20(\text{mod}\ 44)$.

Решение. Замечая, что $24x \equiv 20(\text{mod}\ 44) \Leftrightarrow 6x \equiv 5(\text{mod}\ 11)$ и пользуясь свойствами индексов, мы получим, что

$$24x \equiv 20(\text{mod}\ 44) \Leftrightarrow 6x \equiv 5(\text{mod}\ 11) \Leftrightarrow \text{ind}\ 6x \equiv \text{ind}\ 5(\text{mod}\ 10) \Leftrightarrow$$
$$\Leftrightarrow \text{ind}\ 6 + \textit{ind}\ x \equiv \text{ind}\ 5(\text{mod}\ 10) \Leftrightarrow 9 + \text{ind}\ x \equiv 4(\text{mod}\ 10) \Leftrightarrow$$
$$\Leftrightarrow \text{ind}\ x \equiv 5(\text{mod}\ 10) \Leftrightarrow x \equiv 10(\text{mod}\ 11).$$

Разбивая один класс по модулю 11 на четыре класса по модулю 44, мы получим $x \equiv 10(\text{mod}44)$, $x \equiv 21(\text{mod}44)$, $x \equiv 32(\text{mod}44)$ и $x \equiv 43(\text{mod}\ 44)$. Таким образом, сравнение $24x \equiv 20(\text{mod}\ 44)$ имеет четыре решения: классы $x \equiv 10(\text{mod}\ 44)$, $x \equiv 21(\text{mod}\ 44)$, $x \equiv 32(\text{mod}\ 44)$ и $x \equiv 43(\text{mod}\ 44)$. ▷

5. *Укажите число решений и решите сравнение:* $x^6 \equiv 49(\text{mod}\ 11)$; $x^6 \equiv 52(\text{mod}\ 11)$.

Решение. Замечая, что $49 \equiv 5(\text{mod}\ 11)$ и пользуясь свойствами индексов, мы получим, что

$$x^6 \equiv 49(\text{mod}\ 11) \Leftrightarrow x^6 \equiv 5(\text{mod}\ 11) \Leftrightarrow \text{ind}\ x^6 \equiv \text{ind}\ 5(\text{mod}\ 10) \Leftrightarrow$$
$$6\text{ind}\ x \equiv \text{ind}\ 5(\text{mod}\ 10) \Leftrightarrow 6\text{ind}\ x \equiv 4(\text{mod}\ 10).$$

Поскольку $(6, 10) = 2$ и $2|4$, то сравнение первой степени относительно неизвестной ind x имеет два решения. Следовательно, и сравнение $x^6 \equiv 49(\text{mod}\ 11)$ имеет два решения.

Продолжая рассуждения, мы получим, что

$$6\text{ind}\ x \equiv 4(\text{mod}\ 10) \Leftrightarrow 3\text{ind}\ x \equiv 2(\text{mod}\ 5) \Leftrightarrow$$
$$\Leftrightarrow \text{ind}\ x \equiv 4(\text{mod}\ 5) \Leftrightarrow \text{ind}\ x \equiv 4(\text{mod}\ 10)$$

или

$$\text{ind } x \equiv 9 (\text{mod } 10) \Leftrightarrow x \equiv 5 (\text{mod } 11)$$

или

$$x \equiv 6 (\text{mod } 11).$$

Таким образом, сравнение $x^6 \equiv 49 (\text{mod } 11)$ имеет два решения: классы $x \equiv 5 (\text{mod } 11)$ и $x \equiv 6 (\text{mod } 11)$.

Замечая, что $52 \equiv 8 (\text{mod } 11)$ и *пользуясь свойствами индексов*, мы получим, что

$$x^6 \equiv 52 (\text{mod } 11) \Leftrightarrow x^6 \equiv 8 (\text{mod } 11) \Leftrightarrow \text{ind } x^6 \equiv \text{ind } 8 (\text{mod } 10) \Leftrightarrow$$

$$\Leftrightarrow 6\text{ind } x \equiv \text{ind } 8 (\text{mod } 10) \Leftrightarrow 6\text{ind } x \equiv 3 (\text{mod } 10).$$

Поскольку $(6, 10) = 2$ и $2 \nmid 3$, то сравнение первой степени относительно неизвестной $\text{ind } x$ не имеет решений. Следовательно, и сравнение $x^6 \equiv 52 (\text{mod } 11)$ не имеет решений. ▷

6. Найдите остаток от деления 300^{304} на 11.

Решение. Для нахождения остатка от деления 300^{304} на 11 мы должны найти целое число x, такое что $300^{304} \equiv x (\text{mod } 11)$, и $0 \leqslant x < 11$. Заменив число 300 его остатком 3 от деления на 11 и воспользовавшись свойствами индексов, мы получим, что

$$300^{304} \equiv x (\text{mod } 11) \Leftrightarrow 3^{304} \equiv x (\text{mod } 11) \Leftrightarrow \text{ind } 3^{304} \equiv \text{ind } x (\text{mod } 10) \Leftrightarrow$$

$$\Leftrightarrow 304\text{ind } 3 \equiv \text{ind } x (\text{mod } 10) \Leftrightarrow 304 \cdot 8 \equiv \text{ind } x (\text{mod } 10) \Leftrightarrow$$

$$\Leftrightarrow \text{ind } x \equiv 2 (\text{mod } 10) \Leftrightarrow x \equiv 4 (\text{mod } 11).$$

Таким образом, остаток от деления 300^{304} на 11 равен 4. ▷

7. Найдите остаток от деления $37^{32^{90}}$ на 11.

Решение. Для нахождения остатка от деления $37^{32^{90}}$ на 11 мы должны найти целое число x, такое что $37^{32^{90}} \equiv x (\text{mod } 11)$, и $0 \leqslant x < 11$. Заменив число 37 его остатком 4 от деления на 11 и воспользовавшись свойствами индексов, мы получим, что

$$7^{32^{90}} \equiv x (\text{mod } 11) \Leftrightarrow 4^{32^{90}} \equiv x (\text{mod } 11) \Leftrightarrow \text{ind } 4^{32^{90}} \equiv \text{ind } x (\text{mod } 10) \Leftrightarrow$$

$$\Leftrightarrow 32^{90}\text{ind } 4 \equiv \text{ind } x (\text{mod } 10) \Leftrightarrow 32^{90} \cdot 2 \equiv \text{ind } x (\text{mod } 10) \Leftrightarrow$$

$$\Leftrightarrow 32^{90} \equiv \frac{\text{ind } x}{2} (\text{mod } 5).$$

Поскольку $32 \equiv 2 (\text{mod } 5)$ и $2^4 \equiv 1 (\text{mod } 5)$, то

$$32^{90} \equiv 2^{90} \equiv (2^4)^{22} \cdot 2^2 \equiv 4 (\text{mod } 5),$$

и

$$\frac{\operatorname{ind} x}{2} \equiv 4 (\mathrm{mod}\, 5),$$

откуда следует, что $\operatorname{ind} x \equiv 8 (\mathrm{mod}\, 10)$, и $x \equiv 3 (\mathrm{mod}\, 11)$. Таким образом, остаток от деления $37^{32^{90}}$ на 11 равен 3. ▷

Замечание. Заключительный этап рассуждений можно провести значительно проще, воспользовавшись таблицей индексов по модулю 5. Прежде всего построим эту таблицу, заметив, что 2 является первообразным корнем по модулю 5: $2^4 \equiv 1 (\mathrm{mod}\, 5)$, но $2^1 \neq 1 (\mathrm{mod}\, 5)$, и $2^2 \neq 1 (\mathrm{mod} 5)$. Тогда числа 2^0, 2^1, 2^2, 2^3 образуют приведенную систему вычетов по модулю 5. Именно, $2^0 \equiv 1 (\mathrm{mod}\, 5)$, $2^1 \equiv 2 (\mathrm{mod}\, 5)$, $2^2 \equiv 4 (\mathrm{mod}\, 5)$, $2^3 \equiv 3 (\mathrm{mod}\, 5)$. Таким образом, $\mathrm{ind}1 = 0$, $\mathrm{ind}2 = 1$, $\mathrm{ind}3 = 3$, $\mathrm{ind}4 = 2$, и соответствующая таблица принимает нижеследующий вид.

a	1	2	3	4
$\operatorname{ind} a$	0	1	3	2

Пусть $\operatorname{ind} x/2 = y$. Тогда

$$32^{90} \equiv \frac{\operatorname{ind} x}{2} (\mathrm{mod}\, 5) \Leftrightarrow 32^{90} \equiv y (\mathrm{mod}\, 5) \Leftrightarrow$$

$$\Leftrightarrow 2^{90} \equiv y (\mathrm{mod}\, 5) \Leftrightarrow \operatorname{ind} 2^{90} \equiv \operatorname{ind} y (\mathrm{mod}\, 4) \Leftrightarrow$$

$$\Leftrightarrow 90 \operatorname{ind} 2 \equiv \operatorname{ind} y (\mathrm{mod}\, 4) \Leftrightarrow 90 \cdot 1 \equiv \operatorname{ind} y (\mathrm{mod}\, 4) \Leftrightarrow 90 \equiv \operatorname{ind} y (\mathrm{mod}\, 4) \Leftrightarrow$$

$$\Leftrightarrow \operatorname{ind} y \equiv 2 (\mathrm{mod}\, 4) \Leftrightarrow y \equiv 4 (\mathrm{mod}\, 5) \Leftrightarrow \operatorname{ind} x \equiv 8 (\mathrm{mod}\, 10) \Leftrightarrow x \equiv 3 (\mathrm{mod}\, 11).$$

Таким образом, остаток от деления $37^{32^{90}}$ на 11 равен 3.

8. Найдите все индексы числа 4 по модулю 11.

Решение. Пользуясь построенной выше таблицей индексов по модулю 11, мы можем выписать все принадлежащие ей первообразные корни по модулю 11: числа 2, 6, 7 и 8, индексы которых взаимно просты с 10. Поскольку таблица построена по основанию $g = 2$, то первый индекс β числа 4 мы найдем из таблицы: он равен 2.

Если $g = 6$, то $\operatorname{ind} 4 = \beta_1$, где $4 \equiv 6^{\beta_1} (\mathrm{mod}\, 11)$. Пользуясь свойствами индексов, мы получим сравнение $\beta_1 \cdot \operatorname{ind} 6 \equiv \operatorname{ind} 4 (\mathrm{mod}\, 10)$, или, что то же, сравнение $9\beta_1 \equiv 2 (\mathrm{mod}\, 10)$. Отсюда следует, что $\beta_1 \equiv 8 (\mathrm{mod}\, 10)$, то есть $\beta_1 = 8$.

Если $g = 7$, то $\operatorname{ind} 4 = \beta_2$, где $4 \equiv 7^{\beta_2} (\mathrm{mod}\, 11)$. Пользуясь свойствами индексов, мы получим сравнение $\beta_2 \cdot \operatorname{ind} 7 \equiv \operatorname{ind} 4 (\mathrm{mod}\, 10)$, или, что то же, сравнение $7\beta_2 \equiv 2 (\mathrm{mod}\, 10)$. Отсюда следует, что $7\beta_2 \equiv 42 (\mathrm{mod}\, 10)$, или $\beta_2 \equiv 6 (\mathrm{mod}\, 10)$, то есть $\beta_2 = 6$.

Если $g = 8$, то $\text{ind}\ 4 = \beta_3$, где $4 \equiv 8^{\beta_3} (\text{mod}\ 11)$. Пользуясь свойствами индексов, мы получим сравнение $\beta_3 \cdot \text{ind}\ 8 \equiv \text{ind}\ 4 (\text{mod}\ 10)$, или, что то же, сравнение $3\beta_3 \equiv 2 (\text{mod}\ 10)$. Отсюда следует, что $3\beta_3 \equiv \equiv 12 (\text{mod}\ 10)$, или $\beta_3 \equiv 4 (\text{mod}\ 10)$, то есть $\beta_3 = 4$.

Таким образом, индексами числа 4 по модулю 11 могут быть числа 2, 4, 6 и 8. ▷

9. Найдите $P_{11}(9)$.

Решение. Поскольку $9^{P_{11}(9)} \equiv 1 (\text{mod}\ 11)$, то

$$P_{11}(9)\text{ind}\ 9 \equiv \text{ind}\ 1 (\text{mod}\ 10),$$

или

$$6 \cdot P_{11}(9) \equiv 0 (\text{mod}\ 10).$$

Отсюда следует, что $3 \cdot P_{11}(9) \equiv 0 (\text{mod}\ 5)$, то есть $P_{11}(9) \equiv 0 (\text{mod}\ 5)$. Выбирая из полученного множества целых чисел

$$\{\ldots, -10, -5, 0, 5, 10, \ldots\}$$

наименьшее натуральное число, мы получим, что $P_{11}(9) = 5$. ▷

10. Через какие точки (x, y) с целыми координатами x и y проходит кривая $11y = 7x^4 + 24$?

Решение. Если кривая $11y = 7x^4 + 20$ проходит через точку (x_0, y_0) с целыми координатами x_0 и y_0, то $7x_0^4 + 24 \equiv (\text{mod}\ 11)$, откуда следует, что сравнение $7x^4 \equiv 9 (\text{mod}\ 11)$ разрешимо. Однако

$$7x^4 \equiv 9 (\text{mod}\ 11) \Leftrightarrow \text{ind}\ 7 + 4\text{ind}\ x \equiv \text{ind}\ 9 (\text{mod}\ 10) \Leftrightarrow$$

$$\Leftrightarrow 7 + 4\text{ind}\ x \equiv 6 (\text{mod}\ 10) \Leftrightarrow 4\text{ind}\ x \equiv 9 (\text{mod}\ 10).$$

Поскольку $(4, 10) = 2$ и $2 \nmid 9$, то последнее сравнение не имеет решений. Таким образом, кривая $11y = 7x^4 + 24$ не проходит ни через одну точку (x_0, y_0) с целыми координатами x_0 и y_0. ▷

Упражнения

1. Составьте таблицу индексов по модулю p, где $p \in \{3, 5, 7, 13, 17, 19\}$, используя наименьший натуральной первообразный корень по соответствующему модулю.

2. Глядя в таблицу индексов по модулю p, где $p \in \{3, 5, 7, 13, 17, 19\}$, найдите:

- первообразный корень, по которому составлена таблица;
- все первообразные корни по модулю p;

- все квадратичные вычеты по модулю p;
- все квадратичные невычеты по модулю p;
- все классы $\mathbf{x}_p$, такие что $P_p(x) = (p-1)/2$;
- все классы $\mathbf{x}_p$, такие что $P_p(x) = 2$.

3. Найдите все классы вычетов:

а) $\mathbf{x}_{13}$, для которых $P_{13}(x) = 4$;

б) $\mathbf{x}_{17}$, для которых $P_{17}(x) = 8$;

в) $\mathbf{x}_{19}$, для которых $P_{19}(x) = 3$;

г) $\mathbf{x}_{43}$, для которых $P_{43}(x) = 6$.

4. Решите сравнение первой степени:

а) $7x \equiv 10 (\mathrm{mod}\, 13)$;
б) $2x \equiv 12 (\mathrm{mod}\, 17)$;
в) $7x \equiv 12 (\mathrm{mod}\, 47)$;
г) $8x \equiv 50 (\mathrm{mod}\, 61)$;
д) $24x \equiv 20 (44)$;
е) $40x \equiv 60 (\mathrm{mod}\, 44)$;
ж) $18x \equiv 45 (\mathrm{mod}\, 65)$;
з) $10x \equiv 15 (\mathrm{mod}\, 55)$;
и) $30x \equiv 42 (\mathrm{mod}\, 102)$.

5. Укажите число решений сравнения:

а) $x^6 \equiv 23 (\mathrm{mod}\, 13)$;
б) $2x^{10} \equiv 25 (\mathrm{mod}\, 17)$;
в) $5x^{20} \equiv 34 (\mathrm{mod}\, 19)$;
г) $x^6 \equiv 53 (\mathrm{mod}\, 97)$;
д) $x^{10} \equiv 25 (\mathrm{mod}\, 53)$;
е) $x^{20} \equiv 15 (\mathrm{mod}\, 61)$.

6. Решите сравнение:

а) $31x^6 \equiv 20 (\mathrm{mod}\, 73)$;
б) $36x^{12} \equiv 16 (\mathrm{mod}\, 79)$;
в) $16x^{18} \equiv 24 (\mathrm{mod}\, 97)$;
г) $12x^{18} \equiv 54 (\mathrm{mod}\, 13)$;
д) $16x^{82} \equiv 32 (\mathrm{mod}\, 17)$;
е) $77x^{77} \equiv 33 (\mathrm{mod}\, 19)$;
ж) $32x^{28} \equiv 50 (\mathrm{mod}\, 61)$;
з) $50x^{50} \equiv 50 (\mathrm{mod}\, 47)$;
и) $3^x \equiv 7 (\mathrm{mod}\, 11)$;
к) $6^x \equiv -3 (\mathrm{mod}\, 13)$;
л) $15^{2x} \equiv -3 (\mathrm{mod}\, 61)$;
м) $8^x \equiv -3 (\mathrm{mod}\, 47)$.

7. Найдите остаток от деления:

а) 100^{300} на 13;
б) 100^{300} на 47;
в) 100^{300} на 41;
г) 200^{400} на 17;
д) 300^{500} на 19;
е) 400^{300} на 47;
ж) 100^{200} на 61;
з) 21^{49} на 97.

8. Найдите остаток от деления:

а) $29^{30^{10}}$ на 71;
б) $49^{10^{20}}$ на 67;
в) $37^{32^{19}}$ на 83;
г) $44^{22^{33}}$ на 61;
д) $55^{66^{77}}$ на 73;
е) $34^{56^{78}}$ на 79;
ж) $33^{333^{3333}}$ на 59;
з) $22^{222^{222}}$ на 53.

9. Найдите все индексы:

а) числа 7 по модулю 13;
б) числа 4 по модулю 7;
в) числа 20 по модулю 17;
г) числа 50 по модулю 19.

10. Найдите:

а) $P_7(12)$;
б) $P_{13}(22)$;
в) $P_{17}(4)$;
г) $P_{19}(11)$;
д) $P_{61}(12)$;
е) $P_{47}(2)$.

11. Через какие точки (x, y) с целыми координатами x и y проходит кривая:

а) $19y = 3x^4 + 22$;
б) $13y = 3x^2 + 20$.

Задачи

1. Составьте таблицу индексов по модулю 19, используя наибольший отрицательный первообразный корень по модулю 19; укажите число всех возможных таблиц индексов по модулю 19.

2. Используя таблицу индексов по модулю p, где $p \in \{37, 47, 61, 67, 89\}$, укажите:

- первообразный корень, по которому построена таблица;
- все первообразные корни по модулю p;
- все классы $\mathbf{x_p}$, такие что $P_p(x) = (p-1)/2$;
- все квадратичные вычеты по модулю p;
- все квадратичные невычеты по модулю p;
- все вычеты 12-й степени по модулю p;
- все невычеты 4-й степени по модулю p.

3. Пусть p_n — n-е простое число, где $n = N - 5\lfloor N/5 \rfloor + 5$, $N \in \{1, 2, 3, \ldots, 25\}$. Пользуясь таблицей индексов по модулю p_n, укажите:

- все первообразные корни по модулю p_n, принадлежащие промежутку $[100, 120]$;
- все квадратичные вычеты по модулю p_n, принадлежащие промежутку $[-10, 10]$;

- все квадратичные невычеты по модулю p_n, принадлежащие промежутку $[-10, 0]$;
- все классы $\mathbf{x}_{p_n}$, такие что $P_{p_n}(x) = \dfrac{p_n - 1}{2}$;
- все числа a, такие что $P_{p_n}(a) = 2$, $a \in [-15, -2]$.

4. Укажите все классы $\mathbf{x}_{43}$, такие что $P_{43}(x) = 7$.

5. Укажите все классы $\mathbf{x}_{47}$, такие что $P_{47}(x) = 23$.

6. Найдите наименьший натуральный первообразный корень по модулю p, $p \in \{71, 79, 83, 97\}$.

7. Найдите показатель, которому принадлежит число a по модулю p, если $a \in \{5, 10, 15, 20\}$, а $p \in \{23, 29, 31, 37, 41, 43\}$.

8. Найдите все вычеты степени 4 по модулю p, $p \in \{11, 13, 17\}$.

9. Найдите все невычеты степени 3 по модулю p, $p \in \{11, 13, 17\}$.

10. Является ли число 2 вычетом степени n по модулю 11, если $n \in \{2, 3, 4, 5, 6, 7, 8, 9, 10\}$?

11. Докажите, что число вычетов степени n в приведенной системе вычетов по модулю p равно δ, где $\delta = (n, p - 1)$.

12. Найдите все индексы числа a по модулю p, если $a \in \{6, 7, 8, 9\}$, а $p \in \{17, 19, 23, 29\}$.

13. Зная, что ind 2 по модулю 29 равен единице, найдите все первообразные корни по модулю 29.

14. Не пользуясь таблицами индексов, найдите: ind 12 по модулю 13; ind 60 по модулю 61.

15. Сколько решений имеет сравнение:

а) $x^{12} \equiv 1 \pmod{77}$;
б) $x^{12} \equiv 1 \pmod{91}$;
в) $x^{12} \equiv 1 \pmod{143}$;
г) $3x^{12} \equiv 31 \pmod{41}$;
д) $x^{15} \equiv 1 \pmod{451}$;
е) $x^{15} \equiv 1 \pmod{287}$;
ж) $x^{15} \equiv 1 \pmod{143}$;
з) $x^{60} \equiv 79 \pmod{97}$;
и) $x^{18} \equiv 1 \pmod{77}$;
к) $x^{18} \equiv 1 \pmod{91}$;
л) $x^{18} \equiv 1 \pmod{143}$;
м) $x^{55} \equiv 17 \pmod{97}$?

16. Решите сравнение:

а) $3^{15}x \equiv 5^{20} \pmod{7}$;
б) $2^{20}x \equiv 4 \pmod{101}$;
в) $3^{20}x \equiv -4 \pmod{29}$;
г) $2x^{13} \equiv 5 \pmod{19}$;
д) $71x^{12} \equiv 10 \pmod{97}$;
е) $27x^{13} \equiv 16 \pmod{79}$;
ж) $14x^{15} \equiv 39 \pmod{61}$;
з) $32x^{333} \equiv 23 \pmod{205}$;
и) $132x^{42} \equiv 51 \pmod{61}$;
к) $156x^{108} \equiv -63 \pmod{101}$;
л) $19x^{25} \equiv 39 \pmod{61}$;
м) $73x^{18} \equiv 17 \pmod{67}$;

н) $27x^{49} \equiv 23 (\mathrm{mod}\, 71)$;
о) $16x^{30} \equiv 18 (\mathrm{mod}\, 73)$;
п) $16x^{35} \equiv 27 (\mathrm{mod}\, 43)$.

17. Решите сравнение:

а) $7(x+5)^{28} \equiv 30 (\mathrm{mod}\, 61)$;
б) $-10(2x-4)^{16} \equiv 17 (\mathrm{mod}\, 31)$;
в) $34(x+45)^{55} \equiv 7 (\mathrm{mod}\, 59)$;
г) $65(x-1)^{14} \equiv 39 (\mathrm{mod}\, 59)$;
д) $3x^2 + 4x + 7 \equiv 0 (\mathrm{mod}\, 31)$;
е) $10^x \equiv 1 (\mathrm{mod}\, 41 \cdot 31)$;
ж) $9x^2 + 45x - 36 \equiv 0 (\mathrm{mod}\, 3 \cdot 23)$;
з) $25x^{35} \equiv -8^{16} (\mathrm{mod}\, 41 \cdot 17)$;
и) $21x^{15} \equiv -2 (\mathrm{mod}\, 11 \cdot 19)$;
к) $3^{15}x^{19} \equiv 7^{17} (\mathrm{mod}\, 29 \cdot 73)$.

18. Для n-го простого числа p_n, где $n = N - 5\lfloor N/5 \rfloor + 10$, $N \in \{1, 2, 3, \ldots, 25\}$, решите сравнение: $1000 \cdot p_{n-1} \cdot p_{n-2} \cdot x^{100p_{n-3}} \equiv 2p_{n-4} (\mathrm{mod}\ p_n)$.

19. Разрешимо ли сравнение $7^{x^2} \equiv 38 (\mathrm{mod}\, 97)$?

20. Найдите остаток от деления:

а) $18^{11^{19}}$ на 23;
б) $34^{333^{333}}$ на 61;
в) $15^{202^{215}}$ на 31;
г) $21^{21^{20}}$ на 47;
д) $27^{48^{30}}$ на 59;
е) $12^{12^{12}}$ на 17.

21. Найдите остаток от деления $21^{30} \cdot 20^{23} \cdot 17^{31}$ на 83.

22. Найдите наибольший отрицательный и наименьший неотрицательный вычеты числа $43^{18} \cdot 39^{22} \cdot 37^{19} - 15 \cdot 59^{95}$ по модулю 291.

23. Для n-го простого числа p_n, где $n = N - 5\lfloor N/5 \rfloor + 5$, $N \in \{1, 2, 3, \ldots, 25\}$, найдите остаток от деления $1000^{p_{n-1}^{p_{n-2}}}$ на p_n.

24. В какой класс вычетов по модулю 79 попадает число 2^{99}?

25. Найдите наименьшее по абсолютной величине число, с которым $35^{747^{606}}$ сравнимо по модулю 43.

26. Вычислите:

а) $P_{2^7 \cdot 11^5 \cdot 47}(7)$;
б) $P_{2^7 \cdot 13^3 \cdot 29}(11)$;
в) $P_{2^6 \cdot 7^3 \cdot 31}(3)$;
г) $P_{2^5 \cdot 11^3 \cdot 41^4}(3)$;
д) $P_{2^7 \cdot 13^3 \cdot 53}(7)$;
е) $P_{2^5 \cdot 3^3 \cdot 89}(125)$.
ж) $P_{2^5 \cdot 3^3 \cdot 83}(-7)$;
з) $P_{2^3 \cdot 3^2 \cdot 83}(49)$.

27. Найдите длину периода десятичной записи дроби:

а) 1/90241; д) 1/1035; и) 5/506;
б) 15/2870; е) 3/595; к) 1/41;
в) 7/1044; ж) 3/1085; л) 1/37;
г) 9/603; з) 7/638; м) $1/41 \cdot 37$.

28. Найдите длину периода g-ичной записи дроби:

а) $\dfrac{30}{2^6 11^3 41^4}$, $g = 3$; в) $\dfrac{15}{2^2 11^{11} 41^{41}}$, $g = 7$;

б) $\dfrac{1}{79 \cdot 83}$ $g = 24$; г) $\dfrac{1}{61 \cdot 89}$ $g = 56$.

29. Дайте характеристику двенадцатиричной записи дроби $\dfrac{165}{73 \cdot 89 \cdot 7560}$.

30. Для n-го простого числа p_n, где $n = N - 5\lfloor N/5 \rfloor + 5$, $N \in \{1,2,3,\ldots,25\}$, найдите длину периода g-ичной записи дроби

$$\frac{1000}{p_1 \cdot p_2 \cdot p_{n-3} \cdot p_{n-2}}, \quad g = p_n.$$

§ 22. Цепные дроби

Цепная дробь $[a_0, a_1, \ldots, a_n, \ldots]$ определяется как формальная сумма

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{\cdots \cfrac{1}{a_n + \cdots}}},$$

где a_0 — некоторое целое число, а все a_n, $n \in \mathbb{N}$ — натуральные числа, причем последнее, если оно существует, отлично от 1.

Рациональные числа $\delta_k = [a_0, a_1, \ldots, a_k] = P_k/Q_k$, $k = 0, 1, \ldots, n, \ldots$, называются *подходящими дробями* к цепной дроби $[a_0, a_1, \ldots, a_n, \ldots]$. Числа a_k, $k = 0, 1, \ldots, n, \ldots$, называются *неполными частными* цепной дроби $[a_0, a_1, \ldots, a_n, \ldots]$, в то время как величины $\alpha_k = [a_k, a_{k+1}, \ldots, a_n, \ldots]$, $k = 0, 1, \ldots, n, \ldots$, называются *полными частными* цепной дроби $[a_0, a_1, \ldots, a_n, \ldots]$.

Например,

$$[-3, 2, 1, 4] = -3 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{4}}}.$$

Несложный подсчет показывает, что

$$[-3, 2, 1, 4] = -\frac{47}{14}.$$

При этом подходящие дроби имеют вид

$$\delta_0 = [-3] = -3, \quad \delta_1 = [-3, 2] = -3 + \frac{1}{2} = -\frac{5}{2},$$

$$\delta_2 = [-3, 2, 1] = -3 + \frac{1}{2 + \frac{1}{1}} = -\frac{8}{3},$$

$$\delta_4 = [-3, 2, 1, 4] = -3 + \frac{1}{2 + \frac{1}{1 + \frac{1}{4}}} = -\frac{47}{14}$$

(обратите внимание на то, что величина $[-3, 2, 1]$ цепной дробью не является!); неполные частные имеют вид $a_0 = -3$, $a_1 = 2$, $a_2 = 1$, $a_3 = 4$; полные частные имеют вид

$$\alpha_0 = [-3, 2, 1, 4] = -3 + \frac{1}{2 + \frac{1}{1 + \frac{1}{4}}} = -\frac{47}{14},$$

$$\alpha_1 = [2, 1, 4] = 2 + \frac{1}{1 + \frac{1}{4}} = \frac{14}{5},$$

$$\alpha_2 = [1, 4] = 1 + \frac{1}{4} = \frac{5}{4}, \quad \alpha_4 = [4] = 4.$$

Свойства цепных дробей

1. Если $\delta_k = P_k/Q_k$, то $P_0 = a_0$, $P_1 = a_1 a_0 + 1$, и $P_n = a_n P_{n-1} + P_{n-2}$ для всех $n \geqslant 2$.
2. Если $\delta_k = P_k/Q_k$, то $Q_0 = 1$, $Q_1 = a_1$, и $Q_n = a_n Q_{n-1} + Q_{n-2}$ для всех $n \geqslant 2$.
3. $P_n Q_{n-1} - P_{n-1} Q_n = (-1)^{n-1}$.
4. $P_n Q_{n-2} - P_{n-2} Q_n = (-1)^n a_n$.
5. $(P_n, Q_n) = 1$.
6. $1 = Q_0 \leqslant Q_1 < Q_2 < \ldots$.
7. Если $P_0 > 1$, то $P_1 > P_2 > P_3 > \ldots$.
8. $\delta_n - \delta_{n-1} = \dfrac{(-1)^{n-1}}{Q_n Q_{n-1}}$.
9. Каждая конечная цепная дробь является рациональным числом, и каждое рациональное число представимо, причем единственным образом, в виде конечной цепной дроби.

10. Каждая бесконечная цепная дробь является иррациональным числом, и каждое иррациональное число представимо, причем единственным образом, в виде бесконечной цепной дроби.
11. Бесконечная цепная дробь является периодической тогда и только тогда, когда она представляет некоторую *квадратическую иррациональность*, то есть иррациональное число, являющееся корнем квадратного трехчлена с целыми коэффициентами.
12. Квадратическая иррациональность

$$\alpha = \frac{P + \sqrt{D}}{Q},$$

где $P, Q, D \in \mathbb{Z}$, $D > 1$, разлагается в чистопериодическую цепную дробь тогда и только тогда, когда $\alpha > 1$ и сопряженная иррациональность

$$\alpha' = \frac{P - \sqrt{D}}{Q}$$

лежит в интервале $(-1, 0)$.

13. $[a_0, a_1, \ldots, a_n, \ldots] = \dfrac{\alpha_n P_{n-1} + P_{n-2}}{\alpha_n Q_{n-1} + Q_{n-2}}$.
14. Если $\alpha = [a_0, a_1, \ldots, a_n, \ldots]$, то

$$\delta_0 < \delta_2 < \ldots < \delta_{2k} < \ldots \leqslant \alpha \leqslant \ldots < \delta_{2k+1} < \ldots < \delta_3 < \delta_1.$$

15. Если $\alpha = [a_0, a_1, \ldots, a_n, \ldots]$, то $|\alpha - \delta_n| \leqslant \dfrac{1}{Q_n Q_{n+1}}$.

Свойства 1 и 2 проверяются непосредственно. Именно, $\delta_0 = a_0 = a_0/1$, то есть $\delta_0 = P_0/Q_0$, где $P_0 = a_0$, $Q_0 = 1$. Аналогично,

$$\delta_1 = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1},$$

то есть $\delta_0 = P_0/Q_0$, где $P_1 = a_0 a_1 + 1$, $Q_1 = a_1$. Далее, δ_2 может быть получено из δ_1 заменой величины a_1 на величину $a_1 + 1/a_2$, то есть

$$\delta_1 = \frac{a_0\left(a_1 + \dfrac{1}{a_2}\right) + 1}{a_1 + \dfrac{1}{a_2}} = \frac{a_2(a_0 a_1 + 1) + a_0}{a_2 a_1 + 1} = \frac{a_2 P_1 + P_0}{a_2 Q_1 + Q_0},$$

или, что то же, $\delta_2 = P_2/Q_2$, где $P_2 = a_2 P_1 + P_0$, $Q_2 = a_2 Q_1 + Q_0$. Предполагая, что $\delta_{n-1} = P_{n-1}/Q_{n-1}$, где $P_{n-1} = a_{n-1} P_{n-2} + P_{n-3}$, $Q_{n-1} =$

$= a_{n-1}Q_{n-2} + Q_{n-3}$, и замечая, что δ_n может быть получено из δ_{n-1} заменой величины a_{n-1} на величину $a_{n-1} + 1/a_n$, мы получим, что

$$\delta_n = \frac{\left(a_{n-1} + \dfrac{1}{a_n}\right)P_{n-1} + P_{n-2}}{\left(a_{n-1} + \dfrac{1}{a_n}\right)Q_{n-1} + Q_{n-2}} =$$

$$= \frac{a_n(a_{n-1}P_{n-2} + P_{n-3}) + P_{n-2}}{a_n(a_{n-1}Q_{n-2} + Q_{n-3}) + Q_{n-2}} = \frac{a_nP_{n-1} + P_{n-2}}{a_nQ_{n-1} + Q_{n-2}},$$

или, что то же, $\delta_n = P_n/Q_n$, где $P_n = a_nP_{n-1} + P_{n-2}$, $Q_n = a_nQ_{n-1} + Q_{n-2}$. Доказательства остальных свойств можно найти, например, в [3], [31].

Примеры решения задач

1. Разложите в цепную дробь: $173/281$; $(1 - 3\sqrt{5})/2$.

Решение. Запишем для чисел 173 и 281 алгоритм Евклида:

$173 = 281 \cdot 0 + 173$;
$281 = 173 \cdot 1 + 108$;
$173 = 108 \cdot 1 + 65$;
$108 = 65 \cdot 1 + 43$;
$65 = 43 \cdot 1 + 22$;
$43 = 22 \cdot 1 + 21$;
$22 = 21 \cdot 1 + 1$;
$21 = 1 \cdot 21 + 0$.

Теперь нетрудно убедиться в том, что

$$\frac{173}{281} = 0 + \frac{1}{\dfrac{281}{173}}, \quad \frac{281}{173} = 1 + \frac{1}{\dfrac{173}{108}}, \quad \ldots,$$

$$\frac{65}{22} = 1 + \frac{1}{\dfrac{43}{21}}, \quad \frac{43}{21} = 1 + \frac{1}{\dfrac{22}{21}}, \quad \frac{22}{21} = 1 + \frac{1}{21}.$$

Следовательно,

$$\frac{173}{281} = 0 + \cfrac{1}{1 + \cfrac{1}{\ldots + \cfrac{1}{21}}},$$

или, что то же, $173/281 = [0, 1, 1, 1, 1, 1, 1, 21]$.

Таким образом, для того, чтобы получить разложение обыкновенной дроби $P/Q \notin \mathbb{Z}$ в конечную цепную дробь, достаточно выписать

алгоритм Евклида для чисел P и Q, и взять столбец полученных при этом целых частных в качестве неполных частных искомой цепной дроби.

Для разложения числа $\dfrac{(1-3\sqrt{5})}{2}$ проведем рассуждения, обобщающие алгоритм Евклида.

Поскольку $6 < \sqrt{45} < 7$, то для числа $\dfrac{1-3\sqrt{5}}{2}$, равного $\dfrac{1-\sqrt{45}}{2}$, имеет место оценка $-3 < \dfrac{1-3\sqrt{5}}{2} < -2{,}5$, то есть

$$a_0 = \left\lfloor \frac{1-3\sqrt{5}}{2} \right\rfloor = -3.$$

Тогда $\alpha_0 = \dfrac{1-3\sqrt{5}}{2} = -3 + \dfrac{1}{\alpha_1}$, где

$$\frac{1}{\alpha_1} = \frac{1-3\sqrt{5}}{2} - (-3) = \frac{7-3\sqrt{5}}{2}.$$

Следовательно,

$$\alpha_1 = \frac{2}{7-3\sqrt{5}} = \frac{2(7+3\sqrt{5})}{(7-3\sqrt{5})(7+3\sqrt{5})} = \frac{2(7+3\sqrt{5})}{49-45} = \frac{2(7+3\sqrt{5})}{4} = \frac{(7+3\sqrt{5})}{2}.$$

Поскольку $6{,}5 < \dfrac{(7+3\sqrt{5})}{2} < 7$, то

$$a_1 = \left\lfloor \frac{(7+3\sqrt{5})}{2} \right\rfloor = 6, \quad \text{и} \quad \alpha_1 = \frac{7+3\sqrt{5}}{2} = 6 + \frac{1}{\alpha_2},$$

где $\dfrac{1}{\alpha_2} = \dfrac{7+3\sqrt{5}}{2} - 6 = \dfrac{-5+3\sqrt{5}}{2}$.

Следовательно,

$$\alpha_2 = \frac{2}{-5+3\sqrt{5}} = \frac{2(-5-3\sqrt{5})}{(-5+3\sqrt{5})(-5-3\sqrt{5})} = \frac{2(-5-3\sqrt{5})}{25-45} = \frac{2(5+3\sqrt{5})}{20} = \frac{(5+3\sqrt{5})}{10}.$$

Поскольку $1{,}1 < \dfrac{(5+3\sqrt{5})}{2} < 1{,}2$, то

$$a_2 = \left\lfloor \frac{(5+3\sqrt{5})}{10} \right\rfloor = 1, \quad \text{и} \quad \alpha_2 = \frac{5+3\sqrt{5}}{10} = 1 + \frac{1}{\alpha_3},$$

где $\dfrac{1}{\alpha_3} = \dfrac{5+3\sqrt{5}}{10} - 1 = \dfrac{-5+3\sqrt{5}}{10}$.

Следовательно,

$$\alpha_3 = \frac{10}{-5+3\sqrt{5}} = \frac{10(-5-3\sqrt{5})}{(-5+3\sqrt{5})(-5-3\sqrt{5})} = \frac{10(-5-3\sqrt{5})}{25-45} =$$
$$= \frac{10(5+3\sqrt{5})}{20} = \frac{(5+3\sqrt{5})}{2}.$$

Поскольку $5{,}5 < \dfrac{(5+3\sqrt{5})}{2} < 6$, то

$$a_3 = \left\lfloor \frac{(5+3\sqrt{5})}{2} \right\rfloor = 5, \quad \text{и} \quad \alpha_3 = \frac{5+3\sqrt{5}}{2} = 5 + \frac{1}{\alpha_4},$$

где $\dfrac{1}{\alpha_4} = \dfrac{5+3\sqrt{5}}{2} - 5 = \dfrac{-5+3\sqrt{5}}{2}$.

Таким образом,

$$\frac{1}{\alpha_4} = \frac{1}{\alpha_2},$$

то есть $\alpha_4 = \alpha_2$. Отсюда следует, что строка, соответствующая α_4, будет дублировать строку, соответствующую α_2:

$$\alpha_4 = \frac{5+3\sqrt{5}}{10} = 1 + \frac{1}{\alpha_5},$$

где $1/\alpha_5 = \dfrac{-5+3\sqrt{5}}{10}$. В частности, $a_4 = a_2$, и $1/\alpha_5 = 1/\alpha_3$, то есть $\alpha_5 = \alpha_3$. Продолжая рассуждения, получим, что $a_5 = a_3$ и $1/\alpha_6 = 1/\alpha_4$, то есть $\alpha_6 = \alpha_4$; $a_6 = a_4$ и $1/\alpha_7 = 1/\alpha_5$, то есть $\alpha_7 = \alpha_5$, и т. д. Следовательно,

$$\frac{1-3\sqrt{5}}{2} = [a_0, a_1, a_2, a_3, a_4, \ldots] = [-3, 6, 1, 5, 1, 5, 1, 5, \ldots] =$$
$$= [-3, 6, (1, 5)].$$

Формализуя проведенные рассуждения, мы получим алгоритм разложения числа $\dfrac{1-3\sqrt{5}}{2}$ в цепную дробь: начиная с $\alpha_0 = \dfrac{1-3\sqrt{5}}{2}$,

выписываем цепочку равенств, связывающих числа α_i, $a_i = \lfloor \alpha_i \rfloor$ и $\dfrac{1}{\alpha_{i+1}} = \alpha_i - a_i$:

$$\alpha_0 = \frac{1-3\sqrt{5}}{2} = -3 + \frac{1}{\alpha_1}, \text{ где } \frac{1}{\alpha_1} = \frac{7-3\sqrt{5}}{2};$$

$$\alpha_1 = \frac{7+3\sqrt{5}}{2} = 6 + \frac{1}{\alpha_2}, \text{ где } \frac{1}{\alpha_2} = \frac{-5+3\sqrt{5}}{2};$$

$$\alpha_2 = \frac{5+3\sqrt{5}}{10} = 1 + \frac{1}{\alpha_3}, \text{ где } \frac{1}{\alpha_3} = \frac{-5+3\sqrt{5}}{10};$$

$$\alpha_3 = \frac{5+3\sqrt{5}}{2} = 5 + \frac{1}{\alpha_4}, \text{ где } \frac{1}{\alpha_4} = \frac{-5+3\sqrt{5}}{2}.$$

Отслеживая правые части получаемых равенств, мы останавливаемся после первого совпадения величин $1/\alpha_k$ и $1/\alpha_{k+s}$, и выписываем значение $[a_0, a_1, a_2, \ldots]$ соответствующей цепной дроби, раскрывая скобку периода после первого совпадения, и закрывая ее после второго: $[a_0, a_1, a_2, \ldots, a_k, (a_{k+1}, \ldots, a_{k+s})]$. Именно,

$$\frac{1-3\sqrt{5}}{2} = [-3, 6, (1, 5)]. \qquad \triangleright$$

2. Найдите значение цепной дроби $[1, 2, 3, 1, 1, 5]$.

Решение. Для нахождения значения цепной дроби $[1, 2, 3, 1, 1, 5]$ вспомним, что $[a_0, a_1, \ldots, a_n] = P_n/Q_n$, где

$$P_0 = a_0, \quad Q_0 = 1, \quad P_1 = a_1 a_0 + 1, \quad Q_1 = a_1,$$

и

$$P_n = a_n P_{n-1} + P_{n-2}, \quad Q_n = a_n Q_{n-1} + Q_{n-2}$$

для всех $n \geqslant 2$. Для упрощения вычислений удобно добавить в рассмотрение значения

$$P_{-2} = 0, \quad P_{-1} = 1, \quad Q_{-2} = 1, \quad Q_{-1} = 0.$$

Тогда рекуррентные формулы $P_n = a_n P_{n-1} + P_{n-2}$, $Q_n = a_n Q_{n-1} + Q_{n-2}$ будут иметь место для любого $n \geqslant 0$. Результаты вычислений удобно оформить в виде табл. 11.

После вычислений таблица примет вид табл. 12.

Таким образом, $[1, 2, 3, 1, 1, 5] = 128/89$. $\triangleright$

Таблица 11

n	−2	−1	0	1	2	3	4	5
a_n			1	2	3	1	1	5
P_n	0	1						
Q_n	1	0						

Таблица 12

n	−2	−1	0	1	2	3	4	5
a_n			1	2	3	1	1	5
P_n	0	1	1	3	10	13	23	128
Q_n	1	0	1	2	7	9	16	89

3. Найдите значение цепной дроби $[(1)]$.

Решение. Для нахождения значения α цепной дроби

$$[(1)] = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \ldots}}$$

заметим, что в этом случае $\alpha = 1 + 1/\alpha$. После очевидных преобразований мы получим уравнение $\alpha^2 - \alpha - 1 = 0$, корнями которого являются числа $\dfrac{1 \pm \sqrt{5}}{2}$. Поскольку $\lfloor \alpha \rfloor = a_0 = 1$, то $\alpha = \dfrac{1 + \sqrt{5}}{2}$. ▷

4. Найдите значение цепной дроби $[(1, 1, 1, 4)]$.

Решение. Для нахождения значения цепной дроби $[(1, 1, 1, 4)]$ заметим, что в этом случае нулевое полное частное $\alpha_0 = [a_0, a_1, a_2, a_3, a_4, a_5, \ldots] = [1, 1, 1, 4, 1, 1, \ldots]$ совпадает с четвертым полным частным $\alpha_4 = [a_4, a_5, a_6, a_7, a_8, a_9, \ldots] = [1, 1, 1, 4, 1, 1, \ldots]$. Следовательно, для нахождения значения $\alpha = \alpha_0$ цепной дроби $[(1, 1, 1, 4)]$ можно воспользоваться формулой

$$\alpha = \frac{\alpha_n P_{n-1} + P_{n-2}}{\alpha_n Q_{n-1} + Q_{n-2}}$$

при $n = 4$:

$$\alpha = \frac{\alpha P_3 + P_2}{\alpha Q_3 + Q_2}.$$

Таблица 13

а)

n	−2	−1	0	1	2	3
a_n			1	1	1	4
P_n	0	1	1	2	3	14
Q_n	1	0	1	1	2	9

б)

n	−2	−1	0	1	2
a_n			1	2	1
P_n	0	1	1	3	4
Q_n	1	0	1	2	3

При этом значения P_3, P_2, Q_3 и Q_2 можно найти, используя табл. 13 *а*). Таким образом,

$$\alpha = \frac{14\alpha + 3}{9\alpha + 2}.$$

После очевидных преобразований мы получим уравнение

$$9\alpha^2 - 12\alpha - 3 = 0$$

или, что то же, уравнение $3\alpha^2 - 4\alpha - 1 = 0$, корнями которого являются числа $\dfrac{2 \pm \sqrt{7}}{3}$. Поскольку $\lfloor \alpha \rfloor = a_0 = 1$, то $\alpha = \dfrac{2 + \sqrt{7}}{3}$. ▷

5. Найдите значение цепной дроби $[1, 2, 1, (1, 1, 1, 4)]$.

Решение. Для нахождения значения цепной дроби $[1, 2, (1, 1, 1, 4)]$ сначала найдем значение соответствующей чисто-периодической цепной дроби $[(1, 1, 1, 4)]$.

Это было сделано в предыдущей задаче: мы получили, что

$$[(1, 1, 1, 4)] = \frac{2 + \sqrt{7}}{3}.$$

Заметим, что для цепной дроби $[1, 2, 1, (1, 1, 1, 4)]$ величина $[(1, 1, 1, 4)]$ является третьим полным частным: $[(1, 1, 1, 4)] = \alpha_3$.

Следовательно, для нахождения значения α цепной дроби $[1, 2, 1, (1, 1, 1, 4)]$ можно воспользоваться формулой

$$\alpha = \frac{\alpha_n P_{n-1} + P_{n-2}}{\alpha_n Q_{n-1} + Q_{n-2}}$$

при $n = 3$:

$$\alpha = \frac{\alpha_3 P_2 + P_1}{\alpha_3 Q_2 + Q_1}.$$

При этом значения P_2, P_1, Q_2 и Q_1 можно найти, используя табл. 13 *б*).

Таким образом,

$$\alpha = \frac{\frac{2+\sqrt{7}}{3}\cdot 4 + 3}{\frac{2+\sqrt{7}}{3}\cdot 3 + 2}.$$

После очевидных преобразований мы получим окончательный результат: $\alpha = \dfrac{40-\sqrt{7}}{27}$. ▷

Упражнения

1. Разложите в цепную дробь числа:

а) 312/175; в) 72/103; д) −1000/3333;
б) −19/15; г) 3885/2306; е) 27899/36823.

2. Разложите в цепную дробь числа:

а) $\sqrt{11}$;
б) $-\sqrt{5}$;
в) $3\sqrt{3}$;
г) $1-2\sqrt{6}$;
д) $\dfrac{2+\sqrt{13}}{5}$;
е) $\dfrac{2-\sqrt{13}}{5}$;
ж) $\dfrac{1+\sqrt{5}}{2}$;
з) $\dfrac{7+2\sqrt{3}}{4}$.
и) $\dfrac{2+2\sqrt{11}}{2}$;
к) $\dfrac{\sqrt{37}-118}{4}$.

3. Найдите значение цепной дроби:

а) [1, 2, 3, 1, 5]; в) [1, 1, 2, 1, 2, 1, 7];
б) [4, 2, 2, 1, 1, 2]; г) [1, 2, 3, 4, 5].

4. Найдите значение цепной дроби:

а) [(2)]; к) [1, 1, (1, 4)]; у) [−1, (2, 2, 1)];
б) [2, (1)]; л) [−1, 1, 5, (8)]; ф) [−4, (1, 3, 1)];
в) [1, (1, 2)]; м) [1, 5, 2, (3)]; х) [−1, (3, 1, 1)];
г) [0, 2, (8)]; н) [−2, (1, 2, 2)]; ц) [3, 1, 2, 3, (4)];
д) [5, (5, 10)]; о) [6, (2, 2, 12)]; ч) [−5, 1, 4, (10, 5)];
е) [(2, 3, 1)]; п) [1, 3, 4, (1)]; ш) [−1, 2, (2, 1, 1, 1)];
ж) [(1, 4, 1)]; р) [−3, 1, 3(4)]; щ) [−1, 1, 2, (8, 1, 3)];
з) [(2, 1, 1, 4)]; с) [1, 1, (1, 3)]; э) [7, (1, 1, 4, 1, 1, 14)].
и) [1, (2, 1, 4)]; т) [−4, 9, (1, 8)];

Задачи

1. Разложите в цепную дробь числа:

а) 1368/779; в) −1116/899; д) 268/187;
б) −779/1368; г) −424/189; е) 37/328.

2. Разложите в цепную дробь числа:

а) $\sqrt{2}$; е) $\sqrt{17}$; м) $\sqrt{53}$; т) $2\sqrt{6}$;
б) $\sqrt{6}$; ж) $\sqrt{19}$; н) $\sqrt{57}$; у) $5\sqrt{2}$;
в) $\sqrt{10}$; з) $\sqrt{22}$; о) $\sqrt{59}$; ф) $2\sqrt{7}$;
г) $\sqrt{13}$; и) $\sqrt{26}$; п) $\sqrt{65}$; х) $6\sqrt{2}$.
д) $\sqrt{15}$; к) $\sqrt{30}$; р) $2\sqrt{2}$;
л) $\sqrt{37}$; с) $2\sqrt{3}$;

3. Разложите в цепную дробь числа:

а) $\sqrt{21}$; в) $\sqrt{23}$; д) $\sqrt{31}$; ж) $\sqrt{41}$;
б) $-\sqrt{21}$; г) $-\sqrt{23}$; е) $-\sqrt{31}$; з) $-\sqrt{41}$.

4. Разложите в цепную дробь числа:

а) $\frac{1-\sqrt{2}}{3}$; ж) $\frac{2-\sqrt{15}}{11}$; н) $\frac{\sqrt{65}-1}{4}$; у) $\frac{1+\sqrt{13}}{5}$;
б) $\frac{1+\sqrt{2}}{3}$; з) $\frac{2+\sqrt{15}}{11}$; о) $\frac{\sqrt{37}-15}{4}$; ф) $\frac{5+\sqrt{2}}{2}$;
в) $\frac{3+\sqrt{5}}{2}$; и) $\frac{1+\sqrt{26}}{5}$; п) $\frac{6+\sqrt{26}}{5}$; х) $\frac{2-\sqrt{11}}{2}$;
г) $\frac{3-\sqrt{5}}{2}$. к) $\frac{1-\sqrt{26}}{5}$; р) $\frac{\sqrt{53}-2}{7}$; ц) $\frac{1+\sqrt{7}}{5}$;
д) $\frac{2+\sqrt{17}}{13}$; л) $\frac{2+\sqrt{11}}{2}$; с) $\frac{9+\sqrt{21}}{10}$; ч) $\frac{1-\sqrt{13}}{5}$;
е) $\frac{2-\sqrt{17}}{13}$; м) $\frac{1-\sqrt{7}}{5}$; т) $\frac{3+\sqrt{2}}{2}$; ш) $\frac{3+\sqrt{37}}{4}$.

5. Разложите в цепную дробь числа:

а) $\frac{1+3\sqrt{2}}{2}$; г) $\frac{1-3\sqrt{5}}{2}$; ж) $\frac{2-2\sqrt{6}}{5}$; к) $\frac{6-5\sqrt{2}}{7}$;
б) $\frac{1-3\sqrt{2}}{2}$; д) $\frac{1+2\sqrt{6}}{5}$; з) $\frac{2+2\sqrt{6}}{5}$; л) $\frac{-15-6\sqrt{2}}{8}$;
в) $\frac{1+3\sqrt{5}}{2}$; е) $\frac{1+3\sqrt{3}}{2}$; и) $\frac{6+2\sqrt{2}}{7}$; м) $\frac{6\sqrt{2}-15}{8}$.

6. Разложите в цепную дробь числа:

а) $\dfrac{\sqrt{2210}-13}{13}$; б) $\dfrac{169+\sqrt{63005}}{158}$; в) $\dfrac{1170+2\sqrt{93637}}{232}$.

7. Найдите значение конечной цепной дроби:

а) $[1, 2, 3, 4, 6]$;
б) $[-2, 111, 2, 1, 3]$;
в) $[-2, 3, 3, 10]$;
г) $[-1, 2, 3, 10]$;
д) $[-2, 1, 3, 7]$;
е) $[-3, 1, 3, 9, 5]$;
ж) $[1, 2, 3, 4, 6]$;
з) $[0, 8, 1, 6, 2, 2]$.

8. Найдите значение бесконечной цепной дроби:

а) $= [1, (2)]$;
б) $= [2, (4)]$;
в) $= [3, (6)]$;
г) $= [4, (8)]$;
д) $= [5, (10)]$;
е) $= [6, (12)]$;
ж) $= [7, (14)]$;
з) $= [8, (16)]$;
и) $= [2, (1, 4)]$;
к) $= [2, (2, 4)]$;
л) $= [3, (1, 6)]$;
м) $= [3, (2, 6)]$;
н) $= [3, (3, 6)]$;
о) $= [4, (1, 8)]$;
п) $= [4, (2, 8)]$;
р) $[3, (10, 5)]$;
с) $[3, (1, 5)]$;
т) $[3, (4, 1)]$;
у) $[5, (2, 10)]$;
ф) $[-3, 6, (1, 5)]$.

9. Найдите значение бесконечной цепной дроби:

а) $[0, 1, (1, 6)]$;
б) $[-3, (1, 3, 2)]$;
в) $[1, (1, 6, 1)]$;
г) $[1, (1, 3, 3)]$;
д) $[2, (4, 1, 1)]$;
е) $[-3, 8, 1, (16, 2)]$;
ж) $[-3, 1, 9, (5, 10)]$;
з) $[-5, 1, 4, (10, 5)]$;
и) $[-1, 1, 4, (1, 6)]$;
к) $[-1, 5, (1, 1, 4)]$;
л) $[4, (1, 3, 1, 8)]$;
м) $[5, (3, 2, 3, 1)]$;
н) $[4, (1, 3, 1, 8)]$;
о) $[5, (3, 2, 3, 10)]$;
п) $[1, (2, 1, 1, 1)]$;
р) $[-1, 1, 2, (8, 1, 3)]$;
с) $[-5, 4, (1, 8, 1, 3)]$;
т) $[7, (3, 1, 1, 3, 14)]$;
у) $[-7, 1, 1, 1, 1, (2, 12, 1)]$;
ф) $[4, (1, 1, 2, 1, 1, 8)]$.

10. Найдите значение бесконечной цепной дроби:

а) $[-1, 1, 5, 1, (1, 1, 6)]$;
б) $[0, (1, 3, 1, 4, 3, 1)]$;
в) $[4, (2, 1, 3, 1, 2, 8)]$;
г) $[7, (1, 2, 7, 2, 1, 14)]$;
д) $[2, (1, 1, 1, 1, 1, 3)]$;
е) $[4, (1, 2, 4, 2, 1, 8)]$;
ж) $[-5, 2, (2, 1, 1, 8, 1, 1)]$;
з) $[2, (1, 1, 1, 1, 1, 1, 6)]$;

и) $[-2, 2, (1, 1, 1, 3, 1, 1)]$;
к) $[7, (11111, 2, 7, 2, 1, 1, 4)]$;
л) $[2, (1, 1, 1, 1, 1, 1, 8, 1)]$;
м) $[-1, 1, 2, (26, 4, 2, 1, 2, 4)]$;
н) $[5, (1, 1, 3, 5, 3, 1, 1, 10)]$;
о) $[2, (1, 1, 1, 12, 1, 1, 1, 2)]$;
п) $[-6, 2, (3, 5, 3, 1, 1, 10, 1, 1)]$;
р) $[-3, 15, (1, 1, 5, 2, 1, 1, 2, 3, 2, 1, 2, 5, 1, 1, 14)]$.

11. Запишите уравнение, один из корней которого разложим в цепную дробь $[(2, 3, 1)]$.

12. Определите вид цепной дроби, в которую раскладывается число:

а) 12;
б) $\frac{171}{281}$;
в) $\frac{1-3\sqrt{5}}{2}$;
г) $\frac{1+\sqrt{26}}{5}$;
д) π;
е) $\frac{1-2\sqrt[5]{2}}{2}$;
ж) $17.(3)$;
з) $\ln 3$;
и) $\frac{18+\sqrt{401}}{11}$.

13. Найдите величину цепной дроби $[0, 1, (n, 1, 2)]$ для $n = N - 4\lfloor N/4 \rfloor + 5$, где $N \in \{1, 2, 3, \ldots, 25\}$.

14. Найдите величину цепной дроби $[-1, (n, 2n)]$ для $n = N - 4\lfloor N/4 \rfloor + 5$, где $N \in \{1, 2, 3, \ldots, 25\}$.

§ 23. Применения цепных дробей

Цепные дроби имеют многочисленные применения в теории чисел.

I. Прежде всего, они успешно используются для *приближения действительных чисел рациональными*, давая при этом *наилучшие приближения*.

Напомним (см. [3]), что рациональное число a/b называется *наилучшим приближением* к действительному числу α, если не существует рационального числа x/y со знаменателем $x \leqslant b$, которое было бы ближе к α, чем a/b. Другими словами, если a/b — наилучшее приближение к α, то условие $|\alpha - x/y| < |\alpha - a/b|$ выполняется только для рационального числа x/y со знаменателем $y > b$.

Оказывается, *любая подходящая дробь* $\delta_k = [a_0, a_1, \ldots, a_k]$, $k = 1, 2, \ldots$, *является наилучшим приближением к действительному числу* $\alpha = [a_0, a_1, \ldots, a_n, \ldots]$.

В основе практических применений этого утверждения лежит формула

$$|\alpha - \delta_n| \leqslant |\delta_{n+1} - \delta_n| = \frac{1}{Q_{n+1}Q_n}.$$

Для нахождения рационального приближения числа α с указанной точностью Δ мы рассматриваем знаменатели $Q_0, Q_1, \ldots, Q_n, Q_{n+1}, \ldots$ подходящих дробей $\delta_0, \delta_1, \ldots \delta_n, \delta_{n+1}, \ldots$ разложения $[a_0, a_1, \ldots, a_n, a_{n+1}, \ldots]$

числа α в цепную дробь. Как только будет выполнено соотношение $Q_nQ_{n+1} \geqslant \Delta^{-1}$, мы останавливаемся, выбирая в качестве искомого приближения n-ую подходящую дробь δ_n: $\alpha \approx \delta_n$, причем $|\alpha - \delta_n| \leqslant \Delta$.

При этом подходящие дроби $\delta_0, \delta_2, \ldots$ с четными индексами дают приближения числа α с недостатком, тогда как подходящие дроби $\delta_1, \delta_3, \ldots$ с нечетными индексами дают приближения числа α с избытком.

II. Поскольку числители и знаменатели подходящих дробей взаимно просты, то цепные дроби можно использовать для *сокращения обыкновенных дробей*: разложив дробь a/b в конечную цепную дробь $[a_0, a_1, \ldots, a_n]$ и найдя затем значение полученной дроби, мы получим равенство

$$\frac{a}{b} = \frac{P_n}{Q_n},$$

где $(P_n, Q_n) = 1$.

III. Цепные дроби можно использовать и при *решении неопределенных уравнений* $ax + by = c$ первой степени с двумя неизвестными.

Нетрудно проверить, что *уравнение* $ax + by = c$ *с целыми коэффициентами* a, b *и с разрешимо в целых числах, если и только если* $(a, b)|c$; *в этом случае мы имеем бесконечно много решений вида*

$$x = x_0 \pm \frac{b}{(a,b)}t, \quad y = y_0 \mp \frac{a}{(a,b)}t,$$

где t *— произвольное целое число, а пара* (x_0, y_0) *— некоторое частное решение уравнения* $ax + by = c$. Подробное доказательство этого факта можно найти, например, в [28]. Таким образом, нахождение всех решений уравнения $ax + by = c$ (если они существуют) сводится к поиску его частного решения (x_0, y_0).

Считая, что $(a, b) = 1$ (в случае разрешимости уравнения $ax + by = c$ мы можем поделить все три его коэффициента на число (a, b)), мы разложим дробь a/b в конечную цепную дробь $[a_0, a_1, \ldots, a_n]$. Так как $P_sQ_{s-1} - Q_sP_{s-1} = (-1)^{s-1}$, то при $s = n$ мы получим соотношение $P_nQ_{n-1} - Q_nP_{n-1} = (-1)^{n-1}$. Поскольку $a/b = P_n/Q_n$ и $(a, b) = 1$, то $a = P_n$ и $b = Q_n$, то есть $aQ_{n-1} - bP_{n-1} = (-1)^{n-1}$. Домножая каждое слагаемое последнего равенства на число $(-1)^{n-1}c$, мы получим соотношение

$$a((-1)^{n-1}c \cdot Q_{n-1}) + b((-1)^n c \cdot P_{n-1}) = c,$$

то есть найдем частное решение $(x_0, y_0) = ((-1)^{n-1}c \cdot Q_{n-1}), (-1)^n c \cdot P_{n-1})$ уравнения $ax+by = c$. Таким образом, все решения уравнения $ax+by = c$ могут быть получены теперь по формуле $x = x_0 \pm bt$, $y = y_0 \mp at$, где $t \in \mathbb{Z}$.

IV. С помощью цепных дробей можно решать и другие неопределенные уравнения, в частности, *уравнение Пелля* $x^2 - Dy^2 = \pm 1$, где D — натуральное число, не являющееся полным квадратом.

Для решения уравнения $x^2 - Dy^2 = \pm 1$ разложим число $\sqrt{D}$ в цепную дробь. Известно (см. [3]), что данное разложение имеет вид

$$\sqrt{D} = [a_0, (a_1, a_1, \ldots, a_{k-1}, 2a_0)],$$

то есть полученная цепная дробь является периодической. Пусть k — длина периода указанной цепной дроби.

Нетрудно доказать (см. [3]), что все натуральные решения уравнения $x^2 - Dy^2 = 1$ могут быть найдены по формулам $x = P_{kn-1}$, $y = Q_{kn-1}$, где $n \in \mathbb{N}$, причем kn — четно. Другими словами, уравнение $x^2 - Dy^2 = 1$ имеет бесконечно много решений.

Аналогично, все натуральные решения уравнения $x^2 - Dy^2 = -1$ могут быть найдены по формулам $x = P_{kn-1}$, $y = Q_{kn-1}$, где $n \in \mathbb{N}$, причем kn — нечетно. В этом случае $x^2 - Dy^2 = -1$ уравнение не имеет решений при четном k.

V. Наконец, цепные дроби можно использовать и *при решении сравнений* $ax \equiv b (\mathrm{mod}\, n)$ *первой степени с неизвестной величиной.*

Считая, что $(a, n) = 1$, мы разложим дробь n/a в конечную цепную дробь $[a_0, a_1, \ldots, a_k]$. Так как $P_sQ_{s-1} - Q_sP_{s-1} = (-1)^{s-1}$, то при $s = k$ мы получим соотношение $P_kQ_{k-1} - Q_kP_{k-1} = (-1)^{k-1}$. Поскольку $n/a = P_k/Q_k$ и $(a, n) = 1$, то $n = P_k$ и $a = Q_k$, то есть $nQ_{k-1} - aP_{k-1} = (-1)^{k-1}$. Домножая каждое слагаемое последнего равенства на число $(-1)^{k-1}b$, мы получим соотношение $n((-1)^{k-1}b \cdot Q_{k-1}) + a((-1)^k b \cdot P_{k-1}) = b$. Отсюда следует, что $a((-1)^k b \cdot P_{k-1}) \equiv b (\mathrm{mod}\, n)$, то есть $x \equiv (-1)^k \cdot b \cdot P_{k-1} (\mathrm{mod}\, n)$ — искомое решение сравнения $ax \equiv b (\mathrm{mod}\, n)$.

Примеры решения задач

1. Найдите рациональное приближение числа $-\sqrt{15}$ с точностью $\Delta = 10^{-3}$. Укажите, с избытком или с недостатком полученное приближение.

Решение. Разложим число $-\sqrt{15}$ в цепную дробь:

$$\alpha_0 = -\sqrt{15} = -4 + \frac{1}{\alpha_1}, \text{ где } \frac{1}{\alpha_1} = 4 - \sqrt{15};$$

$$\alpha_1 = 4 + \sqrt{15} = 7 + \frac{1}{\alpha_2}, \text{ где } \frac{1}{\alpha_2} = -3 + \sqrt{15};$$

$$\alpha_2 = \frac{3 + \sqrt{15}}{6} = 1 + \frac{1}{\alpha_3}, \text{ где } \frac{1}{\alpha_3} = \frac{-3 + \sqrt{15}}{6};$$

$$\alpha_3 = 3 + \sqrt{15} = 6 + \frac{1}{\alpha_4}, \text{ где } \frac{1}{\alpha_4} = -3 + \sqrt{15}.$$

Таблица 14

n	−2	−1	0	1	2	3	4
a_n			−4	7	1	6	1
P_n	0	1					
Q_n	1	0	1	7	8	55	63

Таблица 15

n	−2	−1	0	1	2	3	4
a_n			−4	7	1	6	1
P_n	0	1	−4	−27	−31	−213	−234
Q_n	1	0	1	7	8	55	63

Таким образом, $-\sqrt{15} = [-4, 7, (1, 6)]$.

Найдем наименьший индекс n, для которого выполняется соотношение $Q_{n+1} \cdot Q_n \geqslant 1/\Delta = 10^3$. Для этого используем табл. 14, заполняя в ней сначала только строку, соответствующую знаменателям подходящих дробей.

Поскольку $1 \cdot 7 < 10^3$, $7 \cdot 8 < 10^3$ и $8 \cdot 55 < 10^3$, в то время как $55 \cdot 63 > 10^3$, то мы остановимся на $Q_4 = 63$. Таким образом, $n = 3$, и искомым приближением числа $-\sqrt{15}$ будет третья подходящая дробь $\delta_3 = P_3/Q_3$. Это приближение является приближением с избытком, поскольку число 3 нечетно. Работа по вычислению P_3 приводит к табл. 15.

Таким образом, $\alpha \approx -213/55$ с точностью 10^{-3}, причем это приближение является приближением с избытком. ▷

2. Найдите наилучшее приближение числа 1315/406 с избытком дробью a/b со знаменателем, не превосходящим 100.

Решение. Разложим число 1315/406 в цепную дробь:

$1315 = 406 \cdot 3 + 97;$

$406 = 97 \cdot 4 + 18;$

$97 = 18 \cdot 5 + 7;$

$18 = 7 \cdot 2 + 4;$

$7 = 4 \cdot 1 + 3;$

$4 = 3 \cdot 1 + 1;$

$3 = 1 \cdot 3 + 0.$

Таблица 16

n	−2	−1	0	1	2	3	4	5
a_n			3	4	5	2	1	1
P_n	0	1						
Q_n	1	0	1	4	21	46	67	113

Таблица 17

n	−2	−1	0	1	2	3	4	5
a_n			3	4	5	2	1	2
P_n	0	1	3	13	68	149		
Q_n	1	0	1	4	21	46	67	113

Таким образом, $1315/406 = [3, 4, 5, 2, 1, 1, 3]$.

Найдем подходящую дробь с нечетным индексом, обладающую наибольшим знаменателем, не превосходящим 100. Для этого используем стандартную таблицу, заполняя в ней сначала только строку, соответствующую знаменателям подходящих дробей. Остановившись на первом элементе строки, большем ста, мы получим табл. 16.

Таким образом, наилучшим приближением числа 1315/406 дробью a/b со знаменателем, не превосходящим 100, будет подходящая дробь δ_4. Однако данное приближение является приближением с недостатком в силу четности индекса 4. Поэтому наилучшим приближением числа 1315/406 с избытком дробью a/b со знаменателем, не превосходящим 100, будет предыдущая подходящая дробь $\delta_3 = P_3/Q_3$. Работа по вычислению P_3 приводит к табл. 17.

Таким образом, искомое приближение числа $-\sqrt{15}$ имеет вид $-\sqrt{15} \approx \approx -149/46$. ▷

3. Сократите дробь $-667/580$.

Решение. Разложим число 667/580 в цепную дробь:

$667 = 580 \cdot 1 + 87;$

$580 = 87 \cdot 6 + 58;$

$87 = 58 \cdot 1 + 29;$

$58 = 29 \cdot 2 + 0.$

Таким образом, $667/580 = [1, 6, 1, 2]$.

Найдем значение цепной дроби $[1, 6, 1, 2]$, используя стандартную таблицу (табл. 18).

Таблица 18

n	−2	−1	0	1	2	3
a_n			1	6	1	2
P_n	0	1	1	7	8	23
Q_n	1	0	1	6	7	20

Таблица 19

n	−2	−1	0	1	2	3
a_n			3	1	1	20
P_n	0	1	3	4	7	144
Q_n	1	0	1	1	2	41

Таким образом, $667/580 = 23/20$, и $-667/580 = -23/20$, причем дробь $-23/20$ несократима. ▷

4. Решите сравнение $123x \equiv 57 (\mathrm{mod}\, 342)$.

Решение. Перейдя к сравнению $41x \equiv 19 (\mathrm{mod}\, 114)$, получим разложение дроби $38/41$ в цепную дробь:
$114 = 41 \cdot 3 + 21$;
$41 = 21 \cdot 1 + 20$;
$21 = 20 \cdot 1 + 1$;
$20 = 1 \cdot 20 + 0$.
Таким образом, $114/41 = [3, 1, 1, 20]$.
Найдем числители и знаменатели подходящих к цепной дроби $[3, 1, 1, 20]$ дробей, используя стандартную таблицу (табл. 19).
Так как $P_sQ_{s-1} - Q_sP_{s-1} = (-1)^{s+1}$, то при $s = 3$ мы получаем, что $144 \cdot 2 - 41 \cdot 7 = 1$, откуда следует, что $41 \cdot (-7) \equiv 1 (\mathrm{mod}\, 114)$, или $41 \cdot (-7) \cdot 19 \equiv 19 (\mathrm{mod}\, 114)$.
Таким образом, $x \equiv (-7) \cdot 19 \equiv -133 \equiv -19 (\mathrm{mod}\, 114)$. Разбивая один класс по модулю 114 на три класса по модулю 342, мы получим окончательный результат: решениями сравнения $123x \equiv 57 (\mathrm{mod}\, 342)$ являются классы $x \equiv -19 (\mathrm{mod}\, 342)$, $x \equiv 95 (\mathrm{mod}\, 342)$ и $x \equiv 223 (\mathrm{mod}\, 342)$. ▷

5. Решите неопределенное уравнение $33x + 51y = 21$.

Решение. Приведя уравнение к виду $11x + 17y = 7$, разложим число $17/11$ в цепную дробь:

Таблица 20

n	−2	−1	0	1	2	3
a_n			1	1	1	5
P_n	0	1	1	2	3	17
Q_n	1	0	1	1	2	11

$17 = 11 \cdot 1 + 6;$
$11 = 6 \cdot 1 + 5;$
$6 = 5 \cdot 1 + 1;$
$5 = 1 \cdot 5 + 0.$

Таким образом, $17/11 = [1, 1, 1, 5]$.

Найдем числители и знаменатели подходящих к цепной дроби $[1, 1, 1, 5]$ дробей, используя стандартную таблицу (табл. 20).

Так как $P_sQ_{s-1} - Q_sP_{s-1} = (-1)^{s-1}$, то при $s = 3$ мы получаем, что $17 \cdot 2 - 11 \cdot 3 = 1$, или, что то же, $11 \cdot (-3) + 17 \cdot 2 = 1$, откуда следует, что $11 \cdot (-21) + 17 \cdot 14 = 7$. Таким образом, частное решение (x_0, y_0) уравнения $11x + 17y = 7$ имеет вид $(-21, 14)$. В этом случае все решения уравнения $11x + 17y = 7$ могут быть получены по формулам $x = -21 + 17t, y = 14 - 11t$, где $t \in \mathbb{Z}$. ▷

6. Укажите первые четыре натуральных решения уравнения $x^2 - 3y^2 = 1$; уравнения $x^2 - 3y^2 = -1$.

Решение. Разложим число $\sqrt{3}$ в цепную дробь:

$$\alpha_0 = \sqrt{3} = 1 + \frac{1}{\alpha_1}, \text{ где } \frac{1}{\alpha_1} = -1 + \sqrt{3};$$

$$\alpha_1 = \frac{1+\sqrt{3}}{2} = 1 + \frac{1}{\alpha_2}, \text{ где } \frac{1}{\alpha_2} = \frac{-1+\sqrt{3}}{2};$$

$$\alpha_2 = 1 + \sqrt{3} = 2 + \frac{1}{\alpha_3}, \text{ где } \frac{1}{\alpha_3} = -1 + \sqrt{3}.$$

Таким образом, $\sqrt{3} = [1, (1, 2)]$, то есть длина k периода разложения числа $\sqrt{3}$ в цепную дробь равна 2.

Следовательно, все натуральные решения уравнения $x^2 - 3y^2 = 1$ могут быть найдены по формулам $x = P_{2n-1}$, $y = Q_{2n-1}$, где $n \in \mathbb{N}$. Первые четыре натуральных решения (P_1, Q_1), (P_3, Q_3), (P_5, Q_5), (P_7, Q_7) получаются при $n = 1, 2, 3, 4$.

Найдем числители и знаменатели соответствующих подходящих дробей, используя стандартную таблицу (табл. 21).

Таблица 21

n	−2	−1	0	1	2	3	4	5	6	7
a_n			1	1	2	1	2	1	2	1
P_n	0	1	1	2	5	7	19	26	71	97
Q_n	1	0	1	1	3	4	11	15	41	56

Таким образом, первые четыре натуральных решения уравнения $x^2 - 3y^2 = 1$ имеют вид $(P_1, Q_1) = (2, 1)$; $(P_3, Q_3) = (7, 4)$, $(P_5, Q_5) = (26, 15)$, $(P_7, Q_7) = (97, 56)$.

Все натуральные решения уравнения $x^2 - Dy^2 = -1$ могут быть найдены по формулам $x = P_{2n-1}$, $y = Q_{2n-1}$, где $n \in \mathbb{N}$, причем kn — нечетно. Очевидно, что в нашем случае $(k = 2)$ уравнение решений не имеет. ▷

Упражнения

1. Найдите рациональное приближение числа $\sqrt{10}$ с точностью $\Delta = 5 \cdot 10^{-3}$. Укажите, с избытком или с недостатком полученное приближение.
2. Найдите рациональное приближение числа $\sqrt{21}$ с недостатком с точностью $\Delta = 10^{-4}$.
3. Найдите величину бесконечной цепной дроби $[-2, (1, 1, 2)]$ и ее рациональное приближение с недостатком (с избытком) с точностью $\Delta = 10^{-2}$.
4. Найдите наилучшее приближение числа 2500/1441 дробью a/b со знаменателем, не превосходящим 100. Укажите, с избытком или с недостатком полученное приближение.
5. Найдите наилучшее приближение числа 1292/479 с избытком (с недостатком) дробью a/b со знаменателем, не превосходящим 100. Укажите точность приближения.
6. Сократите дробь:

   а) 204/697; б) 1235/1391; в) −2626/1690; г) −1085/980.

7. Решите сравнение:

   а) $28x \equiv 66 (\mathrm{mod}\ 99)$;
   б) $115x \equiv 42 (\mathrm{mod}\ 130)$;
   в) $21x \equiv 76 (\mathrm{mod}\ 81)$;
   г) $55x \equiv 57 (\mathrm{mod}\ 221)$;
   д) $67x \equiv 64 (\mathrm{mod}\ 183)$;
   е) $285x \equiv 177 (\mathrm{mod}\ 924)$;
   ж) $89x \equiv 86 (\mathrm{mod}\ 241)$;
   з) $213x \equiv 137 (\mathrm{mod}\ 516)$;
   и) $-53x \equiv 84 (\mathrm{mod}\ 219)$.

8. Решите неопределенное уравнение:

а) $311x + 28y = 2$; в) $253x - 449y = 3$;

б) $26x + 91y = 11$; г) $73x + 85y = 7$.

9. Укажите первые четыре натуральных решения уравнения:

а) $x^2 - 5y^2 = 1$; в) $x^2 - 19y^2 = 1$;

б) $x^2 - 5y^2 = -1$; г) $x^2 - 19y^2 = -1$.

10. Укажите наименьшее натуральное решение уравнения:

а) $x^2 - 41y^2 = 1$; в) $x^2 - 13y^2 = -1$;

б) $x^2 - 41y^2 = -1$. г) $x^2 - 13y^2 = -1$.

Задачи

1. Найдите значение цепной дроби $[-3, (2, 1, 1)]$ и рациональное приближение к нему с точностью $0{,}5 \cdot 10^{-3}$. Укажите, с избытком или с недостатком полученное приближение.

2. Найдите значение цепной дроби $[3, (1, 2, 2)]$ и рациональное приближение к нему с точностью $0{,}5 \cdot 10^{-3}$. Укажите, с избытком или с недостатком полученное приближение.

3. Является ли $\delta = -39/16$ подходящей дробью к $\alpha = \dfrac{\sqrt{17} - 9}{2}$? Если да, оцените точность приближения α числом δ. Какое из неравенств верно: $\alpha > \delta$ или $\alpha < \delta$?

4. Является ли подходящая дробь $\delta = -13/7$ приближением к $\alpha = \dfrac{\sqrt{10} - 4}{2}$ с точностью 10^{-2}? Какое неравенство верно: $\alpha > \delta$ или $\alpha < \delta$?

5. Найдите рациональное приближение квадратичной иррациональности с точностью 10^{-3}, разложив данную квадратичную иррациональность в цепную дробь:

а) $\sqrt{7}$; в) $\sqrt{11}$; д) $\sqrt{14}$; ж) $\sqrt{18}$; и) $\sqrt{20}$;

б) $\sqrt{10}$; г) $\sqrt{13}$; е) $\sqrt{15}$; з) $\sqrt{19}$; к) $\sqrt{22}$.

6. Найдите наилучшее приближение числа α со знаменателем, не превосходящим b, и оцените точность полученного приближения:

а) $\alpha = \dfrac{\sqrt{77} - 3}{2}$, $b = 100$; в) $\alpha = \dfrac{22 + \sqrt{15}}{7}$, $b = 150$;

б) $\alpha = \dfrac{1 + \sqrt{35}}{2}$, $b = 200$; г) $\alpha = \dfrac{1 + \sqrt{21}}{2}$, $b = 50$.

7. Найдите подходящую дробь наименьшего порядка, приближающую число $98/57$ с точностью $1/150$. Является ли она:

- наилучшим приближением этого числа со знаменателем, не превосходящим 7;
- наилучшим приближением этого числа со знаменателем, не превосходящим 8?

8. Найдите подходящую дробь наименьшего порядка, приближающую число 61/44 с точностью 1/50. Является ли она:

- наилучшим приближением этого числа со знаменателем, не превосходящим 5;
- наилучшим приближением этого числа со знаменателем, не превосходящим 6?

9. Найдите подходящую дробь наименьшего порядка, приближающую число 37/64 с точностью 10^{-2}. Является ли она:

- наилучшим приближением этого числа со знаменателем, не превосходящим 7;
- наилучшим приближением этого числа со знаменателем, не превосходящим 8?

10. Для $n = N - 4\lfloor N/4 \rfloor + 5$, где $N \in \{1, 2, 3, \ldots, 25\}$, разложите в цепную дробь число

$$-\frac{362n}{905 \cdot 2^n}.$$

Найдите наилучшее приближение указанного числа обыкновенной дробью с знаменателем, не превосходящим $20n$. С избытком или с недостатком полученное приближение?

11. Для $n = N - 4\lfloor N/4 \rfloor + 5$, где $N \in \{1, 2, 3, \ldots, 25\}$, разложите в цепную дробь число

$$\frac{\sqrt{37n} - 2n}{2},$$

и найдите его рациональное приближение с точностью 10^{-4}.

12. Найдите рациональное приближение числа α с точностью Δ, если $\alpha \in \{\sqrt{29}; \sqrt{33}, \sqrt{28}, \frac{2-\sqrt{13}}{5}, \frac{1+\sqrt{3}}{2}, \frac{\sqrt{5}-1}{4}\}$, а $\Delta \in \{10^{-4}, 10^{-5}, 10^{-6}, 10^{-7}\}$.

13. Найдите рациональное приближение числа α с точностью Δ, если:

а) $\alpha = \sqrt{2}$, $\Delta = 10^{-2}$;

б) $\alpha = \frac{2+\sqrt{5}}{2}$, $\Delta = 10^{-3}$;

в) $\alpha = \frac{18+\sqrt{401}}{11}$, $\Delta = 10^{-4}$;

г) $\alpha = \dfrac{11+2\sqrt{39}}{7}$, $\Delta = 10^{-5}$;

д) $\alpha = \dfrac{9+\sqrt{101}}{5}$, $\Delta = 10^{-2}$;

е) $\alpha = \dfrac{2+\sqrt{7}}{4}$, $\Delta = 10^{-3}$;

ж) $\alpha = \dfrac{9+\sqrt{21}}{6}$, $\Delta = 10^{-4}$;

з) $\alpha = \dfrac{2-\sqrt{13}}{5}$, $\Delta = 10^{-5}$.

14. Найдите рациональное приближение числа $\sqrt[3]{2}$ с точностью $\delta = 0{,}01$. Укажите, с избытком или с недостатком полученное приближение.

15. Найдите рациональное приближение числа $\sqrt[3]{10}$ с точностью $\delta = 0{,}01$. Укажите, с избытком или с недостатком полученное приближение.

16. Найдите рациональное приближение числа e с точностью $\delta = 0{,}036$. Укажите, с избытком или с недостатком полученное приближение.

17. Сократите дробь:

а) $\dfrac{396}{696}$; б) $\dfrac{871}{3953}$; в) $\dfrac{6821}{2147}$; г) $\dfrac{32671}{10027}$; д) $\dfrac{4355}{19765}$; е) $\dfrac{47747}{15029}$.

18. Решите сравнение:

а) $111x \equiv 81 (\mathrm{mod}\, 447)$;
б) $186x \equiv 374 (\mathrm{mod}\, 422)$;
в) $129x \equiv 321 (\mathrm{mod}\, 471)$;
г) $-73x \equiv 60 (\mathrm{mod}\, 311)$;
д) $78x \equiv 102 (\mathrm{mod}\, 273)$;
е) $116x \equiv 10 (\mathrm{mod}\, 201)$;
ж) $103x \equiv -6 (\mathrm{mod}\, 189)$;
з) $142x \equiv 14 (\mathrm{mod}\, 214)$;
и) $165x \equiv 21 (\mathrm{mod}\, 261)$;
к) $256x \equiv 179 (\mathrm{mod}\, 337)$;
л) $1215x \equiv 560 (\mathrm{mod}\, 2755)$;
м) $1296x \equiv 1105 (\mathrm{mod}\, 2413)$.

19. Для $n = N - 4\lfloor N/4 \rfloor + 5$, где $N \in \{1, 2, 3, \ldots, 25\}$, решите сравнение $517x \equiv n - 338 (\mathrm{mod}\, 599)$.

20. Решите неопределенное уравнение первой степени:

а) $-73x + 85y = 1$;
б) $11x + 16y = 156$;
в) $-53x + 17y = 25$;
г) $482x - 824y = 24$;
д) $-33x + 48y = 207$;
е) $339x - 240y = 21$;
ж) $339x + 240y = -21$;
з) $17x - 16y = 31$;
и) $23x + 15y = 19$;
к) $12x - 37y = -3$;
л) $18x - 33y = 26$;
м) $25x + 36y = 13$;
н) $64x - 47y = 13$;
о) $494x - 703y = 209$;
п) $391x - 663y = 221$.

21. Для $n = N - 4\lfloor N/4 \rfloor + 5$, где $N \in \{1, 2, 3, \ldots, 25\}$, решите уравнение $221x - 39ny = 182$.

22. Укажите, если это возможно, первые два натуральных решения уравнения:

а) $x^2 - 11y^2 = 1$;
б) $x^2 - 11y^2 = -1$;
в) $x^2 - 7y^2 = 1$;
г) $x^2 - 7y^2 = -1$;
д) $x^2 - 39y^2 = 1$;
е) $x^2 - 39y^2 = -1$;
ж) $x^2 - 17y^2 = 1$;
з) $x^2 - 17y^2 = -1$.
и) $x^2 - 30y^2 = 1$;
к) $x^2 - 30y^2 = 1$.

§ 24. Разные теоретико-числовые задачи

1. Найдите все пары натуральных чисел, таких что при делении на 41 их сумма дает остаток 6, а сумма их квадратов дает остаток 20.

2. Два двузначных числа отличаются друг от друга только порядком цифр. Их разность при делении на 11 дает в остатке 1. Найдите эти числа.

3. Найдите наименьшее натуральное трехзначное число, кратное 23, у которого каждая следующая цифра больше предыдущей на единицу.

4. Найдите все натуральные трехзначные числа, которые при делении на 41 дают остаток, равный сумме своих цифр.

5. *Найдите два наименьших положительных* соседних нечетных числа, произведение которых делится на 187.

6. Разделите многочлен $f(x)$ на многочлен $g(x)$ с остатком, считая, что коэффициенты многочленов принадлежат $\mathbb{Z}$ ($\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$):

а) $f(x) = 2x^5 + x^4 + 4x + 3$, $g(x) = 3x^2 + 1$;
б) $f(x) = x^6 - x + 1$, $g(x) = x - 1$;
в) $f(x) = x^4 - 1$, $g(x) = x - 1$;
г) $f(x) = x - 1$, $g(x) = x^2 + x + 5$.

7. Найдите многочлен $r(x)$, если $f(x) \equiv r(x) \pmod{g(x)}$, $\deg r(x) < \deg g(x)$, и коэффициенты многочленов принадлежат $\mathbb{Z}$ ($\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$):

а) $f(x) = x^3 + x^2 + 2x + 2$, $g(x) = x^2 + 1$;
б) $f(x) = 8x^8 + 6x^6 + 4x^4 + 2x^2$, $g(x) = 6x + 3$;
в) $f(x) = x^{20} + x^{10} + 1$, $g(x) = x^5 + 1$.

8. Докажите, что для каждого простого числа p последовательность $a_1, a_2, \ldots, a_n, \ldots$ является периодической с периодом 2, если a_n равно остатку от деления числа p^{n+2} на 24 для любого $n \in \mathbb{N}$.

9. Пусть x_1 и x_2 — корни трехчлена $x^2 + 3x + 1$. Пусть натуральное число m вычисляется как $m = n + f(x_i)$, $i = 1, 2$, где $n \in \mathbb{N}$, а $f(x) = x^6 + 3x^5 + x^4 + x^3 + 4x^2 + 4x + 3$. Найдите значения n, которым соответствует $m = 5,\ 7,\ 103$.

10. Сколько существует упорядоченных пар натуральных чисел a и b, для которых $(a, b) = 6$ и $[a, b] = 6930$? Сформулируйте ответ в общем случае, используя канонические разложения (a, b) и $[a, b]$.

11. Докажите, что десятичная запись квадрата натурального числа не может состоять из одинаковых цифр.

12. Докажите, что для любого натурального числа n существует кратное ему натуральное число m, которое в десятичной системе счисления записывается только цифрами 0 и 1.

13. Разложите на простые множители число $2^{22} + 39 \cdot 2^{10} + 81$.

14. Найдите наименьшее значение выражений $|53^k - 37^l|$, $|36^k - 5^2|$, $k, l \in \mathbb{N}$.

15. Докажите, что ряд $\sum\limits_{p \in P} \dfrac{1}{p \ln p}$ сходится, а ряд $\sum\limits_{p \in P, p \geqslant 3} \dfrac{1}{p \ln \ln p}$ расходится.

16. Найдите все x, для которых $\lfloor x \rfloor = 5$, а $\{x\} = 0.3$.

17. Делится ли $10!$ на $\tau(3)^{15}$?

18. Найдите остаток от деления числа $\tau(275)^{\sigma(275)^{\varphi(275)}}$ на $\tau(12!)$.

19. Приведите пример кольца классов вычетов, в котором верно соотношение:

а) $(\mathbf{a_n} - \mathbf{b_n}) \cdot (\mathbf{a_n} + \mathbf{b_n}) = \mathbf{a_n}^2 - \mathbf{b_n}^2$;

б) $(\mathbf{a_n} + \mathbf{b_n})^2 = \mathbf{a_n}^2 + \mathbf{b_n}^2$;

в) $(\mathbf{a_n} + \mathbf{a_n})^2 \neq \mathbf{a_n}^2 + \mathbf{b_n}^2$.

20. Для каких модулей можно составить приведенную систему вычетов, состоящую из степеней числа 3?

21. Докажите, что произведение всех натуральных чисел, меньших p^2 и не делящихся на p, сравнимо с -1 по модулю p, $p \in P$.

22. Докажите, что $(p-2)! \equiv 1 (\mathrm{mod}\, p)$, где p — простое число вида $4n+1$, $n \in \mathbb{N}$.

23. Докажите, что для любого целого a имеет место сравнение $a^{561} \equiv a (\mathrm{mod}\, 561)$.

24. Приведите пример составного n, удовлетворяющего сравнению $a^n \equiv a (\mathrm{mod}\, n)$ для любого целого a.

25. Найдите наименьшее трехзначное число x, такое что $19^{18} \cdot 42^{24} \cdot 45^{12} + 10 \cdot 28^{45} \equiv x \pmod{235}$.

26. Решите систему сравнений $\begin{cases} x^3 \equiv -1 \pmod{13} \\ 7x \equiv 3 \pmod{10} \end{cases}$.

27. Решите систему сравнений $\begin{cases} 2x \equiv 6 \pmod{5} \\ 4x \equiv -8 \pmod{40} \\ 5x \equiv 8 \pmod{3} \end{cases}$.

28. Решите систему сравнений:

а) $\begin{cases} 3x + 4y - 29 \equiv 0 \pmod{143} \\ 2x - 9y + 84 \equiv 0 \pmod{143} \end{cases}$;

б) $\begin{cases} x + 4y - 1 \equiv 0 \pmod{9} \\ 5x - 8y - 2 \equiv 0 \pmod{9} \end{cases}$;

в) $\begin{cases} 9x + 20y \equiv 0 \pmod{29} \\ 16x - 13y \equiv 0 \pmod{29} \end{cases}$;

г) $\begin{cases} 3x + 4y - 29 \equiv 0 \pmod{143} \\ 2x - 5y + 84 \equiv 0 \pmod{143} \end{cases}$;

д) $\begin{cases} x + 4y - 1 \equiv 0 \pmod{9} \\ 5x - 8y - 1 \equiv 0 \pmod{9} \end{cases}$;

е) $\begin{cases} 9x + 20y - 10 \equiv 0 \pmod{29} \\ 16x - 13y - 21 \equiv 0 \pmod{29} \end{cases}$.

29. Делится ли на 1093^2 число $2^{1093} - 2$?

30. Решите сравнение $3x^2 \equiv 10 \pmod{17^2}$.

31. Решите систему сравнений $\begin{cases} 3x^2 + 5x - 5 \equiv 0 \pmod{17} \\ 2x \equiv 10 \pmod{40} \end{cases}$.

32. Найдите четыре наименьших положительных последовательных нечетных числа, которые делятся на 7, 11, 13 и 17, соответственно.

33. Припишите к числу 12 345 еще пять цифр так, чтобы получилось число, делящееся на 41.

34. Припишите к числу 1234567890 еще пятьдесят цифр так, чтобы получилось число, делящееся на 31.

35. Решите систему сравнений $\begin{cases} 17x + 25y \equiv 3 (\mathrm{mod}\, 47) \\ 10x + 31y \equiv 14 (\mathrm{mod}\, 47) \end{cases}$.

36. Найдите число решений сравнения
$45x^{526} + 43x^{264} - 89x^{263} + 226x^{262} \equiv 20 (\mathrm{mod}\, 263)$.

37. Сколько решений может иметь сравнение $x^2 \equiv a (\mathrm{mod}\, 105)$ при различных целых a?

38. Придумайте сравнение, имеющее ровно 20 решений.

39. Решите сравнение $x^2 \equiv p (\mathrm{mod}\, p^2)$, где $p \in P$.

40. Решите сравнение $x^2 \equiv \dfrac{3p+1}{4} (\mathrm{mod}\, p^2)$, где $p \in P$.

41. Решите сравнение $x^2 \equiv 1 (\mathrm{mod}\, p^n)$, где $p \in P \backslash \{2\}$, а $n \in \mathbb{N}$.

42. Сколько решений имеет сравнение $x^2 \equiv g (\mathrm{mod}\, p)$, если g — первообразный корень по простому модулю p?

43. Докажите, что единственным целым решением уравнения $5x^3 + 11x^3 + 13x^3 = 0$ является тройка $(0, 0, 0)$.

44. Докажите, что уравнение $y^2 = x^3 + 7$ не имеет целых решений.

45. Докажите, что при нечетном a сравнение $a^{2^n} \equiv 1 (\mathrm{mod}\, 2^{n+2})$ справедливо для любого натурального числа n.

46. Для каких простых p справедливо сравнение $32^{p^2-1} \equiv 1 (\mathrm{mod}\, p)$?

47. Сколько решений имеет сравнение $x^{(p-1)/2} \equiv 1 (\mathrm{mod} p)$, если $p \in P \backslash \{2\}$.

48. Докажите, что $((p-1)/2!)^2 \equiv -1 (\mathrm{mod}\, p)$, если $p \in P$, $p \equiv 1 (\mathrm{mod}\, 4)$.

49. Докажите, что $((p-1)/2)! \equiv (-1)^n (\mathrm{mod}\, p)$, если $p \in P$, $p \equiv 3 (\mathrm{mod}\, 4)$, и n — число квадратичных невычетов по модулю p на отрезке $[1, (p-1)/2]$.

50. Найдите все простые числа p, для которых 7 является квадратичным вычетом по модулю p.

51. Вычислите сумму символов Лежандра $\sum\limits_{x=0}^{p-1} \left(\dfrac{ax+b}{p}\right)$, где $a, b \in \mathbb{Z}$, $(a, p) = 1$.

52. Докажите, что сравнение $x^2 + y^2 + a \equiv 0 (\mathrm{mod}\, p)$ разрешимо для любого простого числа p и любого целого a.

53. Докажите, что сравнение $(x^2 - 17)(x^2 - 13)(x^2 - 221) \equiv 0 (\mathrm{mod}\, n)$ разрешимо для любого натурального n.

54. Докажите, что 3 является первообразным корнем для любого простого числа p вида $2^n + 1$, $n > 1$.

55. Может ли 2 быть первообразным корнем по простому модулю p, если $p = 8t \pm 1$, $t \in \mathbb{N}$?

56. Докажите, что $1^n + 2^n + \ldots + (p-1)^n \equiv -1 (\mathrm{mod}\, p)$, если $(p-1) | n$, и $1^n + 2^n + \ldots + (p-1)^n \equiv 0 (\mathrm{mod}\, p)$, если $(p-1) \nmid n$, где $p \in P \backslash \{2\}$, и $n \geqslant 2$.

57. Сколько решений имеет сравнение $x(x-1)(x+1) \equiv 0 (\mathrm{mod}\, 82)$?

58. Индекс числа 3 по модулю 13 с основанием 2 равен 4. Не пользуясь таблицами индексов, найдите индекс числа 3 по модулю 13 с основанием 6.

59. Пусть p — нечетное простое число. Пусть $\delta | (p-1)$. Докажите, что $\delta | \mathrm{ind}_{g_1} a \Leftrightarrow \delta | \mathrm{ind}_{g_2} a$, где $\mathrm{ind}_{g_1} a$ и $\mathrm{ind}_{g_2} a$ — индексы числа a по модулю p с основаниями g_1 и g_2, соответственно.

60. Найдите все комбинации (x, y, z) натуральных чисел от 10 до 20, такие что $3x^2 - y^2 - 7z = 99$.

61. Замените каждое число $1 + 2 + \ldots + n$, $n \in \mathbb{N}$, последней цифрой s_n в его десятичной записи. Докажите, что последовательность $s_1, s_2, s_3, \ldots, s_n, \ldots$ является периодической, и найдите ее наименьший период.

62. Найдите наименьшее натуральное число n, которое составляет от 10.5 % до 11 % от некоторого натурального числа m.

63. Найдите все натуральные n, для которых уравнение $3x + 5y = n$ имеет ровно 57 решений в натуральных числах.

64. Пусть $p, q \in \mathbb{N}$, $p, q > 1$, $(p, q) = 1$. Докажите, что число

$$\alpha = \sum_{n=1}^{\infty} \left(\frac{(p-1)}{q} \right)^{-n!}$$

— трансцендентное.

Глава 2

Задачи для организации промежуточного и итогового контроля

§ 1. Задачи для проведения контрольных работ

1. Постройте график функции:
   а) $f(x) = \{2x - 3\}$; $f(x) = \lfloor 2x - 3 \rfloor$;
   б) $f(x) = \{2/x\}$, $f(x) = \lfloor 2/x \rfloor$;
   в) $f(x) = \{x^2/2\}$; $f(x) = \lfloor x^2/2 \rfloor$;
   г) $f(x) = \{-x^2/2\}$; $f(x) = \lfloor -x^2/2 \rfloor$;
   д) $f(x) = \{2 - x^2\}$; $f(x) = \lfloor 2 - x^2 \rfloor$;
   е) $f(x) = \{x^3/2\}$; $f(x) = \lfloor x^3/2 \rfloor$;
   ж) $f(x) = \{1/3x\}$; $f(x) = \lfloor 1/3x \rfloor$;
   з) $f(x) = \{1 - x^2\}$; $f(x) = \lfloor 1 - x^2 \rfloor$;
   и) $f(x) = \{x^3\}$; $f(x) = \lfloor x^3 \rfloor$;
   к) $f(x) = \{3x^2 - 5\}$; $f(x) = \lfloor 3x^2 - 5 \rfloor$;
   л) $f(x) = \{1/(2x - 1)\}$; $f(x) = \lfloor 1/(2x - 1) \rfloor$;
   м) $f(x) = \{3x^2 - 5\}$; $f(x) = \lfloor 3x^2 - 5 \rfloor$;
   н) $f(x) = \{2x^2 - 2\}$; $f(x) = \lfloor 2x^2 - 2 \rfloor$;
   о) $f(x) = \{-1/(2x^2)\}$; $f(x) = \lfloor -1/(2x^2) \rfloor$;
   п) $f(x) = \{-x^2/2\}$; $f(x) = \lfloor -x^2/2 \rfloor$;
   р) $f(x) = \{ctgx\}$; $f(x) = \lfloor ctgx \rfloor$;
   с) $f(x) = \{|x|/2\}$; $f(x) = \lfloor |x|/2 \rfloor$;
   т) $f(x) = \{1/(3x - 3)\}$; $f(x) = \lfloor 1/(3x - 3) \rfloor$;

у) $f(x) = \{|1 - x|\}$; $f(x) = \lfloor|1 - x|\rfloor$;
ф) $f(x) = \{tgx\}$; $f(x) = \lfloor tgx\rfloor$;
х) $f(x) = \{3\cos 0{,}5x\}$; $f(x) = \lfloor 3\cos 0{,}5x\rfloor$;
ц) $f(x) = \{1/2|x|\}$; $f(x) = \lfloor 1/2|x|\rfloor$;
ч) $f(x) = \{|3x - 5|\}$; $f(x) = \lfloor|3x - 5|\rfloor$;
ш) $f(x) = \{2\sin x - 1\}$; $f(x) = \lfloor 2\sin x - 1\rfloor$;
щ) $f(x) = \{|2x^3 - 4|\}$; $f(x) = \lfloor|2x^3 - 4|\rfloor$.

2. Решите уравнение:

а) $3\lfloor x\rfloor - 5 = 2\{x\}$;
б) $\lfloor x + 3\rfloor - 6 = 2\{x\}$;
в) $5\lfloor x\rfloor - 4 = 3\{x\}$;
г) $4\lfloor x\rfloor - 2 = 3\{x\}$;
д) $3\lfloor x\rfloor - 8 = 2\{x\}$;
е) $\lfloor x + 3\rfloor - 6 = 2\{x\}$;
ж) $\lfloor x + 2\rfloor - 7 = 2\{x\}$;
з) $\lfloor x + 2\rfloor - 3 = 4\{x\}$;
и) $\dfrac{\lfloor x + 2\rfloor - 7}{4} = \{x\}$;
к) $5\lfloor x\rfloor - 4 = 3\{x\}$;
л) $\dfrac{\lfloor x + 1\rfloor - 5}{2} = \{x\}$;
м) $\dfrac{\lfloor x + 2\rfloor - 3}{4} = \{x\}$;
н) $\dfrac{\lfloor x + 1\rfloor - 6}{4} = \{x\}$;
о) $3\lfloor x\rfloor - 5 = 2\{x\}$;
п) $\dfrac{\lfloor x + 1\rfloor - 5}{4} = \{x\}$;
р) $\dfrac{5 - 4\lfloor x\rfloor}{3} = -\{x\}$;
с) $\dfrac{2 - \lfloor 5x\rfloor}{3} = -\{x\}$;
т) $\dfrac{\lfloor 3x\rfloor - 4}{2} = \{x\}$;
у) $\lfloor 3x\rfloor - 4 = 2\{x\}$;
ф) $\lfloor 4x\rfloor - 5 = 3\{x\}$;
х) $\lfloor x\rfloor - 5 = 3\{x\}$;
ц) $4x - 2 = 7\{x\}$;
ч) $3x - 8 = 5\{x\}$;
ш) $3x - 5 = 5\{x\}$;
щ) $5x - 4 = 8\{x\}$.

3. Решите уравнение:

а) $\tau(x) = 55,\ 96|x$;
б) $\tau(x) = 65,\ 160|x$;
в) $\tau(x) = 91,\ 320|x$;
г) $\tau(x) = 57,\ 40|x$;
д) $\tau(x) = 38,\ 24|x$;
е) $\tau(x) = 20,\ 30|x$;
ж) $\tau(x) = 20,\ 105|x$;
з) $\tau(x) = 26,\ 12|x$;
и) $\tau(x) = 34,\ 12|x$;
к) $\tau(x) = 22,\ 18|x$;
л) $\tau(x) = 14,\ 50|x$;
м) $\tau(x) = 15,\ 12|x$;
н) $\tau(x) = 35,\ 50|x$;
о) $\tau(x) = 18,\ 45|x$;
п) $\tau(x) = 18,\ 30|x$;
р) $\tau(x) = 21,\ 40|x$;
с) $\tau(x) = 33,\ 135|x$;
т) $\tau(x) = 15,\ 15|x$;
у) $\tau(x) = 14,\ 50|x$;
ф) $\tau(x) = 34,\ 98|x$;
х) $\tau(x) = 39,\ 54|x$;
ц) $\tau(x) = 77,\ 384|x$;
ч) $\tau(x) = 10,\ 12|x$;
ш) $\tau(x) = 28,\ 70|x$;
щ) $\tau(x) = 45,\ 66|x$.

4. Решите уравнение:

а) $\tau(5x) = \tau(2x)$, $x \in [5, 15]$;
б) $\tau(3x) = \tau(11x)$, $x \in [25, 135]$;
в) $\tau(3x) = \tau(13x)$, $x \in [30, 40]$;
г) $\tau(7x) = \tau(11x)$, $x \in [70, 80]$;
д) $\tau(3x) = \tau(5x)$, $x \in [10, 20]$;
е) $\tau(19x) = \tau(2x)$, $x \in [35, 45]$;
ж) $\tau(7x) = \tau(3x)$, $x \in [15, 25]$;
з) $\tau(2x) = \tau(11x)$, $x \in [20, 30]$;
и) $\tau(2x) = \tau(13x)$, $x \in [15, 25]$;
к) $\tau(2x) = \tau(17x)$, $x \in [55, 70]$;
л) $\tau(3x) = \tau(17x)$, $x \in [10, 40]$;
м) $\tau(19x) = \tau(3x)$, $x \in [10, 35]$;
н) $\tau(7x) = \tau(13x)$, $x \in [70, 100]$;
о) $\tau(5x) = \tau(17x)$, $x \in [80, 100]$;
п) $\tau(16x) = 2\tau(x)$, $x \in [10, 25]$;
р) $\tau(32x) = 2\tau(x)$, $x \in [15, 30]$;
с) $\tau(125x) = 5\tau(x)$, $x \in [15, 25]$;
т) $\tau(343x) = 7\tau(x)$, $x \in [10, 20]$;
у) $\tau(8x) = 2\tau(x)$, $x \in [20, 30]$;
ф) $\tau(81x) = 3\tau(x)$, $x \in [10, 20]$;
х) $\tau(625x) = 5\tau(x)$, $x \in [15, 25]$;
ц) $\tau(27x) = 3\tau(x)$, $x \in [10, 20]$;
ч) $\tau(81x) = 3\tau(x)$, $x \in [10, 20]$;
ш) $\tau(625x) = 5\tau(x)$, $x \in [15, 25]$;
щ) $\tau(27x) = 3\tau(x)$, $x \in [10, 20]$.

5. а) Запишите каноническое разложение числа $(2\tau(\sigma(15)) - 1)!$.
б) Запишите каноническое разложение числа $(2\tau(\sigma(22)) - 2)!$.
в) Запишите каноническое разложение числа $(3\tau(\sigma(21)) - 2)!$.
г) Запишите каноническое разложение числа $(2\tau(\sigma(30)) - 9)!$.
д) Запишите каноническое разложение числа $(3\tau(\sigma(26)) - 7)!$.
е) Запишите каноническое разложение числа $(2\tau(\sigma(24)) - 6)!$.
ж) Запишите каноническое разложение числа $(2\tau(\varphi(15)) + 1)!$.
з) Запишите каноническое разложение числа $(2\tau(\varphi(22)) + 2)!$.
и) Запишите каноническое разложение числа $(3\tau(\varphi(21)) + 2)!$.
к) Запишите каноническое разложение числа $(2\tau(\varphi(30)) - 9)!$.
л) Запишите каноническое разложение числа $(3\tau(\varphi(26)) - 7)!$.
м) Делится ли $\tau(1368)!$ на $(\sigma(11))^7$?
н) Делится ли $\tau(2800)!$ на $(\sigma(15))^8$?
о) Делится ли $\tau(960)!$ на $(\sigma(20))^3$?
п) Делится ли $\tau(288)!$ на $(\sigma(14))^5$?
р) Делится ли $\tau(200)!$ на $(\sigma(8))^2$?
с) Делится ли $\tau(\varphi(2888))!$ на $(\sigma(11))^7$?
т) Делится ли $\tau(\varphi(1644))!$ на $(\sigma(7))^6$?
у) Делится ли $\tau(\varphi(2800))!$ на $(\sigma(15))^8$?
ф) Делится ли $\tau(\varphi(960))!$ на $(\sigma(20))^3$?
х) Делится ли $\tau(288)!$ на $(\sigma(14))^5$?
ц) Делится ли $\tau(200)!$ на $(\sigma(8))^2$?

ч) Является ли целым число $\dfrac{41\cdot\ldots\cdot 90}{(\sigma(\tau(960)))^3}$?

ш) Является ли целым число $\dfrac{91\cdot\ldots\cdot 140}{(\sigma(\tau(2800)))^{11}}$?

щ) Является ли целым число $\dfrac{121\cdot\ldots\cdot 170}{(\sigma(\tau(288)))^6}$?

6. а) Сколькими нулями оканчивается $\sigma(\tau(432))!$ в 24-й системе счисления?

б) Сколькими нулями оканчивается $\sigma(\tau(200))!$ в 12-й системе счисления?

в) Сколькими нулями оканчивается $\sigma(\tau(288))!$ в 18-й системе счисления?

г) Сколькими нулями оканчивается $\sigma(\tau(864))!$ в 50-й системе счисления?

д) Сколькими нулями оканчивается $\sigma(\tau(2592))!$ в 40-й системе счисления?

е) Сколькими нулями оканчивается $\sigma(\tau(1024))!$ в 45-й системе счисления?

ж) Сколькими нулями оканчивается $\sigma(\tau(3072))!$ в 45-й системе счисления?

з) Сколькими нулями оканчивается $\sigma(\tau(2520))!$ в 14-й системе счисления?

и) Сколькими нулями оканчивается $\tau(\varphi(12800))$ в 10-й системе счисления?

к) Сколькими нулями оканчивается $\tau(\varphi(12800)$ в 24-й системе счисления?

л) Сколькими нулями оканчивается $\sigma(\varphi(1280)!$ в 10-й системе счисления?

м) Сколькими нулями оканчивается $\sigma(\varphi(1024))!$ в 24-й системе счисления?

н) Сколькими нулями оканчивается $\sigma(\varphi(200))!$ в 12-й системе счисления?

о) Сколькими нулями оканчивается $\sigma(\varphi(288))!$ в 18-й системе счисления?

п) Сколькими нулями оканчивается $\sigma(\varphi(864))!$ в 50-й системе счисления?

р) Сколькими нулями оканчивается $\sigma(\varphi(2592))!$ в 40-й системе счисления?

с) Сколькими нулями оканчивается $\varphi(\tau(1024))!$ в 45-й системе счисления?

т) Сколькими нулями оканчивается $\varphi(\tau(3072))!$ в 45-й системе счисления?

у) Сколькими нулями оканчивается $\varphi(\tau(2520))!$ в 14-й системе счисления?

ф) Найдите число правильных несократимых дробей вида $\frac{a}{\tau(6144)!}$.

х) Найдите число правильных несократимых дробей вида $\frac{a}{\tau(576)!}$.

ц) Найдите число правильных несократимых дробей вида $\frac{a}{\tau(6250)!}$.

ч) Найдите число правильных несократимых дробей вида $\frac{a}{\tau(5120)!}$.

ш) Найдите число правильных несократимых дробей вида $\frac{a}{\tau(2560)!}$.

щ) Найдите число правильных несократимых дробей вида $\frac{a}{\tau(5676)!}$.

7. В кольце классов вычетов $\mathbb{Z}/n\mathbb{Z}$ укажите все делители нуля и решите уравнение:

а) $3_6 \cdot x_6 = 9_6$;
б) $4_{12} \cdot x_{12} = 8_{12}$;
в) $2_{22} \cdot x_{22} = 4_{22}$;
г) $3_{15} \cdot x_{15} = 9_{15}$;
д) $4_8 \cdot x_8 = 8_8$;
е) $2_{12} \cdot x_{12} = 10_{12}$;
ж) $7_{18} \cdot x_{18} = 14_{18}$;
з) $6_8 \cdot x_8 = 2_8$;
и) $4_{12} \cdot x_{12} = 20_{12}$;
к) $4_{18} \cdot x_{18} = 16_{18}$;
л) $3_{18} \cdot x_{18} = 6_{18}$;
м) $3_{15} \cdot x_{15} = 21_{15}$;
н) $3_{15} \cdot x_{15} = 6_{15}$;
о) $4_{16} \cdot x_{16} = 12_{16}$;
п) $4_{28} \cdot x_{28} = 16_{28}$;
р) $5_{10} \cdot x_{10} = 10_{10}$;
с) $3_9 \cdot x_9 = 6_9$;
т) $13_{26} \cdot x_{26} = 39_{26}$;
у) $4_6 \cdot x_6 = 18_6$;
ф) $3_{18} \cdot x_{18} = 15_{18}$;
х) $2_{26} \cdot x_{26} = 10_{26}$;
ц) $3_{21} \cdot x_{21} = 12_{21}$;
ч) $4_{20} \cdot x_{20} = 12_{20}$;
ш) $2_{14} \cdot x_{14} = 18_{14}$;
щ) $2_{22} \cdot x_{22} = 6_{22}$.

8. При каких n имеет место равенство:

а) $|\text{ПрСВ}_{2n}| = |\text{ПрСВ}_{7n}|$;
б) $|\text{ПрСВ}_{2n}| = |\text{ПрСВ}_{3n}|$;
в) $|\text{ПрСВ}_{5n}| = |\text{ПрСВ}_{7n}|$;
г) $|\text{ПрСВ}_{3n}| = |\text{ПрСВ}_{7n}|$;
д) $|\text{ПрСВ}_{11n}| = |\text{ПрСВ}_{3n}|$;
е) $|\text{ПрСВ}_{13n}| = |\text{ПрСВ}_{7n}|$;
ж) $|\text{ПрСВ}_{3n}| = |\text{ПрСВ}_{17n}|$
з) $|\text{ПрСВ}_n| = 14$;
и) $|\text{ПрСВ}_n| = 10$;
к) $|\text{ПрСВ}_n| = 5$;
л) $|\text{ПрСВ}_n| = 6$;
м) $|\text{ПрСВ}_n| = 10$;
н) $|\text{ПрСВ}_n| = 3$;
о) $|\text{ПрСВ}_n| = 7$;
п) $|\text{ПрСВ}_n| = 22$;
р) $|\text{ПрСВ}_n| = 46$;

с) $17|\text{ПрСВ}_n| = 16|\text{ПСВ}_n|$;
т) $17|\text{ПрСВ}_n| = 8|\text{ПСВ}_n|$;
у) $13|\text{ПрСВ}_n| = 6|\text{ПСВ}_n|$;
ф) $9|\text{ПСВ}_n| = 19|\text{ПрСВ}_n|$;
х) $10|\text{ПСВ}_n| = 11|\text{ПрСВ}_n|$;
ц) $11|\text{ПрСВ}_n| = 5|\text{ПСВ}_n|$;
ч) $|\text{ПрСВ}_n| = 3|\text{ПСВ}_n|$;
ш) $8|\text{ПСВ}_n| = 13|\text{ПрСВ}_n|$;
щ) $8|\text{ПСВ}_n| = 11|\text{ПрСВ}_n|$?

9. Докажите:

а) $a \equiv b(\text{mod}\, n) \Rightarrow ka \equiv kb(\text{mod}\, d)$, $k \in \mathbb{Z}$, $d|n$, $d > 1$;
б) $a \equiv b(\text{mod}\, n)$, $c \equiv q(\text{mod}\, n) \Rightarrow ac \equiv bq(\text{mod}\, d)$, $d|n$, $d > 1$;
в) $a \equiv b(\text{mod}\, n)$, $c \equiv q(\text{mod}\, n) \Rightarrow a + c \equiv b + q(\text{mod}\, d)$, $d|n$, $d > 1$;
г) $a \equiv b(\text{mod}\, n)$, $c \equiv q(\text{mod}\, n) \Rightarrow a - c \equiv b - q(\text{mod}\, d)$, $d|n$, $d > 1$;
д) $a \equiv b(\text{mod}\, n) \Rightarrow ka \equiv kb(\text{mod}\, d)$, $k \in \mathbb{Z}$, $d|k$, $d > 1$;
е) $a \equiv b(\text{mod}\, n)$, $d|a$, $d|n \Rightarrow d|b$, $d \in \mathbb{Z}$;
ж) $a \equiv b(\text{mod}\, n) \Rightarrow (a, d) = (b, d)$, $d|n$, $d > 1$;
з) $ka \equiv kb(\text{mod}\, n)$, $(k, n) = 1 \Rightarrow a \equiv b(\text{mod}\, d)$, $d|n$, $d > 1$;
и) $a \equiv b(\text{mod}\, n) \Rightarrow ka \equiv kb(\text{mod}\, kd)$, $k \in \mathbb{N}$, $d|n$, $d > 1$;
к) $a \equiv b(\text{mod}\, n) \Rightarrow a^k \equiv b^k(\text{mod}\, d)$, $k \in \mathbb{N}$, $d|n$, $d > 1$;
л) $a \equiv b(\text{mod}\, kn)$, $c \equiv q(\text{mod}\, kn) \Rightarrow a + c \equiv b + q(\text{mod}\, d)$, $d|n$, $d > 1$;
м) $a \equiv b(\text{mod}\, kn)$, $c \equiv q(\text{mod}\, kn) \Rightarrow a - c \equiv b - q(\text{mod}\, d)$, $d|n$, $d > 1$;
н) $a \equiv b(\text{mod}\, n)$, $d|(a, n) \Rightarrow d|b$, $d \in \mathbb{Z}$;
о) $a \equiv b(\text{mod}\, kn)$, $d|a$, $d|n \Rightarrow d|b$, $d \in \mathbb{N}$;
п) $ka \equiv kb(\text{mod}\, n)$, $(k, n) = 1 \Rightarrow (a, d) = (b, d)$, $d|n$, $d > 1$;
р) $ka \equiv kb(\text{mod}\, kn) \Rightarrow a \equiv b(\text{mod}\, d)$, $d|n$, $d > 1$;
с) $a \equiv b(\text{mod}\, n) \Rightarrow ka \equiv kb(\text{mod}\, dn)$, $k \in \mathbb{N}$, $d|k$, $d > 1$;
т) $a \equiv b(\text{mod}\, kn) \Rightarrow ka \equiv kb(\text{mod}\, kd)$, $k \in \mathbb{N}$, $d|n$, $d > 1$;
у) $a \equiv b(\text{mod}\, kn)$, $d|(a, n) \Rightarrow d|b$, $d \in \mathbb{Z}$;
ф) $ka \equiv kb(\text{mod}\, kn)$, $d|b$, $d|n \Rightarrow d|a$, $d \in \mathbb{N}$;
х) $ka \equiv kb(\text{mod}\, kn) \Rightarrow (a, d) = (b, d)$, $d|n$, $d \in \mathbb{Z}$;
ц) $a \equiv b(\text{mod}\, n)$, $d|b$, $d|n \Rightarrow d|a$, $d \in \mathbb{N}$;
ч) $a \equiv b(\text{mod}\, kn) \Rightarrow (a, d) = (b, d)$, $d|n$, $d > 1$;
ш) $a \equiv b(\text{mod}\, kn) \Rightarrow a \equiv b(\text{mod}\, kd)$, $d|n$, $d > 1$;
щ) $a \equiv b(\text{mod}\, kn) \Rightarrow a^k \equiv b^k(\text{mod}\, d)$, $k \in \mathbb{N}$, $d|n$, $d > 1$.

10. Найдите остаток от деления:

а) $354^{7^{2000}}$ на 352;
б) $210^{5^{2000}}$ на 208;
в) $228^{7^{1000}}$ на 225;
г) $430^{7^{2000}}$ на 425;
д) $178^{3^{1000}}$ на 176;
е) $300^{3^{1000}}$ на 297;
ж) $280^{7^{1000}}$ на 275;
з) $354^{5^{2000}}$ на 351;
и) $350^{7^{2000}}$ на 352;
к) $206^{5^{2000}}$ на 208;
л) $222^{7^{1000}}$ на 225;
м) $420^{7^{2000}}$ на 425;
н) $174^{3^{1000}}$ на 176;
о) $294^{3^{1000}}$ на 297;
п) $270^{7^{1000}}$ на 275;
р) $-352^{7^{2010}}$ на 352;
с) $-210^{5^{2010}}$ на 208;
т) $-230^{7^{1010}}$ на 225;
у) $-430^{7^{2010}}$ на 425;
ф) $-178^{3^{1010}}$ на 176;
х) $-300^{3^{1010}}$ на 297;
ц) $-280^{7^{1010}}$ на 275;
ч) $-354^{5^{2010}}$ на 351;
ш) $-350^{7^{2010}}$ на 352;
щ) $-206^{5^{2010}}$ на 208.

11. Решите систему сравнений первой степени:

а) $\begin{cases} 4x \equiv 2 \pmod{10} \\ 3x \equiv 3 \pmod{6} \\ 28x \equiv 4 \pmod{60} \end{cases}$;

б) $\begin{cases} 32x \equiv -4 \pmod{60} \\ 9x \equiv -3 \pmod{6} \\ 6x \equiv 8 \pmod{10} \end{cases}$;

в) $\begin{cases} 17x \equiv 2 \pmod{7} \\ 4x \equiv 16 \pmod{12} \\ 4x \equiv -2 \pmod{10} \end{cases}$;

г) $\begin{cases} 2x \equiv 2 \pmod{5} \\ 8x \equiv 4 \pmod{12} \\ 6x \equiv 4 \pmod{14} \end{cases}$;

д) $\begin{cases} 32x \equiv 56 \pmod{60} \\ -3x \equiv 9 \pmod{6} \\ 6x \equiv -2 \pmod{10} \end{cases}$;

е) $\begin{cases} -4x \equiv 9 \pmod{7} \\ 16x \equiv -8 \pmod{12} \\ 4x \equiv 18 \pmod{10} \end{cases}$;

ж) $\begin{cases} 4x \equiv 8 \pmod{14} \\ 15x \equiv 12 \pmod{27} \\ 5x \equiv 4 \pmod{6} \end{cases}$;

з) $\begin{cases} 15x \equiv -21 \pmod{36} \\ 3x \equiv 7 \pmod{8} \\ 3x \equiv -6 \pmod{15} \end{cases}$;

и) $\begin{cases} 3x \equiv 1 \pmod{7} \\ 5x \equiv 1 \pmod{12} \\ 5x \equiv 5 \pmod{20} \end{cases}$;

к) $\begin{cases} 14x \equiv -10 \pmod{24} \\ -9x \equiv 18 \pmod{45} \\ 5x \equiv 9 \pmod{8} \end{cases}$;

л) $\begin{cases} 5x \equiv 9 \pmod{8} \\ 12x \equiv -9 \pmod{15} \\ 21x \equiv -15 \pmod{36} \end{cases}$;

м) $\begin{cases} 16x \equiv -2 \pmod{30} \\ 12x \equiv -4 \pmod{20} \\ 9x \equiv -3 \pmod{6} \end{cases}$;

н) $\begin{cases} 4x \equiv -18 (\mathrm{mod}\, 10) \\ 6x \equiv 6 (\mathrm{mod}\, 12) \\ 28x \equiv 4 (\mathrm{mod}\, 60) \end{cases}$;

о) $\begin{cases} 6x \equiv -8 (\mathrm{mod}\, 10) \\ 8x \equiv -4 (\mathrm{mod}\, 12) \\ 4x \equiv 5 (\mathrm{mod}\, 7) \end{cases}$;

п) $\begin{cases} 4x \equiv -4 (\mathrm{mod}\, 12) \\ 3x \equiv 8 (\mathrm{mod}\, 5) \\ 8x \equiv 10 (\mathrm{mod}\, 14) \end{cases}$;

р) $\begin{cases} 4x \equiv 13 (\mathrm{mod}\, 7) \\ 15x \equiv -5 (\mathrm{mod}\, 20) \\ 7x \equiv -1 (\mathrm{mod}\, 12) \end{cases}$;

с) $\begin{cases} 11x \equiv -2 (\mathrm{mod}\, 6) \\ 10x \equiv 6 (\mathrm{mod}\, 14) \\ 12x \equiv 15 (\mathrm{mod}\, 27) \end{cases}$;

т) $\begin{cases} 28x \equiv -20 (\mathrm{mod}\, 48) \\ 3x \equiv 7 (\mathrm{mod}\, 8) \\ 9x \equiv -18 (\mathrm{mod}\, 45) \end{cases}$;

у) $\begin{cases} 15x \equiv 15 (\mathrm{mod}\, 36) \\ 3x \equiv -1 (\mathrm{mod}\, 8) \\ 3x \equiv 9 (\mathrm{mod}\, 15) \end{cases}$;

ф) $\begin{cases} 32x \equiv -4 (\mathrm{mod}\, 60) \\ 9x \equiv 3 (\mathrm{mod}\, 6) \\ 4x \equiv -8 (\mathrm{mod}\, 10) \end{cases}$;

х) $\begin{cases} 16x \equiv 28 (\mathrm{mod}\, 30) \\ 12x \equiv 16 (\mathrm{mod}\, 20) \\ 18x \equiv 6 (\mathrm{mod}\, 12). \end{cases}$;

ц) $\begin{cases} 28x \equiv 20 (\mathrm{mod}\, 48) \\ 6x \equiv -2 (\mathrm{mod}\, 16) \\ 9x \equiv 27 (\mathrm{mod}\, 45) \end{cases}$;

ч) $\begin{cases} 30x \equiv -42 (\mathrm{mod}\, 72) \\ 9x \equiv -3 (\mathrm{mod}\, 8) \\ 3x \equiv 9 (\mathrm{mod}\, 15) \end{cases}$;

ш) $\begin{cases} 92x \equiv 56 (\mathrm{mod}\, 60) \\ 9x \equiv 3 (\mathrm{mod}\, 6) \\ 4x \equiv -4 (\mathrm{mod}\, 10) \end{cases}$;

щ) $\begin{cases} 16x \equiv -32 (\mathrm{mod}\, 30) \\ 24x \equiv -8 (\mathrm{mod}\, 40) \\ 9x \equiv 3 (\mathrm{mod}\, 6). \end{cases}$

12. Решите сравнение:

а) $888x^{963} - 101x^{404} + 52x^{211} + 88x^{323} + 119 \equiv 0 (\mathrm{mod}\, 7)$;

б) $372x^{541} + 107x^{297} - 32x^{239} + 63x^{65} + 129 \equiv 0 (\mathrm{mod}\, 5)$;

в) $445x^{526} + 43x^{264} - 89x^{263} + 226x^{262} + 102 \equiv 0 (\mathrm{mod}\, 7)$;

г) $1003x^{573} + 174x^{345} - 251x^{282} - 102x^{103} + 101x^{48} - 92 \equiv 0 (\mathrm{mod}\, 5)$;

д) $773x^{330} - 461x^{478} + 125x^{101} - 69x^{99} - 1 \equiv 0 (\mathrm{mod}\, 7)$;

е) $333x^{333} - 281x^{281} + 134x^{134} + 103x^{103} - 84x^{84} + 53 \equiv 0 (\mathrm{mod}\, 5)$;

ж) $748x^{903} - 318x^{524} + 129x^{337} + 81x^{203} + 84 \equiv 0 (\mathrm{mod}\, 7)$;

з) $283x^{283} - 601x^{601} + 55x^{55} - 33x^{33} + 28 \equiv 0 (\mathrm{mod}\, 5)$;

и) $803x^{396} - 601x^{484} + 55x^{221} - 83x^{105} + 34 \equiv 0 (\mathrm{mod}\, 7)$;

к) $152x^{343} - 704x^{201} + 105x^{75} - 102x^{29} + 2317 \equiv 0 (\mathrm{mod}\ 5)$;
л) $305x^{406} + 113x^{204} - 159x^{143} + 296x^{142} + 32 \equiv 0 (\mathrm{mod}\ 7)$;
м) $353x^{401} - 202x^{253} - 103x^{209} - 68x^{25} + 111 \equiv 0 (\mathrm{mod}\ 5)$;
н) $881x^{969} - 108x^{410} + 59x^{211} + 88x^{323} + 119 \equiv 0 (\mathrm{mod}\ 7)$;
о) $883x^{963} - 106x^{484} + 59x^{241} + 87x^{233} + 84 \equiv 0 (\mathrm{mod}\ 5)$;
п) $438x^{532} + 50x^{270} - 82x^{269} + 226x^{262} + 102 \equiv 0 (\mathrm{mod}\ 7)$;
р) $377x^{545} - 102x^{293} - 37x^{243} + 63x^{65} + 129 \equiv 0 (\mathrm{mod}\ 5)$;
с) $452x^{520} + 50x^{270} - 82x^{269} + 226x^{262} + 102 \equiv 0 (\mathrm{mod}\ 7)$;
т) $998x^{577} - 171x^{349} - 256x^{286} - 102x^{103} + 101x^{48} - 92 \equiv 0 (\mathrm{mod}\ 5)$;
у) $780x^{336} - 468x^{472} + 125x^{107} - 69x^{99} - 1 \equiv 0 (\mathrm{mod}\ 7)$;
ф) $338x^{329} + 284x^{285} - 131x^{130} + 103x^{103} - 84x^{84} + 53 \equiv 0 (\mathrm{mod}\ 5)$;
х) $741x^{909} - 311x^{530} + 122x^{331} + 81x^{203} + 84 \equiv 0 (\mathrm{mod}\ 7)$;
ц) $288x^{279} + 604x^{605} + 550x^{55} - 33x^{33} + 28 \equiv 0 (\mathrm{mod}\ 5)$;
ч) $817x^{390} - 615x^{460} + 90x^{226} - 83x^{105} + 34 \equiv 0 (\mathrm{mod}\ 7)$;
ш) $192x^{347} + 801x^{205} + 1005x^{95} - 102x^{29} + 2317 \equiv 0 (\mathrm{mod}\ 5)$;
щ) $340x^{412} + 120x^{210} - 152x^{149} + 296x^{142} + 32 \equiv 0 (\mathrm{mod}\ 7)$.

13. Вычислите значение символа Лежандра:

а) $(-288/509)$;
б) $(-363/701)$;
в) $(-288/401)$;
г) $(-363/563)$;
д) $(-288/709)$;
е) $(-363/577)$;
ж) $(-288/733)$;
з) $(-363/433)$;
и) $(-288/593)$;
к) $(-363/743)$;
л) $(-288/449)$;
м) $(-363/607)$;
н) $(-288/761)$;
о) $(-363/457)$;
п) $(-288/613)$;
р) $(-363/769)$;
с) $(-288/461)$;
т) $(-363/617)$;
у) $(-288/773)$;
ф) $(-363/463)$;
х) $(-288/619)$;
ц) $(-363/787)$;
ч) $(-288/467)$;
ш) $(-363/631)$;
щ) $(-288/797)$.

14. Сколько решений имеет сравнение:

а) $x^2 \equiv 56 (\mathrm{mod}\ 13)$;
б) $x^2 \equiv 10 (\mathrm{mod}\ 13)$;
в) $x^2 \equiv 10 (\mathrm{mod}\ 17)$;
г) $x^2 \equiv 14 (\mathrm{mod}\ 17)$;
д) $x^2 \equiv 40 (\mathrm{mod}\ 79)$;
е) $x^2 \equiv 21 (\mathrm{mod}\ 79)$;
ж) $x^2 \equiv 33 (\mathrm{mod}\ 97)$;
з) $x^2 \equiv 26 (\mathrm{mod}\ 97)$;
и) $x^2 \equiv 66 (\mathrm{mod}\ 19)$;
к) $x^2 \equiv 130 (\mathrm{mod}\ 19)$;
л) $x^2 \equiv 99 (\mathrm{mod}\ 23)$;
м) $x^2 \equiv 77 (\mathrm{mod}\ 23)$;
н) $x^2 \equiv 40 (\mathrm{mod}\ 29)$;
о) $x^2 \equiv 10 (\mathrm{mod}\ 29)$;
п) $x^2 \equiv 21 (\mathrm{mod}\ 31)$;
р) $x^2 \equiv 15 (\mathrm{mod}\ 31)$;
с) $x^2 \equiv 22 (\mathrm{mod}\ 37)$;
т) $x^2 \equiv 26 (\mathrm{mod}\ 37)$;
у) $x^2 \equiv 14 (\mathrm{mod}\ 41)$;
ф) $x^2 \equiv 21 (\mathrm{mod}\ 41)$;
х) $x^2 \equiv 10 (\mathrm{mod}\ 43)$;
ц) $x^2 \equiv 35 (\mathrm{mod}\ 43)$;
ч) $x^2 \equiv 34 (\mathrm{mod}\ 47)$;
ш) $x^2 \equiv 39 (\mathrm{mod}\ 47)$;
щ) $x^2 \equiv 10 (\mathrm{mod}\ 53)$?

15. Сколько решений имеет сравнение:

а) $x^2+5x-4\equiv 0(\mathrm{mod}\,19)$;
б) $x^2+2x+4\equiv 0(\mathrm{mod}\,19)$;
в) $x^2+x+8\equiv 0(\mathrm{mod}\,23)$;
г) $x^2-x-8\equiv 0(\mathrm{mod}\,23)$;
д) $x^2+5x-1\equiv 0(\mathrm{mod}\,13)$;
е) $x^2-5x+1\equiv 0(\mathrm{mod}\,13)$;
ж) $x^2+2x+3\equiv 0(\mathrm{mod}\,17)$;
з) $x^2-2x-7\equiv 0(\mathrm{mod}\,17)$;
и) $x^2+3x+2\equiv 0(\mathrm{mod}\,29)$;
к) $x^2-3x+4\equiv 0(\mathrm{mod}\,29)$;
л) $x^2+5x-2\equiv 0(\mathrm{mod}\,31)$;
м) $x^2-5x+3\equiv 0(\mathrm{mod}\,31)$;
н) $x^2+x+4\equiv 0(\mathrm{mod}\,37)$;
о) $x^2-x+5\equiv 0(\mathrm{mod}\,37)$;
п) $x^2+6x+1\equiv 0(\mathrm{mod}\,41)$;
р) $x^2-6x+1\equiv 0(\mathrm{mod}\,41)$;
с) $x^2+5x+3\equiv 0(\mathrm{mod}\,43)$;
т) $x^2+3x+5\equiv 0(\mathrm{mod}\,43)$;
у) $x^2-x+7\equiv 0(\mathrm{mod}\,47)$;
ф) $x^2-x-7\equiv 0(\mathrm{mod}\,47)$;
х) $x^2+5x+5\equiv 0(\mathrm{mod}\,53)$;
ц) $x^2+4x+1\equiv 0(\mathrm{mod}\,53)$;
ч) $x^2-x+1\equiv 0(\mathrm{mod}\,57)$;
ш) $x^2+x-11\equiv 0(\mathrm{mod}\,57)$;
щ) $x^2-x-11\equiv 0(\mathrm{mod}\,59)$?

16. Сколько решений имеет сравнение:

а) $70x^2-2x+13\equiv 0(\mathrm{mod}\,695)$;
б) $70x^2+2x+23\equiv 0(\mathrm{mod}\,695)$;
в) $36x^2+x+40\equiv 0(\mathrm{mod}\,321)$;
г) $36x^2-x+17\equiv 0(\mathrm{mod}\,321)$;
д) $55x^2-x+17\equiv 0(\mathrm{mod}\,545)$;
е) $55x^2+x+18\equiv 0(\mathrm{mod}\,545)$;
ж) $86x^2-x+17\equiv 0(\mathrm{mod}\,346)$;
з) $86x^2+x+43\equiv 0(\mathrm{mod}\,346)$;
и) $57x^2+x+16\equiv 0(\mathrm{mod}\,339)$;
к) $57x^2-2x+19\equiv 0(\mathrm{mod}\,339)$;
л) $66x^2-x+35\equiv 0(\mathrm{mod}\,262)$;
м) $66x^2+x+33\equiv 0(\mathrm{mod}\,262)$;
н) $75x^2-x+24\equiv 0(\mathrm{mod}\,745)$;
о) $75x^2+x-26\equiv 0(\mathrm{mod}\,745)$;
п) $90x^2-x+44\equiv 0(\mathrm{mod}\,905)$;
р) $90x^2+x-29\equiv 0(\mathrm{mod}\,905)$;
с) $51x^2+x+23\equiv 0(\mathrm{mod}\,453)$;
т) $51x^2-x+38\equiv 0(\mathrm{mod}\,453)$;
у) $105x^2-2x+35\equiv 0(\mathrm{mod}\,633)$;
ф) $105x^2-x+53\equiv 0(\mathrm{mod}\,633)$;
х) $35x^2-x-17\equiv 0(\mathrm{mod}\,515)$;
ц) $35x^2+x+11\equiv 0(\mathrm{mod}\,515)$;
ч) $94x^2+x+47\equiv 0(\mathrm{mod}\,849)$;
ш) $94x^2-x+71\equiv 0(\mathrm{mod}\,849)$;
щ) $74x^2-x+35\equiv 0(\mathrm{mod}\,446)$?

17. Найдите:

а) $P_{13}(8)$;
б) $P_{17}(9)$;
в) $P_{19}(16)$;
г) $P_{23}(4)$;
д) $P_{29}(25)$;
е) $P_{31}(27)$;
ж) $P_{37}(8)$;
з) $P_{41}(32)$;
и) $P_{43}(16)$;
к) $P_{47}(4)$;
л) $P_{53}(9)$;
м) $P_{57}(32)$;
н) $P_{59}(27)$;
о) $P_{61}(49)$;
п) $P_{67}(25)$;
р) $P_{71}(32)$;
с) $P_{73}(49)$;
т) $P_{79}(27)$;
у) $P_{83}(64)$;
ф) $P_{87}(25)$;
х) $P_{89}(16)$;
ц) $P_{97}(81)$;
ч) $P_{61}(32)$;
ш) $P_{67}(16)$;
щ) $P_{71}(49)$.

18. Найдите:

а) $P_{43\cdot65^4}(12)$;
б) $P_{23\cdot65^5}(12)$;
в) $P_{41\cdot65^6}(12)$;
г) $P_{29\cdot33^4}(10)$;
д) $P_{19\cdot33^5}(10)$;
е) $P_{13\cdot33^6}(10)$;
ж) $P_{47\cdot91^4}(12)$;
з) $P_{53\cdot91^5}(12)$;
и) $P_{11\cdot91^6}(12)$;
к) $P_{59\cdot77^4}(10)$;
л) $P_{31\cdot77^5}(10)$;
м) $P_{17\cdot77^6}(10)$;
н) $P_{61\cdot65^4}(12)$;
о) $P_{13\cdot65^5}(12)$;
п) $P_{19\cdot65^6}(12)$;
р) $P_{67\cdot33^4}(10)$;
с) $P_{53\cdot33^5}(10)$;
т) $P_{47\cdot33^6}(10)$;
у) $P_{71\cdot91^4}(12)$;
ф) $P_{79\cdot91^5}(12)$;
х) $P_{31\cdot91^6}(12)$;
ц) $P_{83\cdot77^4}(10)$;
ч) $P_{89\cdot77^5}(10)$;
ш) $P_{29\cdot77^6}(10)$;
щ) $P_{97\cdot65^4}(12)$.

19. Найдите длину периода десятичной записи дроби:

а) 6/14;
б) 10/65;
в) 12/21;
г) 10/26;
д) 8/14;
е) 15/65;
ж) 9/21;
з) 8/26;
и) 10/14;
к) 20/65;
л) 3/21;
м) 18/26;
н) 4/14;
о) 30/65;
п) 6/21;
р) 24/26;
с) 2/14;
т) 25/65;
у) 15/21;
ф) 6/26;
х) 12/14;
ц) 45/65;
ч) 18/21;
ш) 24/26;
щ) 2/26.

20. Найдите длину периода g-ичной записи дроби:

а) $33/(37\cdot210^6)$, $g=10$;
б) $39/(59\cdot130^4)$, $g=14$;
в) $35/(23\cdot150^6)$, $g=12$;
г) $35/(37\cdot42^7)$, $g=15$;
д) $14/(61\cdot105^6)$, $g=10$;
е) $55/(23\cdot195^4)$, $g=12$;
ж) $77/(53\cdot42^6)$, $g=15$;
з) $85/(23\cdot195^4)$, $g=12$;
и) $21/(31\cdot330^5)$, $g=10$;
к) $91/(71\cdot130^4)$, $g=14$;
л) $91/(73\cdot105^6)$, $g=10$;
м) $175/(37\cdot42^8)$, $g=15$;
н) $20/(43\cdot195^4)$, $g=12$;
о) $35/(23\cdot30^5)$, $g=14$;
п) $15/(23\cdot390^4)$, $g=10$;
р) $21/(13\cdot77^{15})$, $g=22$;
с) $85/(23\cdot30^6)$, $g=14$;
т) $15/(19\cdot66^5)$, $g=11$;
у) $65/(17\cdot210^6)$, $g=12$;
ф) $21/(31\cdot66^5)$, $g=10$;
х) $21/(19\cdot140^5)$, $g=22$;
ц) $49/(17\cdot70^5)$, $g=15$;
ч) $18/(47\cdot210^6)$, $g=14$;
ш) $15/(17\cdot110^4)$, $g=11$;
щ) $65/(17\cdot105^6)$, $g=10$.

21. Решите сравнение:

а) $19x^{25} \equiv 39 (\mathrm{mod}\, 61)$;
б) $10x^{18} \equiv 17 (\mathrm{mod}\, 67)$;
в) $44x^{49} \equiv 48 (\mathrm{mod}\, 71)$;
г) $66x^{40} \equiv 33 (\mathrm{mod}\, 89)$;
д) $81x^{18} \equiv 73 (\mathrm{mod}\, 97)$;
е) $42x^{25} \equiv 22 (\mathrm{mod}\, 61)$;
ж) $124x^{18} \equiv 50 (\mathrm{mod}\, 67)$;
з) $27x^{49} \equiv 23 (\mathrm{mod}\, 71)$;
и) $23x^{40} \equiv 56 (\mathrm{mod}\, 89)$;
к) $16x^{18} \equiv 24 (\mathrm{mod}\, 97)$;
л) $29x^{42} \equiv 10 (\mathrm{mod}\, 61)$;
м) $57x^{18} \equiv 50 (\mathrm{mod}\, 67)$;
н) $112x^{40} \equiv 56 (\mathrm{mod}\, 89)$;
о) $178x^{18} \equiv 73 (\mathrm{mod}\, 97)$;
п) $92x^{42} \equiv 51 (\mathrm{mod}\, 61)$;
р) $77x^{18} \equiv 84 (\mathrm{mod}\, 67)$;
с) $155x^{40} \equiv 33 (\mathrm{mod}\, 89)$;
т) $32x^{18} \equiv 48 (\mathrm{mod}\, 97)$;
у) $32x^{42} \equiv 51 (\mathrm{mod}\, 61)$;
ф) $77x^{18} \equiv 17 (\mathrm{mod}\, 67)$;
х) $166x^{18} \equiv 49 (\mathrm{mod}\, 97)$;
ц) $90x^{42} \equiv 10 (\mathrm{mod}\, 61)$;
ч) $113x^{18} \equiv 24 (\mathrm{mod}\, 97)$;
ш) $90x^{42} \equiv 10 (\mathrm{mod}\, 61)$;
щ) $105x^{116} \equiv 273 (\mathrm{mod}\, 97)$.

22. Используя таблицы индексов, найдите:

а) все $x \in [20, 30]$, такие что $P_{31}(x) = 15$;
б) все $x \in [1, 10]$, такие что $P_{37}(x) = 12$;
в) все $x \in [20, 30]$, такие что $P_{43}(x) = 14$;
г) все $x \in [5, 15]$, такие что $P_{47}(x) = 23$;
д) все $x \in [20, 50]$, такие что $P_{61}(x) = 15$;
е) все $x \in [5, 20]$, такие что $P_{31}(x) = 10$;
ж) все $x \in [5, 15]$, такие что $P_{37}(x) = 3$;
з) все $x \in [10, 30]$, такие что $P_{43}(x) = 7$;
и) все $x \in [5, 20]$, такие что $P_{47}(x) = 2$;
к) все $x \in [15, 25]$, такие что $P_{61}(x) = 30$;
л) все $x \in [20, 30]$, такие что $P_{31}(x) = 6$;
м) все $x \in [20, 35]$, такие что $P_{37}(x) = 18$;
н) все $x \in [20, 30]$, такие что $P_{43}(x) = 21$;
о) все $x \in [5, 25]$, такие что $P_{47}(x) = 23$;
п) все $x \in [20, 40]$, такие что $P_{61}(x) = 10$;
р) все $x \in [1, 15]$, такие что $P_{31}(x) = 5$;
с) все $x \in [10, 35]$, такие что $P_{37}(x) = 4$;
т) все $x \in [20, 30]$, такие что $P_{43}(x) = 6$;
у) все $x \in [20, 45]$, такие что $P_{61}(x) = 5$;
ф) все $x \in [25, 45]$, такие что $P_{31}(x) = 2$;
х) все $x \in [20, 35]$, такие что $P_{37}(x) = 6$;

ц) все $x \in [1, 20]$, такие что $P_{43}(x) = 2$;
ч) все $x \in [10, 40]$, такие что $P_{61}(x) = 12$;
ш) все $x \in [10, 30]$, такие что $P_{43}(x) = 14$;
щ) все $x \in [15, 40]$, такие что $P_{61}(x) = 6$.

23. Используя таблицы индексов, найдите все первообразные корни:
а) по модулю 47 на отрезке $[5, 20]$;
б) по модулю 29 на отрезке $[5, 20]$;
в) по модулю 37 на отрезке $[25, 35]$;
г) по модулю 41 на отрезке $[10, 22]$;
д) по модулю 43 на отрезке $[10, 20]$;
е) по модулю 47 на отрезке $[15, 22]$;
ж) по модулю 61 на отрезке $[1, 11]$;
з) по модулю 29 на отрезке $[1, 25]$;
и) по модулю 37 на отрезке $[20, 34]$;
к) по модулю 41 на отрезке $[20, 38]$;
л) по модулю 43 на отрезке $[10, 20]$;
м) по модулю 47 на отрезке $[15, 23]$;
н) по модулю 61 на отрезке $[1, 12]$;
о) по модулю 29 на отрезке $[5, 14]$;
п) по модулю 37 на отрезке $[2, 18]$;
р) по модулю 41 на отрезке $[3, 19]$;
с) по модулю 47 на отрезке $[4, 14]$;
т) по модулю 37 на отрезке $[25, 36]$;
у) по модулю 41 на отрезке $[20, 42]$;
ф) по модулю 47 на отрезке $[6, 21]$;
х) по модулю 37 на отрезке $[18, 36]$;
ц) по модулю 47 на отрезке $[15, 23]$;
ч) по модулю 37 на отрезке $[4, 24]$;
ш) по модулю 47 на отрезке $[15, 26]$;
щ) по модулю 47 на отрезке $[6, 15]$.

24. Используя таблицы индексов, найдите:
а) все квадратичные вычеты по модулю 19 на отрезке $[3, 15]$;
б) все квадратичные вычеты по модулю 31 на отрезке $[1, 12]$;
в) все квадратичные невычеты по модулю 37 на отрезке $[10, 15]$;
г) все квадратичные невычеты по модулю 41 на отрезке $[1, 9]$;

д) все квадратичные невычеты по модулю 43 на отрезке [15, 25];
е) все квадратичные невычеты по модулю 47 на отрезке [10, 15];
ж) все квадратичные вычеты по модулю 61 на отрезке [20, 25];
з) все квадратичные невычеты по модулю 19 на отрезке [3, 15].
и) все квадратичные невычеты по модулю 31 на отрезке [10, 20];
к) все квадратичные вычеты по модулю 37 на отрезке [1, 10];
л) все квадратичные вычеты по модулю 41 на отрезке [10, 18];
м) все квадратичные вычеты по модулю 43 на отрезке [10, 20];
н) все квадратичные вычеты по модулю 47 на отрезке [3, 15].
о) все квадратичные вычеты по модулю 61 на отрезке [15, 25];
п) все квадратичные вычеты по модулю 31 на отрезке [1, 12];
р) все квадратичные невычеты по модулю 37 на отрезке [10, 20].
с) все квадратичные невычеты по модулю 41 на отрезке [1, 9];
т) все квадратичные вычеты по модулю 43 на отрезке [1, 8];
у) все квадратичные вычеты по модулю 47 на отрезке [1, 7].
ф) все квадратичные невычеты по модулю 61 на отрезке [1, 10].
х) все квадратичные невычеты по модулю 31 на отрезке [10, 20];
ц) все квадратичные невычеты по модулю 37 на отрезке [10, 15];
ч) все квадратичные вычеты по модулю 41 на отрезке [10, 18];
ш) все квадратичные невычеты по модулю 43 на отрезке [15, 25];
щ) все квадратичные невычеты по модулю 47 на отрезке [3, 15].

25. Найдите остаток от деления:

а) $37^{32^{19}}$ на 83;
б) $46^{32^{19}}$ на 83;
в) $10^{49^{17}}$ на 23;
г) $13^{49^{17}}$ на 23;
д) $27^{48^{30}}$ на 59;
е) $32^{48^{30}}$ на 59;
ж) $16^{31^{21}}$ на 53;
з) $37^{31^{21}}$ на 53;
и) $33^{18^{46}}$ на 83;
к) $50^{18^{46}}$ на 83;
л) $21^{31^{47}}$ на 59;
м) $38^{31^{47}}$ на 59;
н) $40^{32^{20}}$ на 83;
о) $43^{32^{20}}$ на 83;
п) $12^{49^{40}}$ на 23;
р) $11^{49^{40}}$ на 23;
с) $34^{48^{15}}$ на 59;
т) $25^{48^{15}}$ на 59;
у) $30^{31^{25}}$ на 53;
ф) $23^{31^{25}}$ на 53;
х) $55^{18^{44}}$ на 83;
ц) $28^{18^{44}}$ на 83;
ч) $20^{31^{50}}$ на 59;
ш) $39^{31^{50}}$ на 59;
щ) $14^{48^{16}}$ на 59.

26. Найдите:

а) все индексы числа 39 по модулю 11;
б) все индексы числа 27 по модулю 11;
в) все индексы числа 17 по модулю 11;

г) все индексы числа 28 по модулю 11;
д) все индексы числа -16 по модулю 11;
е) все индексы числа -50 по модулю 11;
ж) все индексы числа -27 по модулю 11;
з) все индексы числа -39 по модулю 11;
и) все индексы числа 28 по модулю 13;
к) все индексы числа 21 по модулю 13;
л) все индексы числа 31 по модулю 13;
м) все индексы числа 34 по модулю 13;
н) все индексы числа -11 по модулю 13;
о) все индексы числа -18 по модулю 13;
п) все индексы числа -21 по модулю 13;
р) все индексы числа -31 по модулю 13;
с) все индексы числа 23 по модулю 19;
т) все индексы числа 42 по модулю 19.
у) все индексы числа 14 по модулю 19;
ф) все индексы числа 33 по модулю 19;
х) все индексы числа -10 по модулю 19;
ц) все индексы числа -30 по модулю 19;
ч) все индексы числа -12 по модулю 19;
ш) все индексы числа -15 по модулю 19;
щ) все индексы числа -34 по модулю 19.

27. а) Найдите рациональное приближение числа $\dfrac{-7+\sqrt{17}}{4}$ с точностью $\Delta = 10^{-2}$ с избытком.

б) Найдите рациональное приближение числа $\dfrac{-15+\sqrt{85}}{10}$ с точностью $\Delta = 10^{-2}$ с недостатком.

в) Найдите рациональное приближение числа $\dfrac{-5+\sqrt{10}}{3}$ с точностью $\Delta = 10^{-2}$ с избытком.

г) Найдите рациональное приближение числа $\dfrac{-10+\sqrt{10}}{3}$ с точностью $\Delta = 10^{-2}$ с недостатком.

д) Найдите рациональное приближение числа $\dfrac{-17+\sqrt{85}}{6}$ с точностью $\Delta = 10^{-2}$ с избытком.

е) Найдите рациональное приближение числа $\dfrac{-5+\sqrt{17}}{2}$ с точностью $\Delta = 10^{-2}$ с избытком.

ж) Найдите рациональное приближение числа $\dfrac{-4+\sqrt{10}}{2}$ с точностью $\Delta = 10^{-2}$ с недостатком.

з) Найдите рациональное приближение числа $\dfrac{-17+\sqrt{17}}{4}$ с точностью $\Delta = 10^{-2}$ с избытком.

и) Найдите число $\alpha = [-1, (2, 2, 1)]$ и его рациональное приближение с точностью $\Delta = 10^{-2}$ с недостатком.

к) Найдите число $\alpha = [-3, (1, 2, 1)]$ и его рациональное приближение с точностью $\Delta = 10^{-2}$ с избытком.

л) Найдите число $\alpha = [-1, (2, 1, 1)]$ и его рациональное приближение с точностью $\Delta = 10^{-2}$ с избытком.

м) Найдите число $\alpha = [-2, (1, 2, 2)]$ и его рациональное приближение с точностью $\Delta = 10^{-2}$ с избытком.

н) Найдите число $\alpha = [-1, (3, 1, 1)]$ и его рациональное приближение с точностью $\Delta = 10^{-2}$ с избытком.

о) Найдите число $\alpha = [-1, (1, 1, 3)]$ и его рациональное приближение с точностью $\Delta = 10^{-2}$ с избытком.

п) Найдите число $\alpha = [-4, (1, 3, 1)]$ и его рациональное приближение с точностью $\Delta = 10^{-2}$ с избытком.

р) Найдите число $\alpha = [-1, (1, 1, 2)]$ и его рациональное приближение с точностью $\Delta = 10^{-2}$ с недостатком.

с) Найдите число $\alpha = [-1, (2, 1, 1)]$ и его наилучшее приближение a/b со знаменателем $b \leqslant 20$. Укажите, с избытком или с недостатком полученные приближение.

т) Найдите число $\alpha = [-2, (1, 2, 2)]$ и его наилучшее приближение a/b со знаменателем $b \leqslant 30$. Укажите, с избытком или с недостатком полученное приближение.

у) Найдите число $\alpha = [-4, (1, 3, 1)]$ и его наилучшее приближение a/b со знаменателем $b \leqslant 40$. Укажите, с избытком или с недостатком полученные приближение.

ф) Найдите число $\alpha = [-3, (1, 2, 1)]$ и его наилучшее приближение a/b со знаменателем $b \leqslant 20$. Укажите, с избытком или с недостатком полученные приближение.

х) Найдите число $\alpha = [-1, (2, 1, 1)]$ и его наилучшее приближение a/b со знаменателем $b \leqslant 20$. Укажите, с избытком или с недостатком полученные приближение.

ц) Найдите для числа $\alpha = \dfrac{-4+\sqrt{10}}{2}$ его наилучшее приближение a/b со знаменателем $b \leqslant 40$. Укажите, с избытком или с недостатком полученное приближение.

ч) Найдите для числа $\alpha = \dfrac{-15+\sqrt{85}}{10}$ его наилучшее приближение a/b со знаменателем $b \leqslant 20$. Укажите, с избытком или с недостатком полученное приближение.

ш) Найдите для числа $\alpha = \dfrac{-7+\sqrt{17}}{4}$ его наилучшее приближение a/b со знаменателем $b \leqslant 10$. Укажите, с избытком или с недостатком полученное приближение.

щ) Найдите для числа $\alpha = \dfrac{-5+\sqrt{17}}{2}$ его наилучшее приближение a/b со знаменателем $b \leqslant 20$. Укажите, с избытком или с недостатком полученное приближение.

28. Сократите дробь:

а) 1558/2736;
б) 2736/1558;
в) 4961/8712;
г) 8712/4961;
д) 2054/936;
е) 936/2054;
ж) 1027/480;
з) 480/1027;
и) 1368/779;
к) 779/1368;
л) 1584/902;
м) 902/1584;
н) 2232/1798;
о) 1798/2239;
п) 1872/1508;
р) 1508/1872;
с) 3094/1972;
т) 1972/3094;
у) 1276/2002;
ф) 2002/1296;
х) 1116/899;
ц) 899/1116;
ч) 1547/986;
ш) 1027/468;
щ) 468/1027.

29. Решите уравнение:

а) $848y + 378x = -6$;
б) $342y + 286x = -4$;
в) $206x - 762y = -4$;
г) $855y - 715x = 10$;
д) $309y - 1143x = 6$;
е) $1050y - 618x = 30$;
ж) $424x - 189y = 3$;
з) $171y + 143x = 2$;
и) $103x - 381y = 2$;
к) $175x - 103y = 5$;
л) $525y - 309x = 15$;
м) $848y - 378x = 12$;
н) $286x - 342y = 8$;
о) $762x - 206y = 12$;
п) $855x + 715y = -15$;
р) $309x - 1143y = 9$;

с) $618y + 1050x = 6$;
т) $189x + 424y = -5$;
у) $143y - 171x = 7$;
ф) $103x + 381y = -8$;
х) $175y + 103x = 10$;
ц) $309y + 525x = -6$;
ч) $848x + 378y = 26$;
ш) $342y - 286x = -22$;
щ) $206y - 762x = 14$.

30. а) Найдите все целые решения (x, y) уравнений $x^2 - Dy^2 = \pm 1$, удовлетворяющие условию $x, y \in [-200, 200]$, если $\sqrt{D} = [3, (3, 6)]$.

б) Найдите все целые решения (x, y) уравнений $x^2 - Dy^2 = \pm 1$, удовлетворяющие условию $|x| \leqslant 100$, если $\sqrt{D} = [2, (2, 4)]$.

в) Найдите все целые решения (x, y) уравнений $x^2 - Dy^2 = \pm 1$, удовлетворяющие условию $|y| \leqslant 300$, если $\sqrt{D} = [5, (5, 10)]$.

г) Найдите все целые решения (x, y) уравнений $x^2 - Dy^2 = \pm 1$, удовлетворяющие условию $x, y \in [-220, 220]$, если $\sqrt{D} = [3, (1, 6)]$.

д) Найдите все целые решения (x, y) уравнений $x^2 - Dy^2 = \pm 1$, удовлетворяющие условию $x, y \in [-90, 90]$, если $\sqrt{D} = [2, (1, 4)]$.

е) Найдите все целые решения (x, y) уравнений $x^2 - Dy^2 = \pm 1$, удовлетворяющие условию $|y| \leqslant 200$, если $\sqrt{D} = [6, (4, 12)]$.

ж) Найдите все целые решения (x, y) уравнений $x^2 - Dy^2 = \pm 1$, удовлетворяющие условию $|x| \leqslant 350$, если $\sqrt{D} = [8, (2, 16)]$.

з) Найдите все целые решения (x, y) уравнений $x^2 - Dy^2 = \pm 1$, удовлетворяющие условию $x, y \in [-11, 100]$, если $\sqrt{D} = [4, (1, 8)]$.

и) Найдите все целые решения (x, y) уравнений $x^2 - 6y^2 = \pm 1$, удовлетворяющие условию $x, y \in [-150, 100]$.

к) Найдите все целые решения (x, y) уравнений $x^2 - 11y^2 = \pm 1$, удовлетворяющие условию $|y| \leqslant 100$.

л) Найдите все целые решения (x, y) уравнений $x^2 - 72y^2 = \pm 1$, удовлетворяющие условию $x, y \in [-320, 320]$.

м) Найдите все целые решения (x, y) уравнений $x^2 - 8y^2 = \pm 1$, удовлетворяющие условию $|x| \leqslant 95$.

н) Найдите все целые решения (x, y) уравнений $x^2 - 99y^2 = \pm 1$, удовлетворяющие условию $x, y \in [-90, 90]$.

о) Найдите все целые решения (x, y) уравнений $x^2 - 32y^2 = \pm 1$, удовлетворяющие условию $|x| \leqslant 350$.

п) Найдите все целые решения (x, y) уравнений $x^2 - 24y^2 = \pm 1$, удовлетворяющие условию $x, y \in [-100, 100]$.

р) Найдите все целые решения (x, y) уравнений $x^2 - 39y^2 = \pm 1$, удовлетворяющие условию $|y| \leqslant 200$.

с) Найдите все целые решения (x, y) уравнений $x^2 - 44y^2 = \pm 1$, удовлетворяющие условию $x, y \in [-200, 200]$.

т) Найдите все целые решения (x, y) уравнений $x^2 - 54y^2 = \pm 1$, удовлетворяющие условию $|x| \leqslant 100$.

у) Найдите все целые решения (x, y) уравнений $x^2 - 60y^2 = \pm 1$, удовлетворяющие условию $x, y \in [-220, 220]$.

ф) Найдите все целые решения (x, y) уравнений $x^2 - 15y^2 = \pm 1$, удовлетворяющие условию $|x| \leqslant 220$.

х) Найдите все целые решения (x, y) уравнений $x^2 - 27y^2 = \pm 1$, удовлетворяющие условию $x, y \in [-250, 100]$.

ц) Найдите все целые решения (x, y) уравнений $x^2 - 96y^2 = \pm 1$, удовлетворяющие условию $|x| \leqslant 100$.

ч) Найдите все целые решения (x, y) уравнений $x^2 - 15y^2 = \pm 1$, удовлетворяющие условию $x, y \in [-220, 120]$.

ш) Найдите все целые решения (x, y) уравнений $x^2 - 3y^2 = \pm 1$, удовлетворяющие условию $|x| \leqslant 220$.

щ) Найдите все целые решения (x, y) уравнений $x^2 - 108y^2 = \pm 1$, удовлетворяющие условию $x, y \in [-100, 210]$.

§ 2. Задачи лабораторной работы по теме «Сравнения по составному модулю»

Решите сравнение:

1. $x^5 - 2x^4 + 4x^3 - 6x^2 + 5x \equiv 0 (\mathrm{mod}\ 18)$;
2. $5x^2 + 7x + 2 \equiv 0 (\mathrm{mod}\ 36)$;
3. $x^3 + 17x^2 + 16x + 12 \equiv 0 (\mathrm{mod}\ 40)$
4. $x^5 - 2x^4 + 4x^3 - 6x^2 + 5x \equiv 0 (\mathrm{mod}\ 54)$;
5. $x^3 - 10x^2 + 6x - 24 \equiv 0 (\mathrm{mod}\ 72)$;
6. $5x^2 - x - 4 \equiv 0 (\mathrm{mod}\ 72)$;
7. $x^4 - 3x^3 + 4x^2 + 2x + 12 \equiv 0 (\mathrm{mod}\ 72)$;
8. $6x^5 - 17x^4 + 5x^3 + 15x^2 - 11x + 20 \equiv 0 (\mathrm{mod}\ 72)$;
9. $x^{100} + x^{50} + 9x + 11 \equiv 0 (\mathrm{mod}\ 88)$;
10. $x^4 + x^3 - 3x^2 - 4x + 1 \equiv 0 (\mathrm{mod}\ 100)$;
11. $x^4 - x^3 + 2x^2 + 12x + 18 \equiv 0 (\mathrm{mod}\ 108)$;
12. $x^5 - 2x^4 + 4x^3 - 6x^2 + 17x + 3 \equiv 0 (\mathrm{mod}\ 135)$;
13. $x^5 + 3x^4 - 7x^3 + 4x^2 + 4x - 10 \equiv 0 (\mathrm{mod}\ 175)$;

14. $5x^4 + 2x + 12 \equiv 0 (\mathrm{mod}\, 216)$;
15. $31x^4 + 57x^3 + 96x + 191 \equiv 0 (\mathrm{mod}\, 225)$;
16. $126x^4 + 100x^3 + 100x^2 + 200x + 149 \equiv 0 (\mathrm{mod}\, 225)$;
17. $4x^5 + 3x + 9 \equiv 0 (\mathrm{mod}\, 288)$;
18. $18x^3 + 3x + 18 \equiv 0 (\mathrm{mod}\, 288)$;
19. $x^3 + 5x \equiv 0 (\mathrm{mod}\, 400)$;
20. $2x^6 - 6x^4 - 7x^2 - 4 \equiv 0 (\mathrm{mod}\, 441)$;
21. $x^3 - x^2 + 2x + 4 \equiv 0 (\mathrm{mod}\, 480)$;
22. $9x^5 + 3x + 96 \equiv 0 (\mathrm{mod}\, 480)$;
23. $x^3 - 2x^2 + 15x + 4 \equiv 0 (\mathrm{mod}\, 504)$;
24. $x^6 - x^5 + 3x^4 - 5 \equiv 0 (\mathrm{mod}\, 675)$;
25. $8x^4 - x \equiv 0 (\mathrm{mod}\, 675)$;
26. $6x^4 + 5x^3 - 3x^2 + 12x + 135 \equiv 0 (\mathrm{mod}\, 675)$;
27. $x^3 + 6x + 7 \equiv 0 (\mathrm{mod}\, 675)$;
28. $3x^3 + 4x^2 + 6x + 9 \equiv 0 (\mathrm{mod}\, 792)$;
29. $x^3 + 4x + 4 \equiv 0 (\mathrm{mod}\, 800)$;
30. $x^3 + x^2 + 4x + 4 \equiv 0 (\mathrm{mod}\, 800)$;
31. $x^5 - x^4 + 6x^2 + 15x + 36 \equiv 0 (\mathrm{mod}\, 864)$;
32. $2x^5 - x^4 + x + 50 \equiv 0 (\mathrm{mod}(1000)$;
33. $x^3 + 6x + 20 \equiv 0 (\mathrm{mod}\, 1000)$;
34. $x^4 - 2x^2 - 2x + 16 \equiv 0 (\mathrm{mod}\, 1120)$;
35. $2x^6 - 3x^4 + 5x^2 + 50 \equiv 0 (\mathrm{mod}\, 1125)$;
36. $x^4 + x^3 - 6x^2 + 15x + 45 \equiv 0 (\mathrm{mod}\, 1323)$;
37. $x^5 - 6x^4 + 2x^3 - 7x^2 + 21x + 392 \equiv 0 (\mathrm{mod}\, 1372)$;
38. $x^3 + x^2 + 27x - 42 \equiv 0 (\mathrm{mod}\, 2025)$;
39. $x^3 - 16x^2 - 5x + 20 \equiv 0 (\mathrm{mod}\, 56)$;
40. $2x^3 - 2x^2 - 4x \equiv 0 (\mathrm{mod}\, 72)$;
41. $x^3 - 20x^2 - 26x + 45 \equiv 0 (\mathrm{mod}\, 135)$;
42. $x^3 - 12x^2 + 12x - 55 \equiv 0 (\mathrm{mod}\, 135)$;
43. $18x^4 + 3x + 6 \equiv 0 (\mathrm{mod}\, 144)$;
44. $x^3 - 17x^2 + 66x + 178 \equiv 0 (\mathrm{mod}\, 250)$;
45. $x^4 + 4x^3 + 5x - 58 \equiv 0 (\mathrm{mod}\, 375)$;
46. $x^3 + 2x^2 + 3x + 2 \equiv 0 (\mathrm{mod}\, 440)$;
47. $4x^3 + 7x^2 - 7x - 10 \equiv 0 (\mathrm{mod}\, 450)$;
48. $x^5 + x^4 + x^3 + x^2 + x + 1 \equiv 0 (\mathrm{mod}\, 567)$;
49. $x^5 - x^4 + 6x^2 + 75x + 225 \equiv 0 (\mathrm{mod}\, 675)$;

50. $3x^2 + 6x + 45 \equiv 0 (\mathrm{mod}\, 675)$;
51. $x^5 + 2x^4 + 3x^3 + 2x^2 - 2x - 2 \equiv 0 (\mathrm{mod}\, 686)$
52. $x^3 - 21x^2 + 128x + 506 \equiv 0 (\mathrm{mod}\, 686)$;
53. $x^5 + x^4 + x^3 + x^2 + x - 5 \equiv 0 (\mathrm{mod}\, 1080)$;
54. $x^5 + x^4 - x^3 + 5x^2 + 30x - 45 \equiv 0 (\mathrm{mod}\, 1125)$;
55. $2x^5 + x^2 + 3x + 81 \equiv 0 (\mathrm{mod}\, 2025)$;
56. $x^3 + 4x^2 - 3 \equiv 0 (\mathrm{mod}\, 3375)$;
57. $x^3 - 5x^2 + x + 10 \equiv 0 (\mathrm{mod}\, 8575)$;
58. $x^4 + 4x^3 + 2x^2 + x + 12 \equiv 0 (\mathrm{mod}\, 8575)$;
59. $5x^2 + 7x + 2 \equiv 0 (\mathrm{mod}\, 18)$;
60. $31x^3 + 57x^2 + 77x + 191 \equiv 0 (\mathrm{mod}\, 100)$;
61. $15x^5 + 7x^4 + 3x^2 + 11x - 2 \equiv 0 (\mathrm{mod}\, 180)$;
62. $3x^4 + 2x^3 + x^2 + 44 \equiv 0 (\mathrm{mod}\, 200)$;
63. $4x^4 + 4x^3 + 8x^2 + 2x + 36 \equiv 0 (\mathrm{mod}\, 216)$;
64. $x^3 + x^2 + x + 1 \equiv 0 (\mathrm{mod}\, 216)$;
65. $x^3 + x^2 - 9x + 30 \equiv 0 (\mathrm{mod}\, 221)$;
66. $x^4 + 5x^3 - 6x^2 - 5x + 8 \equiv 0 (\mathrm{mod}\, 288)$;
67. $x^5 - 2x^3 + x + 15 \equiv 0 (\mathrm{mod}\, 392)$;
68. $x^4 - 4x^3 + 3x^2 - x + 1 \equiv 0 (\mathrm{mod}\, 432)$;
69. $x^4 + x^3 + x^2 + 3x + 6 \equiv 0 (\mathrm{mod}\, 675)$;
70. $x^4 - 2x^3 - 4x + 5 \equiv 0 (\mathrm{mod}\, 800)$;
71. $x^3 + x + 2 \equiv 0 (\mathrm{mod}\, 1440)$;
72. $x^5 - 4x^4 + 3x^3 + 4x + 28 \equiv 0 (\mathrm{mod}\, 1960)$;
73. $x^5 + 2x^3 + 4x^2 - 3x + 5 \equiv 0 (\mathrm{mod}\, 2260)$;
74. $x^4 - 5x^3 - 3x^2 + 21 \equiv 0 (\mathrm{mod}\, 2268)$;
75. $x^3 + 4x^2 + 3 \equiv 0 (\mathrm{mod}\, 3375)$;
76. $x^4 + x^3 + x^2 + 9x + 45 \equiv 0 (\mathrm{mod}\, 4725)$;
77. $2x^3 + 4x^2 - x + 15 \equiv 0 (\mathrm{mod}\, 6075)$;
78. $x^4 + x^3 - x^2 - 161x + 5 \equiv 0 (\mathrm{mod}\, 10125)$;
79. $x^3 + x^2 - 9x + 55 \equiv 0 (\mathrm{mod}\, 11507)$;
80. $x^4 - 2x^2 - 2x + 16 \equiv 0 (\mathrm{mod}\, 75000)$.
81. Придумайте и решите сравнение с использованием не менее двух случаев теоремы: $f(x) \equiv 0 (\mathrm{mod}\, p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3})$, $\alpha_1 \geqslant 2, \alpha_2 \geqslant 2, \alpha_3 \geqslant 2$.
82. Придумайте и решите сравнение с использованием не менее двух случаев теоремы: $f(x) \equiv 0 (\mathrm{mod}\, p_1^{\alpha_1} p_2^{\alpha_2} p_3)$, $\alpha_1 \geqslant 2, \alpha_2 \geqslant 2$, $p_3 > p_2 > p_1 > 2$.

83. Придумайте и решите сравнение с использованием не менее двух случаев теоремы: $f(x) \equiv 0 (\mathrm{mod}\, p_1^{\alpha_1} p_2^{\alpha_2})$, $\alpha_1 \geqslant 4, \alpha_2 \geqslant 3$.
84. Придумайте и решите сравнение с использованием не менее двух случаев теоремы: $f(x) \equiv 0 (\mathrm{mod}\, p_1^{\alpha_1} p_2^{\alpha_2})$, $\alpha_1 \geqslant 5, \alpha_2 \geqslant 2$.
85. Придумайте и решите сравнение с использованием не менее двух случаев теоремы: $f(x) \equiv 0 (\mathrm{mod}\, p_1^{\alpha_1} p_2^{\alpha_2})$, $\alpha_1 \geqslant 2, \alpha_2 \geqslant 2, p_2 > p_1 > 2$.
86. Придумайте и решите сравнение с использованием всех трех случаев теоремы: $f(x) \equiv 0 (\mathrm{mod}\, p_1^{\alpha_1} p_2^{\alpha_2})$, $\alpha_1 \geqslant 3, \alpha_2 \geqslant 2, p_2 > p_1 > 2$.
87. Придумайте и решите сравнение с использованием всех трех случаев теоремы: $f(x) \equiv 0 (\mathrm{mod}\, p_1^{\alpha_1} p_2^{\alpha_2})$, $\alpha_1 \geqslant 4, \alpha_2 \geqslant 2$.
88. Придумайте и решите сравнение с использованием всех трех случаев теоремы: $f(x) \equiv 0 (\mathrm{mod}\, p_1^{\alpha_1} p_2)$, $\alpha_1 \geqslant 5$.
89. Придумайте и решите сравнение с использованием всех трех случаев теоремы: $f(x) \equiv 0 (\mathrm{mod}\, p_1^{\alpha_1} p_2^{\alpha_2} p_3)$, $\alpha_1 \geqslant 5, \alpha_2 \geqslant 1$.
90. Придумайте и решите сравнение с использованием всех трех случаев теоремы: $f(x) \equiv 0 (\mathrm{mod}\, p_1^{\alpha_1} p_2^{\alpha_2} p_3)$, $\alpha_1 \geqslant 2, \alpha_2 \geqslant 2, p_3 > p_2 > p_1 > 2$.

§ 3. Задачи лабораторной работы по теме «Цепные дроби»

1. а) Запишите в виде цепной дроби: 1381/966; 562/393; 858/257.
   б) Найдите величину цепной дроби: [1, 1, 19, 2, 2, 2]; [1, 1, 1, 1, 13, 2]; [1, 3, 2, 1, 2, 2, 15].
   в) Решите в целых числах уравнение: $551x - 247y = 4522$; $180x + 264y = 2304$.
   г) Запишите в виде цепной дроби: $\dfrac{-10+\sqrt{2}}{4}$; $\dfrac{24-4\sqrt{3}}{11}$.
   д) Найдите величину цепной дроби: $[1, 4, (2, 1, 3)]$; $[-1, 1, 3, (1, 5, 5)]$.
   е) Найдите приближение 1252/545 подходящей дробью с точностью $2 \cdot 10^{-5}$.
   ж) Найдите приближение $\dfrac{-4+\sqrt{1155}}{67}$ подходящей дробью с точностью $9{,}1 \cdot 10^{-4}$.
   з) Найдите приближение $-3\pi/5$ подходящей дробью с точностью $1{,}1 \cdot 10^{-3}$.
2. а) Запишите в виде цепной дроби: 3251/985; 1381/401; 743/544.
   б) Найдите величину цепной дроби: [2, 1, 2, 2, 1, 17]; [3, 1, 1, 2, 3, 20, 2]; [2, 2, 15, 1, 2, 2].

в) Решите в целых числах уравнение:
$140x + 290y = 2380$; $324x + 336y = 3444$.

г) Запишите в виде цепной дроби: $\dfrac{-7-\sqrt{399}}{10}$; $\dfrac{14+\sqrt{101}}{19}$.

д) Найдите величину цепной дроби: $[-1, 4, (3, 1, 1)]$; $[-1, 3, (2, 2, 4)]$.

е) Найдите приближение 7952/3257 подходящей дробью с точностью 10^{-5}.

ж) Найдите приближение $\dfrac{-59+\sqrt{629}}{46}$ подходящей дробью с точностью $1{,}3 \cdot 10^{-4}$.

з) Найдите приближение $-e/2$ подходящей дробью с точностью 0,067.

3. а) Запишите в виде цепной дроби: 3853/1862; 3197/931; 191/150.

б) Найдите величину цепной дроби: $[3, 2, 2, 1, 2, 13, 2]$; $[2, 1, 3, 20, 3, 3]$; $[1, 14, 2, 3, 2, 2]$.

в) Решите в целых числах уравнение:
$361x - 475y = 5358$; $143x + 299y = 2574$.

г) Запишите в виде цепной дроби: $\dfrac{16-\sqrt{82}}{29}$; $\dfrac{-5+\sqrt{195}}{34}$.

д) Найдите величину цепной дроби:
$[0, 1, 3, (1, 4)]$; $[-2, 5, (1, 1, 3)]$.

е) Найдите приближение 9049/2524 подходящей дробью с точностью $8 \cdot 10^{-5}$.

ж) Найдите приближение $\dfrac{-6-\sqrt{2}}{4}$ подходящей дробью с точностью $7{,}2 \cdot 10^{-4}$.

з) Найдите приближение $-5e/4$ подходящей дробью с точностью 0,067.

4. а) Запишите в виде цепной дроби: 1199/359; 539/223; 1633/435.

б) Найдите величину цепной дроби: $[3, 3, 3, 2, 16, 3]$; $[1, 19, 1, 3, 2, 1, 3]$; $[3, 2, 3, 17, 2, 2]$.

в) Решите в целых числах уравнение:
$234x - 450y = 3258$; $425x - 238y = 4012$.

г) Запишите в виде цепной дроби: $\dfrac{32+\sqrt{37}}{21}$; $\dfrac{-6-\sqrt{323}}{41}$.

д) Найдите величину цепной дроби: $[0, 2, (3, 1, 3, 3)]$; $[-1, 5, (2, 5, 4)]$.

е) Найдите приближение 1791/1693 подходящей дробью с точностью $7 \cdot 10^{-5}$.

ж) Найдите приближение $\dfrac{51-3\sqrt{5}}{142}$ подходящей дробью с точностью $1{,}2\cdot 10^{-3}$.

з) Найдите приближение $2e$ подходящей дробью с точностью 0,036.

5. а) Запишите в виде цепной дроби: 1783/717; 789/235; 2947/1213.

б) Найдите величину цепной дроби: [2,3,3,15,2,3,2]; [1,1,18,1,2,2,2]; [1, 1, 3, 3, 17, 3, 3].

в) Решите в целых числах уравнение:
$140x - 190y = 2460$; $225x + 285y = 2385$.

г) Запишите в виде цепной дроби: $\dfrac{-9-\sqrt{21}}{10}$; $\dfrac{13+\sqrt{37}}{12}$.

д) Найдите величину цепной дроби: $[1,3,(5,1,1)]$; $[-2,1,3,(4,1,5)]$.

е) Найдите приближение 2683/1379 подходящей дробью с точностью $7\cdot 10^{-5}$.

ж) Найдите приближение $\dfrac{-12-\sqrt{15}}{43}$ подходящей дробью с точностью $5{,}1\cdot 10^{-4}$.

з) Найдите приближение $-\dfrac{e}{5}$ подходящей дробью с точностью $7\cdot 10^{-3}$.

6. а) Запишите в виде цепной дроби: 857/308; 601/152; 1386/601.

б) Найдите величину цепной дроби:
[1, 2, 2, 1, 3, 12, 3]; [1, 2, 1, 13, 1, 2]; [2, 3, 1, 2, 2, 20].

в) Решите в целых числах уравнение:
$216x + 204y = 3000$; $275x - 121y = 2959$.

г) Запишите в виде цепной дроби: $\dfrac{25-\sqrt{1093}}{18}$; $\dfrac{-\sqrt{530}}{10}$.

д) Найдите величину цепной дроби:
$[0,2,(2,4,1,3)]$; $[0,1,(2,5,5)]$.

е) Найдите приближение 7619/2126 подходящей дробью с точностью $4\cdot 10^{-5}$.

ж) Найдите приближение $\dfrac{-20+3\sqrt{11}}{43}$ подходящей дробью с точностью $1{,}4\cdot 10^{-5}$.

з) Найдите приближение $-\pi$ подходящей дробью с точностью 0,018.

7. а) Запишите в виде цепной дроби: 953/423; 1287/896; 2563/1128.

б) Найдите величину цепной дроби:
[3, 13, 3, 2, 2, 2]; [2, 1, 2, 14, 1, 3]; [1, 3, 21, 3, 2, 1, 3].

в) Решите в целых числах уравнение:
$375x + 285y = 2985$; $276x - 264y = 1908$.

г) Запишите в виде цепной дроби: $\frac{-1+\sqrt{101}}{25}$; $\frac{29+\sqrt{365}}{34}$.

д) Найдите величину цепной дроби:
$[3, 1, 4, (1, 3)]$; $[-1, 2, (2, 1, 5)]$.

е) Найдите приближение 6873/4619 подходящей дробью с точностью $5 \cdot 10^{-5}$.

ж) Найдите приближение $\frac{25+\sqrt{37}}{12}$ подходящей дробью с точностью $2{,}7 \cdot 10^{-3}$.

з) Найдите приближение $5\pi/3$ подходящей дробью с точностью $1{,}6 \cdot 10^{-4}$.

8. а) Запишите в виде цепной дроби: 4013/1221; 727/270; 1560/1091.

б) Найдите величину цепной дроби:
$[2, 1, 2, 1, 1, 16]$; $[2, 1, 1, 12, 1, 3, 2]$; $[3, 1, 3, 3, 12, 2, 3]$.

в) Решите в целых числах уравнение:
$405x - 390y = 2355$; $190x - 209y = 2071$.

г) Запишите в виде цепной дроби: $\frac{20+\sqrt{10}}{30}$; $\frac{-1-\sqrt{65}}{4}$.

д) Найдите величину цепной дроби:
$[-1, 3, (4, 3, 1, 1)]$; $[-1, 1, 3, (2, 1, 2)]$.

е) Найдите приближение 2502/1733 подходящей дробью с точностью $9 \cdot 10^{-5}$.

ж) Найдите приближение $\frac{-26-\sqrt{10}}{18}$ подходящей дробью с точностью $9{,}7 \cdot 10^{-3}$.

з) Найдите приближение $-e$ подходящей дробью с точностью 0,036.

9. а) Запишите в виде цепной дроби: 985/929; 592/549; 1131/545.

б) Найдите величину цепной дроби:
$[1, 3, 13, 1, 2, 3, 3]$; $[3, 3, 2, 2, 2, 17, 3]$; $[1, 12, 2, 3, 2, 1, 3]$.

в) Решите в целых числах уравнение:
$225x + 240y = 1695$; $406x - 322y = 2940$.

г) Запишите в виде цепной дроби: $\frac{26-\sqrt{145}}{9}$; $\frac{31+\sqrt{323}}{29}$.

д) Найдите величину цепной дроби:
$[-3, 3, (2, 4, 1, 2)]$; $[-1, 2, (1, 4, 3)]$.

е) Найдите приближение 7742/2633 подходящей дробью с точностью 10^{-5}.

ж) Найдите приближение $\dfrac{-5+\sqrt{229}}{34}$ подходящей дробью с точностью $3{,}8 \cdot 10^{-4}$.

з) Найдите приближение $3\pi/5$ подходящей дробью с точностью $6{,}6 \cdot 10^{-3}$.

10. а) Запишите в виде цепной дроби: 579/296; 958/749; 391/149.

б) Найдите величину цепной дроби:
$[2, 1, 1, 3, 15, 1, 3]$; $[1, 17, 2, 1, 2, 2]$; $[3, 3, 1, 1, 14, 3, 2]$.

в) Решите в целых числах уравнение:
$110x - 187y = 1628$; $460x + 340y = 5240$.

г) Запишите в виде цепной дроби: $\dfrac{5-\sqrt{30}}{2}$; $\dfrac{-25+\sqrt{170}}{65}$.

д) Найдите величину цепной дроби:
$[-1, 5, (2, 2, 4)]$; $[0, 2, 3, (2, 5)]$.

е) Найдите приближение 5211/1696 подходящей дробью с точностью $5 \cdot 10^{-5}$.

ж) Найдите приближение $\dfrac{11-\sqrt{15}}{2}$ подходящей дробью с точностью $2{,}8 \cdot 10^{-3}$.

з) Найдите приближение 2π подходящей дробью с точностью 0,013.

11. а) Запишите в виде цепной дроби: 445/266; 6527/1962; 4847/1469.

б) Найдите величину цепной дроби:
$[2, 1, 3, 1, 3, 1, 15]$; $[1, 3, 3, 19, 1, 2]$; $[3, 1, 2, 2, 3, 2, 14]$.

в) Решите в целых числах уравнение:
$442x - 493y = 4131$; $195x - 345y = 1935$.

г) Запишите в виде цепной дроби: $\dfrac{12-\sqrt{3}}{47}$; $\dfrac{-10+\sqrt{1023}}{71}$.

д) Найдите величину цепной дроби:
$[0, 3, (2, 1, 3, 2)]$; $[-1, 1, 1, (4, 5, 2)]$.

е) Найдите приближение 8803/2318 подходящей дробью с точностью $4 \cdot 10^{-5}$.

ж) Найдите приближение $\dfrac{2-\sqrt{37}}{11}$ подходящей дробью с точностью 0,067.

з) Найдите приближение $-e/3$ подходящей дробью с точностью $4{,}4 \cdot 10^{-3}$.

12. а) Запишите в виде цепной дроби: 381/269; 391/172; 1652/559.

б) Найдите величину цепной дроби:
$[3, 1, 1, 2, 3, 18, 2]$; $[3, 2, 3, 2, 3, 15]$; $[1, 2, 1, 1, 3, 15]$.

в) Решите в целых числах уравнение:
$570x - 209y = 3097$; $304x - 192y = 3824$.

г) Запишите в виде цепной дроби: $\dfrac{37+\sqrt{3965}}{118}$; $\dfrac{-20-\sqrt{101}}{13}$.

д) Найдите величину цепной дроби:
$[0, 1, 4, (1, 3, 5)]$; $[-1, 5, (2, 1, 3, 4)]$.

е) Найдите приближение 7837/2347 подходящей дробью с точностью $9 \cdot 10^{-5}$.

ж) Найдите приближение $\dfrac{9-\sqrt{21}}{30}$ подходящей дробью с точностью $4{,}5 \cdot 10^{-4}$.

з) Найдите приближение $-5e/4$ подходящей дробью с точностью 0,067.

13. а) Запишите в виде цепной дроби: 3967/1929; 701/538; 1752/649.

б) Найдите величину цепной дроби:
$[2, 3, 3, 3, 2, 13]$; $[2, 1, 2, 3, 3, 3, 15]$; $[1, 2, 2, 3, 2, 2, 17]$.

в) Решите в целых числах уравнение:
$156x - 336y = 2868$; $252x - 270y = 4752$.

г) Запишите в виде цепной дроби: $\dfrac{-23-\sqrt{145}}{24}$; $\dfrac{-\sqrt{15}}{3}$.

д) Найдите величину цепной дроби:
$[0, 3, (3, 3, 1, 1)]$; $[-1, 1, 3, (2, 5)]$.

е) Найдите приближение 6379/2160 подходящей дробью с точностью $5 \cdot 10^{-5}$.

ж) Найдите приближение $\dfrac{-37-\sqrt{229}}{38}$ подходящей дробью с точностью 0,012.

з) Найдите приближение $-4e/5$ подходящей дробью с точностью 0,034.

14. а) Запишите в виде цепной дроби: 2593/688; 998/597; 2959/2797.

б) Найдите величину цепной дроби:
$[1, 2, 18, 1, 2, 3]$; $[1, 1, 2, 1, 19]$; $[3, 1, 1, 14, 1, 3]$.

в) Решите в целых числах уравнение:
$297x - 319y = 2112$; $289x - 255y = 4522$.

г) Запишите в виде цепной дроби: $\dfrac{27-\sqrt{365}}{14}$; $\dfrac{12-\sqrt{30}}{12}$.

д) Найдите величину цепной дроби:
$[1, 1, 4, (2, 3)]$; $[0, 4, 4, (3, 1, 3)]$.

е) Найдите приближение 2573/2424 подходящей дробью с точностью $8 \cdot 10^{-5}$.

ж) Найдите приближение $\dfrac{9-\sqrt{15}}{3}$ подходящей дробью с точностью $1{,}4 \cdot 10^{-3}$.

з) Найдите приближение $-5e$ подходящей дробью с точностью 0,029.

15. а) Запишите в виде цепной дроби: 2144/1041; 903/439; 327/130.

б) Найдите величину цепной дроби:
$[3, 3, 2, 16, 2, 3]$; $[2, 1, 2, 2, 1, 3, 17]$; $[1, 3, 1, 3, 3, 15]$.

в) Решите в целых числах уравнение:
$143x - 234y = 3029$; $156x - 216y = 2448$.

г) Запишите в виде цепной дроби: $\dfrac{3-\sqrt{285}}{6}$; $\dfrac{9+\sqrt{7221}}{170}$.

д) Найдите величину цепной дроби:
$[0, 1, (1, 1, 3, 2)]$; $[-1, 2, (3, 5, 1)]$.

е) Найдите приближение 6839/2832 подходящей дробью с точностью $5 \cdot 10^{-5}$.

ж) Найдите приближение $\dfrac{26+\sqrt{82}}{27}$ подходящей дробью с точностью $5{,}9 \cdot 10^{-3}$.

з) Найдите приближение $\pi/4$ подходящей дробью с точностью 0,023.

16. а) Запишите в виде цепной дроби: 1163/562; 587/442; 4159/2908.

б) Найдите величину цепной дроби:
$[3, 2, 16, 3, 3, 1, 3]$; $[1, 2, 2, 2, 19, 3]$; $[3, 16, 3, 2, 2, 2]$.

в) Решите в целых числах уравнение:
$460x - 600y = 5060$; $253x - 187y = 3179$.

г) Запишите в виде цепной дроби: $\dfrac{-1+\sqrt{221}}{22}$; $\dfrac{12-3\sqrt{11}}{5}$.

д) Найдите величину цепной дроби:
$[1, 1, 3, (2, 1, 4)]$; $[1, 2, (3, 2, 1)]$.

е) Найдите приближение 1678/547 подходящей дробью с точностью $6 \cdot 10^{-5}$.

ж) Найдите приближение $\dfrac{21+\sqrt{195}}{41}$ подходящей дробью с точностью $9{,}9 \cdot 10^{-4}$.

з) Найдите приближение $-\pi$ подходящей дробью с точностью 0,018.

17. а) Запишите в виде цепной дроби: 1617/1546; 1324/405; 2819/1156.

б) Найдите величину цепной дроби:
$[1, 3, 3, 21, 2, 3]$; $[1, 3, 3, 1, 1, 3, 13]$; $[2, 2, 3, 14, 2, 3]$.

в) Решите в целых числах уравнение:
$198x + 187y = 2761$; $351x - 364y = 1469$.

г) Запишите в виде цепной дроби: $\dfrac{-51-\sqrt{629}}{58}$; $\dfrac{18-\sqrt{35}}{17}$.

д) Найдите величину цепной дроби:
$[-1, 3, (1, 3, 2)]$; $[-3, 1, 3, (3, 4, 4)]$.

е) Найдите приближение 3301/3156 подходящей дробью с точностью $8 \cdot 10^{-5}$.

ж) Найдите приближение $\dfrac{22-2\sqrt{2}}{17}$ подходящей дробью с точностью $2{,}1 \cdot 10^{-4}$.

з) Найдите приближение $-5\pi/3$ подходящей дробью с точностью 0,051.

18. а) Запишите в виде цепной дроби: 1012/577; 2367/974; 1293/377.

б) Найдите величину цепной дроби:
$[2, 1, 3, 1, 1, 1, 19]$; $[3, 16, 1, 3, 3, 3]$; $[1, 17, 1, 3, 3, 2]$.

в) Решите в целых числах уравнение:
$198x - 486y = 1872$; $165x - 435y = 2115$.

г) Запишите в виде цепной дроби: $\dfrac{67+\sqrt{1085}}{74}$; $\dfrac{19-\sqrt{221}}{14}$.

д) Найдите величину цепной дроби:
$[0, 1, 3, (2, 1, 4)]$; $[0, 2, (1, 1, 3)]$.

е) Найдите приближение 4512/1813 подходящей дробью с точностью $2 \cdot 10^{-5}$.

ж) Найдите приближение $2\sqrt{34}/17$ подходящей дробью с точностью $5{,}7 \cdot 10^{-4}$.

з) Найдите приближение π подходящей дробью с точностью $8{,}4 \cdot 10^{-5}$.

19. а) Запишите в виде цепной дроби: 2049/695; 3238/1413; 748/699.

б) Найдите величину цепной дроби:
$[3, 1, 2, 3, 13, 1, 2]$; $[3, 3, 2, 17, 1, 3]$; $[3, 3, 1, 1, 2, 13]$.

в) Решите в целых числах уравнение:
$250x + 170y = 1540$; $390x - 285y = 4485$.

г) Запишите в виде цепной дроби: $\dfrac{-17+\sqrt{37}}{9}$; $\dfrac{-1-2\sqrt{2}}{6}$.

д) Найдите величину цепной дроби:
$[-1, 2, (1, 2, 2, 3)]$; $[-1, 2, 2, (1, 1, 4)]$.

е) Найдите приближение 4593/4382 подходящей дробью с точностью 10^{-5}.

ж) Найдите приближение $\dfrac{-15+\sqrt{1677}}{22}$ подходящей дробью с точностью $2{,}7 \cdot 10^{-4}$.

з) Найдите приближение $2\pi/5$ подходящей дробью с точностью 0,036.

20. а) Запишите в виде цепной дроби: 1234/313; 455/193; 2029/882.

б) Найдите величину цепной дроби:
$[1, 1, 1, 15, 2, 2]$; $[2, 3, 1, 2, 3, 18]$; $[2, 1, 2, 13, 1, 3, 2]$.

в) Решите в целых числах уравнение:
$270x + 285y = 2115$; $475x - 247y = 48\,067$.

г) Запишите в виде цепной дроби: $\dfrac{4-\sqrt{26}}{5}$; $\dfrac{-1-\sqrt{101}}{5}$.

д) Найдите величину цепной дроби:
$[0, 5, (1, 1, 3)]$; $[0, 1, 3, (5, 1, 2)]$.

е) Найдите приближение 6395/2662 подходящей дробью с точностью 10^{-5}.

ж) Найдите приближение $\dfrac{33+3\sqrt{87}}{34}$ подходящей дробью с точностью $1{,}1 \cdot 10^{-3}$.

з) Найдите приближение e подходящей дробью с точностью 0,084.

21. а) Запишите в виде цепной дроби: 2603/763; 1138/373; 1827/1745.

б) Найдите величину цепной дроби:
$[2, 2, 17, 3, 1, 1, 2]$; $[3, 3, 3, 16, 1, 2, 2]$; $[2, 3, 3, 16, 1, 1, 3]$.

в) Решите в целых числах уравнение:
$150x - 190y = 1210$; $187x - 154y = 1551$.

г) Запишите в виде цепной дроби: $\dfrac{41-13\sqrt{5}}{38}$; $\dfrac{-6-\sqrt{15}}{7}$.

д) Найдите величину цепной дроби:
$[-1, 5, (1, 3, 1, 3)]$; $[-3, 1, 1, (3, 2)]$.

е) Найдите приближение 1721/887 подходящей дробью с точностью $3 \cdot 10^{-5}$.

ж) Найдите приближение $2\sqrt{31}/5$ подходящей дробью с точностью 10^{-4}.

з) Найдите приближение π подходящей дробью с точностью $8{,}4 \cdot 10^{-5}$.

22. а) Запишите в виде цепной дроби: 417/314; 3085/822; 1094/685.

б) Найдите величину цепной дроби:
$[1, 2, 3, 1, 14, 3]$; $[3, 2, 2, 2, 18, 2, 3]$; $[2, 1, 16, 2, 3, 3]$.

в) Решите в целых числах уравнение:
$290x - 140y = 1640$; $323x - 285y = 3496$.

г) Запишите в виде цепной дроби: $\dfrac{1+\sqrt{11663}}{238}$; $\dfrac{4+2\sqrt{138}}{67}$.

д) Найдите величину цепной дроби:
$[-1, 1, 2, (5, 2, 3)]$; $[-3, 3, (1, 1, 2)]$.

е) Найдите приближение 2515/1539 подходящей дробью с точностью 10^{-4}.

ж) Найдите приближение $\dfrac{-15+\sqrt{30}}{13}$ подходящей дробью с точностью $6{,}1 \cdot 10^{-3}$.

з) Найдите приближение $-3e/2$ подходящей дробью с точностью $6{,}5 \cdot 10^{-3}$.

23. а) Запишите в виде цепной дроби: 641/172; 293/151; 797/595.

б) Найдите величину цепной дроби:
$[2, 1, 13, 3, 1, 2]$; $[1, 1, 1, 20, 1, 1, 3]$; $[3, 1, 3, 3, 2, 21]$.

в) Решите в целых числах уравнение:
$143x - 312y = 211$; $285x - 323y = 5282$.

г) Запишите в виде цепной дроби: $\dfrac{8-\sqrt{82}}{3}$; $\dfrac{-6-8\sqrt{15}}{21}$.

д) Найдите величину цепной дроби:
$[0, 2, (4, 1, 4)]$; $[-1, 3, (2, 1, 4)]$.

е) Найдите приближение 5133/1459 подходящей дробью с точностью $6 \cdot 10^{-5}$.

ж) Найдите приближение $\dfrac{-11+2\sqrt{95}}{37}$ подходящей дробью с точностью $2{,}6 \cdot 10^{-3}$.

з) Найдите приближение $2e$ подходящей дробью с точностью 0,016.

24. а) Запишите в виде цепной дроби: 4558/1307; 1108/399; 2369/972.

б) Найдите величину цепной дроби:
$[1, 2, 19, 3, 2, 2]$; $[3, 1, 14, 3, 1, 2]$; $[1, 1, 14, 1, 3, 2, 3]$.

в) Решите в целых числах уравнение:
$414x - 198y = 4824$; $510x - 323y = 4709$.

г) Запишите в виде цепной дроби: $\dfrac{-19-\sqrt{2605}}{102}$; $\dfrac{25+\sqrt{145}}{24}$.

д) Найдите величину цепной дроби:
$[1, 1, (3, 4, 2)]$; $[-1, 1, 1, (4, 2, 2)]$.

е) Найдите приближение 8106/2159 подходящей дробью с точностью $7 \cdot 10^{-5}$.

ж) Найдите приближение $\dfrac{29-4\sqrt{3}}{13}$ подходящей дробью с точностью $7{,}7 \cdot 10^{-3}$.

з) Найдите приближение $-3\pi/4$ подходящей дробью с точностью 0,17.

25. а) Запишите в виде цепной дроби: 3016/2331; 391/264; 2641/859.

б) Найдите величину цепной дроби:
$[2, 1, 1, 3, 12, 2]$; $[1, 17, 1, 1, 3, 3, 2]$; $[3, 3, 1, 3, 1, 21]$.

в) Решите в целых числах уравнение:
$275x - 176y = 2981$; $110x + 260y = 1010$.

г) Запишите в виде цепной дроби: $\dfrac{-2-\sqrt{26}}{11}$; $\dfrac{13-\sqrt{15}}{22}$.

д) Найдите величину цепной дроби:
$[0, 1, (2, 1, 3, 3)]$; $[0, 2, 1, (1, 1, 5)]$.

е) Найдите приближение 8752/3763 подходящей дробью с точностью 10^{-5}.

ж) Найдите приближение $\dfrac{-67+\sqrt{1085}}{74}$ подходящей дробью с точностью $7 \cdot 10^{-3}$.

з) Найдите приближение $-3e/5$ подходящей дробью с точностью 0,067.

§ 4. Типовые задания обязательного минимума по арифметике и теории чисел

1. Найдите остаток от деления:

а) 20 на 14;	ж) 39 на 4;	н) −20 на 14;
б) 44 на 7;	з) 28 на 3;	о) -44 на 7;
в) 38 на 8;	и) 55 на 6;	п) -38 на 8;
г) 22 на 5;	к) 79 на 10;	р) -22 на 5;
д) 100 на 11;	л) 67 на 12;	с) -100 на 11;
е) 88 на 9;	м) 28 на 13;	т) -88 на 9.

2. Делится ли:

а) −20 на -14;	ж) 39 на -4;	н) -20 на 7;
б) -44 на -11;	з) 28 на 14;	о) -44 на 22;
в) 38 на -8;	и) 55 на 6;	п) -38 на 8;
г) 22 на -11;	к) 76 на -38;	р) -24 на 12;
д) -110 на 11;	л) 67 на 12;	с) −100 на 11;
е) 88 на -8;	м) - 28 на 14;	т) −88 на -22?

3. Приведите пример двузначного числа, которое делится на n, если:

а) $n = 2$;	е) $n = 7$;	л) $n = -4$;	р) $n = -9$;
б) $n = 3$;	ж) $n = 8$;	м) $n = -5$;	с) $n = 10$;
в) $n = 4$;	з) $n = 9$;	н) $n = -6$;	т) $n = 11$.
г) $n = 5$;	и) $n = -2$;	о) $n = -7$;	
д) $n = 6$;	к) $n = -3$;	п) $n = -8$;	

4. Укажите все простые числа на промежутке:

а) $(3, 12)$;	е) $[4, 17]$;	л) $(13, 24]$;	р) $[27, 47)$;
б) $[5, 14]$;	ж) $(5, 19]$;	м) $[19, 29)$;	с) $(12, 30)$;
в) $(7, 19]$;	з) $[13, 23)$;	н) $(23, 33)$;	т) $[2, 23]$.
г) $[11, 21)$;	и) $(11, 23)$;	о) $[23, 32]$;	
д) $(3, 14)$;	к) $[12, 23]$;	п) $(29, 49]$;	

5. Разложите на простые множители числа:

а) 124;	д) 148;	и) 162;	н) 188;	с) 198;
б) 128;	е) 150;	к) 164;	о) 192;	т) 201.
в) 135;	ж) 156;	л) 172;	п) 195;	
г) 140;	з) 160;	м) 180;	р) 196;	

6. Является ли простым число:

а) 101;	е) 127;	л) 211;	р) 239;
б) 103;	ж) 131;	м) 223;	с) 241;
в) 107;	з) 193;	н) 227;	т) 251?
г) 109;	и) 197;	о) 229;	
д) 113;	к) 199;	п) 233;	

7. Простым или составным является число:

а) 1124;	е) 3365;	л) 8421;	р) 1233;
б) 3788;	ж) 4975;	м) 9543;	с) 2127;
в) 4596;	з) 6395;	н) 1111;	т) 2827?
г) 5272;	и) 6327;	о) 1133;	
д) 2125;	к) 7113;	п) 2167;	

8. Найдите наибольший общий делитель и наименьшее общее кратное чисел:

а) -20 и -14;	е) 22 и -8;	л) 18 и 12;	р) −24 и 12;
б) -44 и -11;	ж) 39 и -6;	м) -28 и 14;	с) −26 и 12;
в) 38 и -8;	з) 28 и 14;	н) −20 и 25;	т) -82 и -12.
г) 22 и 11;	и) 15 и 6;	о) -44 и 22;	
д) -10 и -15;	к) -16 и -38;	п) −38 и 8;	

9. Найдите наибольший общий делитель чисел a и b, пользуясь алгоритмом Евклида:

а) $a = 20, b = 14$; ж) $a = 22, b = 6$; н) $a = 32, b = 14$;
б) $a = -30, b = 21$; з) $a = -33, b = 9$; о) $a = -48, b = 21$;
в) $a = 40, b = 28$; и) $a = 44, b = 12$; п) $a = 64, b = 28$;
г) $a = 34, b = 10$; к) $a = 18, b = 14$; р) $a = 18, b = 10$;
д) $a = -51, b = 15$; л) $a = -27, b = 21$; с) $a = -27, b = 15$;
е) $a = 68, b = 20$; м) $a = 36, b = 28$; т) $a = 26, b = 18$.

10. Являются ли числа a и b взаимно простыми:

а) $a = 10, b = 7$; ж) $a = 11, b = 3$; н) $a = 16, b = 7$;
б) $a = -10, b = 7$; з) $a = -11, b = 3$; о) $a = -16, b = 7$;
в) $a = 30, b = 21$; и) $a = 33, b = 9$; п) $a = 32, b = 14$;
г) $a = 17, b = 5$; к) $a = 9, b = 7$; р) $a = 9, b = 5$;
д) $a = -17, b = 5$; л) $a = -9, b = 7$; с) $a = -9, b = 5$;
е) $a = 51, b = 15$; м) $a = 18, b = 14$; т) $a = 36, b = 15$?

11. Приведите пример двузначного числа, взаимно простого с n, и пример двузначного числа, не являющегося взаимно простым с n, если:

а) $n = 2$; ж) $n = 8$; н) $n = -6$;
б) $n = 3$; з) $n = 9$; о) $n = -7$;
в) $n = 4$; и) $n = -2$; п) $n = -8$;
г) $n = 5$; к) $n = -3$; р) $n = -9$;
д) $n = 6$; л) $n = -4$; с) $n = 10$;
е) $n = 7$; м) $n = -5$; т) $n = 11$.

12. Найдите:

а) $\lfloor 5{,}6 \rfloor$; е) $\{15{,}78\}$; л) $\lfloor -2{,}29 \rfloor$; р) $\{-49{,}6\}$;
б) $\{5{,}6\}$; ж) $\lfloor -18{,}22 \rfloor$; м) $\{-2{,}29\}$; с) $\lfloor 45 \rfloor$;
в) $\lfloor -2{,}3 \rfloor$; з) $\{-18{,}22\}$; н) $\lfloor 39{,}1 \rfloor$; т) $\{45\}$.
г) $\{-2{,}3\}$; и) $\lfloor 3{,}45 \rfloor$; о) $\{39{,}1\}$;
д) $\lfloor 15{,}78 \rfloor$; к) $\{3{,}45\}$; п) $\lfloor -49{,}6 \rfloor$;

13. Разложите на простые множители:

а) 5!; ж) 11!; н) 17!;
б) 6!; з) 12!; о) 18!;
в) 7!; и) 13!; п) 19!;
г) 8!; к) 14!; р) 20!;
д) 9!; л) 15!; с) 21!;
е) 10!; м) 16!; т) 22!.

14. Вычислите:

а) $\tau(10)$;	ж) $\tau(28)$;	н) $\sigma(16)$;
б) $\tau(12)$;	з) $\tau(30)$;	о) $\sigma(18)$;
в) $\tau(14)$;	и) $\tau(32)$;	п) $\sigma(20)$;
г) $\tau(16)$;	к) $\sigma(10)$;	р) $\sigma(28)$;
д) $\tau(18)$;	л) $\sigma(12)$;	с) $\sigma(30)$;
е) $\tau(20)$;	м) $\sigma(14)$;	т) $\sigma(12)$.

15. Вычислите:

а) $\varphi(10)$;	ж) $\varphi(28)$;	н) $\varphi(18)$;
б) $\varphi(12)$;	з) $\varphi(30)$;	о) $\varphi(20)$;
в) $\varphi(14)$;	и) $\varphi(10)$;	п) $\varphi(28)$;
г) $\varphi(16)$;	к) $\varphi(12)$;	р) $\varphi(30)$;
д) $\varphi(18)$;	л) $\varphi(14)$;	с) $\varphi(32)$;
е) $\varphi(20)$;	м) $\varphi(16)$;	т) $\varphi(33)$.

16. Вычислите:

а) $\mu(10)$;	ж) $\mu(35)$;	н) $\mu(12)$;
б) $\mu(14)$;	з) $\mu(42)$;	о) $\mu(16)$;
в) $\mu(15)$;	и) $\mu(66)$;	п) $\mu(18)$;
г) $\mu(22)$;	к) $\mu(70)$;	р) $\mu(20)$;
д) $\mu(30)$;	л) $\mu(105)$;	с) $\mu(45)$;
е) $\mu(33)$;	м) $\mu(110)$;	т) $\mu(56)$.

17. Приведите пример числа, сравнимого с a по модулю n, если:

а) $a = 2$, $n = 4$;	ж) $a = -3$, $n = 10$;	н) $a = -33$, $n = 9$;
б) $a = -1$, $n = 5$;	з) $a = 14$, $n = 4$;	о) $a = 23$, $n = 10$;
в) $a = 12$, $n = 6$;	и) $a = 31$, $n = 5$;	п) $a = -12$, $n = 4$;
г) $a = -14$, $n = 7$;	к) $a = -47$, $n = 9$;	р) $a = 63$, $n = 5$;
д) $a = 12$, $n = 8$;	л) $a = 31$, $n = 7$;	с) $a = -44$, $n = 6$;
е) $a = 4$, $n = 9$;	м) $a = -10$, $n = 8$;	т) $a = -77$, $n = 7$.

18. Приведите пример числа, не сравнимого с a по модулю n, если:

а) $a = 20$, $n = 4$;	ж) $a = -32$, $n = 10$;	н) $a = -36$, $n = 9$;
б) $a = -11$, $n = 5$;	з) $a = 18$, $n = 4$;	о) $a = 28$, $n = 10$;
в) $a = 13$, $n = 6$;	и) $a = 33$, $n = 5$;	п) $a = -64$, $n = 4$;
г) $a = -15$, $n = 7$;	к) $a = -41$, $n = 9$;	р) $a = 64$, $n = 5$;
д) $a = 10$, $n = 8$;	л) $a = 32$, $n = 7$;	с) $a = -40$, $n = 6$;
е) $a = 40$, $n = 9$;	м) $a = -14$, $n = 8$;	т) $a = -66$, $n = 6$.

19. Являются ли числа a и b сравнимыми по модулю n, если:

а) $a = -10$, $b = 11$, $n = 3$;
б) $a = 3$, $b = 47$, $n = 4$;
в) $a = -12$, $b = 3$, $n = 5$;
г) $a = 4$, $b = -21$, $n = 6$;
д) $a = -44$, $b = 5$, $n = 7$;
е) $a = 3$, $b = 27$, $n = 8$;
ж) $a = -2$, $b = 52$, $n = 9$;
з) $a = 35$, $b = -1$, $n = 3$;
и) $a = -34$, $b = 2$, $n = 4$;
к) $a = 6$, $b = -14$, $n = 5$;
л) $a = -29$, $b = 1$, $n = 6$;
м) $a = 32$, $b = -3$, $n = 7$;
н) $a = 67$, $b = 3$, $n = 8$;
о) $a = 17$, $b = -11$, $n = 21$;
п) $a = 22$, $b = -14$, $n = 13$;
р) $a = 19$, $b = -11$, $n = 10$;
с) $a = 2$, $b = -14$, $n = 3$;
т) $a = -34$, $b = 11$, $n = 4$?

20. Какому классу вычетов по модулю n принадлежит число a, если:

а) $a = 23$, $n = 4$;
б) $a = -12$, $n = 5$;
в) $a = 14$, $n = 6$;
г) $a = -21$, $n = 7$;
д) $a = 14$, $n = 8$;
е) $a = 30$, $n = 9$;
ж) $a = -12$, $n = 10$;
з) $a = 15$, $n = 4$;
и) $a = 32$, $n = 5$;
к) $a = -47$, $n = 6$;
л) $a = 38$, $n = 7$;
м) $a = -15$, $n = 8$;
н) $a = -34$, $n = 9$;
о) $a = 22$, $n = 10$;
п) $a = -16$, $n = 4$;
р) $a = 68$, $n = 5$;
с) $a = -50$, $n = 6$;
т) $a = 77$, $n = 7$?

21. Выпишите полную систему вычетов по модулю n, содержащую число a, если:

а) $a = 22$, $n = 4$;
б) $a = -11$, $n = 5$;
в) $a = 12$, $n = 6$;
г) $a = -14$, $n = 7$;
д) $a = 12$, $n = 8$;
е) $a = 34$, $n = 9$;
ж) $a = -13$, $n = 10$;
з) $a = 14$, $n = 4$;
и) $a = 31$, $n = 5$;
к) $a = -47$, $n = 6$;
л) $a = 31$, $n = 7$;
м) $a = -10$, $n = 8$;
н) $a = -33$, $n = 9$;
о) $a = 23$, $n = 10$;
п) $a = -12$, $n = 4$;
р) $a = 63$, $n = 5$;
с) $a = -44$, $n = 6$;
т) $a = -77$, $n = 7$.

22. Выпишите приведенную систему вычетов по модулю n, содержащую число a, если:

а) $a = 21$, $n = 4$;
б) $a = -11$, $n = 5$;
в) $a = 13$, $n = 6$;
г) $a = -12$, $n = 7$;
д) $a = 15$, $n = 8$;
е) $a = 34$, $n = 9$;
ж) $a = -13$, $n = 10$;
з) $a = 17$, $n = 4$;
и) $a = 31$, $n = 5$;
к) $a = -47$, $n = 6$;
л) $a = 31$, $n = 7$;
м) $a = -11$, $n = 8$;
н) $a = -37$, $n = 9$;
о) $a = 23$, $n = 10$;
п) $a = -19$, $n = 4$;
р) $a = 63$, $n = 5$;
с) $a = -43$, $n = 6$;
т) $a = -78$, $n = 7$.

23. Найдите остаток от деления a на n, если:

а) $a = 3^{147}$, $n = 5$;
б) $a = 2^{188}$, $n = 7$;
в) $a = 4^{123}$, $n = 11$;
г) $a = 2^{148}$, $n = 13$;
д) $a = 12^{30}$, $n = 5$;
е) $a = 23^{26}$, $n = 7$;
ж) $a = 35^{34}$, $n = 11$;
з) $a = 41^{26}$, $n = 13$;
и) $a = 11^{30}$, $n = 6$;
к) $a = 23^{20}$, $n = 8$;
л) $a = 3^{222}$, $n = 8$;
м) $a = 2^{123}$, $n = 9$;
н) $a = 7^{666}$, $n = 10$;
о) $a = 5^{234}$, $n = 12$;
п) $a = 11^{22}$, $n = 8$;
р) $a = 22^{44}$, $n = 9$;
с) $a = 33^{11}$, $n = 10$;
т) $a = 55^{66}$, $n = 12$.

24. Решите сравнение:

а) $2x \equiv 3 (\mathrm{mod}\, 5)$;
б) $3x \equiv 2 (\mathrm{mod}\, 4)$;
в) $-2x \equiv 1 (\mathrm{mod}\, 3)$;
г) $-3x \equiv 2 (\mathrm{mod}\, 5)$;
д) $-5x \equiv 3 (\mathrm{mod}\, 6)$;
е) $2x \equiv 4 (\mathrm{mod}\, 7)$;
ж) $-4x \equiv 5 (\mathrm{mod}\, 3)$;
з) $3x \equiv -1 (\mathrm{mod}\, 4)$;
и) $2x \equiv -1 (\mathrm{mod}\, 5)$;
к) $-2x \equiv 3 (\mathrm{mod}\, 7)$;
л) $3x \equiv -1 (\mathrm{mod}\, 4)$;
м) $14x \equiv 28 (\mathrm{mod}\, 5)$;
н) $27x \equiv 2 (\mathrm{mod}\, 4)$;
о) $31x \equiv 1 (\mathrm{mod}\, 3)$;
п) $55x \equiv -2 (\mathrm{mod}\, 6)$;
р) $48x \equiv 1 (\mathrm{mod}\, 7)$;
с) $45x \equiv 3 (\mathrm{mod}\, 8)$;
т) $43x \equiv 14 (\mathrm{mod}\, 4)$.

25. Решите сравнение:

а) $x^5 - 2x^2 + 1 \equiv 0 (\mathrm{mod}\, 3)$;
б) $x^7 + 4x - 3 \equiv 0 (\mathrm{mod}\, 5)$;
в) $x^8 - 6x^2 + 2 \equiv 0 (\mathrm{mod}\, 7)$;
г) $x^6 + 6x - 2 \equiv 0 (\mathrm{mod}\, 3)$;
д) $x^6 - 11x^2 + 3 \equiv 0 (\mathrm{mod}\, 5)$;
е) $x^7 + 4x + 5 \equiv 0 (\mathrm{mod}\, 7)$;
ж) $x^5 - x - 12 \equiv 0 (\mathrm{mod}\, 3)$;
з) $x^5 - 2x^2 + 1 \equiv 0 (\mathrm{mod}\, 5)$;
и) $x^7 + 2x - 3 \equiv 0 (\mathrm{mod}\, 7)$;
к) $x^5 - 3x^2 + 2 \equiv 0 (\mathrm{mod}\, 3)$;
л) $x^7 - x - 1 \equiv 0 (\mathrm{mod}\, 5)$;
м) $x^8 - 10x^2 + 3 \equiv 0 (\mathrm{mod}\, 7)$;
н) $x^5 + 11x + 5 \equiv 0 (\mathrm{mod}\, 3)$;
о) $x^5 - 4x - 12 \equiv 0 (\mathrm{mod}\, 5)$;
п) $x^8 + x^4 - 5 \equiv 0 (\mathrm{mod}\, 7)$;
р) $x^3 - x^2 + 7 \equiv 0 (\mathrm{mod}\, 3)$;
с) $x^7 + x - 11 \equiv 0 (\mathrm{mod}\, 5)$;
т) $x^7 + x - 20 \equiv 0 (\mathrm{mod}\, 7)$.

26. Сколько решений имеет сравнение:

а) $x^2 \equiv 12 (\mathrm{mod}\, 5)$;
б) $x^2 \equiv 13 (\mathrm{mod}\, 7)$;
в) $x^2 \equiv 14 (\mathrm{mod}\, 11)$;
г) $x^2 \equiv -17 (\mathrm{mod}\, 5)$;
д) $x^2 \equiv -12 (\mathrm{mod}\, 7)$;
е) $x^2 \equiv -13 (\mathrm{mod}\, 11)$;
ж) $x^2 \equiv 24 (\mathrm{mod}\, 5)$;
з) $x^2 \equiv 38 (\mathrm{mod}\, 7)$;
и) $x^2 \equiv 14 (\mathrm{mod}\, 11)$;
к) $x^2 \equiv -13 (\mathrm{mod}\, 5)$;
л) $x^2 \equiv 18 (\mathrm{mod}\, 7)$;
м) $x^2 \equiv -10 (\mathrm{mod}\, 11)$;
н) $x^2 \equiv -8 (\mathrm{mod}\, 5)$;
о) $x^2 \equiv -30 (\mathrm{mod}\, 7)$;
п) $x^2 \equiv 24 (\mathrm{mod}\, 11)$;
р) $x^2 \equiv 37 (\mathrm{mod}\, 5)$;
с) $x^2 \equiv 33 (\mathrm{mod}\, 7)$;
т) $x^2 \equiv 48 (\mathrm{mod}\, 11)$?

27. Вычислите:

а) $P_5(3)$;	е) $P_{10}(3)$;	л) $P_9(20)$;	р) $P_4(15)$;
б) $P_6(5)$;	ж) $P_5(12)$;	м) $P_{10}(17)$;	с) $P_{11}(21)$;
в) $P_7(2)$;	з) $P_6(17)$;	н) $P_{13}(5)$;	т) $P_{12}(5)$.
г) $P_8(3)$;	и) $P_7(37)$;	о) $P_{10}(12)$;	
д) $P_9(4)$;	к) $P_8(27)$;	п) $P_3(5)$;	

28. Найдите длину периода десятичной записи дроби:

а) 2/3;	е) 7/9;	л) 10/15;	р) 10/22;
б) 1/3;	ж) 2/11;	м) 15/27;	с) 18/33;
в) 1/7;	з) 3/11;	н) 8/18;	т) 20/55.
г) 5/9;	и) 5/11;	о) 6/33;	
д) 4/9;	к) 9/11;	п) 21/77;	

29. Найдите значение цепной дроби:

а) [1, 2, 3];	е) [3, 2, 3];	л) [−2, 2, 2];	р) [3, 3, 2];
б) [3, 2, 2];	ж) [−1, 2, 2];	м) [−1, 2, 3];	с) [3, 1, 4];
в) [3, 1, 2];	з) [−3, 2, 2];	н) [3, 1, 3];	т) [2, 1, 4].
г) [2, 1, 3];	и) [−3, 1, 2];	о) [2, 3, 3];	
д) [2, 2, 3];	к) [−2, 1, 3];	п) [1, 3, 3];	

30. Разложите в цепную дробь:

а) 3/5;	е) 16/7;	л) 5/3;	р) 7/5;
б) 11/13;	ж) 9/5;	м) 13/11;	с) 17/7;
в) 9/7;	з) 17/5;	н) 7/9;	т) 12/7.
г) 10/7;	и) 5/17;	о) 9/13;	
д) 13/9;	к) 7/10;	п) 7/16;	

Ответы и решения

В этом разделе мы даем ответы и рассматриваем решения некоторых избранных задач курса. Нумерация ответов соответствует разделам задачника и последовательности задач в соответствующих параграфах первой главы. Ответы разбиты на группы по принадлежности к параграфам задачника. Чтобы, например, найти ответ ко **2-й задаче** (не упражнению!) из **§ 10** (под названием «Функция Эйлера»), нужно найти группу ответов «Ответы и решения задач из § 10», а в ней — ответ к задаче **2**.

Ответы и решения задач из § 4.

4. 5; 15.

5. 1111.

14. 175.

15. 12; 13.

Ответы и решения задач из § 5.

1 г) 67;

1 д) 23;

1 е) 29.

2 б) $(n+1, 3)$;

2 в) $(n+1, 2)$.

Ответы и решения задач из § 8.

10. Поскольку $1 = 1^2 + 0^2 = (-1)^2 + 0^2 = 0^2 + 1^2 = 0^2 + (-1)^2$, то $r_2(1) = 4 \neq 1$. Это показывает, что данная функция не является мультипликативной. Однако функция $r_2(n)/4$ мультипликативной является.

Ответы и решения задач из § 9.

2 ж) $x = pq^2$; $x = p^5$.

2 н) $x = 3^\alpha 13^\alpha$, $\alpha \geqslant 0$.

6. 36.

8. 28; 22.

Ответы и решения задач из § 10.

3 б) Нет.

6. 2001.

12. 72.

13 а) 30; 15; 16; 24; 20;

13 б) 13; 26; 28; 36; 42; 21;

13 в) нет решений;

13 г) 17; 34; 40; 60; 48; 32;

13 д) 25; 44; 50; 66; 33;

13 е) 39; 45; 52; 56; 35; 72; 70; 78; 84; 90;

13 ж) 575; 41; 55; 150; 82; 110; 132; 100; 88.

14. 14; 26; 28; 34; 38; 46.

20. 1125.

24. $n > 2$.

Ответы и решения задач из § 12.

3 а) да;

3 б) да;

3 в) нет;

3 г) нет.

5 а) 2; 59; 118.

7 з) 1; 2; ...; 25; 26.

8 г) $n \leqslant 62$.

Ответы и решения задач из § 15.

14 а) 32;

14 б) 9;

14 в) 0;

14 г) 43;

14 д) 64;

14 е) 28.

26. 2, если $n \geqslant 3$ или $n = 1$; 4, если $n = 2$.

27. 10, если $n \geqslant 2$; 5, если $n = 1$.

Ответы и решения задач из § 16.

2 е) $x \equiv 9; 50; 91; 132 (\mathrm{mod}\ 164)$.

5 ж) $x \equiv 31; 87; 143; 199; 255; 311 (\mathrm{mod}\ 336)$;

5 з) $x \equiv -4 + 18k (\mathrm{mod}\ 108), k = 0, \ldots, 5$;

5 и) $x \equiv 14 + 35t (\mathrm{mod}\ 5250), t = 0, \ldots, 149$.

7 а) $x \equiv 8479 (\mathrm{mod}\ 15015)$;

7 б) $x \equiv 22 (\mathrm{mod}\ 30)$;

7 в) $x \equiv -2 (\mathrm{mod}\ 420)$.

9 б) $x \equiv 3p \left(\mathrm{mod}\ \dfrac{p^2 - 1}{2} \right)$.

Ответы и решения задач из § 18.

1 а) 22; 53;

1 б) 113;

1 в) 125; 1; 53.

3 а) $x \equiv 100b - 99a (\mathrm{mod}\ 225)$;

3 б) $x \equiv 1000b - 999a (\mathrm{mod}\ 3375)$;

3 в) $x \equiv 28a - 27b \mathrm{mod}\ 108)$.

4 а) Указание: проверьте, что $x \equiv -1; 4; 9; 14; 19 (\mathrm{mod}\ 25)$, и $x \equiv 7 (\mathrm{mod}\ 27)$.

4 б) $x \equiv 22; 76; 122; 176 (\mathrm{mod}\ 225)$.
Указание: проверьте, что $x \equiv 1; -3 (\mathrm{mod}\ 25)$, и $x \equiv 4; 5 (\mathrm{mod}\ 9)$;

4 г) Указание: проверьте, что $x \equiv -2 (\mathrm{mod}\ 25)$, и $x \equiv -2; 4; 7; 13; 16; 22 (\mathrm{mod}\ 27)$;

4 д) Указание: проверьте, что $x \equiv 1; 3 (\mathrm{mod}\ 4)$, и $x \equiv -12; -1; 5; 8; 14; 17; 23 (\mathrm{mod} 27)$;

4 е) Указание: проверьте, что $x \equiv 1; 3 (\mathrm{mod}\ 4)$, и $x \equiv 3; 4; 6; 12; 15; 21; 24 (\mathrm{mod}\ 27)$.

5 а) 4;

5 б) 20;

5 в) 20;

5 г) 6.

Ответы и решения задач из § 19.

6 б) да;

6 в) нет;

6 г) да;

6 д) нет.

11. 0; $p - 1$.

Ответы и решения задач из § 20.

1 а) 1210 ($35424 = 2^5 \cdot 3^3 \cdot 41$);

1 б) 378 ($334368 = 2^5 \cdot 3^5 \cdot 43$);

1 д) 990 ($46575 = 3^4 \cdot 5^2 \cdot 23$);

1 е) 56 ($48608 = 2^5 \cdot 7^2 \cdot 31$);

1 ж) 210 ($28768 = 2^5 \cdot 29 \cdot 31$);

1 з) 84 ($203056 = 2^4 \cdot 7^3 \cdot 37$).

1 и) 20 ($343 = 7^3$);

1 о) 36: ($63072 = 2^5 \cdot 3^3 \cdot 73$).

Ответы и решения задач из § 21.

4. 4_{43}; 11_{43}; 16_{43}; 21_{43}; 35_{43}; 41_{43}.

5. 2_{47}; 3_{47}; 4_{47}; 6_{47}; 7_{47}; 8_{47}; 9_{47}; 12_{47}; 14_{47}; 16_{47}; 17_{47}; 18_{47}; 21_{47}; 24_{47}; 25_{47}; 27_{47}; 28_{47}; 32_{47}; 34_{47}; 36_{47}; 37_{47}; 42_{47}.

16 а) $x \equiv 3 (\mathrm{mod}\ 7)$;

16 в) $x \equiv 1 (\mathrm{mod}\ 29)$;

16 г) $x \equiv 12 (\mathrm{mod}\ 19)$.

17 б) $x \equiv -8; 12 (\mathrm{mod}\ 31)$;

17 в) $x \equiv 39 (\mathrm{mod}\ 59)$;

17 г) $x \equiv -30; 31 (\mathrm{mod}\ 59)$;

17 д) $x \equiv -5; 14 (\mathrm{mod}\ 31)$;

17 е) $x \equiv 0 (\mathrm{mod}\ 15)$, $x \geqslant 0$;

21. 47.

26 а) $23 \cdot 2^4 \cdot 5 \cdot 11^4$;

26 б) $2^4 \cdot 3^3 \cdot 13^2 \cdot 7$;

26 в) $3 \cdot 2^4 \cdot 5 \cdot 7^2$;

26 ж) $2^2 \cdot 3^3 \cdot 41$;

26 з) $3^3 \cdot 41$.

27 а) 105.

Ответы и решения задач из § 22.

1 в) $[-2, 1, 3, 7]$;

1 г) $[-3, 1, 3, 9, 5]$;

1 д) $[1, 2, 3, 4, 6]$;

1 е) $[0, 8, 1, 6, 2, 2]$.

2 а) $\sqrt{2} = [1, (2)]$;

2 б) $\sqrt{6} = [2, (2, 4)]$;

2 в) $\sqrt{10} = [3, (3, 6)]$;

2 г) $\sqrt{13} = [3, (1, 1, 1, 1, 6)]$;

2 д) $\sqrt{15} = [3, (1, 6)]$;

2 е) $\sqrt{17} = [4, (8)]$;

2 ж) $\sqrt{19} = [4, (2, 1, 3, 1, 2, 8)]$;

2 з) $\sqrt{22} = [4, (1, 2, 4, 2, 1, 8)]$;

2 ф) $2\sqrt{7} = [5, (3, 2, 3, 10)]$;

2 х) $6\sqrt{2} = [8, (2, 1, 6)]$.

3 д) $\sqrt{31} = [5, (1, 1, 3, 5, 3, 1, 1, 10)]$;

3 е) $-\sqrt{31} = [-6, 2, (3, 5, 3, 1, 1, 10, 1, 1)]$;

3 ж) $\sqrt{41} = [6, (2, 2, 12)]$;

3 з) $-\sqrt{41} = [-7, 1, 1, 1, 1, (2, 12, 1)]$.

4 в) $\dfrac{3+\sqrt{5}}{2} = [2, (1)]$;

4 г) $\dfrac{3-\sqrt{5}}{2} = [0, (1)]$;

4 д) $\dfrac{2+\sqrt{17}}{13} = [0, 2, (8)]$;

4 е) $\dfrac{2-\sqrt{17}}{13} = [-1, 1, 5, (8)]$;

4 ж) $\dfrac{2-\sqrt{15}}{11} = [-1, 1, 4, (1, 6)]$;

4 з) $\dfrac{2+\sqrt{15}}{11} = [0, 1, (1, 6)]$;

4 и) $\dfrac{1+\sqrt{26}}{5} = [(1, 4, 1)]$;

4 к) $\dfrac{1-\sqrt{26}}{5} = [-1, 5, (1, 1, 4)]$.

5 а) $\dfrac{1+3\sqrt{2}}{2} = [2, (1, 1, 1, 1, 1, 3)]$;

5 б) $\dfrac{1-3\sqrt{2}}{2} = [-2, 2(1, 1, 1, 3, 1, 1)]$;

5 в) $\dfrac{1+3\sqrt{5}}{2} = [3, (1, 5)]$;

5 г) $\dfrac{1-3\sqrt{5}}{2} = [-3, 6, (1.5)]$.

6 а) $\dfrac{\sqrt{2210}-13}{13}=[2,(1,1,1,1,1,1,6)]$;

7 а) $[1,2,3,4,6]=268/187$;

7 в) $[-2,3,3,10]=-175/103$.

7 з) $[0,8,1,6,2,2]=37/328$.

8 а) $[1,(2)]=\sqrt{2}$.

10 а) $\dfrac{6-\sqrt{50}}{7}$;

10 б) $\dfrac{\sqrt{53}-2}{7}$;

10 в) $\sqrt{19}$;

10 г) $\sqrt{59}$;

10 д) $\dfrac{1+3\sqrt{2}}{2}$;

10 ж) $-\sqrt{21}$;

10 з) $\dfrac{\sqrt{2210}-13}{13}$.

11. $x^2-6x-7=0$.

Ответы и решения задач из § 23.

6 а) $\alpha=[2,(1,7)]$, $\delta_6=231/80$, $\Delta<10^{-4}$;

6 г) $\alpha=[2,1,(3,1)]$, $\delta_6=67/24$, $\Delta<10^{-3}$.

14. Запишем несколько шагов разложения числа $\sqrt[3]{2}$ в цепную дробь:

$$\alpha_0=\sqrt[3]{2}=1+\frac{1}{\alpha_1},\quad \text{где } \frac{1}{\alpha_1}=\sqrt[3]{2}-1;$$

$$\alpha_1=\frac{1}{\sqrt[3]{2}-1}=\frac{\sqrt[3]{4}+\sqrt[3]{2}+1}{2-1}=3+\frac{1}{\alpha_2},\quad \text{где } \frac{1}{\alpha_2}=\sqrt[3]{4}+\sqrt[3]{2}-2;$$

$$\alpha_2=\frac{1}{\sqrt[3]{4}+\sqrt[3]{2}-2}=\frac{1}{(\sqrt[3]{2}-1)(\sqrt[3]{2}+2)}=$$

$$=\frac{(\sqrt[3]{4}+\sqrt[3]{2}+1)(\sqrt[3]{4}-2\sqrt[3]{2}+4)}{(2-1)(2+8)}=\frac{3\sqrt[3]{4}+4\sqrt[3]{2}+2}{10}=1+\frac{1}{\alpha_3},$$

$$\text{где } \frac{1}{\alpha_3}=\frac{3\sqrt[3]{4}+4\sqrt[3]{2}-8}{10};$$

$$\alpha_3=\frac{10}{3\sqrt[3]{4}+4\sqrt[3]{2}-8}=5+\frac{1}{\alpha_4},\quad \text{и т. д.}$$

Теперь несложно убедиться в том, что $\sqrt[3]{2}\approx 1.25$.

15. Указание: убедитесь том, что $\sqrt[3]{10} = [2, 6, 2, \ldots]$, и, следовательно, $\delta_1 = 2$, $\delta_2 = 13/6$, $\delta_3 = 28/13$.

16. $e = 2{,}718281828\ldots = [2, 1, 2, 1, 1, \ldots] \approx 11/4$.

Именно, $\alpha_0 = e = 2 + \dfrac{1}{\alpha_1}$, где $\dfrac{1}{\alpha_1} = 0{,}718 + \epsilon$;

$\alpha_1 = \dfrac{1000}{718 + \epsilon \cdot 10^3} = 1 + \dfrac{1}{\alpha_2}$, где $\dfrac{1}{\alpha_2} = \dfrac{1000 - 718 - \epsilon_1}{718 + \epsilon_1}$;

$\alpha_2 = \dfrac{718 + \epsilon_1}{282 - \epsilon_1} = 2 + \dfrac{1}{\alpha_3}$, где $\dfrac{1}{\alpha_3} = \dfrac{718 + \epsilon_1 - 2 \cdot 282 + 2\epsilon_1}{282 - \epsilon_1}$;

$\alpha_3 = \dfrac{282 - \epsilon_1}{154 + 3\epsilon_1} = 1 + \dfrac{1}{\alpha_4}$, где $\dfrac{1}{\alpha_4} = \dfrac{282 - \epsilon_1 - 154 - 3\epsilon_1}{154 + 3\epsilon_1}$.

$\alpha_4 = \dfrac{154 + 3\epsilon_1}{128 - 4\epsilon_1} = 1 + \dfrac{1}{\alpha_5}$, где $\dfrac{1}{\alpha_5} = \dfrac{154 + 3\epsilon_1 - 128 = 4\epsilon_1}{128 - 4\epsilon_1}$;

$\alpha_5 = \dfrac{128 - 4\epsilon_1}{26 + 7\epsilon_1} = 4 + \dfrac{1}{\alpha_6}$, где $\dfrac{1}{\alpha_6} = \dfrac{128 - 4\epsilon_1 - 104 - 28\epsilon_1}{26 + 7\epsilon_1}$.

При этом знаменвтели подходящих дробей образуют последовательность 1, 1, 3, 4, 7, ..., в которой $4 \cdot 7 = 28$, и $1/28 = 0{,}03587 < 0{,}036$.

18 а) $x \equiv 41; 190; 339 (\mathrm{mod}\, 447)$;

18 б) $x \equiv 61; 272 (\mathrm{mod}\, 422)$;

18 в) $x \equiv 39; 196; 353 (\mathrm{mod}\, 471)$;

18 г) $x \equiv 29 (\mathrm{mod}\, 311)$;

18 д) сравнение не имеет решений.

Ответы и решения задач из § 24.

8. Указание: убедитесь, что a_n делится на 24.

9. 3; 5; 101;

10. 16 пар; в общем случае — 2^k пар, где k — колчество простых делителей числа $\dfrac{[a, b]}{(a, б)}$.

28 а) (100; 111).

28 б) (6; 1); (3; 4); (0; 7);

28 в) $(x; x)$;

28 г) (29; 57);

28 д) нет решений;

28 е) $(n, n + 15)$.

29. Да.

35. (100; 111).

60. (12; 16; 11); (13; 17; 17); (13; 18; 12). Указание: перейдите к остаткам при делении на семь.

61. 20. Заметим, что число $1 + 2 + 3 + \ldots + n = \dfrac{n(n+1)}{2}$ называется *треугольным* (см. [11]).

62. 19.

63. 848; 853; 854; 856; 862; 864; 865; 867; 870.

Таблица простых чисел, не превосходящих 10000

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541
547	557	563	569	571	577	587	593	599	601
607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733
739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863
877	881	883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997	1009	1013
1019	1021	1031	1033	1039	1049	1051	1061	1063	1069
1087	1091	1093	1097	1103	1109	1117	1123	1129	1151
1153	1163	1171	1181	1187	1193	1201	1213	1217	1223
1229	1231	1237	1249	1259	1277	1279	1283	1289	1291

1297	1301	1303	1307	1319	1321	1327	1361	1367	1373
1381	1399	1409	1423	1427	1429	1433	1439	1447	1451
1453	1459	1471	1481	1483	1487	1489	1493	1499	1511
1523	1531	1543	1549	1553	1559	1567	1571	1579	1583
1597	1601	1607	1609	1613	1619	1621	1627	1637	1657
1663	1667	1669	1693	1697	1699	1709	1721	1723	1733
1741	1747	1753	1759	1777	1783	1787	1789	1801	1811
1823	1831	1847	1861	1867	1871	1873	1877	1879	1889
1901	1907	1913	1931	1933	1949	1951	1973	1979	1987
1993	1997	1999	2003	2011	2017	2027	2029	2039	2053
2063	2069	2081	2083	2087	2089	2099	2111	2113	2129
2131	2137	2141	2143	2153	2161	2179	2203	2207	2213
2221	2237	2239	2243	2251	2267	2269	2273	2281	2287
2293	2297	2309	2311	2333	2339	2341	2347	2351	2357
2371	2377	2381	2383	2389	2393	2399	2411	2417	2423
2437	2441	2447	2459	2467	2473	2477	2503	2521	2531
2539	2543	2549	2551	2557	2579	2591	2593	2609	2617
2621	2633	2647	2657	2659	2663	2671	2677	2683	2687
2689	2693	2699	2707	2711	2713	2719	2729	2731	2741
2749	2753	2767	2777	2789	2791	2797	2801	2803	2819
2833	2837	2843	2851	2857	2861	2879	2887	2897	2903
2909	2917	2927	2939	2953	2957	2963	2969	2971	2999
3001	3011	3019	3023	3037	3041	3049	3061	3067	3079
3083	3089	3109	3119	3121	3137	3163	3167	3169	3181
3187	3191	3203	3209	3217	3221	3229	3251	3253	3257
3259	3271	3299	3301	3307	3313	3319	3323	3329	3331
3343	3347	3359	3361	3371	3373	3389	3391	3407	3413
3433	3449	3457	3461	3463	3467	3469	3491	3499	3511
3517	3527	3529	3533	3539	3541	3547	3557	3559	3571
3581	3583	3593	3607	3613	3617	3623	3631	3637	3643
3659	3671	3673	3677	3691	3697	3701	3709	3719	3727

3733	3739	3761	3767	3769	3779	3793	3797	3803	3821
3823	3833	3847	3851	3853	3863	3877	3881	3889	3907
3911	3917	3919	3923	3929	3931	3943	3947	3967	3989
4001	4003	4007	4013	4019	4021	4027	4049	4051	4057
4073	4079	4091	4093	4099	4111	4127	4129	4133	4139
4153	4157	4159	4177	4201	4211	4217	4219	4229	4231
4241	4243	4253	4259	4261	4271	4273	4283	4289	4297
4327	4337	4339	4349	4357	4363	4373	4391	4397	4409
4421	4423	4441	4447	4451	4457	4463	4481	4483	4493
4507	4513	4517	4519	4523	4547	4549	4561	4567	4583
4591	4597	4603	4621	4637	4639	4643	4649	4651	4657
4663	4673	4679	4691	4703	4721	4723	4729	4733	4751
4759	4783	4787	4789	4793	4799	4801	4813	4817	4831
4861	4871	4877	4889	4903	4909	4919	4931	4933	4937
4943	4951	4957	4967	4969	4973	4987	4993	4999	5003
5009	5011	5021	5023	5039	5051	5059	5077	5081	5087
5099	5101	5107	5113	5119	5147	5153	5167	5171	5179
5189	5197	5209	5227	5231	5233	5237	5261	5273	5279
5281	5297	5303	5309	5323	5333	5347	5351	5381	5387
5393	5399	5407	5413	5417	5419	5431	5437	5441	5443
5449	5471	5477	5479	5483	5501	5503	5507	5519	5521
5527	5531	5557	5563	5569	5573	5581	5591	5623	5639
5641	5647	5651	5653	5657	5659	5669	5683	5689	5693
5701	5711	5717	5737	5741	5743	5749	5779	5783	5791
5801	5807	5813	5821	5827	5839	5843	5849	5851	5857
5861	5867	5869	5879	5881	5897	5903	5923	5927	5939
5953	5981	5987	6007	6011	6029	6037	6043	6047	6053
6067	6073	6079	6089	6091	6101	6113	6121	6131	6133
6143	6151	6163	6173	6197	6199	6203	6211	6217	6221
6229	6247	6257	6263	6269	6271	6277	6287	6299	6301
6311	6317	6323	6329	6337	6343	6353	6359	6361	6367

6373	6379	6389	6397	6421	6427	6449	6451	6469	6473
6481	6491	6521	6529	6547	6551	6553	6563	6569	6571
6577	6581	6599	6607	6619	6637	6653	6659	6661	6673
6679	6689	6691	6701	6703	6709	6719	6733	6737	6761
6763	6779	6781	6791	6793	6803	6823	6827	6829	6833
6841	6857	6863	6869	6871	6883	6899	6907	6911	6917
6947	6949	6959	6961	6967	6971	6977	6983	6991	6997
7001	7013	7019	7027	7039	7043	7057	7069	7079	7103
7109	7121	7127	7129	7151	7159	7177	7187	7193	7207
7211	7213	7219	7229	7237	7243	7247	7253	7283	7297
7307	7309	7321	7331	7333	7349	7351	7369	7393	7411
7417	7433	7451	7457	7459	7477	7481	7487	7489	7499
7507	7517	7523	7529	7537	7541	7547	7549	7559	7561
7573	7577	7583	7589	7591	7603	7607	7621	7639	7643
7649	7669	7673	7681	7687	7691	7699	7703	7717	7723
7727	7741	7753	7757	7759	7789	7793	7817	7823	7829
7841	7853	7867	7873	7877	7879	7883	7901	7907	7919
7927	7933	7937	7949	7951	7963	7993	8009	8011	8017
8039	8053	8059	8069	8081	8087	8089	8093	8101	8111
8117	8123	8147	8161	8167	8171	8179	8191	8209	8219
8221	8231	8233	8237	8243	8263	8269	8273	8287	8291
8293	8297	8311	8317	8329	8353	8363	8369	8377	8387
8389	8419	8423	8429	8431	8443	8447	8461	8467	8501
8513	8521	8527	8537	8539	8543	8563	8573	8581	8597
8599	8609	8623	8627	8629	8641	8647	8663	8669	8677
8681	8689	8693	8699	8707	8713	8719	8731	8737	8741
8747	8753	8761	8779	8783	8803	8807	8819	8821	8831
8837	8839	8849	8861	8863	8867	8887	8893	8923	8929
8933	8941	8951	8963	8969	8971	8999	9001	9007	9011
9013	9029	9041	9043	9049	9059	9067	9091	9103	9109
9127	9133	9137	9151	9157	9161	9173	9181	9187	9199

9203	9209	9221	9227	9239	9241	9257	9277	9281	9283
9293	9311	9319	9323	9337	9341	9343	9349	9371	9377
9391	9397	9403	9413	9419	9421	9431	9433	9437	9439
9461	9463	9467	9473	9479	9491	9497	9511	9521	9533
9539	9547	9551	9587	9601	9613	9619	9623	9629	9631
9643	9649	9661	9677	9679	9689	9697	9719	9721	9733
9739	9743	9749	9767	9769	9781	9787	9791	9803	9811
9817	9829	9833	9839	9851	9857	9859	9871	9883	9887
9901	9907	9923	9929	9931	9941	9949	9967	9973	

Таблицы индексов

$p = 3, p - 1 = 2, g = 2.$

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	1								0	1	2								

$p = 5, p - 1 = 2^2, g = 2.$

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	1	3	2						0	1	2	4	3						

$p = 7, p - 1 = 2 \cdot 3, g = 3.$

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	2	1	4	5	3				0	1	3	2	6	4	5				

$p = 11, p - 1 = 2 \cdot 5, g = 2.$

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	1	8	2	4	9	7	3	6	0	1	2	4	8	5	10	9	7	3	6
1	5										1										

$p = 13, p - 1 = 2^2 \cdot 3, g = 2.$

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	1	4	2	9	5	11	3	8	0	1	2	4	8	3	6	12	11	9	5
1	10	7	6								1	10	7								

$p = 17, p - 1 = 2^4, g = 3.$

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	14	1	12	5	15	11	10	2	0	1	3	9	10	13	5	15	11	16	11
1	3	7	13	4	9	6	8				1	8	7	4	12	2	6				

$p = 19$, $p - 1 = 2 \cdot 3^2$, $g = 2$.

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	1	13	2	16	14	6	3	8	0	1	2	4	8	16	13	7	14	9	18
1	17	12	15	5	7	11	4	10	9		1	17	15	11	3	6	12	5	10		

$p = 23$, $p - 1 = 2 \cdot 11$, $g = 5$.

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	2	16	4	1	18	19	6	10	0	1	5	2	10	4	20	8	17	16	11
1	3	9	20	14	21	17	8	7	12	15	1	9	22	18	21	13	19	3	15	6	7
2	5	13	11								2	12	14								

$p = 29$, $p - 1 = 2^2 \cdot 7$, $g = 2$.

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	1	5	2	22	6	12	3	10	0	1	2	4	8	16	3	6	12	24	19
1	23	25	7	18	13	27	4	21	11	9	1	9	18	7	14	28	27	25	21	13	26
2	24	17	26	20	8	16	19	15	14		2	23	17	5	10	20	11	22	15		

$p = 31$, $p - 1 = 2 \cdot 3 \cdot 5$, $g = 3$.

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	24	1	18	20	25	28	12	2	0	1	3	9	27	19	26	16	17	20	29
1	14	23	19	11	22	21	6	7	26	4	1	25	13	8	24	10	30	28	22	4	12
2	8	29	17	27	13	10	5	3	16	9	2	5	15	14	11	2	6	18	23	7	21
3	15																				

$p = 37$, $p - 1 = 2^2 \cdot 3^2$, $g = 2$.

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	1	26	2	23	27	32	3	16	0	1	2	4	8	16	32	27	17	34	31
1	24	30	28	11	33	13	4	7	17	35	1	25	13	26	15	30	23	9	18	36	35
2	25	22	31	15	29	10	12	6	34	21	2	33	29	21	5	10	20	3	6	12	24
3	14	9	5	20	8	19	18				3	11	22	7	14	28	19				

$p = 41$, $p - 1 = 2^3 \cdot 5$, $g = 6$.

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30	0	1	6	36	11	25	27	39	29	10	19
1	8	3	27	31	25	37	24	33	16	9	1	32	28	4	24	21	3	18	26	33	34
2	34	14	29	36	13	4	17	5	11	7	2	40	35	5	30	16	14	2	12	31	22
3	23	28	10	18	19	21	2	32	35	6	3	9	13	37	17	20	38	23	15	8	7
4	20																				

$p = 43$, $p - 1 = 2 \cdot 3 \cdot 7$, $g = 3$.

N	0	1	2	3	4	5	6	7	8	9	*Ind*	0	1	2	3	4	5	6	7	8	9
0		0	27	1	12	25	28	35	39	2	0	1	3	9	27	38	28	41	37	25	32
1	10	30	13	32	20	26	24	38	29	19	1	10	30	4	12	36	22	23	26	35	19
2	37	36	15	16	40	8	17	3	5	41	2	14	42	40	34	16	5	15	2	6	18
3	11	34	9	31	23	18	14	7	4	33	3	11	33	13	39	31	7	21	20	17	8
4	22	6	21								4	24	29								

$p = 47$, $p - 1 = 2 \cdot 23$, $g = 5$.

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	18	20	36	1	38	32	8	40	0	1	5	25	31	14	23	21	11	8	40
1	19	7	10	11	4	21	26	16	12	45	1	12	13	18	43	27	41	17	38	2	10
2	37	6	25	5	28	2	29	14	22	35	2	3	15	28	46	42	22	16	33	24	26
3	39	3	44	27	34	33	30	42	17	31	3	36	39	7	35	34	29	4	20	6	30
4	9	15	24	13	43	41	23				4	9	45	37	44	32	19				

$p = 53$, $p - 1 = 2^2 \cdot 13$, $g = 2$.

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	1	17	2	47	18	14	3	34	0	1	2	4	8	16	32	11	22	44	35
1	48	6	19	24	15	12	4	10	35	37	1	17	34	15	30	7	14	28	3	6	12
2	49	31	7	39	20	42	25	51	16	46	2	24	48	43	33	13	26	52	51	49	45
3	13	33	5	23	11	9	36	30	38	41	3	37	21	42	31	9	18	36	19	38	23
4	50	45	32	22	8	29	40	44	21	28	4	46	39	25	50	47	41	29	5	10	20
5	43	27	26								5	40	27								

$p = 59$, $p - 1 = 2 \cdot 29$, $g = 2$.

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	1	50	2	6	51	18	3	42	0	1	2	4	8	16	32	5	10	20	40
1	7	25	52	45	19	56	4	40	43	38	1	21	42	25	50	41	23	46	33	7	14
2	8	10	26	15	53	12	46	34	20	28	2	28	56	53	47	35	11	22	44	29	58
3	57	49	5	17	41	24	44	55	39	37	3	57	55	51	43	27	54	49	39	19	38
4	9	14	11	33	27	48	16	23	54	36	4	17	34	9	18	36	13	26	52	45	31
5	13	32	47	22	35	31	21	30	29		5	3	6	12	24	48	37	15	30		

$p = 61$, $p - 1 = 2^2 \cdot 3 \cdot 5$, $g = 2$.

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	1	6	2	22	7	49	3	12	0	1	2	4	8	16	32	3	6	12	24
1	23	15	8	40	50	28	4	47	13	26	1	48	35	9	18	36	11	22	44	27	54
2	24	55	16	57	9	44	41	18	51	35	2	47	33	5	10	20	40	19	38	15	30
3	29	59	5	21	48	11	14	39	27	46	3	60	59	57	53	45	29	58	55	49	37
4	25	54	56	43	17	34	58	20	10	38	4	13	26	52	43	25	50	39	17	34	7
5	45	53	42	33	19	37	52	32	36	31	5	14	28	56	51	41	21	42	23	46	31
6	30																				

$p = 67$, $p - 1 = 2 \cdot 3 \cdot 11$, $g = 2$.

N	0	1	2	3	4	5	6	7	8	9	Ind	0	1	2	3	4	5	6	7	8	9
0		0	1	39	2	15	40	23	3	12	0	1	2	4	8	16	32	64	61	55	43
1	16	59	41	19	24	54	4	64	13	10	1	19	38	9	18	36	5	10	20	40	13
2	17	62	60	28	42	30	20	51	25	44	2	26	52	37	7	14	28	56	45	23	46
3	55	47	5	32	65	38	14	22	11	58	3	25	50	33	66	65	63	59	51	35	3
4	18	53	63	9	61	27	29	50	43	46	4	6	12	24	48	29	58	49	31	62	57
5	31	37	21	57	52	8	26	49	45	36	5	47	27	54	41	15	30	60	53	39	11
6	56	7	48	35	6	34	33				6	22	44	21	42	17	34				

$p = 71$, $p - 1 = 2 \cdot 5 \cdot 7$, $g = 7$.

N	0	1	2	3	4	5	6	7	8	9
0		0	6	26	12	28	32	1	18	52
1	34	31	38	39	7	54	24	49	58	16
2	40	27	37	15	44	56	45	8	13	68
3	60	11	30	57	55	29	64	20	22	65
4	46	25	33	48	43	10	21	9	50	2
5	62	5	51	23	14	59	19	42	4	3
6	66	69	17	53	36	67	63	47	61	41
7	35									

Ind	0	1	2	3	4	5	6	7	8	9
0	1	7	49	59	58	51	2	14	27	47
1	45	31	4	28	54	23	19	62	8	56
2	37	46	38	53	16	41	3	21	5	35
3	32	11	6	42	10	70	64	22	12	13
4	20	69	57	44	24	26	40	67	43	17
5	48	52	9	63	15	34	25	33	18	55
6	30	68	50	66	36	39	60	65	29	61

$p = 73$, $p - 1 = 2^3 \cdot 3^2$, $g = 5$.

N	0	1	2	3	4	5	6	7	8	9
0		0	8	6	16	1	14	33	24	12
1	9	55	22	59	41	7	32	21	20	62
2	17	39	63	46	30	2	67	18	49	35
3	15	11	40	61	29	34	28	64	70	65
4	25	4	47	51	71	13	54	31	38	66
5	10	27	3	53	26	56	57	68	43	5
6	23	58	19	45	48	60	69	50	37	52
7	42	44	36							

Ind	0	1	2	3	4	5	6	7	8	9
0	1	5	25	52	41	59	3	15	2	10
1	50	31	9	45	6	30	4	20	27	62
2	18	17	12	60	8	40	54	51	36	34
3	24	47	16	7	35	29	72	68	48	21
4	32	14	70	58	71	63	23	42	64	28
5	67	43	69	53	46	11	55	56	61	13
6	65	33	19	22	37	39	49	26	57	66
7	38	44								

$p = 79$, $p - 1 = 2 \cdot 3 \cdot 13$, $g = 3$.

N	0	1	2	3	4	5	6	7	8	9
0		0	4	1	8	62	5	53	12	2
1	66	68	9	34	57	63	16	21	6	32
2	70	54	72	26	13	46	38	3	61	11
3	67	56	20	69	25	37	10	19	36	35
4	74	75	58	49	76	64	30	59	17	28
5	50	22	42	77	7	52	65	33	15	31
6	71	45	60	55	24	18	73	48	29	27
7	41	51	14	44	23	47	40	43	39	

Ind	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	2	6	18	54	4	12
1	36	29	8	24	72	58	16	48	65	37
2	32	17	51	74	64	34	23	69	49	68
3	46	59	19	57	13	39	38	35	26	78
4	76	70	52	77	73	61	25	75	67	43
5	50	71	55	7	21	63	13	14	42	47
6	62	28	5	15	45	56	10	30	11	33
7	20	60	22	66	40	41	44	53		

$p = 83$, $p - 1 = 2 \cdot 41$, $g = 2$.

N	0	1	2	3	4	5	6	7	8	9
0		0	1	72	2	27	73	8	3	62
1	28	24	74	77	9	17	4	56	63	47
2	29	80	25	60	75	54	78	52	10	12
3	18	38	5	14	57	35	64	20	48	67
4	30	40	81	71	26	7	61	23	76	16
5	55	46	79	59	53	51	11	37	13	34
6	19	66	39	70	6	22	15	45	58	50
7	36	33	65	69	21	44	49	32	68	43
8	31	42	41							

Ind	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	45	7	14
1	28	56	29	58	33	66	49	15	30	60
2	37	74	65	47	11	22	44	5	10	20
3	40	80	77	71	59	35	70	57	31	62
4	41	82	81	79	75	67	51	19	38	76
5	69	55	27	54	25	50	17	34	68	53
6	23	46	9	18	36	72	61	39	78	73
7	63	43	3	6	12	24	48	13	26	52
8	21	42								

$p = 89$, $p - 1 = 2^3 \cdot 11$, $g = 3$.

N	0	1	2	3	4	5	6	7	8	9
0		0	16	1	32	70	17	81	48	2
1	86	84	33	23	9	71	64	6	18	35
2	14	82	12	57	49	52	39	3	25	59
3	87	31	80	85	22	63	34	11	51	24
4	30	21	10	29	28	72	73	54	65	74
5	68	7	55	78	19	66	41	36	75	43
6	15	69	47	83	8	5	13	56	38	58
7	79	62	50	20	27	53	67	77	40	42
8	46	4	37	61	26	76	45	60	44	

Ind	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	81	65	17	51	64	14
1	42	37	22	66	20	60	2	6	18	54
2	73	41	34	13	39	28	84	74	44	43
3	40	31	4	12	36	19	57	82	68	26
4	78	56	79	59	88	86	80	62	8	24
5	72	38	25	75	47	52	67	23	69	29
6	87	83	71	35	16	48	55	76	50	61
7	5	15	45	46	49	58	85	77	53	70
8	32	7	21	63	11	33	10	30		

$p = 97$, $p - 1 = 2^5 \cdot 3$, $g = 5$.

N	0	1	2	3	4	5	6	7	8	9
0		0	34	70	68	1	8	31	6	44
1	35	86	42	25	65	71	40	89	78	81
2	69	5	24	77	76	2	59	18	3	13
3	9	46	74	60	27	32	16	91	19	95
4	7	85	39	4	58	45	15	84	14	62
5	36	63	93	10	52	87	37	55	47	67
6	43	64	80	75	12	26	94	57	61	51
7	66	11	50	28	29	72	53	21	33	30
8	41	88	23	17	73	90	38	83	92	54
9	79	56	49	20	22	82	48			

Ind	0	1	2	3	4	5	6	7	8	9
0	1	5	25	28	43	21	8	40	6	30
1	53	71	64	29	48	46	36	83	27	38
2	93	77	94	82	22	13	65	34	73	74
3	79	7	35	78	2	10	50	56	86	42
4	16	80	12	60	9	45	31	58	96	92
5	72	69	54	76	89	57	91	67	44	26
6	33	68	49	51	61	14	70	59	4	20
7	3	15	75	84	32	63	24	23	18	90
8	62	19	95	87	47	41	11	55	81	17
9	85	37	88	52	66	39				

Литература

1. *Александров В. А., Горшенин С. М.* Задачник-практикум по теории чисел. М.: Просвещение, 1972.
2. *Баврин И. И., Фрибус Е. А.* Старинные задачи. М.: Просвещение, 1994.
3. *Бухштаб А. А.* Теория чисел. М.: Просвещение, 1966.
4. *Василенко О. Н., Галочкин А. И.* Сборник задач по теории чисел. М.: Изд-во МГУ, 1995.
5. *Виноградов И. М.* Основы теории чисел. М.: Наука, 1981.
6. *Галкин В. Я., Сычугов Д. Ю., Хорошилова Е. В.* Конкурсные задачи, основанные на теории чисел. М.: Изд-во МГУ, 2002.
7. *Галочкин А. И., Нестеренко Ю. В., Шидловский А. Б.* Введение в теорию чисел. М.: Изд-во МГУ, 1995.
8. *Грибанов В. У., Титов П. И.* Сборник упражнений по теории чисел. М.: Просвещение, 1964.
9. *Девеннорт Г.* Высшая арифметика. 2-е изд. М.: Книжный дом «Либроком»/URSS, 2010.
10. *Девеннорт Г.* Мультипликативная теория чисел. М.: Наука, 1971.
11. *Деза Е. И.* Специальные числа натурального ряда. М.: Книжный дом «Либроком»/URSS, 2011.
12. *Депман И. Я.* История арифметики. 6-е изд. М.: Книжный дом «Либроком»/URSS, 2011.
13. *Жмулева А. В.* Сборник задач по теории чисел. М.: Изд-во МГУ, 2009.
14. *Зубов А. Ю., Зязин А. В., Овчинников В. Н., Рамоданов С. М.* Олимпиады по криптографии и математике. М.: МЦНМО, 2006.
15. *Ингам А. Е.* Распределение простых чисел. 4-е изд. М.: Книжный дом «Либроком»/URSS, 2009.
16. *Карацуба А. А.* Основы аналитической теории чисел. 2-е изд. М.: URSS, 2004.
17. *Коблиц Н.* Курс теории чисел и криптографии. М.: Научн. изд-во ТВП, 2001.
18. *Куликов Л. Я., Москаленко А. И., Фомин А. А.* Сборник задач по алгебре и теории чисел. М.: Просвещение, 1993.
19. Неопубликованные материалы Эйлера по теории чисел / Под ред. Н. И. Невской СПб.: Наука, 1997.

20. *Нечаев В. И.* Элементы криптографии (Основы теории защиты информации). М.: Высшая школа, 1999.
21. *Ожигова Е. П.* Развитие теории чисел в России. 3-е изд. М.: URSS, 2011.
22. *Перельман Я. И.* Занимательная арифметика. Загадки и диковинки в мире чисел. М.: Изд-во Русанова, 1994.
23. *Прахар К.* Распределение простых чисел. М.: Мир, 1967.
24. *Радемахер Г., Теплиц О.* Числа и фигуры. Опыты математического мышления. 4-е изд. М.: Издательство ЛКИ/URSS, 2007.
25. *Серпинский В.* Что мы знаем и чего не знаем о простых числах. Л.: Гос. изд-во физ.-мат. литературы, 1963.
26. *Серпинский В.* 250 задач по элементарной теории чисел. М.: Просвещение, 1968.
27. *Степанова Л. Л.* Избранные главы элементарной теории чисел. М.: Прометей, 2001.
28. *Степанова Л. Л., Жмулева А. В., Деза Е. И.* Практикум по элементарной математике: Арифметика. М.: МЦНМО, 2008.
29. *Титчмарш Е. К.* Теория дзета-функции Римана. М.: Иностранная литература, 1953.
30. *Топунов В. Л.* Комбинаторика. М.: МПГУ, 2001.
31. *Хинчин А. Я.* Цепные дроби. 2-е изд. М.: URSS, 2003.
32. *Чандрасекхаран К.* Арифметические функции. М.: Наука, 1975.
33. *Чистяков В. Д.* Старинные задачи по элементарной математике. Минск, 1978.
34. *Ященко В. В.* Введение в криптографию. М.: МЦНМО, 1998.
35. *Conway J. H., Guy R. K.* The Book of Numbers. New York: Springer-Verlag, 1996.
36. *Courant R. and Robbins H.* What Is Mathematics?: An Elementary Approach to Ideas and Methods. 2-nd ed. Oxford University Press, 1996.
37. *Dickson L. E.* History of the Theory of Numbers. New York: Dover, 2005.
38. *Gauss C. F.* Disquisitiones Arithmeticae. Leipzig, 1801.
39. *Guy R. K.* Unsolved Problems in Number Theory. 2-nd ed. New York: Springer-Verlag, 1994.
40. *Hardy G. H., Wright E. M.* An Introduction to the Theory of Numbers. 5-th ed. Oxford: Clarendon Press, 1979.
41. *Ore O.* Number Theory и Its History. Dover Publications, 1948.
42. [Электронный ресурс] PlanetMath.org: http://planetmath.org/encyclopedia/
43. *Ribenboim P.* New Book of Prime Number Records. New York: Springer-Verlag, 1996.
44. *Riesel H.* Prime Numbers and Computer Methods for Factorization. 2-nd ed. Basel: Birkhouser, 1994.
45. *Shanks D.* Solved and Unsolved Problems in Number Theory. 4-th ed. New York: Chelsea, 1993.
46. *Sloane N. J.* The On-line Encyclopedia of Integer Sequences. [Электронный ресурс] http://www.research.att.com/ njas/sequences/
47. *Weisstein E. W.* Concise Encyclopedia of Mathematics. CRC Press, 1999.
48. [Электронный ресурс] Wikipedia, the Free Encyclopedia: http://en.wikipedia.org.

Другие книги нашего издательства:

Дифференциальные уравнения

Филиппов А. Ф. **Введение в теорию дифференциальных уравнений.**
Филиппов А. Ф. **Сборник задач по дифференциальным уравнениям.**
Эльсгольц Л. Э. **Дифференциальные уравнения.**
Степанов В. В. **Курс дифференциальных уравнений.**
Немыцкий В. В., Степанов В. В. **Качественная теория дифференциальных уравнений.**
Федорюк М. В. **Обыкновенные дифференциальные уравнения.**
Федорюк М. В. **Асимптотика: Интегралы и ряды.**
Федорюк М. В. **Метод перевала.**
Краснов М. Л. **Интегральные уравнения. Введение в теорию.**
Коддингтон Э. А., Левинсон Н. **Теория обыкновенных дифференциальных уравнений.**
Сикорский Ю. С. **Обыкновенные дифференциальные уравнения.**
Понтрягин Л. С. **Дифференциальные уравнения и их приложения.**
Трикоми Ф. Дж. **Дифференциальные уравнения.**
Трикоми Ф. Дж. **Лекции по уравнениям в частных производных.**
Филипс Г. **Дифференциальные уравнения.**
Амелькин В. В. **Автономные и линейные многомерные дифференциальные уравнения.**
Амелькин В. В. **Дифференциальные уравнения в приложениях.**
Беллман Р. **Теория устойчивости решений дифференциальных уравнений.**
Лефшец С. **Геометрическая теория дифференциальных уравнений.**
Ловитт У. В. **Линейные интегральные уравнения.**

Алгебра

Чеботарев Н. Г. **Основы теории Галуа.** В 2 кн.
Вейль Г. **Классические группы. Их инварианты и представления.**
Фробениус Ф. Г. **Теория характеров и представлений групп.**
Эйзенхарт Л. П. **Непрерывные группы преобразований.**
Бэр Р. **Линейная алгебра и проективная геометрия.**
Никифоров В. А., Шкода Б. В. **Линейная алгебра и аналитическая геометрия.**
Шевалле К. **Введение в теорию алгебраических функций.**
Супруненко Д. А., Тышкевич Р. И. **Перестановочные матрицы.**
Яглом И. М. **Необыкновенная алгебра.**
Уокер Р. **Алгебраические кривые.**
Хамермеш М. **Теория групп и ее применение к физическим проблемам.**
Бауэр Э. **Введение в теорию групп и ее приложения к квантовой физике.**
Петрашень М. И., Трифонов Е. Д. **Применение теории групп в квантовой механике.**

Серия «Физико-математическое наследие: математика (алгебра)»

Чеботарев Н. Г. **Введение в теорию алгебр.**
Чеботарев Н. Г. **Теория Галуа.**
Чеботарев Н. Г. **Теория алгебраических функций.**
Александров П. С. **Введение в теорию групп.**
Маркус М., Минк Х. **Обзор по теории матриц и матричных неравенств.**
Бохер М. **Введение в высшую алгебру.**
Млодзеевский Б. К. **Основы высшей алгебры.**
Шмидт О. Ю. **Абстрактная теория групп.**

Другие книги нашего издательства:

URSS

Теория графов

Оре О. **Графы и их применение.**
Оре О. **Теория графов.**
Харари Ф. **Теория графов.**
Емеличев В. А., Мельников О. И. и др. **Лекции по теории графов.**
Мельников О. И. **Теория графов в занимательных задачах.**
Мельников О. И. **Обучение дискретной математике.**
Мельников О. И. **Незнайка в стране графов.**
Березина Л. Ю. **Графы и их применение.**
Малинин Л. И., Малинина Н. Л. **Изоморфизм графов в теоремах и алгоритмах.**
Панюкова Т. А. **Комбинаторика и теория графов.**
Родионов В. В. **Методы четырехцветной раскраски вершин плоских графов.**
Деза Е. И., Модель Д. Л. **Основы дискретной математики.**
Эвнин А. Ю. **Вокруг теоремы Холла.**

Теория вероятностей и математическая статистика

Гнеденко Б. В. **Очерк по истории теории вероятностей.**
Гнеденко Б. В. **Математика и контроль качества продукции.**
Гнеденко Б. В., Коваленко И. Н. **Введение в теорию массового обслуживания.**
Хинчин А. Я. **Работы по математической теории массового обслуживания.**
Хинчин А. Я. **Асимптотические законы теории вероятностей.**
Хинчин А. Я. **Математические основания квантовой статистики.**
Феллер В. **Введение в теорию вероятностей и ее приложения.** В 2 т.
Боровков А. А. **Теория вероятностей.**
Боровков А. А. **Эргодичность и устойчивость случайных процессов.**
Сенатов В. В. **Центральная предельная теорема: Точность аппроксимации и асимптотические разложения.**
Дворяткина С. Н., Ляхов Л. Н. **Лекции по классической теории вероятностей.**
Пытьев Ю. П. **Возможность. Элементы теории и применения.**
Григорян А. А. **Закономерности и парадоксы развития теории вероятностей.**
Кац М. **Вероятность и смежные вопросы в физике.**
Яглом А. М., Яглом И. М. **Вероятность и информация.**
Мизес Р. **Вероятность и статистика.**
Хмаладзе Э. В. **Статистические методы в демографии и страховании жизни.**
Кудлаев Э. М. **Разделимые статистики и их применения.**
Дмитриев Е. А. **Математическая статистика в почвоведении.**
Тактаров Н. Г. **Теория вероятностей и математическая статистика.**
Ивченко Г. И., Медведев Ю. И. **Введение в математическую статистику.**

Серия «Классический университетский учебник»

Гнеденко Б. В. **Курс теории вероятностей.**
Колмогоров А. Н., Драгалин А. Г. **Математическая логика.**
Петровский И. Г. **Лекции по теории обыкновенных дифференциальных уравнений.**
Кононович Э. В., Мороз В. И. **Общий курс астрономии.**
Ишханов Б. С., Капитонов И. М., Юдин Н. П. **Частицы и атомные ядра.**
Квасников И. А. **Термодинамика и статистическая физика.** В 4 т.

Другие книги нашего издательства:

Учебники и задачники по математике

Краснов М. Л. и др. **Вся высшая математика.** Т. 1–7.
Краснов М. Л., Киселев А. И., Макаренко Г. И. **Сборники задач «Вся высшая математика» с *подробными решениями*.**
Босс В. **Лекции по математике.** Т. 1–16:
Т. 1: **Анализ**; Т. 2: **Дифференциальные уравнения**; Т. 3: **Линейная алгебра**;
Т. 4: **Вероятность, информация, статистика**; Т. 5: **Функциональный анализ**;
Т. 6: **От Диофанта до Тьюринга**; Т. 7: **Оптимизация**; Т. 8: **Теория групп**; Т. 9: **ТФКП**;
Т. 10. **Перебор и эффективные алгоритмы**; Т. 11. **Уравнения математической физики**;
Т. 12. **Контрпримеры и парадоксы**; Т. 13. **Топология**;
Т. 14. **Теория чисел**; Т. 15. **Нелинейные операторы и неподвижные точки**;
Т. 16. **Теория множеств: От Кантора до Коэна.**
Алексеев В. М. (ред.) **Избранные задачи по математике из журнала "АММ".**
Жуков А. В. и др. **Элегантная математика. Задачи и решения.**
Медведев Г. Н. **Участникам олимпиад и вступительных испытаний по математике.**
Александров И. И. **Сборник геометрических задач на построение (с решениями).**
Попов Г. Н. **Сборник исторических задач по элементарной математике.**
Золотаревская Д. И. **Теория вероятностей. Задачи с решениями.**
Золотаревская Д. И. **Сборник задач по линейной алгебре.**
Мостеллер Ф. **Пятьдесят занимательных вероятностных задач с решениями.**
Антоневич А. Б. и др. **Задачи и упражнения по функциональному анализу.**
Городецкий В. В. и др. **Методы решения задач по функциональному анализу.**
Грищенко А. Е. и др. **Теория функций комплексного переменного: Решение задач.**
Гамов Г., Стерн М. **Занимательные задачи.**
Яглом А. М., Яглом И. М. **Неэлементарные задачи в элементарном изложении.**
Супрун В. П. **Математика для старшеклассников.** Кн. 1, 2.
Базылев Д. Ф. **Олимпиадные задачи по математике.**
Куланин Е. Д., Федин С. Н. **Геометрия треугольника в задачах.**
Эвнин А. Ю. **Задачник по дискретной математике.**
Кравцов А. В., Майков А. Р. **ТФКП: Методы решения задач.**
Киселев А. П. **Задачи и упражнения к «Элементам алгебры».**
Киселев А. П. **Систематический курс арифметики.**

От м. Профсоюзная:

8 мин. пешком
или одна остановка
наземным транспортом:

автобусы № 67, 67к, 130;

троллейбус № 49

до остановки
«Ул. Ивана Бабушкина»

От м. Университет:

трамваи № 14, 39
до остановки
«Черемушкинский рынок»;

трамваи № 22, 26
до остановки
«Ул. Вавилова»;

автобусы № 67, 67г, 130;
троллейбус № 49
до остановки
«Ул. Ивана Бабушкина»

Елена Ивановна ДЕЗА

Кандидат физико-математических наук. В 1983 г. окончила математический факультет Московского государственного педагогического института, в 1992 г. — аспирантуру по кафедре теории чисел МГПИ. С 1988 г. преподает на математическом факультете МГПИ (ныне — МПГУ). Автор нескольких книг по теории чисел, дискретной математике и теории метрических пространств, в том числе учебных пособий «Специальные числа натурального ряда» (М.: URSS, 2011), «Численные методы» (3-е изд. М.: URSS, 2012; совм. с Ю. Н. Шаховым) и «Основы дискретной математики» (2-е изд. М.: URSS, 2011; совм. с Д. Л. Моделем). Автор двух книг, изданных за рубежом: «Dictionary of Distances» (Elsever, 2006) и «Encyclopedia of Distances» (Springer, 2009); обе написаны совместно с французским математиком, вице-президентом Европейской академии наук, профессором Мишелем Деза.

Лидия Владимировна КОТОВА

Окончила математический факультет Московского педагогического государственного университета в 2000 г., аспирантуру по кафедре теории чисел в 2003 г. С 2000 г. преподает на кафедре теории чисел МПГУ. Область научных интересов — теория чисел, криптография.