В.М. Ситников

ТЕОРИЯ ЧИСЕЛ

Учебное пособие

Челябинск
2014

Министерство образования и науки РФ
Федеральное государственное бюджетное образовательное
учреждение высшего профессионального образования
«Челябинский государственный педагогический
университет»

В.М. Ситников

ТЕОРИЯ ЧИСЕЛ

Учебное пособие

Челябинск
2014

УДК 511.2 (021)
ББК 22.13я73
С 41

Ситников, В.М. Теория чисел: учебное пособие / В.М. Ситников. – Челябинск: Изд-во Челяб. гос. пед. ун-та, 2014. – 116 с.

ISBN 978-5-906777-06-5

Учебное пособие разработано на основе курса лекций «Теория чисел».

В нем излагается теоретический материал по теории делимости и теории сравнений целых чисел. В заключительной части содержатся индивидуальные задания по теории чисел.

Пособие предназначено для студентов дневного и заочного отделений факультетов педагогических вузов по профилю «математика».

Рецензенты: Р.Ж. Алеев, д-р физ-мат. наук, профессор
А.С. Макаров, канд. физ-мат. наук

ISBN 978-5-906777-06-5

ВВЕДЕНИЕ

Настоящее учебное пособие предназначено для студентов физико-математических факультетов педагогических университетов и составлено в соответствии с курсом лекций «Теория чисел».

Пособие состоит из двух глав и приложения. Главы разбиты на параграфы, а параграфы на пункты. В приложении даются задания к самостоятельной работе по теории чисел, приводится таблица индексов и список простых чисел малой величины.

В первой главе излагается теория делимости в кольце целых чисел, простые числа, числовые функции и цепные дроби, а также системы счисления. Вторая глава содержит теорию сравнений и некоторые приложения теории чисел к школьной математике. Изложение теоретического материала сопровождается примерами, которые помогают раскрыть суть вводимых понятий.

Пособие может послужить базой для презентации лекционного курса «Теория чисел».

ГЛАВА I. ТЕОРИЯ ДЕЛИМОСТИ

§1. Делимость целых чисел

1. Делимость целых чисел. В курсе теории чисел в основном рассматривается множество целых чисел $Z = \{0, \pm1, \pm2, \pm3, \dots\}$. В дальнейшем, как правило, под **числами** будем понимать целые числа, и считать известными основные свойства операций сложения и умножения чисел.

- Число a **делит** число b, если существует $c \in Z$ такое, что $b = ac$, записывается $a \mid b$, где b – **делимое**, a – **делитель**, c – **полное частное** (инверсное отношение: $b \vdots a$ – число b **делится** на число a, или число b **кратно** a).

►$2 \mid 6$, так как $6 = 2 \cdot 3$. $4 \nmid 6$, так как для любого $c \in Z$ справедливо $4c \neq 6$.◄

Свойства делимости

Пусть a, b, c, λ – целые числа.

СВОЙСТВО 1.1. $1 \mid a$.

СВОЙСТВО 1.2. $a \mid 0$.

СВОЙСТВО 1.3. Если $a \mid b$ и $b \mid c$, то $a \mid c$.

СВОЙСТВО 1.4. Если $a \mid b$ и $a \mid c$, то $a \mid b \pm c$.

СВОЙСТВО 1.5. Если $a \mid b$, то $a \mid \lambda b$ для любого $\lambda \in Z$.

СВОЙСТВО 1.6. $\forall a, a_1, \dots, a_n, \lambda_1, \dots, \lambda_n \in Z((a \mid a_1 \wedge \dots \wedge a \mid a_n) \rightarrow a \mid \lambda_1 a_1 + \dots + \lambda_n a_n)$.

СВОЙСТВО 1.7. Если число a делит все слагаемые, кроме может быть одного из целочисленного равенства $\lambda_1 a_1 + \dots + \lambda_n a_n = \mu_1 b_1 + \cdots \mu_n b_n$, то a делит все слагаемые.

СВОЙСТВО 1.8. Если a и b натуральные числа и $a \mid b$, то $b \geq a$.

■ Докажем некоторые из них.

2. $a \mid 0$, так как $0 = a \cdot 0$, что требовалось доказать (далее – ч.т.д.).

3. Пусть $a \mid b$ и $b \mid c$. Тогда существуют числа b_1 и c_1 такие, что $b = ab_1$ и $c = bc_1$. Следовательно, $c = ab_1c_1$ и $a \mid c$, ч.т.д.

8. Так как $a \mid b$, то $b = ac$ для некоторого $c \in N$. В силу $c \geq 1$ следует $b = ac \geq a$, ч.т.д.

Остальные свойства непосредственно вытекают из определения делимости. ■

2. Деление с остатком. Число $b \neq 0$ *делит число* a *с остатком*, если существуют числа q, r такие, при которых

$$a = bq + r, \text{ причем } 0 \leq r < |b|. \qquad (1)$$

Следовательно, *разделить* число a на $b \neq 0$ с остатком *означает найти* целые числа q, r удовлетворяющие условию (1).

► Разделим с остатком 7 на 3; -7 на 3; 7 на -3:

$7 = 3 \cdot 2 + 1$, где $q = 2$, $r = 1$,

$-7 = 3 \cdot (-3) + 2$, где $q = -3$, $r = 2$,

$7 = (-3) \cdot (-2) + 1$, где $q = -2$, $r = 1$ ◄

Теорема о делении с остатком 1.1. Произвольное целое число можно разделить с остатком на целое число, отличное от нуля, причем единственным образом:

$$\forall a, b \in Z\ (b \neq 0 \rightarrow \exists!\, q, r \in Z(a = bq + r \wedge 0 \leq r < |b|)) \qquad (2)$$

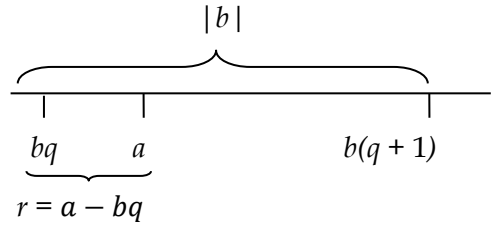
■ Докажем, что существует разложение (1).

Пусть $b > 0$. По свойству Архимеда последовательность

$$\ldots < -b < 0b < 1b < 2b < \cdots$$

строго и бесконечно возрастает. Возьмем наибольшее целое q такое, что

$$bq \le a \text{ и } a < b(q + 1):$$



Положим $r = a - bq$. Тогда из $a < bq + b$ следует $0 \le r < b$. Осталось заметить, что $a = bq + (a - bq) = bq + r$, где $0 \le r < b = |b|$.

Предположим теперь, что $b < 0$. Тогда $-b > 0$ и по доказанному выше, существуют числа q_1 ,r такие, при которых $a = (-b) \cdot q_1 + r$, причем $0 \le r < -b = |b|$. Отсюда $a = b \cdot (-q_1) + r$, где $0 \le r < |b|$, ч.т.д.

Теперь докажем единственность разложения. Пусть число a представимо в виде:

$$a = bq_1 + r_1, \qquad 0 \le r_1 < |b|;$$
$$a = bq_2 + r_2, \qquad 0 \le r_2 < |b|, r_2 \ge r_1.$$

Вычтем из первого равенства второе. Получим $0 = b(q_1 - q_2) + (r_1 - r_2)$, и $r_2 - r_1 = b(q_1 - q_2)$. Следовательно, $|r_1 - r_2| = |b| \cdot |q_1 - q_2|$.

Если $q_2 - q_1 \ne 0$, то получим $|r_2 - r_1| \ge |b|$, что невозможно. Следовательно, $q_2 - q_1 = 0$ и $q_2 = q_1$. Но тогда $r_1 = r_2$ и единственность разложения доказана. ■

§ 2. Наибольший общий делитель

1. Алгоритм Евклида. Общим делителем чисел $a_1, \ldots, a_n$ называется такое число d, которое делит каждое из этих чисел.

• **Наибольшим общим делителем** чисел $a_1, \ldots, a_n$, $n \geq 2$ называется наибольший (максимальный) делитель среди всех их общих делителей, обозначается $(a_1, \ldots, a_n)$, или $HOD\ (a_1, \ldots, a_n)$.

Предложение 2.1. Если $a = bq + r$, то $(a, b) = (b, r)$.

■ Обозначим через $D_{m,n}$ – множество общих делителей чисел m и n. Достаточно доказать равенство множеств общих делителей: $D_{a,b} = D_{b,r}$.

Пусть $d \in D_{a,b}$. Тогда, $d \mid a,b$ и по свойству 1.6, $d \mid a - bq = r$. Поэтому, $d \mid b$, r и $d \in D_{b,r}$, т.е. $D_{a,b} \subseteq D_{b,r}$. (1)

Пусть $d \in D_{b,r}$. Следовательно, $d \mid b$, r и по свойству 1.6, $d \mid bq + r = a$. Поэтому $d \mid a$, b и $d \in D_{a,b}$, т.е. $D_{b,r} \subseteq D_{a,b}$. (2)

Из (1) и (2) следует требуемое равенство и $НОД\ (a, b) = НОД\ (b, r)$. ■

Пусть a и b, не равные нулю, числа и пусть число b не делит a. Осуществим деление с остатком по следующей схеме (последовательно делим делитель на остаток, начиная с деления числа a на b):

$$\begin{cases} a = bq_1 + r_1, & 0 < r_1 < |b|, \\ b = r_1q_2 + r_2, & 0 < r_2 < r_1, \\ r_1 = r_2\,q_2 + r_3, & 0 < r_3 < r_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ r_{n-2} = r_{n-1}q_n + r_n, & 0 < r_n < r_{n-1}, \\ r_{n-1} = r_nq_{n+1} + 0. \end{cases} \qquad (3)$$

Заметим, что процесс последовательного деления (3) конечен, так как конечна убывающая последовательность остатков $r_1 > \ldots > r_n > 0$.

Теорема о НОД двух чисел 2.2. Пусть a и b – целые числа, не равные нулю, и пусть число b не делит a. Тогда *НОД (a, b)* равен последнему ненулевому остатку по алгоритму Евклида.

■ Для чисел a и b осуществим последовательное деление с остатком по алгоритму Евклида и получим (3). В силу предложения 2.1 и системы равенств (3) имеем $(a, b) = (b, r_1) = (r_1, r_2) = (r_2, r_3) = \ldots = (r_{n-1}, r_n) = r_n$, ч.т.д. ■

В качестве следствия получаем следующий критерий о б щ е г о д е л и т е л я двух чисел.

Предложение 2.3 (характеристическое свойство НОД). Общий положительный делитель двух чисел является наибольшим общим делителем тогда и только тогда, когда он делится на любой общий делитель этих чисел.

■ ($\Longrightarrow$)Пусть число c делит числа a и b Из свойств делимости в силу равенств (3) следует, что это число делит $r_1, r_2, \ldots, r_n$ (спуск вниз), т.е. $c \mid (a, b) = r_n$, ч.т.д.

($\Longleftarrow$) Если общий положительный делитель делится на любой их общий делитель, то он является в силу свойства 1.8 по определению наибольшим общим делителем. ■

• Числа a и b называются **взаимно простыми**, если $(a, b) = 1$.

Например, 0 и 1 являются взаимно простыми; 0 и 2 не являются взаимно простыми.

Свойства НОД

Пусть a и b – положительные целые числа.

СВОЙСТВО 2.1. Если $a|b$, то $(a, b) = a$.

СВОЙСТВО 2.2. $(ma, mb) = m\,(a, b)$, где $m \in N$.

СВОЙСТВО 2.3. Если $d \mid a, b$, то $(a, b) = (\frac{a}{d}, \frac{b}{d}) \cdot d$.

СВОЙСТВО 2.4. Если a и b – взаимно простые числа, то $(ac, b) = (c, b)$, где $c \in Z$.

СВОЙСТВО 2.5. Если число c – целое, $b \mid ac$ и $(a, b) = 1$, то $b \mid c$.

СВОЙСТВО 2.6. Если каждое из чисел $a_1 \ldots, a_n$ взаимно простое с каждым из чисел $b_1 \ldots b_m$, то $(a_1 \ldots a_n, b_1 \ldots b_m) = 1$.

■ 1. Пусть $d = (a, b)$. Так как $d \mid a$, то $d \leq a$. С другой стороны, $a|a, b$. Следовательно, $a \leq d$. Поэтому $d = a = (a, b)$, ч.т.д.

2. Осуществим деление числа a на число b с остатком по алгоритму Евклида и умножим полученные соотношения на m. Получим:

$$\begin{cases} am = bmq_1 + r_1m, 0 < r_1m < bm, \\ bm = r_1mq_2 + r_2m, 0 < r_2m < r_1m, \\ r_1m = r_2mq_2 + r_3m, 0 < r_3m < r_2m, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ r_{n-2}m = r_{n-1}mq_n + r_nm, 0 < r_nm < r_{n-1}m, \\ r_{n-1}m = r_nmq_{n+1} + 0. \end{cases}$$

По теореме о НОД следует, что $(ma, mb) = mr_n = m \cdot (a, b)$, ч.т.д.

3. Имеем $(a, b) = \left(\frac{a}{d} \cdot d, \frac{b}{d} \cdot d\right) = \left(\frac{a}{d}; \frac{b}{d}\right) \cdot d$, ч.т.д.

4. По определению НОД имеем $(ac, b) \mid ac, bc$, и по предложению 2.3 $(ac, b) \mid (ac, bc) = (a, c) \cdot b = c$, так как по условию $(a, b) = 1$. Следовательно, $(ac,b) \mid c,b$ и по предложению 2.3 $(ac, b) \mid (c, b)$.

С другой стороны, $(c, b) \mid ac, b$. Значит, $(c, b) \mid (ac, b)$. Следовательно $(ac, b) = (c, b)$, ч.т.д.

5. По свойству 2.1 и условию $b|ac$ имеем $b = (b, ac)$. По свойству 2.4 получаем $b = (b, ac) = (b, c)$. Следовательно, $b \mid c$, ч.т.д.

6. По свойству 2.4 имеем $(a_1 \cdot a_2 \ldots a_n, b_k) = (a_2 \ldots a_n, b_k) = \ldots = (a_n, b_k) = 1$, $k = 1, 2, \ldots, m$. Положим, $A = (a_1\, a_2 \ldots a_m)$. Аналогично получаем *(A, $b_1b_2\ldots b_m$) = (A, $b_2\ldots b_m$) = …* $= (A, b_m) = 1$, ч.т.д. ■

§3. Линейная форма НОД. Наименьшее общее кратное

1. Линейная форма НОД. Пусть d – наибольший общий делитель чисел α и b.

• Говорят, что d линейно выражается через α и b, если существуют числа u, v такие, при которых

$$d = a \cdot u + b \cdot v. \qquad (1)$$

Равенство (1) называется **линейной формой НОД** чисел a и b.

• **Линейно выразить** (представить) НОД (a, b) через a и b означает **найти** числа u, v, удовлетворяющие (1).

Критерий НОД 3.1. Общий делитель $d > 0$ чисел a и b является наибольшим общим делителем тогда и только тогда, когда он представим в виде целочисленной линейной комбинации этих чисел.

■ (=>) Пусть a и b – целые неотрицательные числа. Если a делит b, то $d = (a, b) = a = 1 \cdot a + 0 \cdot b$ и утверждение теоремы справедливо.

Предположим теперь, что $a < b$ и $a|b$. Найдем наибольший общий делитель $d = (a, b)$ с помощью алгоритма Евклида:

$$\begin{cases} a = b \cdot q_1 + r_1, & 0 < r_1 < b, \\ b = r_1 \cdot q_1 + r_2, & 0 < r_2 < r_1, \\ \dots & \dots \\ r_{n-3} = r_{n-2} \cdot q_{n-1} + r_{n-1}, & 0 < r_{n-1} < r_{n-2}, \\ r_{n-2} = r_{n-1} \cdot q_n + r_n, & 0 < r_n < r_{n-1}, \\ r_{n-1} = r_n \cdot q_{n+1}. \end{cases} \quad (2)$$

Здесь $d = (a, b) = r_n$.

Поднимаясь вверх по равенствам (2) и выражая остатки r_k через r_{k-1} и r_{k-2}, начиная с предпоследнего равенства $(k = n, n-1, \dots, 2, 1)$, получим выражение для r_n через a и b:

$$r_n = a \cdot u + b \cdot v, \text{ ч.т.д.}$$

($\Leftarrow$) Пусть натуральное число d является общим делителем чисел a, b и пусть $d = a \cdot u + b \cdot v$ для некоторых чисел u, v. Из свойств делимости следует, что каждый общий делитель чисел a и b делит число d. Следовательно, $d = (a, b)$, ч.т.д. ■

В качестве следствия получим следующий критерий.

Критерий взаимной простоты 3.2. Положительные числа a и b являются взаимно простыми тогда и только тогда, когда существуют числа u, v такие, что $a \cdot u + b \cdot v = 1$.

■ Здесь общий делитель $d = 1$ линейно выражается через числа a и b. ■

► Найти линейную форму НОД(115, 14).

Р е ш е н и е. Применим метод последовательного деления (алгоритм Евклида) для чисел 115 и 14:

$$\begin{array}{l} \begin{array}{r|l} 115 & 14 \\ \underline{112} & 8 \end{array} \\ \begin{array}{r|l} 14 & 3=r_1 \\ \underline{12} & 4 \end{array} \quad \Rightarrow \underline{115}=14\cdot 8+3 \\ \begin{array}{r|l} 3 & 2=r_2 \\ \underline{2} & 1 \end{array} \quad \Rightarrow \underline{14}=3\cdot 4+2 \\ \begin{array}{r|l} 2 & 1=r_3 \\ \underline{2} & 2 \end{array} \quad \Rightarrow 3=2\cdot 1+1 \\ 0=r_4 \quad \Rightarrow 2=2\cdot 1+0 \end{array}$$

Последний отличный от нуля остаток равен $r_3 = 1$. Следовательно, $(115,14) = 1$. Последовательно выразим r_3 через предыдущие остатки. Получим $1 = 3 - \underline{\underline{2}} \cdot 1 = \underline{\underline{3}} - \\ - \left(\underline{14} - \underline{\underline{3}} \cdot 4\right) = \left(\underline{115} - \underline{14} \cdot 8\right) - \left(\underline{14} - \left(\underline{115} - \underline{14} \cdot 8\right) \cdot 4\right) = 5 \cdot \\ \cdot \underline{115} - 41 \cdot \underline{14}$.

О т в е т. $1 = \underline{115} \cdot 5 + \underline{14} \cdot (-41)$. ◄

2. Наименьшее общее кратное (НОК). Рассматриваются неотрицательные целые числа.

1) Число a **кратно** b, если a делится на число b.

2) Число c называется **общим кратным** чисел $a_1, a_2, \dots, a_n$, если оно кратно каждому из этих чисел.

3) **Наименьшим общим кратным** (НОК) чисел $a_1, a_2, \dots, a_n$ называется число $m = [a_1, a_2, \dots, a_n]$, равное наименьшему из положительных общих кратных этих чисел.

► $[6,9] = 18$, $[14,21] = 42$. ◄

Теорема 3.3. Наименьшее общее кратное чисел a и b делит любое общее кратное этих чисел.

■ Пусть $m = [a, b]$ и пусть n – общее кратное чисел a и b. Разделим n на m с остатком: $n = m \cdot q + r, 0 \le r < m$. Так как $a, b \mid m, n$, то $a, b \mid n - m \cdot q = r$, Таким образом, r –

неотрицательное общее кратное чисел a и b. Из определения НОК теперь следует, что $r = 0$ ч.т.д. ■

Формула НОК 3.4. Наименьшее общее кратное натуральных чисел a и b равно $[a, b] = \frac{a \cdot b}{(a,b)}$. (3)

■ Пусть $d = (a, b)$ и пусть $a = a_1 d$, $b = b_1 d$. Из свойств НОД следует $(a_1, b_1) = 1$. Поэтому

$$\frac{a \cdot b}{(a,b)} = \frac{a_1 \cdot d \cdot b_1 \cdot d}{d} = a_1 \cdot d \cdot b_1 = \underline{a} \cdot b_1 = a_1 \cdot \underline{b.}$$

Следовательно, $\frac{a \cdot b}{(a,b)}$ является общим кратным чисел a и b. Поэтому по теореме 3.3 и определению НОК получим $[a, b] \leq \frac{a \cdot b}{(a,b)}$.

С другой стороны, если s – общее кратное чисел a и b, то $s = a \cdot n = a_1 \cdot d \cdot n$ для некоторого $n \in N$. Так как $b = b_1 \cdot d | s = a_1 \cdot d \cdot n$, то $b_1 | a_1 \cdot n$, Из условия $(a_1, b_1) = 1$ следует, что $b_1 | n$, т.е. $n = b_1 \cdot t$, где $t \in N$.

Таким образом, любое общее кратное представимо в виде $s = a \cdot b_1 \cdot t = \frac{a \cdot b}{(a,b)} \cdot t$, где $t \in N$. Наименьшее кратное получится при $t = 1$, ч.т.д. ■

Следствие 3.5. Если целое число $c > 0$, то $[ac, bc] = c[a, b]$.

■ По формуле НОК имеем $[ac, bc] = \frac{ac \cdot bc}{(ac,bc)} = \frac{ac \cdot bc}{c(a,b)} =$

$= c \cdot \frac{a \cdot b}{(a,b)} = c \cdot [a, b]$. ■

Теорема 3.6. Справедлива следующая формула НОК для n чисел:

$$[a_1, a_2, \dots, a_n] = [\big[[a_1, a_2], a_3\big], \dots, a_n], n \geq 3.$$

■ Доказательство проведем индукцией по n.

Б.И. Проверим справедливость формулы при $n = 3$. Пусть M – множество общих кратных чисел a_1, a_2, a_3, а T – множество общих кратных чисел $[a_1, a_2]$ и a_3. В силу теоремы 3.3 M=T. Следовательно, $[a_1,\ a_2,\ a_3] = [[a_1, a_2], a_3]$.

П.И. Пусть формула справедлива для m чисел, где $m < n$ и $n > 3$: $[a_1, a_2, \dots, a_m] = [[\dots [a_1, a_2], \dots, a_{m-1}], a_m]$.

Ш.И. Пусть M – множество общих кратных чисел $a_1, a_2, \dots, a_n$ и пусть T – множество положительных общих кратных чисел $[[a_1, a_2], \dots, a_{n-1}]$ и a_n.

В силу теоремы 3.3 имеем $M = T$, что доказывает справедливость формулы НОК. ■

§4. Простые числа

Простые числа. Будем рассматривать только неотрицательные целые числа. Произвольное натуральное число больше единицы всегда имеет два **тривиальных делителя**: единицу и само число. Некоторые натуральные числа не имеют других делителей, отличных от тривиальных.

• Число $p \neq 0, 1$ называется **простым числом**, если оно делится только на единицу и число p; в противоположном случае оно называется **составным числом**.

Таким образом:

• Натуральное число $p > 1$ является **простым числом**, если

$$\forall a, b \in N(p = a \cdot b \to a = 1 \vee b = 1); \qquad (1)$$

• Натуральное число $p > 1$ является **составным числом**, если

$$\exists a, b \in N(p = a \cdot b \wedge a \neq 1 \wedge b \neq 1). \quad (2)$$

Свойства

СВОЙСТВО 4.1 (характеристическое). Натуральное число отличное от единицы является простым числом тогда и только тогда, когда любое целое число либо взаимно просто с ним, либо делится на него.

■ (=>) Пусть p – простое число. Тогда p имеет среди натуральных чисел своими делителями только 1 и p. Следовательно, для любого натурального числа a наибольший общий делитель $(a, p) = 1$ или $(a, p) = p$, ч.т.д.

(<=) Пусть число $p > 1$ удовлетворяет условию: $\forall a \in N\big((a,p) = 1 \vee (a,p) = p\big)$. Предположим, что $p = a \cdot b$ для некоторых чисел a и b. Тогда наибольший общий делитель $(a,p) = a$. С другой стороны, по условию, $(a,p) = 1$ или $(a,p) = p$. Если $(a,p) = 1$, то $a = 1$ и $b = p$. Если $(a,p) = p$, то $a = p$ и $b = 1$. Следовательно, по определению (1), число p является простым числом. ■

СВОЙСТВО 4.2. Наименьший неединичный натуральный делитель числа является простым числом.

■ Пусть p – неединичный натуральный делитель числа $a > 1$. Если число $d > 1$ является делителем числа p, то в силу свойства транзитивности делимости следует $d|a$. Но так как p – наименьший неединичный положительный делитель числа a, то $d = p$. Следовательно, число p имеет только тривиальные делители, ч.т.д. ■

СВОЙСТВО 4.3. Пусть p – наименьший неединичный натуральный делитель составного положительного числа a. Тогда $p \leq \sqrt{a}$.

■ По свойству 4.2 число p – простое. Так как число a – составное, то $a = p \cdot b$ для некоторого числа b, причем $b > 1$ и $b|a$. Из условия следует, что $p \leq b$. Умножив обе части этого равенства на p получим $p^2 \leq b \cdot p = a$. Откуда вытекает $p \leq \sqrt{a}$. ■

По логическому закону контрапозиции получаем:

СВОЙСТВО 4.4. Положительное число $a > 1$, которое не делится на числа, больше 1 и не превосходящие $\sqrt{a}$, является простым.

СВОЙСТВО 4.5. Пусть p и q – простые числа. Если $p|q$, то $p = q$.

■ Утверждение следует из определения простого числа. ■

Критерий простого числа 4.1. Натуральное число, больше единицы, является простым числом тогда и только тогда, когда из делимости произведения нескольких чисел на это число следует, что некоторый сомножитель этого произведения делится на это число.

■ (=>) Пусть p – простое число. Индукцией по числу n сомножителей произведения чисел докажем справедливость следующего предиката:

$\forall n, a_1, a_2, \dots, a_n \in N\ (p|a_1 a_2 \dots a_n \rightarrow \exists k \in \{1, 2, \dots, n\}(p \mid a_k))$. (3)

Б.И. $n = 2$. Пусть $p \mid a_1 \cdot a_2$ для некоторых чисел a_1 и a_2. Предположим, что pa_1. По свойству 4.1 имеем $(a_1, p) = 1$. Из условия и свойства 2.4 для НОД следует, что $p = (p, a_1 a_2) =$ $= (p, a_2)$, т.е. $p|a_2$, ч.т.д.

П.И. Пусть утверждение (3) справедливо, когда число сомножителей меньше n, где $n > 2$.

Ш.И. Пусть число p делит произведение n чисел $(a_1 a_2 \dots a_{n-1}) \cdot a_n$. По Б.И. p делит или $a_1 a_2 \dots a_{n-1}$,

или a_n. Если p делит a_n, то утверждение справедливо. Пусть $p|a_1a_2 \dots a_{n-1}$. Тогда по П.И. найдется число a_i ($i \in \{1, 2, \dots, n-1\}$), которое делится на p. Таким образом один из множителей произведения $a_1a_2 \dots a_n$ делится на p. По принципу математической индукции предикат (3) истинен на *N*.

(<=) Пусть число $p > 1$ удовлетворяет условию (3). Предположим, что *p* является составным числом, т.е. существуют неединичные натуральные числа a_1 и a_2 такие, что $p = a_1 \cdot a_2$. По условию (3) *p* делит или a_1 или a_2. Если $p|a_1$, то $a_1 = p \cdot c$ для некоторого числа *c*. Но тогда $p = pca_2$, и $a_2 = 1$, что противоречит предположению. Следовательно, число *p* – простое. ■

Теорема Евклида 4.2. Множество положительных простых чисел бесконечно.

■ Предположим противное. Пусть $p_1, p_2, \dots p_n$– все положительные простые числа. Рассмотрим число $a = p_1p_2 \dots p_n + 1$. В силу предположения число *a* является составным. Пусть p – наименьший среди неединичных положительных делителей числа a. По свойству 4.2 число p – простое. Следовательно, по предположению $p = p_i$ для некоторого простого числа из списка $\{p_1, p_2, \dots, p_n\}$. Но тогда $p|p_1p_2 \dots p_n, a$. Из свойств делимости вытекает $p|a - p_1p_2 \dots p_n = 1$, что противоречиво. Полученное противоречие доказывает, что множество простых чисел является бесконечным. ■

Решето Эратосфена. Для нахождения всех простых чисел из промежутка от 2 до *n* используют метод, основанный на свойстве 4.4, называемый «решетом Эратосфена»:

Шаг 1. Выписывают подряд все числа от 2 до *n*.

Шаг 2. Обводят первое по порядку число списка кружком, которое еще не было обведено кружком. Потом вычеркивают все кратные этого числа из списка.

Шаг 3. Сравнивают квадрат последнего обведенного числа с числом n. Если квадрат числа строго меньше n, то возвращаются к шагу 2. Если квадрат числа не меньше n, то на этом процесс вычеркивания чисел из списка заканчивается.

Шаг 4. Обведенные и незачеркнутые числа из списка образуют множество всех простых чисел из промежутка $[2, n]$.

► Составить все положительные простые числа не превосходящие 50.

Р е ш е н и е. 1. Составим таблицу чисел от 2 до 50.

(2)	(3)	~~4~~	(5)	~~6~~	(7)	~~8~~	~~9~~	~~10~~	
(11)	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~

2. Применяя «решето Эратосфена», обведем кружком сначала число 2, потом 3, затем 5 и, наконец, число 7. На этом процесс вычеркивания заканчивается, т.к. квадраты последующих незачеркнутых чисел больше 50.

О т в е т. {2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47}.◄

Теорема 4.3 (разложение чисел на простые множители). Произвольное натуральное число $a > 1$ представимо в виде произведения простых чисел, причём единственным образом с точностью до порядка сомножителей.

■ Пусть a – целое число больше единицы. Докажем вначале существование разложения числа a на простые множители.

Пусть p_1 – наименьший положительный неединичный делитель числа a. Тогда по свойству 4.2 число p_1 – простое и $a = p_1 a_1$ для некоторого $a_1 \in N$. Если $a_1 = 1$, то $a = p_1$ – искомое разложение. Пусть $a_1 \neq 1$. Рассмотрим опять наименьший неединичный делитель p_2 числа a_1. Тогда $a_1 = p_2 a_2$ и $a = p_1 p_2 a_2$.

Если $a_2 = 1$, то $a = p_1 p_2$ – искомое разложение.

Продолжая этот процесс, мы либо на некотором шаге получим искомое разложение

$$a = p_1 p_2 \dots p_n, \qquad (1)$$

либо процесс будет бесконечен.

Однако второй случай невозможен, так как в этом случае при любом n имеем $a > p_1 p_2 \dots p_n \geq 2^n$, а 2^n неограниченно возрастает при $n = 1, 2, \dots$.

Единственность разложения докажем индукцией по числу *n* сомножителей в разложении (1).

Б.И. $n = 1$. Пусть $a = p_1$ – простое число. Единственность разложения следует из свойств простых чисел.

П.И. Пусть единственность разложения выполняется, если число сомножителей в разложении меньше n, где $n > 1$.

Ш.И. Пусть наряду с разложением (1) существует другое разложение

$$a = q_1 q_2 \cdots q_m, \quad \text{где } m \geq n. \qquad (2)$$

Следовательно,

$$a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m. \qquad (3)$$

Так как $p_1 | q_1 q_2 \cdots q_m$, то по критерию простого числа следует, что один из сомножителей $q_1, q_2, \dots, q_m$ делится на p_1. С точностью до нумерации будем считать $p_1 | q_1$. Но тогда $(p_1, q_1) = p_1$ и по определению простого числа следует $p_1 = q_1$. Сократив равенство (3) на p_1, получим

$$a_1 = p_2 \cdots p_n = q_2 \cdots q_m.$$

Так как число a_1 в своём разложении имеет меньше n простых сомножителей, то по индуктивному предположению $n = m$ и с точностью до нумерации, имеем $p_2 = q_2, \dots, p_n = q_n$.

Таким образом, число a единственным образом представимо в виде произведения простых чисел с точностью до порядка. ■

Каноническое разложение числа на простые множители позволяет найти его делители, сумму делителей и их число.

Теорема 4.4. Пусть $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ – каноническое разложение натурального числа n на простые множители. Тогда:

1) множество чисел вида

$$d = p_1^{\beta_1} \cdots p_k^{\beta_k}, \text{ где } 0 \le \beta_i \le \alpha_i,\ i = 1,2, \dots, k \qquad (1)$$

исчерпывает множество натуральных делителей числа n;

2) число натуральных делителей числа n равно

$$\tau(n) = (1 + \alpha_1) \cdots (1 + \alpha_k); \qquad (2)$$

3) сумма натуральных делителей числа n равна

$$\sigma(n) = \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}-1}{p_2-1} \cdots \frac{p_k^{\alpha_k+1}-1}{p_k-1}. \qquad (3)$$

■ 1. Если d – натуральный делитель числа n, то каждый простой делитель числа d является делителем n. Поэтому

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}, \text{ причём } 0 \le \alpha_i \le \beta_i,\ i = 1,2, \dots, k, \qquad (4)$$

так как из условия $p_i^{\beta_i} | n = p_1^{\alpha_1} \cdots p_i^{\alpha_i} \cdots p_k^{\alpha_k}$ следует $p_i^{\beta_i} | p_i^{\alpha_i}$.

Обратно, число d вида (4) делит n, так как $n = d \cdot (p_1^{\alpha_1-\beta_1} \cdots p_k^{\alpha_k-\beta_k})$.

2. По пункту 1 теоремы каждый натуральный делитель числа n однозначно определяется последовательностью чисел $(\beta_1, \beta_2, \dots \beta_k)$, где $0 \le \beta_i \le \alpha_i$, $i = 1, 2, \dots, k$. Число таких последовательностей равно $(1 + \alpha_1) \cdots (1 + \alpha_k)$, ч.т.д.

3. В силу пункта 1 сумма $\sigma(n)$ натуральных делителей числа n равна $\sum_{(\beta_1,\beta_2,\dots\beta_k)} p_1^{\beta_1} \cdots p_k^{\beta_k} = \left(1 + p_1 \cdots + p_1^{\beta_1} + \cdots + + p_1^{\alpha_1}\right) \cdots (1 + p_k + \cdots + p_k^{\beta_k} + \cdots + p_k^{\alpha_k})$, так как раскрыв скобки в правой части, получим каждое слагаемое из левой части. Осталось заметить, что $1 + p_i + \cdots + p_i^{\alpha_i} = \frac{p_i^{\alpha_i+1}-1}{p_i-1}$ как сумма геометрической прогрессии со знаменателем, равным p_i, $i = 1, 2, \dots, k$. ■

Каноническое разложение чисел на простые множители позволяет найти НОД и НОК чисел.

Теорема 4.5. Пусть $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ и $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m}$, где $\alpha_i \ge 0, \beta_i \ge 0$ $(i = 1, 2, \dots, k)$ – канонические разложения чисел a и b на простые множители. Тогда:

1) НОД $(a, b) = p_1^{\min\{\alpha_1,\beta_1\}} \cdots p_m^{\min\{\alpha_m,\beta_m\}}$;

2) НОК $[a, b] = p_1^{\max\{\alpha_1,\beta_1\}} \cdots p_m^{\max\{\alpha_m,\beta_m\}}$.

Здесь, возможно, число $p_i (i = 1, 2, \dots, m)$ входит только в одно из разложений.

Утверждение вытекает из представления делителей чисел a и b и свойств простых чисел. Доказательство провести самостоятельно.

► 1. Найти число делителей и сумму делителей числа $n = 10000$.

Р е ш е н и е. Имеем $10000 = 10^4 = 2^4 \cdot 5^4$. Следовательно, $\tau(10^4) = (1 + 4) \cdot (1 + 4)$, $\sigma(10^4) = \frac{2^5-1}{2-1} \cdot \frac{5^5-1}{5-1}$.

О т в е т. $\tau(10^4) = 25$, $\sigma(10^4) = 31 \cdot 781 = 24211$.

2. Найти натуральное число n , которое имеет ровно два простых делителя, сумма делителей числа равна 104, а число всех делителей равно 6.

Р е ш е н и е. По условию $n = p^\alpha q^\beta$, где p и q – различные простые числа, $\alpha \geq 1$, $\beta \geq 1$ и $\tau(n) = (1+\alpha)(1+\beta) = 6 = 2 \cdot 3$. Следовательно, без ограничения общности, $\alpha = 1, \beta = 2$ и $n = p \cdot q^2$. По формуле для суммы делителей имеем

$$\sigma(pq^2) = \frac{p^2-1}{p-1} \cdot \frac{q^3-1}{q-1} = (1+p)(q^2+q+1) = 104 = 13 \cdot 8.$$

Ясно, что $q < 11$. При q равном 2, или 5, или 7 число $q^2 + q + 1$ не делит 104. Пусть $q = 3$. Тогда $q^2 + q + 1 = 3^2 + +3 + 1 = 13$, следовательно, 1+$p$=8 и p=7.

О т в е т. $n = 7 \cdot 3^2 = 63$. ◄

§5. Распределение простых чисел

1. **Распределение простых чисел.** Из теоремы Евклида следует, что множество простых чисел бесконечно. С другой стороны, существуют числовые промежутки произвольной длины, которые не содержат простых чисел. Так для $n > 1$ последовательность $n! + 2$, $n! + 3$, …, $n! + n$ не содержит простых чисел, так как первое число делится на 2, второе – на 3 и т.д., последнее делится на n. Это показывает сложность закона распределения простых чисел.

Математики конца XVIII и начала XIX веков обратились к изучению таблиц простых чисел.

● Обозначим через $\pi(x)$ число простых чисел на промежутке $[2, x]$.

● Говорят, что функции $f(x)$ и $g(x)$ **асимптотически равны**, если они бесконечно велики и $\lim_{x\to\infty}\frac{f(x)}{g(x)} = 1$, записывают $f(x)\sim g(x)$.

В 1808 году Лежандр опубликовал гипотезу: $\pi(x)\sim\frac{x}{\ln x - 1{,}08356\ldots}$.

Ещё ранее великий немецкий математик Карл Гаусс (1777–1858) предположил, что $\pi(x)\sim\int_2^x\frac{dt}{\ln t}$ (интегральный логарифм), но не опубликовал.

В 1849 году выдающийся русский математик Пафнутий Львович Чебышев показал, что гипотеза Лежандра ложна, а через год доказал следующие неравенства:

$0{,}92129 < \frac{\pi(x)}{x/\ln x} < 1{,}10555.$

Используя идеи немецкого математика Римана для функций комплексного переменного, одновременно французский математик Адамар и бельгийский математик Валле-Пуссен доказали *асимптотический закон распределения простых чисел:* $\pi(x)\sim\frac{x}{\ln x}\sim\int_2^x\frac{dt}{\ln t}$, который является центральным результатом в теории чисел.

Так как натуральный ряд является частным случаем арифметической прогрессии, то естественно возникал вопрос о распределении простых чисел в арифметических прогрессиях вида $an + b$, $n = 0, 1, 2, \ldots$.

Заметим, если $d = (a, b) > 1$, то каждый член прогрессии делится на d и в ней не будет простых чисел.

В 1837 году немецкий математик Дирихле доказал следующее обобщение теоремы Евклида.

Теорема Дирихле 5.1. Если $(a, b) = 1$, то прогрессия $an + b$, $n = 0, 1, 2, \ldots$, содержит бесконечно много простых чисел.

Рассмотрим некоторые частные случаи этой теоремы.

Теорема 5.2. Арифметическая последовательность $4n + 3$ $(n = 0, 1, 2, \ldots)$ содержит бесконечно много простых чисел.

■ Достаточно показать, что для любого натурального n существует простое число $p > n$ такое, что $p = 4k + 3$ для некоторого $k \in N$.

Пусть $n \in N$ и $M = 4n! - 1$. Заметим, что каждое простое число, которое делит M, будет больше n, так как в противном случае оно делит $M - 4n! = 1$, что невозможно.

Пусть простое число $p \mid M$. Тогда $p = 4k + 3$ или $p = 4s + 1$ для некоторых $k, s \in N$. Если $p = 4k + 3$, то теорема справедлива. Предположим, что все простые делители числа M имеют вид $4k + 1$. Учитывая, что $(4k + 1)(4s + 1) = 4(4ks + k + s) + 1$ для любых $k, s \in N$, получим, что $M = 4m + 1$ для некоторого $m \in N$, что невозможно, так как $M = 4n! - 1$ при делении на 4 даёт в остатке 3. Следовательно, имеется простой делитель числа M, который имеет вид $4k + 3$ ■

Аналогично доказывается и следующая теорема.

Теорема 5.3. Арифметическая последовательность $6n + 5 (n = 0, 1, 2, \ldots)$ содержит бесконечно много простых чисел.

■ Рассмотрим число $M = 6n! - 1$, где $n \in N$, которое представимо в виде $M = 6m + 5$ для некоторого $m \in N$. Любой простой делитель p числа M будет больше n и $p = 6k + 5$

или $p = 6s + 1$ для некоторых $k, s \in N$. Если все простые делители числа M имели бы вид $6s + 1$, то из равенства

$$(6s + 1)(6k + 1) = 6(6ks + k + s) + 1$$

следовало бы, что $M = 6t + 1$ для некоторого $t \in N$, что невозможно. Следовательно, существует простой делитель числа M вида $4k + 5$, который больше n. ■

Теорема 5.4. Арифметическая последовательность $4n + 1 (n = 0, 1, 2, ...)$ содержит бесконечно много простых чисел.

■ Достаточно показать, что для любого $n \in N$ существует простое число $p > n$ такое, что $p = 4k + 1$ для некоторого $k \in N$.

Пусть $n \in N$ и $n > 1$. Рассмотрим число $M = (n!)^2 + 1$. Так как M – нечетное число, то оно разлагается в произведение нечетных простых чисел: $M = q_1 q_2 \dots q_t$.

Заметим, что $q_i > n$, $i = 1, 2, \dots, t$, так как в противном случае $q_i | n!$ и $q_i | M - n! = 1$, что невозможно.

Пусть p – простой делитель M. Так как p – нечетное число, то $p = 4s + 1$ или $p = 4k + 3$. Если $p = 4s + 1$, то утверждение доказано.

Предположим, что $p = 4k + 3$. Тогда
$p - 1 = 4k + 2 = 2(2k + 1) = 2m$, где m – нечетное число.

Для нечетного m и натурального числа a справедливо тождество $a^m + 1 = (a + 1)(a^{m-1} + a^{m-2} + \dots + a + 1)$, то есть $a + 1 | a^m + 1$. Полагая $a = (n!)^2$ и $m = 2k + 1$, получаем $M = (n!)^2 + 1 | (n!)^{2(2k+1)} + 1$. Откуда следует, что $M | (n!)^{2(2k+1)} \cdot n! + n! = (n!)^p + n!$.

Так как $p | M$, то $p | (n!)^p + n!$. (1)

С другой стороны, по теореме Ферма (если $(a, p) = 1$, где p – простое число, то $p | a^p - a$) получаем $p | (n!)^p - n!$. (2)

Из (1) и (2) следует, что $p \mid 2(n!)^p$, что невозможно, ибо $p > n$. Таким образом, все простые делители $(n!)^2 + 1$ имеют вид $4k + 1$ и утверждение доказано. ■

2. Простые числа Ферма и Мерсена. Простое число a называется **числом Ферма**, если оно представимо в виде $2^m + 1$ для некоторого натурального числа m.

Предложение 5.5. Если число $2^m + 1$ является простым, то необходимо, чтобы $m = 2^n$ для некоторого $n \in N$.

■ Пусть m имеет нечётный делитель $k > 1$, то есть $m = k \cdot l$ для некоторого $l \geq 1$. Обозначим через $q = 2^l$. Тогда число $2^m + 1 = 2^{k \cdot l} + 1 == q^k + 1 = (q + 1)(q^{k-1} + q^{k-2} + + \cdots + 1)$ не является простым. ■

Следствие 5.6. Простое число Ферма представимо в виде $F_n = 2^{2^n} + 1$ для некоторого целого $n \geq 0$.

При $n = 0, 1, 2, 3, 4$ получаем простые числа Ферма: $F_0 = 3$; $F_1 = 5$; $F_2 = 17$; $F_3 = 257$; $F_4 = 65537$.

В 1650 году французский математик П. Ферма предположил, что числа F_n – простые для любого натурального n. Однако Л. Эйлер в 1832 году показал, что число $F_5 = = 2^{2^5} + 1 = 641 \cdot 6700417$ не является простым. В настоящее время не известны простые числа Ферма при $n \geq 5$.

● Простое число a называется **числом Мерсена,** если оно представимо в виде $2^m - 1$, где $m \in N$.

Названия чисел даны в честь французского монаха XVII века М. Мерсена, который изучал простые числа.

Предложение 5.7. Если $2^m - 1$ является простым числом, то необходимо, чтобы m было простым числом.

■ Пусть $a = 2^m - 1$ – простое число Мерсена. Предположим, что $m = k \cdot l$, где $k > 1$ и $l > 1$. Обозначим через

$q = 2^l$. Тогда число $2^m - 1 = 2^{k \cdot l} — 1 = q^k - 1 = (q - -1)\left(q^{k-1} + q^{k-2} + \cdots + 1\right)$ не является простым. ■

Таким образом, простые числа Мерсена имеют вид $M_p = 2^p - 1$, где p – некоторое простое число.

Числа $M_2 = 3,\ M_3 = 7,\ M_5 = 31,\ M_7 = 127$ – простые. В 1883 году русский священник-математик И.М. Первушин доказал, что число M_{31} является простым. К настоящему времени найдено 39 простых чисел Мерсена, самое большое из которых имеет вид $M_{13.466.917} = 2^{13.466.917} - 1$.

§ 6. Непрерывные дроби

1. **Цепные дроби.** Пусть α – действительное число, $\alpha > 0$. Тогда $\alpha = [\alpha] + \{\alpha\}$, где $[\alpha] = q_0$– целая часть, $\{\alpha\} = r_1$ – дробная часть числа α. Последовательно выделяя целую и дробную часть из обратных для дробной части, получим следующие равенства:

$$\alpha = \alpha_0 = q_0 + r_1 = q_0 + \frac{1}{\alpha_1}\ , \alpha_1 > 1,$$

$$\alpha_1 = \frac{1}{r_1} = q_1 + r_2 = q_1 + \frac{1}{\alpha_2},\ \alpha_2 > 1, \qquad \alpha = q_0 + \frac{1}{q_1 + \frac{1}{\alpha_2}},$$

$$\alpha_2 = q_2 + \frac{1}{\alpha_3}, \alpha_3 > 1, \qquad \alpha = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\alpha_3}}}, \qquad (1)$$

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

$$\alpha_{n-1} = q_{n-1} + \frac{1}{\alpha_n}, \alpha_n > 1, \qquad \alpha = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \cdots + \frac{1}{q_{n-1} + \frac{1}{\alpha_n}}}}.$$

Здесь $\alpha_k = \frac{1}{r_k}$, где r_k и q_k– дробная и целая части числа α_{k-1} и α_k, k=$\overline{1, n}$.

Выражение (1) записывается сокращенно $\alpha = [q_0;\ q_1, \dots, q_n, \alpha_n]$ и называется **непрерывной (цепной) дробью** числа *a*. Возможны два случая.

Существует натуральное *n* такое, что α_n – целое число.

Следовательно, $r_{n+1} = 0$ и $\alpha = [q_0; q_1, \dots, q_n]$. Эта запись называется **конечной непрерывной дробью**.

Во втором случае, для любого натурального *n* число α_n не является целым, и последовательность (1) бесконечна. При этом число α записывается в виде $\alpha = [q_0;\ q_1, q_2, \dots]$ и называется **бесконечной непрерывной дробью.**

Теорема 6.1. Действительное число является рациональным числом тогда и только тогда, когда оно представимо в виде конечной непрерывной дроби.

■ ($\Leftarrow$) Пусть число $\alpha = [q_0;\ q_1, \dots, q_n]$представимо в виде конечной непрерывной дроби. Сворачивая выражение (1) получим рациональное число.

($\Rightarrow$) Пусть $\alpha = \frac{a}{b}$ – рациональное число, где, $a, b \in N$. Применим последовательное деление по алгоритму Евклида:

$$a = bq_0 + r_1\ , 0\ < r_1 < b\ \Rightarrow \frac{a}{b} = q_0 + \frac{1}{\frac{b}{r_1}},$$

$$b = r_1q_1 + r_2\ , 0 < r_2 < r_1\ \Rightarrow \frac{a}{b} = q_0 + \frac{1}{q_1 + \frac{1}{\frac{r_1}{r_2}}},$$

$$r_1 = r_2q_2 + r_3, 0 < r_3 < r_2\ \Rightarrow\ \frac{a}{b} = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\frac{r_2}{r_3}}}},$$

… … … … … … … … … … … …

$$r_{n-2} = r_{n-1}q_{n-1} + r_n\ , 0 < r_n < r_{n-1},$$

$$r_{n-1} = r_n q_n + 0 \;\Rightarrow \frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}.$$

Следовательно, число $\alpha = \frac{a}{b} = [q_0; q_1, \dots, q_n]$ представимо в виде конечной непрерывной дроби, ч.т.д. ■

Пусть вещественное число α представимо в виде непрерывной дроби $\alpha = [q_0; q_1, \dots, q_n, \alpha_{n+1}]$.

• Число $A_k = [q_0; q_1, \dots, q_k]$, $0 \le k \le n$, называется **k-й подходящей дробью числа α.**

Предложение 6.2. Подходящая дробь A_k получается из A_{k-1} формальной заменой q_{k-1} на $q_{k-1} + \frac{1}{q_k}$.

■ Имеем $A_{k-1} = q_0 + \cfrac{1}{q_1 + \ddots + \cfrac{1}{q_{k-1}}}$. Заменим в этой записи q_{k-1} на $q_{k-1} + \frac{1}{q_k}$. Получим, $q_0 + \cfrac{1}{q_1 + \cdots + \cfrac{1}{q_{k-1} + \cfrac{1}{q_k}}} = A_k$. ■

Найдем формулу для вычисления подходящих дробей. Пусть $\alpha = [q_0; q_1, \dots, q_n]$. Определим индуктивно следующие числа:

$P_{-2} = 0; P_{-1} = 1; Q_{-2} = 1; Q_{-1} = 0.$

$$k = \overline{0,n}: \begin{cases} P_k = q_k P_{k-1} + P_{k-2}; \\ Q_k = q_k Q_{k-1} + Q_{k-2}. \end{cases} \qquad (2)$$

Величины P_k, Q_k удобно вычислять по следующей схеме:

k	–2	–1		0	1	…	k-2	k-1	k	…
q_k	—	—		q_0	q_1	…	q_{k-2}	q_{k-1}	q_k	…
P_k	0	1		$q_0 = P_0$	P_1	…	P_{k-2}	P_{k-1}	P_k	…
Q_k	1	0		$1 = Q_0$	Q_1	…	Q_{k-2}	Q_{k-1}	Q_k	…

Теорема о подходящих дробях 6.3. Если число a представимо в виде $\alpha = [q_0; q_1, \dots, q_n]$, то подходящая дробь

$$A_k = [q_0; q_1, \dots, q_k] = \frac{P_k}{Q_k}, k = 0,1, \dots, n.$$

(Таким образом, P_k – числитель, Q_k – знаменатель k-й подходящей дроби.)

■ Доказательство проведём индукцией по $k \in N \cup \{0\}$.

Б.И. k=0 , $A_0 = [q_0] = q_0 = \frac{q_0}{1} \overset{(2)}{=} \frac{P_0}{Q_0}$, ч.т.д.

П.И. Утверждение справедливо для подходящих дробей A_m, где $m < k$, когда $k \geq 1$.

Ш.И. Найдем A_kв силу предложения из представления A_{k-1} с помощью замены q_{k-1} на $q_{k-1} + \frac{1}{q_k}$. Имеем

$A_{k-1} \overset{П.И.}{=} \frac{P_{k-1}}{Q_{k-1}} \overset{(2)}{=} \frac{q_{k-1}P_{k-2} + P_{k-3}}{q_{k-1}Q_{k-2} + Q_{k-3}}$. Следовательно,

$$A_k = \frac{\left(q_{k-1} + \frac{1}{q_k}\right)P_{k-2} + P_{k-3}}{\left(q_{k-1} + \frac{1}{q_k}\right)Q_{k-2} + Q_{k-3}} \overset{умн. \text{ на } q_k}{=} \frac{q_k\left(q_{k-1}P_{k-2} + P_{k-3}\right) + P_{k-2}}{q_k\left(q_{k-1}Q_{k-2} + Q_{k-3}\right) + Q_{k-2}} \overset{(2)}{=} \frac{q_kP_{k-1} + P_{k-2}}{q_kQ_{k-1} + Q_{k-2}} \overset{(2)}{=} \frac{P_k}{Q_k},$$

ч.т.д. ■

► Представим в виде непрерывной дроби число $\frac{11}{4}$.

$$
\begin{array}{r|l}
11 & 4 \\
\cline{2-2}
8 & 2=q_0 \\
\cline{1-1}
4 & 3 \\
\cline{2-2}
3 & 1=q_1 \\
\cline{1-1}
3 & 1 \\
\cline{2-2}
3 & 3=q_2 \\
\cline{1-1}
0 &
\end{array}
$$

Проверим: $2+\frac{1}{1+\frac{1}{3}}=2+\frac{1}{\frac{4}{3}}=2+\frac{3}{4}=\frac{11}{4}$.

О т в е т. $\frac{11}{4}=[2;1,3]$. ◄

2. Свойства подходящих дробей.

СВОЙСТВО 6.1.

$$\begin{vmatrix} P_{k-1} & P_k \\ Q_{k-1} & Q_k \end{vmatrix} = P_{k-1}Q_k - P_kQ_{k-1} = (-1)^k, k = 0, 1, \dots, n \quad (3)$$

■ Доказательство свойства 6.1 проведем индукцией по $k \in N \cup \{0\}$.

Б.И. Пусть $k=0$. Тогда $P_{-1}Q_0 - P_0Q_{-1} = 1\cdot 1 - q_0\cdot 0 = 1 = 1^0$ ч.т.д.

П.И. Формула (3) справедлива для $m < k$, где $k \geq 1$.

Ш.И. Имеем $P_{k-1}Q_k - P_kQ_{k-1} \underset{=}{^{(2)}} P_{k-1}(q_kQ_{k-1}+Q_{k-2}) - (q_kP_{k-1} + P_{k-2})Q_{k-1} = P_{k-1}Q_{k-2} - P_{k-2}Q_{k-1} = -[P_{k-2}Q_{k-1} - P_{k-1}Q_{k-2}] \underset{=}{^{\text{П.И.}}} (-1)\cdot (-1)^{k-1} = (-1)^k$, ч.т.д. ■

Следствие 6.4. $A_{k-1} - A_k = \dfrac{P_{k-1}}{Q_{k-1}} - \dfrac{P_k}{Q_k} = \dfrac{(-1)^k}{Q_{k-1}Q_k}$.

СВОЙСТВО 6.2. Подходящие дроби несократимы.

■ По свойству 6.1 имеем $P_{k-1}Q_k - P_kQ_{k-1} = (-1)^k$. Отсюда $Q_k[(-1)^kP_{k-1}] + P_k[(-1)^{k+1}Q_{k-1}] = (-1)^{2k} = 1$.

По критерию НОД получаем, что P_k и Q_k – взаимно простые. ■

СВОЙСТВО 6.3. а) Подходящие дроби с четными номерами образуют возрастающую последовательность;

б) подходящие дроби с нечетными номерами образуют убывающую последовательность:

$$\frac{P_0}{Q_0} < \frac{P_2}{Q_2} < \ldots < \frac{P_{2k}}{Q_{2k}}; \frac{P_1}{Q_1} > \frac{P_3}{Q_3} > \ldots > \frac{P_{2k+1}}{Q_{2k+1}}.$$

■ *И*меем $A_{2k+2} - A_{2k} = \frac{P_{2k+2}}{Q_{2k+2}} - \frac{P_{2k}}{Q_{2k}} = \frac{P_{2k+2}Q_{2k} - P_{2k}Q_{2k+2}}{Q_{2k}Q_{2k+2}} \overset{(2)}{=}$

$$\overset{(2)}{=} \frac{(q_{2k+2}P_{2k+1} + P_{2k})Q_{2k} - P_{2k}(q_{2k+2}Q_{2k+1} + Q_{2k})}{Q_{2k}Q_{2k+2}} =$$

$$= \frac{q_{2k+2}(P_{2k+1}Q_{2k} - P_{2k}Q_{2k+1})}{Q_{2k}Q_{2k+2}} = \frac{q_{2k+2}(-1)\cdot(-1)^{2k+1}}{Q_{2k}Q_{2k+2}} > 0.$$

Следовательно, $A_{2k+2} > A_{2k}$, ч.т.д.

Аналогично доказывается, что подходящие дроби с нечетными номерами образуют убывающую последовательность.■

СВОЙСТВО 6.4. $A_{2k} < A_{2k-1}, A_{2k+1}$.

■ *И*меем

$$A_{2k} - A_{2k-1} = \frac{P_{2k}}{Q_{2k}} - \frac{P_{2k-1}}{Q_{2k-1}} = \frac{P_{2k}Q_{2k-1} - P_{2k-1}Q_{2k}}{Q_{2k}Q_{2k-1}} = \frac{(-1)\cdot(-1)^{2k}}{Q_{2k}Q_{2k-1}} < 0.$$

Следовательно, $A_{2k} < A_{2k-1}$. Аналогично доказывается $A_{2k} < A_{2k+1}$. ■

СВОЙСТВО 6.5. Каждая подходящая дробь с четным номером меньше любой подходящей дроби с нечетным номером.

■ Пусть $\frac{P_{2l}}{Q_{2l}}$ и $\frac{P_{2k+1}}{Q_{2k+1}}$ – произвольные подходящие дроби. Если $l \le k$, то по свойству 6.3 (а) $\frac{P_{2l}}{Q_{2l}} \le \frac{P_{2k}}{Q_{2k}}$ и по свойству 6.4 $\frac{P_{2k}}{Q_{2k}} < \frac{P_{2k+1}}{Q_{2k+1}}$. Следовательно, $\frac{P_{2l}}{Q_{2l}} < \frac{P_{2k+1}}{Q_{2k+1}}$.

Рассмотрим теперь случай $l > k$. Имеем $\frac{P_{2l}}{Q_{2l}} < \frac{P_{2l+1}}{Q_{2l+1}}$ в силу свойства 6.4 и $\frac{P_{2l+1}}{Q_{2l+1}} < \frac{P_{2k+1}}{Q_{2k+1}}$ в силу свойства 6.3 (б).

Поэтому $\frac{P_{2l}}{Q_{2l}} < \frac{P_{2k+1}}{Q_{2k+1}}$, ч.т.д. ■

СВОЙСТВО 6.6. Положительное действительное число при его разложении в цепную дробь находится между подходящими дробями с четными и нечетными номерами.

■ Пусть $\alpha = [q_0; q_1 ... q_n, \alpha_{n+1}]$, $n > 1$. Заметим, что $q_0 = \frac{P_0}{Q_0} = A_0 < \alpha$, так как $\alpha = q_0 + \frac{1}{q_1 + ...}$, где $\frac{1}{q_1 + ...} > 0$.

Следующая подходящая дробь

$A_1 = q_0 + \frac{1}{q_1} > \alpha = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + ...}}$, так как $q_1 < q_1 + \frac{1}{q_2 + ...}$ и

$\frac{1}{q_1} > \frac{1}{q_1 + \frac{1}{q_2 + ...}}$.

Далее подходящая дробь

$A_2 = q_0 + \dfrac{1}{q_1 + \dfrac{1}{q_2}} < \alpha = q_0 + \dfrac{1}{q_1 + \dfrac{1}{q_2 + \dfrac{1}{q_3 + \ldots}}}$, так как

$q_1 + \dfrac{1}{q_2} > q_1 + \dfrac{1}{q_2 + \dfrac{1}{q_3 + \ldots}}$, и, следовательно, дробь

$\dfrac{1}{q_1 + \dfrac{1}{q_2}} < \dfrac{1}{q_1 + \dfrac{1}{q_2 + \ldots}}$.

Продолжая находить последовательно подходящие дроби, убеждаемся, что подходящие дроби с четными номерами не превосходят число α, а подходящие дроби с нечетными номерами не меньше его. ■

Следствие 6.5. $\left|\alpha - \dfrac{P_k}{Q_k}\right| < \dfrac{1}{Q_k Q_{k+1}}$.

■ В силу свойства 6.6 число α находится между подходящими дробями $\dfrac{P_k}{Q_k}$ и $\dfrac{P_{k+1}}{Q_{k+1}}$. Следовательно,

$$\left|\alpha - \frac{P_k}{Q_k}\right| \le \left|\frac{P_k}{Q_k} - \frac{P_{k+1}}{Q_{k+1}}\right| = \frac{\left|P_k Q_{k+1} - P_{k+1} Q_k\right|}{Q_k Q_{k+1}} \overset{св.1}{=} \frac{1}{Q_k Q_{k+1}}. \blacksquare$$

► Требуется найти рациональное приближение действительного числа $\sqrt{2}$ с точностью до ε =0, 001.

Р е ш е н и е. а) Представим $\sqrt{2}$ в виде непрерывной дроби:

$\alpha_0 = \sqrt{2} = \left[\sqrt{2}\right] + \left\{\sqrt{2}\right\} = 1 + \left(\sqrt{2} - 1\right)$, где $r_1 = \sqrt{2} - 1$.

$\alpha_1 = \frac{1}{r_1} = \frac{1}{\sqrt{2}-1} = \frac{\sqrt{2}+1}{(\sqrt{2}-1)\cdot(\sqrt{2}+1)} = \sqrt{2}+1 = 2+(\sqrt{2}-1)$,

где $r_2 = \sqrt{2}-1$.

Так как $r_2 = r_1$, то получаем бесконечную периодическую непрерывную дробь: $\sqrt{2} = [1;2,2,,\ldots] = [1;(2)]$.

б) Найдем подходящую дробь $\frac{P_k}{Q_k}$ из условия $Q_k Q_{k+1} > \frac{1}{\varepsilon} = 1000$.

q_k	–	–	1	2	2	2	2	2
P_k	0	1	1	3	7	17	41	99
Q_k	1	0	1	2	5	12	29	70

Так как $29 \cdot 70 > 1000$, то $\frac{41}{29}$ – искомое рациональное приближение. Действительно, $\sqrt{2} = 1{,}41421\ldots$, $\frac{41}{29} = 1{,}41379\ldots$ и $\left|\sqrt{2} - \frac{41}{29}\right| < 0{,}001$. ◄

3. Неопределённые уравнения первой степени с двумя неизвестными.

Рассматриваются уравнения вида $ax + by = c$ (1) с неизвестными x, y и целыми коэффициентами a, b, c.

Требуется найти целочисленные решения этого уравнения.

Заметим, если число $d = (a, b)$ не делит c, то уравнение неразрешимо.

Действительно, в этом случае при любых целых x, y левая часть $ax + by$ уравнения делится на d, а правая часть, равная c, не делится на d, т.е. не будет выполняться равенство.

Пусть число $d = (a, b)$ делит c.

Тогда $a = a_1 d, b = b_1 d, c = c_1 d$ и $(a_1, b_1) = 1$.

Разделив на d уравнение (1) получим равносильное уравнение $a_1 x + b_1 x = c_1$, где $(a_1, b_1) = 1$. Поэтому в дальнейшем можно считать, что $(a, b) = 1$.

Теорема 6.6. Пусть дано уравнение $ax + by = c$, (2)

где a, b, c – целые числа и $(a, b) = 1$. Тогда:

1) уравнение разрешимо в целых числах;

2) если (x_0, y_0) – частное решение, то общее решение уравнения имеет вид:

$$\begin{cases} x = x_0 + bt, \\ y = y_0 - at, t \in Z. \end{cases} \quad (3)$$

■ 1. Разложим дробь $\frac{a}{b}$ в цепную дробь $[q_0;\ q_1,\ q_2, \dots,\ q_n]$ и найдем подходящие дроби $A_k = \frac{P_k}{Q_k} (k = 0, 1, 2, \dots, n)$ по схеме:

q_k	–	–	q_0	q_1	$\cdots$	q_{n-1}	q_n
P_k	$P_{-2} = 0$	$P_{-1} = 1$	$P_0 = q_0$	P_1	$\cdots$	P_{n-1}	a
Q_k	$Q_{-2} = 1$	$Q_{-1} = 0$	$Q_0 = 1$	Q_1	$\cdots$	Q_{n-1}	b

Здесь $P_k = q_k P_{k-1} + P_{k-2}$, $Q_k = q_k Q_{k-1} + Q_{k-2}$, $b = \overline{1, n}$ и $P_n = a$, $Q_n = b$, так как $(a, b) = 1$.

По свойству подходящих дробей определитель $\begin{vmatrix} P_{n-1} & a \\ Q_{n-1} & b \end{vmatrix} = P_{n-1} b - -aQ_{n-1} = (-1)^n$.

Умножив это равенство на $(-1)^n \cdot c$, получим

$$\underbrace{a[(-1)^{n+1} \cdot Q_{n-1}}_{x_0} \cdot c] + b[\underbrace{(-1)^n \cdot P_{n-1}}_{y_0} \cdot c] = c.$$

Здесь (x_0, y_0) – частное решение уравнения.

2. Пусть (x, y) – произвольное решение уравнения $ax + by = c$. Вычтем из $ax + by = c$ равенство $ax_0 + by_0 = c$. Получим $a(x - x_0) + +b(y - y_0) = 0$. Отсюда $a(x - x_0) = b(y_0 - y)$. (4)

Так как по условию $(a, b) = 1$, то число a делит $y_0 - y$. Поэтому существует $t \in Z$ такое , что $at = y_0 - y$ и $y = y_0 - at$.

Подставив $y_0 - y = at$ в (4) , получим $a(x - x_0) = abt$ и $x = x_0 + bt$.

Таким образом, $\begin{cases} x = x_0 + bt, \\ y = y_0 - at, t \in Z \end{cases}$.

Обратно, пусть $t \in Z$ и (x_0, y_0) – решение уравнения (1). Подставим значения $x = x_0 + bt$, и $y = y_0 - at$ в это уравнение. Получим $a(x_0 + bt) + b(y_0 - at) = ax_0 + by_0 = c$. Следовательно, (x, y) является решением уравнения. Теорема доказана. ■

► Решим уравнение $64x + 25y = 2$.

Р е ш е н и е. Так как $(64,25) = 1$, то уравнение разрешимо.

Разложим дробь $\frac{64}{25}$ в непрерывную дробь: $\frac{64}{25} =$ $= [2; 1, 1, 3, 1, 2]$.

64	25	
50	2	$= q_0$
25	14	
14	1	$= q_1$
14	11	
11	1	$= q_2$
3		

11	3	
9	3	$= q_3$
3	2	
2	1	$= q_4$
2	1	
2	2	$= q_5$
0		

Составим подходящие дроби по схеме:

q_k	–	–	2	1	1	3	1	2
P_k	0	1	2	3	5	16	23	64
Q_k	1	0	1	1	2	7	9	25

$$\begin{vmatrix} 23 & 64 \\ 9 & 25 \end{vmatrix} = 23 \cdot \underline{25} - 9 \cdot \underline{64} = -1 | \cdot (-c) = -2 \Longrightarrow$$

$$\Rightarrow \underline{25} \cdot (-46) + \underline{64} \cdot 18 = 2$$

Частное решение $(x_0 = 18, y_0 = -46)$.

О т в е т. $\begin{cases} x = 18 - 64t \\ y = -46 + 25t, \quad t \in Z. \end{cases}$ ◄

§7. Целые систематические числа

1. Системы счисления. В десятичной системе счисления для записи натурального числа используются десять цифр: 0, 1, 2, …, 9. Каждая цифра в зависимости от места в записи числа указывает число единиц, десятков, сотен, тысяч и т.д. Например, запись числа $a = 3879$ означает $a = 3 \cdot 10^3 + 8 \cdot 10^2 + 7 \cdot 10 + 9$, т. е. число a есть сумма девяти единиц, семи десятков, восьми сотен и трех тысяч. Таким образом, натуральное число, записанное в десятичной системе счисления в виде $Q = a_n\, a_{n-1} \ldots a_1\, a_0$, где $a_n \neq 0$ и $0 \leq a_i < 10, i = 1, 2, \ldots, n$ равно

$$Q = a_n \cdot 10^n + \ldots + a_1 \cdot 10 + a_0 . \qquad (1)$$

Вместо десятичной системы счисления можно строить и другие q-ичные системы счисления, где q – натуральное число больше единицы. В этом случае числа $0, 1, \ldots, q-1$ обозначаются специальными символами, которые называются «цифрами». Если $1 < q \leq 10$, то цифры обозначаются теми же символами, что и в десятичной системе счисления.

Если $q > 10$, то нужны особые символы для обозначения чисел от 10 до $q - 1$. Например, если $q = 12$, то цифры A, B обозначают натуральные числа 10 и 11, соответственно. Если $q = 16$, то цифры A, B, C, D, E, F обозначают числа 10, 11, 12, 13, 14, 15, соответственно. В этом случае число $a = ABBA_{12}$ записанное в 12-ичной системе счисления обозначает натуральное число $a = 10 \cdot 12^3 + 11 \cdot 12^2 + 11 \cdot 12 + 10 = 19006$ в 10-ичной системе счисления.

В позиционных системах счисления значение применяемых символов (цифр) зависит от места, которое эти символы занимают в записи числа. Чаще всего используют

позиционные системы счисления с основанием q (q – натуральное число больше 1), так называемые $q-$ичные позиционные системы счисления. При этом сдвиг цифры на одно место влево в записи числа влечет увеличение её числового значения в $q-$раз.

Возможность построения $q-$ичной позиционной системы счисления вытекает из следующей теоремы.

Теорема 7.1. Пусть q – натуральное число больше единицы. Тогда любое натуральное число Q единственным образом разлагается по степеням числа q, т.е. представимо в виде

$Q = a_n q^n + \ldots + a_1 q + a_0$, где $a_n \neq 0$, $0 \le a_i < q$, $i = 1, 2, \ldots, n$. (1)

■ Докажем существование разложения (1). Разделим число Q на q с остатком: $Q = Q_1 \cdot q + a_0$, где Q_1 – частное, a_0 – остаток, причем $0 \le a_0 < <q_u$, $Q_1 < Q$. (2)

Далее делим Q_1 на q с остатком. Имеем $Q_1 = Q_2 \cdot q + a_1$, где $0 \le a_1 < q$. Следовательно, $Q = Q_2 \cdot q^2 + a_1 q + a_0$. Продолжая этот процесс, получим разложение (1).

Докажем единственность разложения. Пусть наряду с разложением (1) существует разложение

$$Q = b_m \cdot q^m + \ldots + b_1 \cdot q + b_0 . \quad (3)$$

По теореме о делении с остатком $a_0 = b_0$. Следовательно, $a_n \cdot q^n + \ldots + a_1 \cdot q = =b_m \cdot q^m + \ldots + b_1 \cdot q$. Сократив это равенство на q, получим $Q_1 = a_n \cdot q^{n-1} + \ldots + +a_2 \cdot q + a_1 = b_m \cdot q^{m-1} + + \ldots + b_2 \cdot q + b_1$, где a_1 и b_1 – остатки от деления числа Q_1 на q. Следовательно, $a_1 = b_1$. Повторяя эти рассуждения, получим совпадение разложений (1) и (2), ч.т.д. ■

● Представление (1) натурального числа Q сокращенно записывается в виде $Q = (a_n a_{n-1} \ldots a_1 a_0)_q$ и называется

записью числа в позиционной системе счисления по основанию q, если a_n , a_{n-1},…a_1, a_0 – *цифры счисления.*

Замечание. В десятичной системе счисления индекс $q = 10$ не ставится.

► 1. Требуется составить таблицы сложения и умножения в 5-ичной системе счисления.

Р е ш е н и е. Здесь q = 5. Цифры: 0, 1, 2, 3, 4.

Выпишем таблицы сложения и умножения.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	10
2	2	3	4	10	11
3	3	4	10	11	12
4	4	10	11	12	13

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	11	13
3	0	3	11	14	22
4	0	4	13	22	31

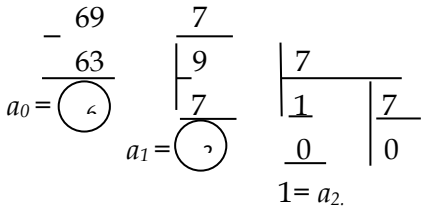
Используя таблицы сложения и умножения чисел, выполним следующие действия2:

$$\begin{array}{r} 23413_5 \\ + \\ 34243_5 \\ \hline 113211_5 \end{array} \qquad \begin{array}{r} 23_5 \\ \times \\ 43_5 \\ \hline 124_5 \\ 202_5 \\ \hline 2144_5 \end{array} \qquad \begin{array}{r|l} 422_5 & 13_5 \\ - & \\ 31 & 24_5 \\ \hline 112 & \\ - & \\ 112 & \\ \hline 0 & \end{array} \qquad \begin{array}{r} 13_5 \\ \times \\ 24_5 \\ \hline 112_5 \\ 31_5 \\ \hline 422_5 \end{array}$$

2. Запишем число $(234)_5$ в 7-ричной системе счисления.

Р е ш е н и е. а) Сначала запишем число в 10-ичной системе счисления: $(234)_5 = 2\cdot5^2 + 3\cdot5 + 4 = 69$.

б) Теперь запишем полученное число в 7-ричной системе счисления:



О т в е т. $(234)_5 = (126)_7$

3. Имеется простой способ перевода из двоичной системы счисления в 8-ричную и обратно. Для этого запишем числа $0, 1, 2, 3, 4, 5, 6, 7$ (цифры 8-ричной системы) в двоичной системе счисления:

0	1	2	3	4	5	6	7
000	001	010	011	100	101	110	111

Чтобы перевести число $(a_n \ \ldots a_1 \ a_0)_8$, записанное в 8-ричной системе счисления в двоичную систему счисления, достаточно заменить каждую цифру данного числа ее двоичным заданием, и обратно. Например:

$(237)_8 = 10.011.111_2$; $11.010.111.110_2 = (3276)_8$.

Аналогичный способ перевода можно применить для двоичной и шестнадцатеричной систем счисления.

16-ичная	0	1	2	3	4	5	6	7
2-ичная	0000	0001	0010	0011	0100	0101	0110	0111
16-ичная	8	9	A	B	C	D	E	F
2-ичная	1000	1001	1010	1011	1100	1101	1110	1111

► $(2EF9)_{16} = (11.1110.1111.1001)_2$;

$(11.1111.1110.0011.0101)_2 = (3FE35)_{16}$. ◄

§8. Числовые функции

1. Функции целой и дробной частей числа. Функция ***целой части*** $[x]$ определена для любого вещественного x и равна наибольшему целому не превосходящему x.

• Функция ***дробной части*** $\{x\}$ определена для любого вещественного x и равна $\{x\} = x - [x]$.

$\{x\}$ – дробная часть

целая часть $[x] \le x < [x]+1$

►$[7] = 7$; $[7{,}3] = 7$; $[-7{,}3] = -8$ $\{7{,}3\} = 0{,}3$; $\{-7{,}3\}0{,}7$. ◄

Предложение 8.1. Показатель, с которым данное простое число p входит в разложение $n!$, равен

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

■ Имеем $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$. Найдем число сомножителей из ряда $1, 2, \ldots, n$, которые делятся на p и обведем их кружочками.

$$1, \ldots, (p), \ldots, (2p), \ldots (tp), \ldots n\ . \qquad (*)$$

Здесь tp – последнее число из ряда (*), которое делится на p. Следовательно, $(t+1) \cdot p > n$ и $t = \left[\frac{n}{p}\right]$. Каждое из этих чисел внесет в показатель степени для p по единице. Некоторые из этих чисел делятся на p^2. Таких чисел будет уже $\left[\frac{n}{p^2}\right]$. Они внесут в показатель степени для p также по единице. Затем учтем числа, которые делятся на p^3, таких

будет $\left[\frac{n}{p^3}\right]$. Они также внесут в показатель степени для p по единице. Продолжая этот процесс, получим, что показатель p в $n!$ равен $\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\ldots$. ■

► Найти показатель степени *3*, делящей *100!*. По формуле имеем

$k=\left[\frac{100}{3}\right]+\left[\frac{100}{3^2}\right]+\left[\frac{100}{3^3}\right]+\cdots=33+11+3+1+0+\cdots=48$.◄

2. Мультипликативные функции. Функция $\theta(a)$, определенная на множестве натуральных чисел, называется ***мультипликативной***, если выполняются следующие условия: 1) $\theta(1)=1$;

2) для любых взаимно простых чисел a и b выполняется $\theta(ab)=\theta(a)\theta(b)$.

I. Степенная функция $\theta(a)=a^s$, где $a>0$, $s\in R$ является мультипликативной, так как $\theta(1)=1^s=1$ и $\theta(ab)=a^s b^s=\theta(a)\cdot\theta(b)$.

II. Функция $\tau(a)$ – числа натуральных делителей числа a и функция $\delta(a)$ – сумма натуральных делителей a являются мультипликативными.

■ Ясно, что $\tau(1)=1$ и $\sigma(a)=1$. Пусть $a=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_m^{\alpha_m}$, $b=q_1^{\beta_1}\cdot q_2^{\beta_2}\cdot\ldots\cdot q_s^{\beta_s}$ – канонические разложения чисел и пусть $(a, b) = 1$. Тогда $ab=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_m^{\alpha_m}q_1^{\beta_1}\cdot q_2^{\beta_2}\cdot\ldots\cdot q_s^{\beta_s}$ – каноническое разложение ab. По теореме о числе положительных делителей натурального числа имеем $\tau(ab)==[(1+\alpha_1)\ldots(1+\alpha_m)]\cdot[(1+\beta_1)\ldots(1+\beta_s)]=\tau(a)\cdot\tau(b)$. По теореме о сумме положительных делителей

натурального числа имеем $\sigma(ab) = \left(\frac{p_1^{\alpha_1+1}-1}{p_1-1} \dots \frac{p_m^{\alpha_m+1}-1}{p_m-1}\right) \cdot \left(\frac{q_1^{\beta_1+1}}{q_1-1} \dots \frac{q_s^{\beta_s+1}}{q_s-1}\right) = \sigma(a)\sigma(b)$. ■

Свойства

СВОЙСТВО 8.1. Если $\theta(a)$ – мультипликативная функция и $a_1, a_2, \dots, a_n$ – попарно взаимно простые числа, то $\theta(a_1 . a_2 \dots a_n) = \theta(a_1) \cdot \theta(a_2) \cdot \dots \cdot \theta(a_n)$.

■ Доказательство проведём индукцией по $n > 2$.

Б.И. Если $(a_1, a_2) = 1$, то по аксиоме 2 $\theta(a_1 \cdot a_2) = = \theta(a_1) \cdot \theta(a_2)$.

П.И. Пусть свойство справедливо для числа множителей меньше *n*, где $n > 2$

Ш.И. Пусть $a_1, a_2, \dots, a_n$ – попарно взаимно простые числа. Тогда $\theta(a_1 \dots a_{n-1}a_n) = \theta(a_1 \dots a_{n-1})\theta(a_n)$, так как $(a_1 \dots a_{n-1}, a_n) = 1$. По П.И. имеем $\theta(a_1, a_s, \dots, a_n) = \theta(a_1) \dots \theta(a_{n-1}) \cdot \theta(a_n)$. Следовательно, свойство справедливо для любого $n \geq 2$. ■

СВОЙСТВО 8.2. Если θ_1 и θ_2 – мультипликативные функции, то функция $\theta_1 \cdot \theta_2$ – мультипликативная.

■ Пусть $\theta_1(a), \theta_2(a)$ – мультипликативные функции, и пусть $\theta_0(a) == \theta_1(a) \cdot \theta_2(a)$. Докажем, что $\theta_0(a)$ – мультипликативная функция. Если $a = 1$, то $\theta_0(1) = \theta_1(1) \cdot \theta_2(1) = 1$. Пусть $(a_1, a_2) = 1$, тогда $\theta_0(a_1, a_2) = \theta_1(a_1a_2) \cdot \theta_2(a_1a_2) = = \theta_1(a_1) \cdot \theta_1(a_2) \cdot \theta_2(a_1) \cdot \theta_2(a_2) = \big(\theta_1(a_1)\theta_2(a_1)\big) \cdot \cdot \big(\theta_1(a_2)\theta_2(a_2)\big) = \theta_0(a_1) \cdot \theta_0(a_2)$. ■

СВОЙСТВО 8.3 (о сумме значений мультипликативной функции по всем натуральным делителям числа). Если $a = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ – каноническое разложение числа, то сумма значений мультипликативной функции θ по всем

положительным делителям числа a равна $\sum_{0<d|a}\theta(d) = \left(1+\theta(p_1)+\cdots+\theta\left(p_1^{\alpha_1}\right)\right)\ldots(1+\theta(p_m+\cdots+\theta\left(p_m^{\alpha_m}\right))$. (1)

■ Произвольный положительный делитель d числа a по теореме.4.4 представим в виде $d = p_1^{\beta_1}\ldots p_i^{\beta_i}\ldots p_m^{\beta_m}$, где $0 \le \beta_i \le a_i, i = 1,2,\ldots,m$. Следовательно,

$$\sum_{0<d|a}\theta(d) = \sum_{(\beta_1,\ldots\beta_i,\ldots\beta_m)}\theta\left(p_1^{\beta_1}\ldots p_m^{\beta_m}\right) =$$

$$= \sum_{(\beta_1\ldots\beta_m)}\theta(p_1^{\beta_1})\ldots\theta\left(p_m^{\beta_m}\right) =$$

$$= \left[1+\theta(p_1)+\ldots+\theta\left(p_1^{\beta_1}\right)+\ldots+\theta(p_1^{\alpha_1})\right]\ldots[1+\theta(p_m)+\ldots+$$

$$+\theta\left(p_m^{\beta_m}\right)+\cdots+\theta(p_m^{\alpha_m})],$$ так как, раскрыв скобки в правой части, мы получим каждое слагаемое из левой части равенства, причем получим все слагаемые. ■

3. Функция Мёбиуса. Функция Мёбиуса $\mu(a)$ определена для всех натуральных чисел a, равна 0, если число a делится на квадрат простого числа, и равна $(-1)^k$, если число a разлагается в произведение k различных простых чисел:

$$\mu(a) = \begin{cases} 0, \text{если существует простое } p \text{ такое, что } p^2 \text{ делит } a, \\ (-1)^k, \text{если } a - \text{произведение различных } k \\ \text{простых чисел.} \end{cases}$$

► $\mu(1) = 1, \mu(2) = -1, \mu(4) = 0, \mu(6) = (-1)^2,$ т.к. $6 = 2\cdot 3$. Заметим, что $\mu(a) = -1$, если a – простое число. ◄

Теорема 8.2. Функция Мёбиуса является мультипликативной.

■ Так как $\mu(1) = 1$, то выполняется аксиома 1 для мультипликативной функции. Пусть $a = p_1^{k_1}\ldots p_m^{k_m}, b = q_1^{l_1}\ldots q_s^{l_s}$ –

каноническое разложение чисел a и b и пусть $(a,b)=1$. Тогда $ab = p_1^{k_1} \dots p_m^{k_m} \cdot q_1^{l_1} \dots q_s^{l_s}$ – каноническое разложение ab.

Если a или b делятся на квадрат простого числа, то $\mu(a)=0$ или $\mu(b)=0$. Так как в этом случае ab так же делится на квадрат простого числа, то $\mu(ab)=0$, следовательно, $\mu(ab)=0=\mu(a)\mu(b)=0$,ч.т.д

Пусть числа a и b не делятся на квадраты простых чисел $\mu(a,b)=1$. Тогда $ab = p_1 \dots p_m \cdot q_1 \dots q_s$, где p_i и q_i все различимы и $\mu(ab) = (-1)^{k+m} = (-1)^k \cdot (-1)^m = \mu(a) \cdot \mu(b)$. ■

Теорема о срезе 8.3. Если θ – мультипликативная функция и $a = p_1^{k_1} \dots p_m^{k_m}$ - каноническое разложение числа a, то справедливо следующее равенство $\sum_{0<d|a} \mu(d) \cdot \theta(d) =$
$= \big(1-\theta(p_1)\big) \dots (1-\theta(p_m))$. (2)

■ Произведение $\mu \cdot \theta$ является мультипликативной функцией и по свойству 8.3 имеем $\sum_{0<d|a} \mu\theta(d) =$
$= \Big(1+\mu\cdot\theta(p_1) + \dots + \mu\cdot\theta\big(p_1^{k_1}\big)\Big) \cdot \dots \cdot$
$\cdot \Big(1+\mu\cdot\theta p_m + \dots + \mu\cdot\theta\big(p_m^{k_m}\big)\Big) = \big(1-\theta(p_1)\big) \cdot \dots \cdot (1-$
$-\theta(p_m))$, т.к. $\mu\cdot\theta(p^s) = \mu(p^s)\cdot\theta(p^s)$ по определению произведения функций и так как $\mu(p^s)=0$, если $s>1$. ■

Следствие 8.4

$$\sum_{0<d|a} \mu(d) = \begin{cases} 0, \text{если } a>1, \\ 1, \text{если } a=1. \end{cases} \quad (3)$$

■ В равенстве (2) положим $\theta(d) = d^0 = 1$ (θ мультипликативная функция).
Тогда $\sum_{0<d|a} \mu(d)\cdot\theta(d) = (1-1)(1-1)\dots(1-1) = 0, a>1$ и $\sum_{0<d|a} \mu(d)\cdot\theta(d) = \mu(d) = \mu(1) = 1$, если $a=1$. ■

Следствие 8.5.

$$\sum_{0<d|a}\frac{\mu(d)}{d}=\begin{cases}\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_k}\right), \text{если } a>1,\\ 1, \text{если } a=1.\end{cases} \quad (4)$$

■ В формуле (2) положим $\theta(d)=d^{-1}=\frac{1}{d}$ (θ – мультипликативная функция). Теперь, если $a>1$, то получим нужное равенство. Если $a=1$, то $\sum_{0<d|a}\frac{\mu(d)}{d}=\frac{1}{1}=1$. ■

Теорема о счетчике 8.6. Пусть заданным натуральным числам $\delta=\delta_1,\delta_2,\dots,\delta_n$ соответствуют вещественные числа $f=f_1,f_2,\dots,f_n$. Если через S' обозначить сумму значений f, соответствующих $\delta=1$, а через S_d сумму значений f, соответствующих δ, которые делятся на $d>0$, тогда выполняется следующее равенство

$$S'=\sum_{0<d:\exists\delta=d|\delta}\mu(d)S_d. \quad (5)$$

В силу следствия 8.4. имеем $S'=\int_1\sum_{0<d|\delta_1}\mu(d)+$ $+\int_2\sum_{0<d|\delta_2}\mu(d)+\dots+\int_n\sum_{0<d|\delta_n}\mu(d)$.

Правая часть равенства получается, если сложить все члены с одним d, а потом вынести $\mu(d)$ за скобки, при этом в скобках получится сумма тех и только тех значений f, которые соответствуют δ кратных d, т.е S_d . ■

► Пусть числам $\delta=2,4,6,9,11$ соответствуют значения $f=2,3,4,5,6,7$. Проверим теорему о счетчике.

Делители чисел δ: $1,2,3,4,6,9$. Ясно, что $S'=f_5+f_6=6+$ $+7=13$. Так же имеем $S'=2\cdot\sum_{0<d|2}\mu(d)+3\sum_{0<d|4}\mu(d)+$ $+4\sum_{0<d|6}\mu(d)+5\sum_{0<d|9}\mu(d)+6\sum_{0<d|1}\mu(d)+7\sum_{0<d|1}\mu(d)=$ $=2\cdot3+3\cdot0+4\cdot0+5\cdot0+6\cdot1+7\cdot1=6+7=13$.

Сгруппируем сумму S' по делителям d чисел δ: $S'=\mu(1)[2+$ $+3+4+5+6+7]+\mu(2)[2+3+4]+\mu(3)[4+5]+\mu(4)[3]+$ $+\mu(6)\cdot4+\mu(9)\cdot5=27-9-9+4+0=13$.

Закон обращения числовых функций 8.7. Пусть a – положительное целое число и на множестве всех натуральных делителей δ числа a определена функция $F(\delta)$ и пусть функция $G(\delta)$ определена равенством $G(\delta) = \sum_{1 \le d|\delta} F(d)$. Тогда $F(a) = \sum_{0<d|a} \mu(d) \cdot G(\frac{a}{d})$.

■ По определению функции $G(\delta)$ надо доказать, что $F(a) = \sum_{0<d|a} \mu(d) \cdot G\left(\frac{a}{d}\right) = \sum_{0<d|a} \mu(d) \cdot \sum_{0<d|\frac{a}{d}} F(\delta) =$
$= \sum_{0<\delta|\frac{a}{d}} F(\delta) \cdot \sum_{0<d|a} \mu(d)$.

Теперь заметим, что $\delta \Big| \frac{a}{d}$ только для тех d, которые делят $\frac{a}{\delta}$, т.е для фиксированного $\frac{\delta}{a}$ числа d пробегают все натуральные делители числа $\frac{a}{\delta}$. Поэтому $\sum_{d|a} \mu(d) \cdot \sum_{0<\delta|\frac{a}{d}} F(\delta) = \sum_{0<\delta|a} F(\delta) \cdot \sum_{0<d|\frac{a}{\delta}} \mu(\delta) = F(a) \cdot \mu(1) +$
$+ \sum_{0<\delta|a, \delta<a} F(\delta) \cdot \sum_{d|\frac{a}{\delta}>1} \mu(d) = F(a)$, т.к. по следствию 8.4 $\mu(1) = 1$ и $\sum_{0<d|\frac{a}{\delta}>1} \mu(d) = 0$. ■

► Пусть $a = 12$. Делители числа a: $\delta = 1, 2, 3, 4, 6, 12$. Положим, $F(\delta) = \delta$ и $G(\delta) = \sum_{d|\delta} F(d)$. Тогда

$$\sum_{0<d|12} \mu(d) \cdot \sum_{\delta|\frac{12}{d}} F(\delta) = \mu(1)[F(1) + F(2) + F(3) + F(4) + F(6) + F(12)]$$
$$+\mu(2)[F(1) + F(2) + F(3) + F(6)] + \mu(3)[F(1) + F(2) + F(4)] +$$
$$\mu(6)[F(1) + F(2)] + \mu(12)F(1) = F(1)[\mu(1) + \mu(2) + \mu(3) + \mu(4) + \mu(6) +$$
$$\mu(12)] + F(2)[\mu(1) + \mu(2) + \mu(3) + \mu(6)] + F(3)[\mu(1) + \mu(2) + \mu(4)] +$$
$$F(6)[\mu(1) + \mu(2)] + F(12)[\mu(1)] = F(12),$$

т.к. суммы в квадратных скобках равны 0 как суммы значений функции Мёбиуса по натуральным делителям чисел больше 1. ◄

4. Функция Эйлера. Функция Эйлера $\varphi(a)$ определена на множестве натуральных чисел a и равна числу неотрицательных взаимно простых с a чисел, меньших его. Таким образом, $\varphi(a)$ – число взаимно простых с a чисел из ряда $0, 1, 2, \dots, a-1$.

Замечание. Вместо ряда $\{0, 1, \dots, a-1\}$ можно взять положительные числа, не превосходящие числа a, т.е. ряд $\{1, 2, \dots, a\}$, т.к. $(0, a) = (a, a) = a$.

Формула Эйлера 8.8. Пусть $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$ – каноническое разложение a, тогда

$$\varphi(a) = a\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right) = (p_1^{\alpha} - p_1^{\alpha-1}) \dots (p_k^{\alpha} - -p_k^{\alpha-1}). \quad (6)$$

В частности, если p – простое число, то $\varphi(p^m) = p^m - -p^{m-1}$.

■ Для доказательства (6) воспользуемся теоремой о счетчике. В качестве последовательности δ возьмём $\delta_j == (j, a), j = 0,1, \dots, a-1$, а в качестве последовательности f возьмём $f_j = 1, j = 0,1, a-1$.Тогда число взаимно простых с a чисел из ряда $j = 0,1, a-1$ равно $\varphi(a)$ и равно сумме δ_j, равных 1, т.е S'

Заметим, если $d = (j, a)$, то $\frac{d}{j}$ (кратно d), причём $j < a$. Следовательно, S_d – число положительных кратных d, которые строго меньше a. Число таких кратных равно $\frac{a}{d}$, поэтому, $S_d = \frac{a}{d}$. По теореме о счётчике имеем

$$\varphi(a) = \sum_{0<d|a} \mu(d) \cdot \frac{a}{d} = a \cdot \sum_{0<d|a} \frac{\mu(d)}{d} =$$

$$= \begin{cases} a \cdot \left(1 - \frac{1}{p_1}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right), \text{если } a > 1, \\ 1, \text{если } a = 1. \end{cases} \blacksquare$$

Теорема 8.9. Функция Эйлера является мультипликативной функцией.

■ Пусть, $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}, b = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_s^{\beta_s}$– взаимно простые числа. Поэтому $ab = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} \cdot q_1^{\beta_1} \cdot \cdot q_2^{\beta_2} \cdot \ldots \cdot q_s^{\beta_s}$ – каноническое разложение ab. Следовательно, по (6)

$$\varphi(ab) = a \cdot b \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right) \cdot \left(1 - \frac{1}{q_1}\right) \cdot \left(1 - \frac{1}{q_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{q_s}\right) = \left[a \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right)\right] \cdot \left[b \cdot \left(1 - \frac{1}{q_1}\right) \cdot \left(1 - \frac{1}{q_2}\right) \cdot \ldots \cdot (1 - \frac{1}{q_s})\right] = \varphi(a) \cdot \varphi(b).$$ ■

Тождество Гаусса 8.10. Сумма значений функции Эйлера по всем натуральным делителям d, числа n равна n, т.е $\sum_{0<d|a} \varphi(d) = n$.

■ Пусть $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ – каноническое разложение n. Тогда в силу тождества о сумме значений мультипликативной функции по натуральным делителям числа имеем $\sum_{0<d|n} \varphi(d) = \sum_{0<d|n} \varphi\left(p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_i^{\beta_i} \cdot \ldots \cdot p_k^{\beta_k}\right) =$ $= \prod_{i=1}^{k} (1 + \varphi(p_i) + \cdots + \varphi\left(p_i^{\beta_i}\right) + \cdots + \varphi(p_i^{\alpha_i})$, так как при раскрытии скобок получим сумму всех значений $\varphi(d)$, где $d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_i^{\beta_i} \cdot \ldots \cdot p_k^{\beta_k}, 0 \le \beta_i \le \alpha_i, i = \overline{1,k}$. Далее так как $\varphi(p^k) = p^k - p^{k-1}$, то $\sum_{0<d|n} \varphi(d) = \prod_{i=1}^{k} (1 + (p_i - 1) + + \cdots + (p_i^{a_i} - p_i^{a_i - 1})) = \prod_{i=1}^{k} p_i^{a_i} = n$. ■

► Пусть $n = 12 = 2^2 \cdot 3$. Делители n: $d = 1, 2, 3,$ $2^2, 6, 12$. Следовательно,

$\sum_{0<d|12} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(2^2) + \varphi(6) + \varphi(12) =$ $= 1 + 1 + 2 + 2 + 2 + 4 = 12$. ◄

ГЛАВА 2. ТЕОРИЯ СРАВНЕНИЙ И АРИФМЕТИЧЕСКИЕ ПРИЛОЖЕНИЯ

§1. Сравнения

1. Сравнения, свойства. Модулем называется натуральное число m больше единицы.

● Говорят, что число a **сравнимо** с числом b **по модулю m**, если модуль m делит разность $a-b$ этих чисел; записывают: $a \equiv b(mod\ m)$.

Критерий сравнения 1.1. Пусть a и b целые числа, m – модуль.

Следующие условия эквивалентны:

1) $a \equiv b(mod\ m)$;

2) числа a и b дают равные остатки при делении на модуль m;

3) существует число k такое, что $a = b + km$.

■ Докажем, что из (1) следует (2). Пусть $m|a-b$.

Разделим a и b на m с остатком:

$a = k_1m + r_1, 0 \le r_1 < m,$

$b = k_2m + r_2, 0 \le r_2 < m.$

Тогда $a - b = (k_1 - k_2)m + (r_1 - r_2)$ и $m|r_1 - r_2 < m$. Следовательно, $r_1 - r_2 = 0$, и $r_1 = r_2$, т.е. a и b имеют равные остатки при делении на m.

Из (2) следует (3), так как, если $a = k_1m + r$ и $b = k_2m + r$ для некоторых $k_1, k_2 \in Z$, то $a = (k_1 - k_2)m + b$.

Наконец, из (3) вытекает (1), так как, если $a = km + b$ для некоторого $k \in Z$, то $m|a-b$. ■

Теорема 1.2. Отношение сравнения по модулю является отношением эквивалентности на множестве целых чисел.

■ Отношение сравнения по модулю m рефлексивно, так как $m|a-a$, для любого целого числа a, т.е. $a \equiv a(mod\ m)$.

Отношение сравнения по модулю m симметрично в силу условия (2) критерия.

Отношение сравнения по модулю m транзитивно. Действительно, если $a \equiv b(mod\ m)$и $b \equiv c(mod\ m)$, то $m|a - -b, b-c$.

Следовательно, $m|(a-b)+(b-c)=a-c$ и $a \equiv c\ (mod\ m)$. ■

Отношение эквивалентности на множестве индуцирует разбиение этого множества на классы эквивалентности.

● **Классом вычетов по модулю m, содержащим число a,** называется множество

$$\bar{a} = \{b \in Z | b \equiv a\ (mod\ m). \qquad (1)$$

В силу критерия 1.1 (п.3) класс вычетов $\bar{a}$ равен

$$\bar{a} = \{a + zm | z \in Z\}.$$

● Любое число класса будем называть **вычетом по модулю m.**

Теорема 1.3. 1. Любые два класса вычетов по модулю m либо совпадают, либо не пересекаются: $\forall a, b \in Z\left(\bar{a} = \bar{b} \vee \bar{a} \cap \bar{b} = \emptyset\right)$.

2. Два класса вычетов $\bar{a}$ и $\bar{b}$ равны тогда и только тогда, когда числа a и b сравнимы по модулю m: $\forall a, b \in Z\left(\bar{a} = \bar{b} \leftrightarrow a \equiv b\ (mod\ m)\right)$.

3. Множество Z распадается точно на m различных классов вычетов по модулю m, в частности

$$Z = \cup_{r=0}^{m-1} \bar{r}\text{, где } \bar{r} = \{r + zm | z \in Z\}, r = \overline{0, m-1}. \qquad (3)$$

■ Утверждения 1–2 следуют из свойств классов эквивалентности.

В силу критерия 1.1. (п. 2) все числа, принадлежащие одному и тому же классу вычетов по модулю m, имеют одинаковые остатки при делении на m. Поэтому в качестве представителя класса вычетов по модулю m можно взять соответствующий остаток, получающийся при делении чисел класса на модуль m.

Следовательно, все классы вычетов по модулю m исчерпываются классами $\overline{0}, \overline{1}, \dots, \overline{m-1}$, число которых равно точно m. ■

Свойства сравнений

Пусть $a, b, c, d -$ целые числа, $m-$ натуральное число больше единицы.

СВОЙСТВО 1.1. Сравнения можно почленно складывать: если $a \equiv b(mod\ m)$ и $c \equiv b(mod\ m)$, то $a + c \equiv b + d(mod\ m)$.

■ Пусть $m|a-b, c-d$. Тогда $m|(a-b)+(c-d) = (a+b)-(b+d)$.

Следовательно, $(a+c) \equiv (b+d)(mod\ m)$. ■

Как следствие получаем

СВОЙСТВО 1.2. Одну часть сравнения можно перенести в другую сторону с противоположным знаком.

СВОЙСТВО 1.3. Сравнения можно почленно перемножать: если

$a \equiv b(mod\ m)$ и $c \equiv d(mod\ m)$, то $ac \equiv bd(mod\ m)$.

■ Имеем $ac - bd = ac - bc - bc - bd = (a-b)c + b(c-d)$.

Так как $m|a-b, c-d$, то $m|ac-bd$ и $ac \equiv bd(mod\ m)$. ■

СВОЙСТВО 1.4. Обе части сравнения можно умножать на целое число: $\forall a,\ b \in Z\ \left(a \equiv b\,(mod\ m) \rightarrow \forall c \in \right.$ $\left. \in Z\ (ac \equiv bc(mod\ m))\right)$.

■ Так как $c \equiv c(mod\ m), c \in Z$, то по свойству 1.3 из $a \equiv b(mod\ m)$ следует $ac \equiv bc(mod\ m)$. ■

СВОЙСТВО 1.5. Обе части сравнения можно возводить в натуральную степень: $\forall a, b \in Z, \forall n \in N\ \left(a \equiv b(mod\ m) \rightarrow \right.$ $\left. \rightarrow a^n \equiv b^n(mod\ m)\right)$.

■ Перемножив по свойству 1.3 сравнение на себя n раз, получим требуемое сравнение $a^n \equiv b^n(mod\ m)$. ■

СВОЙСТВО 1.6. Обе части сравнения можно разделить на их общий делитель, взаимно простой с модулем.

■ Пусть $d|a, b, (d, m) = 1$ и $a \equiv b\ (mod\ m)$. Тогда $a = a_1 d, b = b_1 d$ и $m|a - b = d(a_1 - b_1)$. По условию $(d, m) = 1$, поэтому $m|a_1 - b_1$, и $\frac{a}{d} \equiv \frac{b}{d}(mod\ m)$. ■

СВОЙСТВО 1.7. Обе части сравнения и модуль можно разделить на их общий делитель.

■ Пусть $a \equiv b(mod\ m)$ и $d|a, b, m,$ то есть существуют числа d_1, b_1, m_1 такие, что $a \equiv a_1, d, b = b_1 d, m = m_1 d$. Тогда из условия $m = m_1 d \mid a - b == d(a_1 - b_1)$ следует, что $m_1|a_1 - b_1$. Это означает $\frac{a}{d} \equiv \frac{b}{d}\left(mod\ \frac{m}{d}\right)$. ■

СВОЙСТВО 1.8. Если $a \equiv b\ (mod\ m_1), a \equiv b\ (mod\ m_2)$, $\ldots, a \equiv b(mod\ m_k)$, то $a \equiv b(mod\ [m_1, \ldots, m_k])$.

■ Из условия $m_1, \ldots, m_k|a - b$ и по определению НОК получаем $[m_1, \ldots, m_k]|a - b$, то есть $a \equiv b(mod\ [m_1, \ldots, m_k])$. ■

4. Полная система вычетов, свойства. Множество чисел взятых по одному из каждого класса вычетов, называется **полной системой вычетов** (ПСВ) **по модулю m**.

Критерий полной системы вычетов 1.4. Совокупность из -чисел образует полную систему вычетов по модулю m тогда и только тогда, когда вычеты попарно несравнимы по модулю m.

■ (⇒)Пусть множество $\{x_1, \dots, x_m\}$ образует полную систему вычетов. Тогда модуль равен m и по определению ПСВ они попарно несравнимы, ч.т.д.

(⇐)Пусть $x_1, \dots, x_m$ – попарно несравнимы по модулю m. Следовательно, они из разных классов вычетов. Так как число классов равно m, то они взяты из каждого класса вычетов по модулю m. ■

Теорема о полной системе вычетов 1.5. Пусть a – целое число, $(a, m) = 1$ и пусть x пробегает полную систему вычетов по модулю m. Тогда $y = ax + b, b \in Z$ также пробегает полную систему вычетов по модулю m.

■ Пусть $x_1, x_2, \dots, x_m$ – полная система вычетов по модулю m. Требуется доказать, что числа $y_1, y_2, \dots, y_m$, где $y_i = ax_i + b, i = \overline{1, m}$ образуют полную систему вычетов по модулю m.

В силу критерия ПСВ достаточно показать, что они попарно несравнимы по модулю m. Действительно, если $y_k \equiv y_s (mod\ m)$, где $k \neq s$, то $ax_k + b \equiv ax_s + (mod\ m)$и $ax_k \equiv$ $\equiv ax_s (mod\ m)$. Так как $(a, m) = 1$, то обе части сравнения можно разделить на a: $x_k \equiv x_s (mod\ m)$. Это противоречит условию. Следовательно, $y_1, \dots, y_m$ попарно несравнимы и по критерию они образуют ПСВ по модулю m. ■

5. Приведенная система вычетов.

Предложение 1.5. Все числа из одного и того же класса вычетов $a\ mod\ m$ имеют с модулем m один и тот же наибольший общий делитель, равный (a, m).

■ Пусть $b \in \bar{a} = \{a + zm, z \in Z\}$, т.е. существует число k такое, что $b = a + km$. По предложению 2.1 (гл.1) следует $(b, m) = (a, m)$, ч.т.д. ■

В силу доказанного предложения следующее определение корректно.

● Класс вычетов называется **взаимно простым с модулем m,** если все его вычеты взаимно простые с модулем m.

● **Приведенной системой вычетов** по модулю m (ПрСВ) называется множество чисел, взятых по одному из каждого взаимно простого с модулем m класса вычетов.

Возьмем систему наименьших положительных вычетов по модулю m: $\{1,2, \dots, m\}$. Число чисел из этой системы, взаимно простых с модулем m, равно $\varphi(m)$. Следовательно, приведенная система вычетов по модулю m содержит точно $\varphi(m)$ чисел.

Критерий приведенной системы вычетов 1.7. Совокупность чисел тогда и только тогда образует приведенную систему вычетов, когда удовлетворяет следующим условиям:

1) множество содержит $\varphi(m)$ чисел;
2) числа множества попарно несравнимы по модулю m;
3) все числа системы взаимно простые с модулем m.

■ (⇒) Условия (1)–(3) следуют из определения приведенной системы вычетов.

(⇐)Пусть множество чисел $\{x_1, \dots, x_{\varphi(m)}\}$ удовлетворяет условиям (1)–(3). В силу условия (3) вычеты принадлежат классам вычетов, взаимно простых с модулем m, а в силу условия (2) они лежат в различных классах вычетов. Так как число вычетов в множестве равно $\varphi(m)$, то они образуют приведенную систему вычетов по модулю m. ■

Теорема о приведенной системе вычетов 1.8. Пусть целое число a взаимно просто с модулем m и пусть переменная x принимает все значения из некоторой приведенной системы вычетов. Тогда переменная $y = ax$ также принимает все значения из приведенной системы вычетов по модулю m.

■ Пусть $x_1, \dots, x_{\varphi(m)}$ – приведенная система вычетов по модулю m. Требуется доказать, что числа $y_1 = ax_1, \dots, y_{\varphi(m)} = ax_{\varphi(m)}$ образуют приведенную систему вычетов.

Воспользуемся критерием ПрСВ:

1) y пробегает $\varphi(m)$ значений;

2) значения y попарно несравнимы по модулю m, так как из $ax_k = ax_s (mod\ m)$ следует $x_k \equiv x_s (mod\ m)$, что противоречит условию при $k \neq s$;

3) так как по условию $(a, m) = 1$и $(x_k, m) = 1, k = \overline{1, m}$, то $(ax_k, m) = 1$.

Следовательно, все значения $y = ax$ являются взаимно простыми числами с модулем m. В силу критерия 1.7 совокупность $\{y_1, \dots, y_{\varphi(m)}\}$ образует приведенную систему вычетов по модулю m. ■

6. Теоремы Эйлера и Ферма. В теории сравнений важную роль играет теорема Эйлера.

Теорема Эйлера 1.9. Если целое число a взаимно простое с модулем m, то $a^{\varphi(m)} \equiv 1\ (mod\ m)$, где $\varphi(m)$ – функция Эйлера.

■ Пусть $x_1, x_2, \dots, x_{\varphi(m)}$ − приведенная система наименьших положительных вычетов (взяты из ряда $1, 2, \dots, m$). По теореме о приведенной системе вычетов следует, что множество чисел $\{y_1 = ax_1, \dots, y_{\varphi(m)} = ax_{\varphi(m)}\}$ – является

приведенной системой вычетов. Это означает, что для любого $k = 1, \dots, \varphi(m)$ имеет место $y_1 = ax_1 \equiv x_{i(1)} \, (mod\, m)$, $y_2 = ax_2 \equiv x_{i(2)} \, (mod\, m), \dots, y_{\varphi(m)} = ax_{\varphi(m)} \equiv$
$\equiv x_{i(\varphi(m))} \, (mod\, m)$. Перемножив эти сравнения, получим
$y_{\varphi(m)} = a^{\varphi(m)} x_1 x_2 \dots x_{\varphi(m)} \equiv x_{i(1)} x_{i(2)} \dots x_{i(\varphi(m))} (mod\, m)$.

Произведение $x_1 \cdot x_2 \cdot \dots \cdot x_{\varphi(m)}$ – взаимно просто с m и совпадает с произведением $x_{i(1)} \cdot x_{i(2)} \cdot \dots \cdot x_{i(\varphi(m))}$. Поэтому обе части сравнения можно разделить на их общий множитель. Получим $a^{\varphi(m)} \equiv 1 (mod\, m)$. ■

Теорема Ферма 1.10. Если целое число a не делится на простое число p, то $a^{p-1} \equiv 1 (\, mod\, p)$, в частности, $a^p \equiv a \, (mod\, p)$.

■ Это следует из теоремы Эйлера, так как $\varphi(p) = p - 1$. ■

► Решим сравнение $ax \equiv b (mod\, m)$, где $(a, m) = 1$, применив теорему Эйлера. По теореме Эйлера имеем $a^{\varphi(m)} \equiv 1 (mod\, m)$. Умножив обе части сравнения $ax \equiv b (mod\, m)$ на $a^{\varphi(m)-1}$, получим $a^{\varphi(m)} x \equiv a^{\varphi(m)-1} \cdot$
$\cdot\, b \, (mod\, m)$.

О т в е т. $x \equiv a^{\varphi(m)-1} \cdot b \, (mod\, m)$.

Например, решим сравнение $3x \equiv 2 (mod\, 5)$.

Так как $(3,5) = 1$ и $\varphi(5) = 5 - 1 = 4$, то $3^{\varphi(5)} = 3^4 =$
$= 1 \, (mod\, 5)$.

Умножив обе части сравнения на $3^{\varphi(5)-1} = 3^3$, получим $3^4 x \equiv 3^3 \cdot 2 \, (mod\, 5)$, то есть $x \equiv 54 \equiv 4 \, (mod\, 5)$.

О т в е т. $x \equiv 4 (mod\, 5)$. ◄

7. Формула функции Эйлера $\varphi(m)$. Раннее, в главе 1, была сначала получена формула для функции Эйлера $\varphi(m)$, а потом доказана мультипликативность этой функции. Сейчас, используя свойства сравнений, докажем сна-

чала мультипликативность функции Эйлера $\varphi(m)$, а потом выведем формулу для вычисления $\varphi(m)$.

Напомним, целочисленная функция θ является мультипликативной, если выполняются условия:

1) $\theta(1) = 1$;
2) если $(a, b) = 1$, то $\theta(a \cdot b) = \theta(a) \cdot \theta(b)$.

Пусть $a, b, c \in N$ и $(a, b) = 1$. Условие $(c, ab) = 1$ выполняется тогда и только тогда, когда $(c, a) = 1$ и $(c, b) = 1$.

Найдем по определению функции Эйлера значение $\varphi(ab)$, равное числу взаимно простых с ab чисел из ряда $0, 1, 2, \dots, ab - 1$, которые расположим в виде следующей таблицы:

$$\begin{cases} 0 & 1 & \dots\ k & \dots\ a-1 \\ a & a+1 & \dots\ a+k & \dots\ 2a-1 \\ \dots\dots\dots & \dots\dots\dots & \dots\dots\dots & \dots\dots\dots \\ (b-1)a & (b-1)a+1 & \dots\ (b-1)a+k & \dots\ ba-1. \end{cases}$$

В таблице a столбцов и b строк.

Заметим, что любая строка образует полную систему вычетов по модулю a и каждый столбец состоит из сравнимых между собой чисел по модулю a (они равноостаточны, следовательно, имеют один и тот же наибольший общий делитель с модулем a).

Поэтому, каждый столбец состоит либо только из взаимно простых с модулем a чисел, либо только из не взаимно простых. Таким образом, число взаимно простых с a чисел из таблицы равно $\varphi(a) \cdot b$.

Теперь среди них выберем те, которые взаимно просты с b.

Из теоремы о полной системе вычетов следует, что любой столбец образует полную систему вычетов по модулю b (столбец состоит из значений $ax + k$, где

$x = \{0,1,\dots,b-1\}$ – полная система вычетов по модулю b) и содержит $\varphi(b)$ взаимно простых с b чисел.

Таким образом, число взаимно простых с a и b чисел из таблицы (1) равно $\varphi(ab) = \varphi(a) \cdot \varphi(b)$.

Следовательно, доказана следующая теорема.

Теорема 1.11. Функция Эйлера $\varphi(a)$ является мультипликативной функцией.

Перейдем к доказательству формулы для $\varphi(m)$.

Предложение 1.12. Если p – простое число, то $\varphi(p^n) = p^n - p^{n-1}$.

■ Запишем в ряд все числа от 1 до p^n и кратные числа p обведем кружочками: $1,\dots,(p),\dots,(2p),\dots,(p^{n-1}p)$. Их число равно p^{n-1}. Остальные числа из ряда являются взаимно простыми с p. Следовательно, $\varphi(p^n) = p^n - p^{n-1}$. ■

Формула $\varphi(m)$ 1.13. Пусть $a = p_1^{\delta_1} \cdot p_2^{\delta_2} \cdot \dots \cdot p_k^{\delta_k}$ – каноническое разложение числа a.

Тогда $\varphi(a) = \left(p_1^{\delta_1} - p_1^{\delta_1-1}\right) \dots \left(p_k{}^{\delta_k} - p_k{}^{\delta_k-1}\right) =$

$= a\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_k}\right) = p_1^{\delta_1-1} \dots p_k{}^{\delta_k-1}(p_1-1)\dots(p_k-1).$

■ Так как φ – мультипликативная функция, то

$\varphi(a) = \varphi\left(p_1^{\delta_1} \cdot p_2^{\delta_2} \cdot \dots \cdot p_k^{\delta_k}\right) = \varphi\left(p_1^{\delta_1}\right) \cdot \varphi\left(p_2^{\delta_2}\right) \cdot \dots \cdot \varphi\left(p_k^{\delta_k}\right) =$

$= \left(p_1^{\delta_1} - p_1^{\delta_1-1}\right)\left(p_2^{\delta_2} - p_2^{\delta_2-1}\right) \cdot \dots \cdot \left(p_k^{\delta_k} - p_k^{\delta_k-1}\right) =$

$= a\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right) \cdot \dots \cdot (1-\frac{1}{p_k}).$ ■

§2. Кольцо классов вычетов

1. Кольцо классов вычетов. Пусть Z_m – множество классов вычетов по модулю m:

$$Z_m = \{\overline{0}, \overline{1}, \dots, \overline{k}, \cdots, \overline{m-1} \mid \overline{k} = \{z \in Z \mid z \equiv k \,(mod\, m), k = \overline{0, m-1}\}\}.$$

Определим на множестве Z_m сложение «+» и умножение «·» классов вычетов по модулю m следующими равенствами:

а) $\forall\, \overline{a}, \overline{b} \in Z_m : \overline{a} + \overline{b} = \overline{a+b}$;

б) $\forall\, \overline{a}, \overline{b} \in Z_m : \overline{a} \cdot \overline{b} = \overline{a\,b}$.

Определение операций корректно. Действительно, пусть $a \equiv c \,(mod\, m)$, $b \equiv d \,(mod\, m)$, т. е. $\overline{a} = \overline{c}$ и $\overline{b} = \overline{d}$. Так как сравнения можно складывать и умножать, то $a + b \equiv c + d \,(mod\, m)$ и $a\,b \equiv c\,d \,(mod\, m)$, т.е. $\overline{a+b} = \overline{c+d}$ и $\overline{ab} = \overline{cd}$. Это означает, что результат сложения и умножения классов вычетов не зависит от выбора представителей класса, т.е. соотношения а) и б) являются бинарными операциями на множестве Z_m.

► Пусть $m = 5$. $Z_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$.

Таблицы сложения и умножения классов:

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

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

◄ **Теорема 2.1.** Алгебра $(Z_m, +, \cdot)$ является коммутативным кольцом с единицей и называется **кольцом классов вычетов по модулю m.**

■ Проверим, что алгебра $(Z_m, +, \cdot)$ удовлетворяет аксиомам кольца с единицей.

1. $(Z_m, +)$ – абелева группа.

Коммутативность и ассоциативность операции сложения следуют из соответствующих свойств сложения целых чисел.

Нейтральным элементом (нулем) является класс вычетов $\overline{0}$, так как $\overline{a} + \overline{0} = \overline{a + 0} = \overline{a}$ для любого класса вычетов $\overline{a} \in Z_m$.

Противоположным элементом для элемента $\overline{a} \in Z_m$ является $\overline{-a}$, так как $\overline{a} + \overline{-a} = \overline{a - a} = \overline{0}$.

2. $(Z_m, \cdot)$ – коммутативный моноид.

Коммутативность и ассоциативность умножения классов вычетов вытекает из свойств умножения целых чисел и определения умножения классов вычетов по модулю m.

Нейтральным элементом является класс $\overline{1}$, так как $\overline{a} \cdot \overline{1} = \overline{a \cdot 1} = \overline{a}$ для любого класса вычетов $\overline{a}$ по модулю m.

3. Умножение дистрибутивно относительно сложения, так как:

$\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b + c} = \overline{a\,(b + c)} = \overline{ab + ac} = \overline{ab} + \overline{ac} =$

$= \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$ для любых $\overline{a}, \overline{b}, \overline{c} \in Z_m$. ■

Теорема 2.2. Кольцо Z_m классов вычетов по модулю m является полем тогда и только тогда, когда модуль m – простое число.

■ ($\Rightarrow$) Пусть Z_m – поле. Предположим, что модуль m является составным, т.е. $m = k \cdot l$, где $k > 1, l > 1$. Но тогда $\overline{k} \neq 0, \overline{l} \neq 0$ и $\overline{k} \cdot \overline{l} = \overline{m} = \overline{0}$, что невозможно в поле. Следовательно, m – простое число.

(⇐) Пусть $m = p$ – простое число. Достаточно показать, что каждый отличный от $\bar{0}$ элемент обратим. Пусть $\bar{k} \neq 0$, т. е. $(k, p) = 1$, так как p – простое число. По теореме Эйлера $\bar{k} \cdot \bar{k}^{p-2} = \bar{1}$, т.е. элемент $\bar{k}$ – обратим. ■

1. Мультипликативная группа классов вычетов. В курсе «алгебра» доказывается, что множество K* обратимых элементов ассоциативного кольца K образует относительно умножения в кольце группу, которая называется **мультипликативной группой обратимых элементов кольца.**

Теорема 2.3. Множество классов вычетов по модулю m, взаимно простых с модулем, совпадает с множеством обратимых элементов в кольце классов вычетов по модулю m и образует относительно умножения абелеву группу.

■ Если вычет a взаимно прост с модулем m, то по теореме Эйлера $a^{\varphi(m)} \equiv 1\ (mod\ m)$. Следовательно, $\overline{a} \cdot \overline{a}^{\varphi(m)-1} = \overline{1}$ и класс вычетов $\overline{a}$, взаимно простой с модулем m, всегда обратим.

С другой стороны, если класс $\overline{a}$ обратим в кольце Z_m, то существует класс вычетов $\overline{b}$ такой, что $\overline{a} \cdot \overline{b} = \overline{1}$, т. е. $a \cdot b \equiv 1(mod\ m)$. Откуда следует, что $(a, m) = 1$, т. е. класс $\overline{a}$ взаимно простой с модулем m.

Таким образом множество Z_m^* обратимых элементов кольца Z_m совпадает с множеством классов вычетов, взаимно простых с модулем m. Следовательно, $(Z_m^*, \cdot)$ – является абелевой группой. ■

• Группа $(Z_m^*, \cdot)$ называется **мультипликативной группой классов вычетов, взаимно простых с модулем m.**

Следствие 2.4. Порядок группы Z_m^* равен $\varphi(m)$.

► $Z_8{}^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$.

Таблица умножения в группе Z_8^*:

$\cdot$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{7}$	$\overline{5}$
$\overline{5}$	$\overline{5}$	$\overline{7}$	$\overline{1}$	$\overline{3}$
$\overline{7}$	$\overline{7}$	$\overline{5}$	$\overline{3}$	$\overline{1}$

Замечание. В курсе «алгебра» рассматривается фактор – кольцо $Z/(m)$ кольца целых чисел Z по идеалу $(m) = \{zm|z \in Z\}$, порожденному модулем m:
$Z_{/(m)} = \{(m) + a|a \in Z\}$. ◄

Смежный класс $(m) + a$ по идеалу (m) совпадает с классом вычетов $\bar{a}$, содержащего число a, так как $(m) + a = \{zm + a|z \in Z\} = \bar{a}$.

Следовательно, множества $Z/(m)$ и Z_m равны. Более того, операции сложения и умножения в $Z/(m)$ и Z_m совпадают.

Действительно: $\big((m) + a\big) + \big((m) + b\big) = \big((m) + a + b\big)$ $\Rightarrow \bar{a} + \bar{b} = \overline{a + b}; \big((m) + a\big) \cdot \big((m) + b\big) = \big((m) + ab\big) \Rightarrow \bar{a} \cdot \bar{b} =$ $= \overline{ab}$.

Таким образом, фактор – кольцо $Z/(m)$ и кольцо классов вычетов Z_m изоморфны.

§3. Сравнения с одним неизвестным

1. Сравнения первой степени. Сравнение с неизвестным x, приводимое к виду

$$ax \equiv b \ (mod\ m), \qquad (1)$$

называется **сравнением первой степени с одним неизвестным** по модулю m.

• Число x_0 называется **решением (корнем)** сравнения, если оно ему удовлетворяет: $ax_0 \equiv b\ (mod\ m)$ – верное сравнение.

• **Решить сравнение** – означает найти все его корни или доказать, что оно не имеет корней (неразрешимо).

Заметим, если x_0 – корень сравнения, то все числа $x \equiv x_0\ (mod\ m)$ также являются корнями сравнения. Таким образом, если сравнение разрешимо, то множество его корней бесконечно и является объединением некоторых классов вычетов по модулю m.

• Под **числом решений** сравнения (1) понимают количество всех корней, взятых из полной системы вычетов по модулю m.

Замечание. Число решений сравнения (1) равно числу классов вычетов по модулю m, которые образуют множество всех корней сравнения.

Теорема 3.1. Пусть задано сравнение $ax \equiv b\ (mod\ m)$, где a, b – целые числа и пусть $d = (a, m)$. Тогда:

1) если d не делит b, то сравнение неразрешимо;

2) если $(a, b) = 1$, то сравнение разрешимо и множество его решений образует один класс вычетов по модулю m: $x \equiv a^{\varphi(m)-1}b\ (mod\ m)$;

3) пусть $d = (a, m) > 1$, d делит b и пусть $a = a_1 d, b = = b_1 d, m = m_1 d$. Тогда сравнение разрешимо и равносильно сравнению

$$a_1 x \equiv b_1\ (mod\ m_1). \qquad (2)$$

Если x_0 – корень сравнения (2), то множество корней исходного сравнения распадается на d классов вычетов по модулю m вида:

$$x_1 \equiv x_0 \ (mod\ m), x_2 \equiv x_0 + m_1 (mod\ m), \ldots,$$
$$x_d \equiv x_0 + (d-1)m_1 (mod\ m). \quad (3)$$

■ 1. Пусть $d = (a, m) \nmid b$. Предположим, что существует решение x_0 сравнения. Тогда $b = ax + tm$ для некоторого $t \in Z$, при этом правая часть равенства делится на d, а левая, равная b, не делится на d.

Получили противоречие. Следовательно, сравнение неразрешимо.

2. Пусть *(a, b)* = 1. По теореме Эйлера $a^{\varphi(m)} \equiv 1 \ (mod\ m)$. Умножив обе части исходного сравнения на $a^{\varphi(m)-1}$, получим $a^{\varphi(m)}x \equiv a^{\varphi(m)-1}b \ (mod\ m)$. Откуда следует, что класс вычетов $x \equiv a^{\varphi(m)-1}b \ (mod\ m)$ по модулю m образует всё множество решений сравнения.

3. Пусть $d = (a, b) > 1, d|b, a = a_1 d, b = b_1 d, m = m_1 d$ и $(a_1, m_1) = 1$. Разделив обе части сравнения и модуль на d получим равносильное сравнение

$$a_1 x \equiv b_1 \ (mod\ m_1). \quad (3)$$

По пункту 2 настоящей теоремы множество решений этого сравнения совпадает с классом вычетов $x \equiv a_1^{\varphi(m)-1} \cdot \cdot b_1 \ (mod\ m_1)$.

Пусть x_0 – некоторый вычет из указанного выше класса вычетов. Тогда множество решений сравнения (1) записывается в виде $x = x_0 + tm_1$, где $t \in Z$. Вычеты $x_0 + tm_1$ и $x_0 + sm_1$ сравнимы по модулю m тогда и только тогда, когда $m = m_1 d|(s-t)m_1$, т.е. когда $d|s-t$. Поэтому числа

$$x_0, x_0 + m_1, \ldots, x_0 + (d-1)m_1 \quad (4)$$

лежат в разных классах вычетов по модулю m. Пусть $x = x_0 + tm_1$ – произвольное решение сравнения (1). Разделим с остатком число t на d: $t = qd + r, 0 \le r < d$. Поэтому число $x = x_0 + qdm_1 + rm_1 = x_0 + rm_1 + qm$ сравнимо по модулю m с одним из чисел ряда (4).

Таким образом, множество решений сравнения (1) распадается на d классов вычетов по модулю m:

$$x_1 \equiv x_0 \ (mod\ m), \dots, x_d \equiv x_0 + (d-1)m_1 (mod\ m).$$

Теорема доказана. ■

► Решим сравнение $6x = 9\ (mod\ 33)$.

Р е ш е н и е. Так как $(6,33) \equiv 3$ делит 9, то число решений сравнения равно 3. Разделив обе части сравнения и модуль на 3, получим $2x \equiv 3\ (mod\ 11)$.

Имеем $(2,11) = 1$ и $2^{\varphi(11)} = 2^{10} \equiv 1\ (mod\ 11)$. По пункту 2 теоремы 3.1 получим $x \equiv 2^9 \cdot 3 \equiv 7\ (mod\ 11)$.

О т в е т.

$x_1 \equiv 7\ (mod\ 33), x_2 \equiv 18\ (mod\ 33), x_3 \equiv 29\ (mod\ 33)$. ◄

Наряду с применением теоремы Эйлера – для поиска решений сравнений первой степени – используют также метод, основанный на теории непрерывных дробей.

Пусть дано сравнение $ax \equiv b\ (mod\ m)$, где $(a, m) = 1$. Разложим в непрерывную дробь отношение $\frac{m}{a}$. Пусть $\frac{m}{a} = [q_0;\ q_1, \dots, q_n]$. Согласно свойствам непрерывных дробей имеем $\frac{P_n}{Q_n} = \frac{m}{a}$ и $\begin{vmatrix} P_{n-1} & m \\ Q_{n-1} & a \end{vmatrix} = aP_{n-1} - -m(Q_{n-1}) = (-1)^n$. Умножив это равенство на $(-1)^n b$, получим $a(-1)^n P_{n-1} b + m(-1)^{n+1} Q_{n-1} = b$.

Следовательно, $a(-1)^n\ P_{n-1} b \equiv b\ (mod\ m)$. Таким образом, множество решений сравнения есть класс вычетов $x \equiv \equiv (-1)^n P_{n-1} b\ (mod\ m)$.

Число $(-1)^n P_{n-1}$ можно найти по следующей схеме:

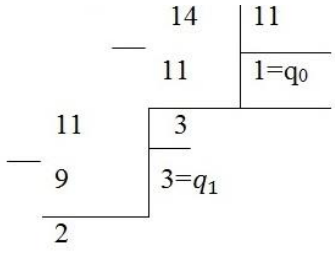
k	–2	–1	0	1	…	n-1	(n)
q_k	–	–	q_0	q_1		q_{n-1}	q_n
P_k	0	1	q_0	P_1	…	P_{n-1}	m

Здесь $P_k = q_k P_{k-1} + P_{k-2}$, $k = \overline{1,n}$.

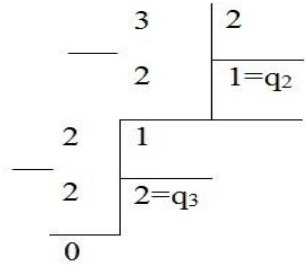
► Решим сравнение $22^x \equiv 6\ (mod\ 28)$.

Р е ш е н и е. $(22,28) = 2$ делит 6. Следовательно, число решений по модулю 28 равно 2. Перейдём к равносильному сравнению $11x \equiv 3\ (mod\ 14)$.

Разложим в непрерывную дробь число $\frac{14}{11}$:



,



.

Следовательно, $\frac{14}{11} = [1; 3, 1, 2]$.

Найдём числители подходящих дробей по схеме:

k	–2	–1	0	1	2	3
q_k	–	–	1	3	1	2
P_k	0	1	1	4	5	14

Таким образом, $n = 3, P_{n-1} = 5$ и множество чисел $x \equiv (-1)^3 \cdot 5 \cdot 3 = -15 \equiv 13\ (mod\ 14)$ совпадает с множеством корней исходного сравнения.

О т в е т. $x_1 \equiv 13\ (mod\ 28)$, $x_2 \equiv 13 + 14 = 27\ (mod\ 28)$. ◄

2. Сравнения высших степеней по простому модулю. Рассмотрим сравнение -й степени по простому модулю вида

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \equiv 0 \ (mod\ p), \qquad (1)$$

где $a_n \not\equiv 0 \ (mod\ p)$ и p – простое число.

• Вычет x_0 называется **решением** сравнения (1), если $f(x_0) \equiv 0 \ (mod\ p)$ является верным сравнением.

Из свойств сравнений следует, если x_0 – решение сравнения (1), то все $x \equiv x_0 \ (mod\ p)$также являются решениями сравнения (бесконечное множество). Этот факт влечет следующее определение.

• Под **числом решений** сравнения (1) понимают число решений из полной системы вычетов по данному модулю p.

Теорема о числе решений 3.2. Число решений сравнения -й степени (1) по простому модулю не превосходит числа n.

■ Доказательство теоремы проведем индукцией по степени n сравнения.

Б.И. $n = 0$. Сравнение (1) имеет вид: $a_0 \equiv 0 \ (mod\ p)$, где $a_0 \not\equiv 0 \ (mod\ p)$.

Это сравнение не имеет решений, т.е. имеет нуль решений, ч.т.д.

П.И. Утверждение справедливо для сравнений степени $< n$, где $n > 0$.

Ш.И. Рассмотрим сравнение (1) n-й степени. Если оно не имеет решений, то утверждение справедливо.

Если, что сравнение (1) имеет решение x_1, то

$$a_n x_1^n + \cdots + a_0 \equiv 0 \ (mod\ p). \qquad (2)$$

Вычтем из сравнения (1) сравнение (2), получим:

$a_n(x^n - x_1^n) + \cdots + a_k\left(x^k - x_1^k\right) + \cdots + a_1(x - x_1) \equiv 0(mod\ p)$. (3)

Учитывая, что $x^k - x_1^k = (x - x_1)\left(x^{k-1} + x^{k-2}x_1 + \cdots + + xx_1^{k-2} + x_1^{k-1}\right)$, преобразуем (3) к виду:

$$(x - x_1)(b_{n-1}x^{n-1} + \cdots + b_0) \equiv 0(mod\ p). \quad (4)$$

Пусть x_2– несравнимое с x_1по модулю p решение сравнения (1), т.е. из сравнения (4) следует:

$(x_2 - x_1)(b_{n-1}x_2^{n-1} + \cdots + b_0) \equiv 0\ (mod\ p)$.

Пусть $g(x) = b_{n-1}x^{n-1} + \cdots + b_0$. Так как по предположению $p \mid x_2 - x_1$и так как p – простое число, то из условия $p|(x_2 - x_1)(b_{n-1}x_2^{n-1} + \cdots + b_0)$ получаем, что $g(x_2) = b_{n-1}x_2^{n-1} + +... + b_0) \equiv 0\ (mod\ p)$,причем степень многочлена $g\ (x)$ равна $n\ - 1$, ибо $b_{\ n-1} =\ a_n$.

Следовательно, любое решение сравнения (1), несравнимое с x_1, является решением сравнения $(n - 1)$ −й степени $g(x) \equiv 0\ (mod\ p)$. По П.И. число решений этого сравнения не превосходит n – 1. Таким образом, число решений сравнений (1) не превосходит n. По принципу математической индукции теорема справедлива для любого $n \in N$.

Следствие 3.3. Если число решений сравнения $a_nx^n + \cdots + a_0 \equiv 0\ (mod\ p)$ больше n, то все его коэффициенты делятся на p.

■ Предположим противное. Тогда существует коэффициент $a_m \not\equiv 0\ (mod\ p)$. Пусть m – наибольший индекс с этим условием. Тогда исходные сравнения равносильно сравнению $a_mx^m + \cdots + a_0 \equiv 0\ (mod\ p), a_m \not\equiv 0\ (p)$, число решений которого по доказанной выше теореме не превосходит m, что противоречит условию. Полученное противоречие доказывает утверждение. ■

Теорема Вильсона 3.4 (критерий простого числа). Натуральное число $m > 1$ является простым тогда и только тогда, когда $(m-1)! + 1 \equiv 0\ (mod\ m)$.

■ (=>) Пусть $m = p$ – простое число. Если $p = 2$, то $(2 - 1)! + 1 \equiv 0\ (mod\ 2)$ является верным сравнением.

Пусть теперь $p > 2$. Рассмотрим сравнение $[(x - -1)\ (x-2)\ldots(x - p + 1)] - [x^{p-1} - 1] \equiv 0\ (mod\ p)$ степени $< p - 1$. Вычеты $1, 2, \ldots, p - 1$ являются решениями этого сравнениями в силу теоремы Ферма. Таким образом, число решений этого сравнения больше его степени. Поэтому по следствию 3.3 его коэффициенты делятся на p, в частности, свободный член, равный $(p-1)! + 1$, ч.т.д.

(<=) Пусть для натурального $m > 1$ верно $(m-1)! + +1 \equiv 0\ (mod\ m)$.

Требуется доказать, что m – простое число. Предположим противное. Тогда существует нетривиальный делитель k числа m, т . е. $1 < k \leq m - 1$ и $k \mid m$. В этом случае по условию k делит $(m-1)!$ и $(m-1)! + 1$, что невозможно.

Полученное противоречие доказывает, что m – простое число. ■

Обобщенная теорема Ферма 3.5. Пусть p – простое число и d – натуральный делитель $p - 1$. Тогда сравнение

$$x^d - 1 \equiv 0\ (mod\ p) \qquad (1)$$

имеет точно d решений в полной системе вычетов по модулю p.

■ Пусть $d > 0, d|p-1$, т. е. $p - 1 = dk$, где $k \in N$. Тогда сравнение x^{p-1}— $1 \equiv 0\ (mod\ p)$ можно записать в виде:

$$x^{p-1} - 1 = \left(x^d - 1\right)\left(x^{d(k-1)} + \cdots + x^d + 1\right) \equiv$$
$$\equiv 0\ (mod\ p). \qquad (2)$$

По следствию из теоремы Ферма сравнение (2) имеет точно $p-1$ решений из некоторой полной системы вычетов. Так как p – простое число, то каждое такое решение должно удовлетворять одному из сравнений: $x^d - 1 \equiv 0\ (mod\ p)$, или $x^{d(k-1)} + \cdots + x^d + 1 \equiv 0\ (mod\ p)$.

По теореме о числе корней по простому модулю следует, что число решений второго сравнения не более $d(k-1) = dk - d = (p-1) - d$. Поэтому первое сравнение должно иметь не менее d решений из данной полной системы вычетов по модулю р. Таким образом, число решений сравнения $x^d - 1 \equiv 0\ (mod\ p)$равно d, ч.т.д. ■

3. Системы сравнений первой степени. Рассматривается **простейшая система** сравнений первой степени одного переменного

$$\begin{cases} x \equiv b_1 (mod\ m_1), \\ x \equiv b_2 (mod\ m_2), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv b_s (mod\ m_s), \end{cases} \qquad (1)$$

где $m_1, m_2, \ldots m_s$ – **попарно взаимно простые** модули.

• **Решением** (корнем) системы (1) называется число x, удовлетворяющее каждому сравнению системы.

• **Решить** систему (1) означает найти все решения системы, если они существуют.

Покажем, что множество решений системы (1) образует класс вычетов по модулю $m = m_1 m_2 \ldots m_s$.

Пусть числа M_k *и* M_k' определяются из условий:

$m_1 m_2 \ldots m_s = M_k m_k, M_k M_k' \equiv 1\ (mod\ m_k), k = 1, 2, \ldots, s$ (2)

и пусть $x_0 = M_1 M_1' b_1 + \ldots + M_k M_k' b_k + \ldots + M_s M_s' b_s$ (3)

Теорема о простейшей системе сравнений 3.6.

1. Простейшая система сравнений первой степени (1) разрешима.

2. Множество решений простейшей системы определяется сравнением

$$x \equiv x_0 \,(mod\, m_1 m_2 \dots m_s)\,. \qquad (4)$$

■ 1. Из определения чисел M_k и M_k' следует, что $M_i \equiv\equiv 0\,(mod\, m_k)$,
если $i \neq k$ и $M_k M_k'^{b_k} \equiv b_k\,(mod\, m_k), k = 1, 2, \dots, s$.
Поэтому

$$x_0 = M_1 M_1' b_1 + \dots + M_k M_k' b_k + \dots + M_s M_s' b_s \equiv b_k\,(mod\, m_k),$$
$$k = 1, 2, \dots, s. \qquad (5)$$

Следовательно, система разрешима, ч.т.д.

2. В силу свойства транзитивности отношения сравнения из (5) следует, что система сравнения (1) равносильна системе

$$\begin{cases} x \equiv x_0\,(mod\, m_1\,), \\ \cdots\cdots\cdots \\ x \equiv x_s\,(mod\, m_s\,). \end{cases} \qquad (6)$$

Число x удовлетворяет системе (6) тогда и только тогда, когда число $x - x_0$ делится на m_k, $k = 1, 2, \dots, s$, т. е. $x - x_0$ кратно НОК [m_1, m_2, …, m_s]. Заметим, что НОК $[m_1, m_2, \dots, m_s] = m_1 m_2 \dots m_s$, так как $m_1, m_2, \dots, m_s$ – попарно взаимно простые модули. Таким образом, число x является решением системы (1) (решением системы (6)) тогда и только тогда, когда число x удовлетворяет сравнению (4), ч.т.д. ■

Следствие 3.7. Если $b_1, b_2, \dots, b_s$ независимо друг от друга пробегают полные системы вычетов попарно взаимно простыми модулям $m_1 m_2 \dots m_s$, соответственно, то x_0 пробегает полную систему вычетов по модулю $m = m_1 m_2 \dots m_s$.

■ Число различных распределений $(b_1, b_2, \ldots, b_s)$ равно $m_1 \cdot m_2 \cdot \ldots \cdot m_s = m$. Различным распределениям соответствуют несравнимые по модулю m значения x_0, так как сравнимые по модулю m числа сравнимы по каждому модулю $m_1, m_2, \ldots, m_s$. Утверждение теперь следует из того, что полная система вычетов по модулю m содержит m вычетов. ■

► Рассмотрим систему с параметрами $b_1, b_2, \ldots, b_s$ $x \equiv b_1 \ (mod\ 4), x \equiv b_2 \ (mod\ 7), x \equiv b_3 \ (mod\ 3)$.

Здесь $4 \cdot 7 \cdot 3 = 21 \cdot 4 = 12 \cdot 7 = 28 \cdot 3$, т.е. $M_1 = 21$, $M_2 = 12$,

$M_3 = 28$. (см. (2)). Имеем $21 \cdot 1 \equiv 1 \ (mod\ 4), 12 \cdot 3 \equiv$ $\equiv 1 \ (mod\ 7), 28 \cdot 1 \equiv 1 \ (mod\ 3)$. Следовательно, $M_1' = 1$, $M_2' = 3, M_3' = 1$.

Поэтому $x_0 = 21 \cdot 1 \cdot b_1 + 12 \cdot 3 b_2 + 28 \cdot 1 \cdot b_3 =$ $= 21b_1 + 36b_2 + + 28b_3$ и множество решений системы можно представить в виде $x \equiv 21b_1 + 36b_2 + 28b_3 \ (mod\ 84)$.

Например, множество решений системы $x \equiv 3 \ (mod\ 4)$, $x \equiv 5 \ (mod\ 7), x \equiv 2 \ (mod\ 3)$ будет $x \equiv 21 \cdot 3 + 36 \cdot 5 +$ $+28 \cdot 2 \equiv 299 \equiv 47 \ (mod\ 84)$.

О т в е т. $x \equiv 47 (mod\ 84)$. ◄

Следствие 3.8. (Теорема об остатках) Если числа $m_1, m_2, \ldots, m_k$ попарно взаимно простые, то для любых чисел $a_1, a_2, \ldots, a_k$ таких, что $0 \le a_j < m_j$ существует (можно найти) такое число b, что остаток от деления b на m_j равен a_j, $j = \overline{1,k}$.

4. **Сравнения высших степеней по составному модулю.** Рассмотрим сравнение

$$f(x) \equiv 0 \ (mod\ m_1 \cdot m_2 \ldots m_k), \qquad (1)$$

где $m_1, m_2, \ldots, m_k$ – *попарно взаимно простые модули.*

• **Решением** сравнения (1) называется число x_0, удовлетворяющее сравнению, т.е. $f\ (x_0)\ \equiv\ 0\ (mod\ m)$ является верным сравнением, где $m = m_1 m_2 \ldots m_k$.

Заметим, если x_0 является решением (1), то числа $x\ \equiv\ x_0\ (mod\ m)$ также являются решениями (1). Следовательно, класс вычетов по модулю m, содержащий x_0, состоит из решений сравнения (1). Таким образом, множество решений (1) является объединением классов вычетов по модулю m.

• **Числом решений** сравнения (1) называется число решений сравнения из некоторой полной системы вычетов по модулю m (число классов вычетов, образующих множество решений).

Предложение 3.9. Сравнение (1) **равносильно** системе сравнений

$$\begin{cases} f(x) \equiv 0\ (mod\ m_1\ ), \\ \ldots\ldots\ldots\ldots \\ f(x) \equiv 0\ (mod\ m_k\ ). \end{cases} \qquad (2)$$

■ Пусть x_0 – решение сравнения (1). Тогда дуль $m\ =\ m_1 m_2 \ldots m_k$ делит число $f(x_0)$. но, $f\ (x_0)\ \equiv\ 0\ (mod\ m_i\ ), i\ =\ 1, 2, \ldots, k$ и x_0 является решением системы (2).

Обратно, пусть x_0 является решением системы (2). Тогда число $f(x_0)$ кратно каждому модулю $m_1, m_2, \ldots, m_k$. Следовательно, $f(x_0)$ кратно НОК$[m_1, m_2, \ldots, m_k]\ =\ m_1 \cdot \cdot\ m_2 \cdot \ldots \cdot\ m_k, f(x) \equiv 0\ (mod\ m_1, m_2, \ldots, m_k)$, ч.т.д. ■

Теорема 3.10. Пусть T_s – число решений отдельного сравнения $f(x) \equiv 0\ (mod\ m_s)$, $s\ =\ 1, 2, \ldots, k$ из системы (2). Тогда число решений сравнения (1) равно $T_1\ \cdot\ T_2 \cdot \ldots \cdot\ T_k$.

■ Пусть число b_s является решением сравнения $f(x) \equiv 0\ (mod\ m_s)$, $s = 1, 2, \ldots, k$. Тогда значения x, удовлетворяющие простейшей системе сравнений

$$\begin{cases} x \equiv b_1\ (mod\ m_1\ ), \\ \quad \ldots\ldots\ldots \\ x \equiv b_s\ (mod\ m_s\ ), \\ \quad \ldots\ldots\ldots \\ x \equiv b_k\ (mod\ m_k\ ), \end{cases} \qquad (3)$$

являются решениями системы (2) и поэтому, в силу предложения, доказанного выше, являются решениями сравнения (1), причем все такие числа образуют класс вычетов по модулю $m_1 \cdot m_2 \ldots m_k = m$.

Так как различным распределениям $(b_1, b_2, \ldots, b_k)$ решений сравнений $f\ (x) \equiv 0\ (mod\ m_s)$ $(s = 1, 2, \ldots, k)$ соответствуют несравнимые по модулю m решения сравнения (1), то число таких решений из фиксированной полной системы вычетов по модулю m равно $T_1 \cdot T_2 \ldots T_k$.

С другой стороны, если x – решение сравнения (1) из фиксированной полной системы вычетов, то x является решением каждого сравнения системы (2). Поэтому $x \equiv b_s\ (mod\ m_s), s = 1, 2, \ldots, k$ для некоторого из учтенных выше распределений $(b_1, b_2, \ldots, b_k)$ решений системы (3). Следовательно, x совпадает с одним из $T_1\ T_2 \ldots T_k$ перечисленных выше решений сравнения (1).

Таким образом, число решений сравнения (1) но $T_1 \cdot T_2 \ldots T_k$. ■

► Сравнение $x^2 - 1 \equiv 0\ (mod\ 84)$, где $m = 84 = 4 \cdot 7 \cdot 3$ равносильно системе сравнений $x^2 - 1 \equiv 0\ (mod\ 4), x^2 - 1 \equiv$ $\equiv 0\ (mod\ 7), x^2 - 1 \equiv 0\ (mod\ 3)$.

Решениями этих сравнений являются, соответственно, $b_1 \in \{1,3\}, b_2 \in \{1,6\}, b_3 \in \{1,2\}$. Решения системы можно записать (см. пример в 5.8) в виде

$$x \equiv 21b_1 + 36b_2 + 28b_3 \ (mod\ 84). \qquad (*)$$

Число решений сравнения равно $2 \cdot 2 \cdot 2 = 8$.

Подставив распределения: (1, 1, 1), (1, 1, 2), (1, 6, 1), (1, 6, 2), (3, 1, 1), (3, 1, 2), (3, 6, 1), (3, 6, 2) в (*) получим решения системы.

О т в е т. $x_1 \equiv 1, x_3 \equiv 13, x_5 \equiv 43, x_7 \equiv 55$, $x_2 \equiv 29$, $x_4 \equiv 41$, $x_6 \equiv 71, x_8 \equiv 83\ (mod\ 84)$. ◄

§4. Первообразные корни и индексы

1. Порядок числа. Показателем (порядком) вычета a по модулю m называется н а и м е н ь ш е е н а т у р а л ь н о е ч и с л о δ такое, при котором $a^{\delta} \equiv 1(mod\ m)$, обозначается $\delta = O\ (a\ mod\ m)$ или $\delta = |a|$.

Предложение 4.1. 1. Целое число имеет порядок по модулю m тогда и только тогда, когда оно взаимно просто с модулем m.

2. Сравнимые по модулю m числа имеют равные порядки.

■ 1. Пусть a – вычет и $(a, m) = 1$. По теореме Эйлера $a^{\varphi(m)} \equiv 1\ (mod\ m)$. Следовательно, вычет a имеют порядок, ч.т.д.

Обратно, пусть вычет a имеет порядок δ. Тогда существует число k, такое, при котором $1 = a^{\delta} + k \cdot m = a \cdot \cdot a^{\delta-1} + m \cdot k$.

По критерию НОД следует, что $(a, m) = 1$, ч.т.д.

2. Пусть $(a, m) = 1$ и $a \equiv b\ (mod\ m)$. Из $(a, m) = 1$ следует, что число a имеет порядок. Так как для любого натурального n имеем: $a^n \equiv b^n\ (mod\ m)$, то $0\ (a\ mod\ m) = 0\ (b\ mod\ m)$, ч.т.д. ■

Таким образом все вычеты из одного класса вычетов по модулю имеют равные порядки. Поэтому следующее определение корректно.

• ***Порядком класса вычетов*** *называется порядок вычетов, содержащихся в нем.*

Свойства порядка

Пусть порядок вычета a по модулю m равен δ.

СВОЙСТВО 4.1. Числа $a, a^2, \ldots, a^\delta$ попарно несравнимы по модулю m.

СВОЙСТВО 4.2. Если n – натуральное число, то $a^n \equiv 1(mod\ m)$ тогда и только тогда, когда n делится на δ, т.е. $n \equiv 0(mod\ \delta)$.

СВОЙСТВО 4.3. Если s, k – натуральное число, то $a^k \equiv a^s(mod\ m)$ тогда и только тогда, когда $k \equiv s(mod\ \delta)$.

СВОЙСТВО 4.4. Если $|a| = \delta$ и $(k, \delta) = d$, то $|a^k| = \frac{\delta}{(\delta,k)}$.

СВОЙСТВО 4.5. Если натуральное число k делит $\delta = |a|$, то $\theta(a^k mod\ m) = \delta | k$.

СВОЙСТВО 4.6. Если $(k, \delta) = 1$, то $O(a^k mod\ m) = \delta$.

■ **1.** Пусть $a^k \equiv a^s(mod\ m)$, где $0 < s \leq k \leq \delta$. Так как $(a, m) = 1$, то обе части сравнения можно сократить на a^s. Получим $a^{k-s} \equiv 1\ (mod\ m)$, где $0 \leq k - s < \delta$. В силу определения порядка вычета получаем $k - s = 0$ и $k = s$, ч.т.д.

2. Пусть $a^t \equiv 1\ (mod\ m)$ для некоторого $t \in N$. Разделим число t на δ с остатком: $t = k\delta + r$, где $0 \leq r < \delta$.

Имеем: $a^t = a^{k\delta+r} = (a^t)^k \cdot a^r \equiv a^r \equiv 1\,(mod\ m)$.

В силу определения порядка следует, что $r = 0$ и $\delta | t$, ч.т.д.

3. Пусть $k \geq s$ и $a^k \equiv a^s\,(mod\ m)$. Так как $(a, m) = 1$, то $a^{k-s} \equiv 1\,(mod\ m)$ и по свойству 2 получаем $k - s \equiv 0\,(mod\ \delta)$, т.е. $k \equiv s\,(mod\ \delta)$, ч.т.д.

Обратно, если $k \equiv s\,(mod\ \delta)$, то существует число $q \in Z$ такое, что $k = s + q \cdot \delta$ и $a^k = a^s \cdot (a^\delta)^q \equiv a^s\,(mod\ m)$, ч.т.д.

4. Пусть $d = (k, \delta), k = k_1 d, \delta = \delta_1 d, (k_1, \delta_1) = 1$ и пусть $t = O\left(a^k\ mod\ m\right)$. Тогда по определению порядка вычета a^k имеем $a^{kt} \equiv 1\,(mod\ m)$.

По свойству 4.2 $\delta = \delta_1 d | kt = k_1 dt$. Следовательно, $\delta_1 |\, k_1 t$.

Так как $(\delta_1, k_1) = 1$, то $\delta_1 | t$.

С другой стороны, $a^{k\delta_1} = a^{k_1 d \delta_1} = (a^\delta)^{k_1} \equiv 1\,(mod\ m)$, и по свойству 4.2 для вычета a^k получаем $t | \delta_1$.

Так как $\delta_1 | t$ и $t | \delta_1$, то $t = \delta_1$. Следовательно, $t = \frac{\delta}{d} =$ $= \frac{\delta}{(k,\delta)}$, ч.т.д.

5. Пусть $k | \delta$. Тогда $(k, \delta) = k$ и по свойству 4.4 имеем $O\,(a^k\ mod\ m) = \frac{\delta}{(k,\delta)} = \frac{\delta}{k}$, ч.т.д.

6. Если $(k, \delta) = 1$, то по свойству 1.4 получаем $O\left(a^k\ mod\ m\right) = \frac{\delta}{(k,\delta)} = \delta$, ч.т.д. ■

Предложение 4.2. Если порядки двух чисел по модулю m – взаимно простые числа, то порядок произведения вычетов равен произведению порядков этих чисел: $\forall\, a, b \in Z\ \left((O(a\ mod\ m), O(b\ mod\ m)\right) = 1 \rightarrow O\,(ab\ mod\ m) =$ $= O\,(a\ mod\ m) \cdot O\,(b\ mod\ m))$.

■ Пусть $\delta = O\ (a\ mod\ m), t = O\ (b\ mod\ m)$ и $(\delta, t) = 1$.

Тогда $(ab)^{\delta t} = (a^{\delta})^{t} \cdot (b^{t})^{\delta} \equiv 1\ (mod\ m)$. Следовательно,

$n = O\ (ab\ mod\ m) | \delta t.$ (3)

С другой стороны, из $(ab)^{n} \equiv 1\ (mod\ m)$ следует

$$(ab)^{n\delta} = (a^{\delta})^{n}\, b^{n\delta} \equiv b^{n\delta} \equiv 1\ (mod\ m).$$

Поэтому по свойству 4.2 следует, что $t | n\delta$. Так как по условию

$$(t, \delta) = 1, \text{то } t | n.$$

Аналогично доказывается, что $\delta | n$. Опять в силу взаимной простоты t и δ следует, что $t\delta | n$. (4)

Из (1) и (2) получаем $n = t\delta$, ч.т.д. ■

Индукцией доказывается следующее

Следствие 4.3. Пусть порядки $\delta_1, \delta_2, \ldots, \delta_n$ чисел $a_1, a_2, \ldots, a_n$, соответственно, попарно взаимно простые числа. Тогда порядок произведения $a_1 \cdot a_2 \ldots a_n$ этих чисел равен произведению $\delta_1 \cdot \delta_2 \cdot \ldots \cdot \delta_n$ их порядков.

► Найдем остаток от деления 44^{2355} на 14.

Р е ш е н и е. Требуется найти число x такое, при которых $0 \le x < 14$ и

$44^{2355} \equiv x(mod\ 14)$. Так как $(44,14) = 2 | x$, то $x \equiv 2y$ и

$44 \cdot 44^{2354} \equiv 2y(mod\ 14), 22 \cdot 44^{2354} \equiv y(mod\ 7).$

а) уменьшим основание степени по модулю 7:

$22 \equiv 1(mod\ 7), 44 \equiv 2(mod\ 7)$. Следовательно, $2^{2354} \equiv y(mod\ 7)$.

б) уменьшим показатель степени. Так как $\varphi(7) = 6$ и $(2,7) = 1$, то $2^{6} \equiv 1(mod\ 7)$. Разделим с остатком 2354 на 6: $2354 = 6 \cdot 392 + 2$. Следовательно, $2^{2354} = (2^{6})^{392} \cdot 2^{2} \equiv$ $\equiv 2^{2}(mod\ 7), y = 4.$

О т в е т. $x = 8$. ◄

2. Первообразные корни по простому модулю. Исследуем числа, имеющие наибольший порядок по простому модулю.

Теорема 4.4. Пусть $p > 2$ – простое число и d – натуральный делитель числа $p - 1$. В приведенной системе вычетов по модулю p существует точно $\varphi(d)$вычетов, имеющих порядок d.

■ Пусть B – приведенная система вычетов по модулю p и пусть d – натуральный делитель $p - 1$. Обозначим через $\psi(d)$ число вычетов из B, порядок которых равен d.

Предположим, что в B существует элемент a порядка d, тогда элементы $a, a^2, \ldots, a^d$ попарно несравнимы по модулю p и являются решениями сравнения $x^d \equiv 1(mod\ p)$. По обобщенной теореме Ферма других решений в B нет. Поэтому все числа порядка d должны быть сравнимы с вычетами из множества $M = \{a, a^2, \ldots, a^d\}$. По свойству 4.6 число a^k имеет порядок d тогда и только тогда, когда $(k, d) = 1$. Отсюда следует, что $\psi(d) = \varphi(d)$.

Таким образом, для любого делителя d числа $p - 1$ имеем

$$\psi(d) = \begin{cases} \varphi\,(d), \text{если в } B \text{ есть элементы порядка } d, \\ 0, \text{если нет элементов порядка } d. \end{cases}$$

Так как каждое число, не кратное p в силу теоремы Эйлера, имеет порядок, который делит $p - 1$, то

$$\sum_{1 \le d|p-1} \Psi\,(d) = p - 1. \qquad (1)$$

С другой стороны, по лемме Гаусса:

$$\sum_{1 \le d|p-1} \varphi\,(d) = p - 1. \qquad (2)$$

Вычтем из равенства (2) равенство (1):

$$\sum_{1 \le d|p-1} \big((\varphi(d) - \Psi(d)\big) = 0. \qquad (3)$$

Так как $\varphi(d) - \psi(d) \geq 0$, то из (3) следует, что $\varphi(d) = \psi(d)$ для любого натурального делителя d числа $p - 1$, что доказывает теорему. ■

• Вычет x называется **первообразным корнем** по модулю m, если $O(a \bmod m) = \varphi(m)$.

Следствие 4.5. Для любого простого числа p, существует первообразный корень по модулю p, причем число первообразных в приведенной системе вычетов по модулю p равно $\varphi(p - 1)$.

В общем случае имеет место следующая теорема.

Теорема о первообразных 4.6. Первообразные корни существуют только лишь для модулей $m = 2, 4, p^k, 2p^k$, где p – простое нечетное число.

Доказательство можно найти в [1].

3. Индексы по простому модулю. Понятие индекса во многом аналогично понятию логарифма и индексы используются при решении показательных и степенных сравнений.

Пусть p – простое число и пусть β – **первообразный корень** по модулю p: $O\ (\beta\ mod\ p)\ =\ p\ -\ 1$.

Из свойств порядка вычетов следует, что числа

$$\beta^1, \ldots, \beta^{p-1} \qquad (1)$$

образуют приведенную систему вычетов.

Поэтому любое число $a \in Z$, взаимно простое с модулем p, сравнимо с одной и только одной степенью из ряда (1), т. е. существует единственное число $k \in \{1, \ldots, p - 1\}$ такое, что

$$a \equiv \beta^k\ (mod\ p). \qquad (2)$$

• **Индексом числа a по модулю простого числа p при основании β** называется число k такое, что

$$a \equiv \beta^k \ (mod\ p), \qquad (3)$$

обозначается $k = ind_\beta a$ или $k = ind\ a$.

Таким образом, по определению индекса имеем

$$\beta^{ind_\beta a} \equiv a \ (mod\ p). \qquad (4)$$

Сравните с основным тождеством для логарифмов $\beta^{log_\beta a} = a$.

►Число $37 \equiv 2 \equiv 5^4 \ (mod\ 7)$. Следовательно, $ind_5\ 37 = 4$ по модулю 7.

Здесь число 5 является первообразным корнем по модулю 7. ◄

Свойства индексов

В основе свойств индексов лежит основное свойство порядка числа по простому модулю p:

если $O(\beta\ mod\ p) = p - 1$, то $\beta^k \equiv \beta^s \ (mod\ p) <=> k \equiv s \ (mod\ p - 1)$.

СВОЙСТВО 1. Индексы числа сравнимы между собой по модулю $p - 1$.

■ Пусть k, s – индексы числа a по модулю p при основании β, т. е. $a \equiv \beta^k \ (mod\ p)$ и $a \equiv \beta^s \ (mod\ p)$. Следовательно, $\beta^k \equiv \beta^s \ (mod\ p)$ и $k \equiv s \ (mod\ p - 1)$, ч.т.д. ■

Аналогично доказывается следующее свойство.

СВОЙСТВО 2. $ind\ (a_1 a_2 \dots a_n) \equiv ind\ a_1 + \dots + ind\ a_n \ (mod\ p - 1)$.

■ По определению индекса справедливы сравнения $\beta^{ind\ \alpha_1} \equiv a_1 (mod\ p), \beta^{ind\ \alpha_2} \equiv a_2 (mod\ p), \dots, \beta^{ind\ \alpha_n} \equiv a_n (mod\ p)$.

Перемножив почленно сравнения, получим $\beta^{ind\ \alpha_1 + \dots + ind\ \alpha_n} \equiv a_1 a_2 \dots a_n (mod\ p)$.

Так как по определению индекса имеем $a_1 a_2 \dots a_n \equiv$ $\equiv \beta^{ind\,(a_1 a_2 \dots a_n)} (mod\ p)$, то по свойству 1 следует $ind\ (a_1 a_2 \dots a_n) \equiv und\ a_1 + \dots + ind\ a_n (mod\ p-1)$. ■

СВОЙСТВО 3. $ind\ a^n \equiv n\ ind\ a (mod\ p-1)$ для любого $n \in N$.

■ Утверждение вытекает из свойства 2 при $a_1 = a_2 =$ $= \dots = a_n = a$. ■

Замечание. Использование свойств 1–3 называется **индексированием**.

►Пусть $p = 13$. Число 2 является первообразным корнем по модулю $p = 13$, так как справедливы следующие сравнения:

$$\begin{array}{lll} 2^1 \equiv 2, & 2^5 \equiv 6, & 2^9 \equiv 5, \\ 2^2 \equiv 4, & 2^6 \equiv 12, & 2^{10} \equiv 10, \\ 2^3 \equiv 8, & 2^7 \equiv 11, & 2^{11} \equiv 7, \\ 2^4 \equiv 3, & 2^8 \equiv 9, & 2^{12} \equiv 1. \end{array} \qquad (mod\ 13).$$

Составим **таблицу индексов** по модулю 13:

N	0	1	2	3	4	5	6	7	8	9
0	–	0	1	4	2	9	5	11	3	8
1	10	7	6							

Здесь цифра *i* строки означает число десятков; цифра *j* столбца означает число единиц. На пересечении *i*-ой строки и *j*-го столбца находится $ind\ \overline{ij}$ числа $\overline{ij} = N$. Например, индекс числа 11, равный 7, лежит в строке с номером 1 и столбце с номером 1; индекс числа 8, равный 3, лежит в строке 0 и столбце с номером 8.

По таблице индексов можно построить таблицу **антииндексов**, которая по индексу i восстанавливает число N: $ind\ N = i$.

i	0	1	2	3	4	5	6	7	8
0	1	2	4	8	3	6	12	11	9
1	10	7							

4. Решение двучленных сравнений с помощью индексов. Рассмотрим двучленные сравнения с одним неизвестным по простому модулю.

а) Степенные сравнения. Требуется решить сравнение вида

$ax^n \equiv b \ (mod\ p)$, где $(a, p) = 1$, p – простое число.

Р е ш е н и е. Индексируя сравнение, переходим к равносильному сравнению по модулю $p - 1$:

$$ind\ a + n\ ind\ x \equiv ind\ b\ (mod\ p - 1). \qquad (5)$$

Полагая $y = ind\ x$ и подставляя значения индексов из таблицы индексов по модулю p, приходим к сравнению вида $ny \equiv c\ (mod\ p)$. (6)

Пусть $y_1, y_2, \ldots, y_s$ – решения сравнения (6) из наименьшей положительной ПСВ по модулю p. По таблице антииндексов находим числа $a_1, a_2, \ldots a_s$ такие, что $ind\ a_1 = y_1, \ldots ind\ a_s = y_s$.

О т в е т. $x_1 \equiv a_1\ (mod\ p), x_2 \equiv a_2\ (mod\ p), \ldots, x_s \equiv$ $\equiv a_s\ (mod\ p)$.

Замечание. Решения степенных сравнений даются по модулю p.

► Решить сравнение $8 \cdot x^4 \equiv 7\ (mod\ 13)$.

Р е ш е н и е. Индексируя сравнение, получим $ind\ 8 + + 4\ ind\ x \equiv ind\ 7\ (mod\ 12)$.

Полагая $y = ind\ x$ и подставляя значения индексов из таблицы индексов по модулю 13, получим:

$$3 + 4\,y \equiv 11\ (mod\ 12),$$
$$4\,y \equiv 8\ (mod\ 12).$$

Так как $(4, 12) = 4|8$, то число решений равно 4. Разделив обе части сравнения и модуль на 4, получим $y \equiv 2\ (mod\ 3)$.

Отсюда $ind\ x_1 \equiv 2\ (mod\ 12), ind\ x_2 \equiv 5\ (mod\ 12), ind\ x_3 \equiv$ $\equiv 8\ (mod\ 12), indx_4 \equiv 11\ (mod\ 12)$.

По таблице антииндексов находим решения исходного сравнения.

О т в е т. $x_1 \equiv 4(\ mod\ 13), x_2 \equiv 6\ (mod\ 13), x_3 \equiv$ $\equiv 9\ (mod\ 13), x_4 \equiv 7\ (mod\ 13)$.

б) Показательные сравнения. Требуется решить сравнение вида

$$a\ b^x \equiv c\ (mod\ p), \text{где } (a, p) = (b, p) = 1.$$

Р е ш е н и е. Индексируя сравнение, получим

$$ind\ a + x\ ind\ b \equiv ind\ c\ (mod\ p - 1).$$

Подставляя значения индексов из таблицы индексов по модулю p, приводим сравнения к виду $A\ x \equiv B\ (mod\ p - 1)$.

Решая это сравнение первой степени, находим **решения исходного сравнения по модулю $m = p - 1$**.

Замечание. Решения показательных сравнений дают по модулю $p - 1$.

► Решим сравнение $8 \cdot 10^x \equiv 7\ (mod\ 13)$.

Р е ш е н и е. Индексируя сравнение, получим

$$ind\ 8 + x\ ind\ 10 \equiv ind\ 7\ (mod\ 12).$$

Подставим значения индексов:

$3 + 10\ x \equiv 11\ (mod\ 12)$. Откуда $10\ x \equiv 8\ (mod\ 12)$.

Так как $(10, 12) = 2|8$, то число решений равно 2. Разделив обе части сравнения и модуль на 2, получим: $5\ x \equiv 4\ (mod\ 6)$.

Методом проб находим $x \equiv 2\ (mod\ 6)$.

О т в е т. $x_1 \equiv 2\ (mod\ 12), x_2 \equiv 8\ (mod\ 12)$. ◄

§5. Арифметические приложения теории сравнений

1. Признаки делимости. Рассмотрим общий признак делимости целых чисел в терминах сравнений, восходящий к французскому математику Пьеру Паскалю (1623–1662).

Теорема 5.1 (общий признак делимости Паскаля). Для того, чтобы натуральное число Q, представленное в произвольной q -ичной системе счисления в виде

$$Q = a_n q^n + a_{n-1} q^{n-1} + \cdots + a_1 q + a_0 = (a_n a_{n-1} \ldots a_1 a_0)_q \quad (1)$$

делилось на число m, необходимо и достаточно, чтобы на m делилось число $T = a_n r_n + a_{n-1} r_{n-1} + \cdots + a_0$, где r_i – абсолютно наименьшие вычеты соответствующих степеней q^i по модулю m, $i = 1, 2, \ldots, n$.

■ Имеем $r_i \equiv q^i (mod\ m)$, $i = 1, 2, \ldots, n$. Поэтому в силу свойств сравнений $Q = a_n q^n + a_{n-1} q^{n-1} + \cdots + a_1 q + a_0 \equiv T = = a_n r_n + a_{n-1} r_{n-1} + + \cdots + a_0 (mod\ m)$. Следовательно, $Q \equiv 0 (mod\ m)$ тогда и только тогда, когда $T \equiv 0 (mod\ m)$. ■

Следствие 5.2. Пусть натуральное число m делит $q - 1$. Тогда для того, чтобы число, записанное в -ичной системе счисления, делилось на m, необходимо и достаточно, чтобы на m делилась сумма его цифр.

■ По условию $q^i \equiv r_i = 1 (mod\ m)$, $i = 1, 2, \ldots, n$. По критерию Паскаля, число $Q = (a_n a_{n-1} \ldots a_1 a_0)_q$ делится на m тогда и только тогда, когда на m делится число $T = a_n + + a_{n-1} + \cdots + a_0$. ■

► ***Признак делимости на 3 и 9***.

Пусть q =10. Тогда $m = 3; 9 | 10 - 1$. Следовательно, по следствию 5.2 число $Q = (a_n a_{n-1} \ldots a_1 a_0)_{10}$ делится на 3 или 9 тогда и только тогда, когда на 3 или 9, соответственно, делится число $T = a_n + a_{n-1} + \cdots + a_0$:

«Целое число, записанное в 10-ичной системе счисления, делится на 3 или 9 тогда и только тогда, когда на 3 или 9, соответственно, делится сумма его цифр». ◄

Следствие 5.3. Пусть натуральное число m делит $q+1$. Тогда для того, чтобы число, записанное в -ичной системе счисления, делилось на m, необходимо и достаточно, чтобы на m делилась разность между суммами цифр на чётных и нечётных местах:

$\forall m, q, Q \in N\big(m|\,(q+1) \to \big(m|Q = (a_n a_{n-1} \dots a_1 a_0)_q \leftrightarrow$

$\leftrightarrow m|((a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots))\big)$.

■ По условию $q \equiv -1(mod\ m)$. Следовательно, $q^i \equiv\equiv (-1)^i = r_i(mod\ m)$.

В этом случае $T = a_n(-1)^n + a_{n-1}(-1)^{n-1} + \cdots a_1(-1) + + a_0 = (a_0 + a_2 + a_4 + \cdots) - (a_1 + a_3 + \cdots)$ и по критерию Паскаля $m|Q \Leftrightarrow m|T$, ч.т.д. ■

► ***Признак делимости на 11***.

Пусть число Q записано в 10-ичной системе, т.е. $Q = a_n a_{n-1} \dots a_1 a_0$. Имеем 11|10+1, т.е. $10 \equiv -1(mod\ 11)$ и $r_i \equiv (-1)^i$. По следствию 5.3 число Q делится на 11 тогда и только тогда, когда на 11 делится $T = (a_0 + a_2 + a_4 + + \cdots) - (a_1 + a_3 + \cdots)$. ◄

«Число, записанное в 10-ичной системе счисления, делится на 11 тогда и только тогда, когда на 11 делится разность между суммой цифр на чётных местах и суммой цифр на нечётных местах».

Следствие 5.4. Пусть натуральное число m делит q^k, где k – наименьшее натуральное с этим условием. Тогда, чтобы число, записанное в -ичной системе счисления, делилось на m, необходимо и достаточно, чтобы число, записанное последними k цифрами данного числа, делилось на m.

■ По условию $q^k \equiv 0(mod\ m)$. Следовательно, $q^i \equiv 0(mod\ m)$, в случае $i \geq k$. Поэтому $Q = a_n q^n + \cdots + a_k q^k + + a_{k-1} q^{k-1} + \cdots + a_1 q + a_0 = a_{k-1} q^{k-1} + \cdots + a_1 q + a_0 (mod\ m)$ и Q делится на m тогда и только тогда, когда на m делится число $a_{k-1} q^{k-1} + \ \ldots + a_1 q + a_0 = (a_{k-1} a_{k-2} \ldots a_1 a_0)_q$. ■

► ***Признаки делимости на 2, 5, 10***.

«Число, записанное в 10-ичной системе счисления, делится на 2, или на 5, или на 10 тогда и только тогда, когда последняя цифра, делится на 2, или на 5, или на 10».

►***Признаки делимости на 4, 25, 50, 100***.

Так как 10^2 делится на 4, 25, 50, 100, то, применяя следствие 5.4, получаем соответствующие признаки делимости на эти числа.

«Натуральное число, записанное в 10-ичной системе счисления, делится на 4, 25, 50 и 100 тогда и только тогда, когда число записанное двумя последними цифрами числа, делится на соответствующее число».

►***Признаки делимости на 7, 11, 13***.

«Для того, чтобы число, записанное в 10-ичной системе счисления, делилось на 7, или на 11, или на 13, необходимо и достаточно, чтобы *разность* между числом, записанным последними тремя цифрами, и числом, записанным остальными цифрами данного числа, делилось на 7, или на 11, или 13».

■ Пусть число $Q = a_n a_{n-1} \ldots a_3 a_2 a_1 a_0$, $N = a_n a_{n-1} \ldots a_3$, $M = a_2 a_1 a_0$.

Запишем Q в виде: $Q = 1000 \cdot N + M = 1000 \cdot N + N + (M - N) \equiv 1001 \cdot N + (M - N)$.

Так как $7 \cdot 11 \cdot 13 = 1001$, то $Q \equiv M - N (mod\ 7 \cdot 11 \cdot 13)$. Следовательно, число Q делится на 7, или на 11, или на 13 тогда и только тогда, когда разность $M - N$ делится на 7, или на 11, или на 13. ■

Число 984841 делится на $11 \cdot 13$, так как число $M - N = 841 - 984 = -143$ делится на $11 \cdot 13$. ◄

2. Систематические дроби. Пусть α – положительное вещественное число. Тогда $a=[\alpha]+\{\alpha\}= Q+ r$, где $Q= [\alpha]$ – целая часть числа, $r= \{\alpha\}$ – дробная часть числа и $0 \le r < 1$.

В курсе «числовые системы» доказывается, что вещественное число $0 \le r < 1$ можно представить в виде суммы ряда

$$r=\frac{a_1}{q}+\frac{a_2}{q^2}+ \dots +\frac{a_k}{q^k} +\dots=\sum_{k=1}^{\infty} \frac{a_k}{q^k}, \text{ где } q>1,\ 0 \le a_k < q_k. \qquad (1)$$

Ряд (1) всегда сходится, так как для любого натурального k справедливо неравенство $\frac{a_k}{q^k} < \frac{1}{q^{k-1}}$ и, следовательно, ряд (1) ограничен суммой убывающей геометрической прогрессии $1 + \frac{1}{q} +\dots+\frac{1}{q^{k-1}}+ \dots =\sum_{k-1}^{\infty} \frac{1}{q^{k-1}} = \frac{q}{q-1}$ со знаменателем $\frac{1}{q} < 1$.

В дальнейшем будем использовать следующую формулу суммы убывающей геометрической прогрессии: $1+ \frac{1}{q^n} +\frac{1}{(q^n)^2} +\dots+\frac{1}{(q^n)^k} +\dots= \sum_{k=0}^{\infty} \frac{1}{(q^n)^k} = \frac{q^n}{q^n-1}$, где $q > 1$.

• Ряд (1) будем записывать в виде

$$r = (0, a_1 a_2 \dots a_{n\dots})_q \qquad (2)$$

и называть **систематической дробью по основанию q (q-ичной систематической дробью)**.

Пусть элементы множества $\{0, 1, 2, \dots, q-1\}$ обозначены определенными символами (цифрами). Тогда представление числа в виде (2) называется **записью систематической дроби в -ичной системе счисления.**

В дальнейшем будем рассматривать только обыкновенные дроби, так как представление целых чисел в -ичной системе счисления изучалось в §7 главы I. Поэтому ограничимся случаем, когда число α – правильная несократимая положительная дробь, т. е. $\alpha = \frac{a}{b}$, $a, b \in$ N, $(a, b) = 1$ и $0 < \frac{a}{b} < 1$.

• Систематическая -ичная дробь называется **конечной**, если она содержит конечное число цифр, которая записывается в виде $(0, a_1 \dots a_m)_q$, где a_m – последняя по порядку цифра, отличная от нуля (q-ичная дробь длины m).

Теорема 5.5. Правильная несократимая дробь $\frac{a}{b}$ представима в виде *конечной -ичной дроби* тогда и только тогда, когда любое простое число, которое делит знаменатель b, делит и основание q счисления. При этом длина -ичной дроби равна наименьшему натуральному m такому, что $b \mid q^m$.

■ (⇒) Пусть $\frac{a}{b} = (0, a_1 \dots a_m)_q$ – конечная -ичная дробь, причём $a_m \neq 0$. По определению -ичной дроби имеем $\frac{a}{b} = \frac{a_1}{q} + \frac{a_2}{q^2} + \dots + \frac{a_m}{q^m} = \frac{a_1 q^{m-1} + a_2 q^{m-2} + \dots + a_m}{q^m} = \frac{c}{q^m}$. Откуда $aq^m = cb$.

Так как $(a, b) = 1$, то $b \mid q^m$ и поэтому каждое простое число, которое делит b, делит и основание q, ч.т.д.

(⇐) Пусть $\frac{a}{b}$ – правильная несократимая дробь и для любого простого числа p, если $p \mid b$ следует $p \mid q$. В этом случае существует натуральное m такое, что $b \mid q^m$ и пусть m – наименьшее натуральное с этим условием. Так как $b \mid q^m$, то существует $c \in Z$ такое, что $q^m = bc$ и $\frac{a}{b} = \frac{aq^m}{bq^m} = \frac{ac}{q^m} < 1$. Следовательно, для некоторых $a_1, \dots, a_m \in Z$ будет $ac = a_1 q^{m-1} + a_2 q^{m-2} + \dots + a_m$, так как $ac < q^m$. Но тогда

дробь $\frac{a}{b} = \frac{a_1 q^{m-1} + a_2 q^{m-2} + \cdots + a_m}{q^m} = \frac{a_1}{q} + \frac{a_2}{q^2} + \ldots + \frac{a_m}{q^m} = (0, a_1 \ldots a_m)_q$, ч.т.д.

Заметим, что $a_m \neq 0$, ибо в противном случае $b \mid q^{m-1}$, что противоречит условию выбора m. ■

► 1. Представим в виде десятичной дроби числа: а) $\frac{3}{4}$, б) $\frac{7}{40}$.

Р е ш е н и е. а) Имеем $4 \mid 10^2$ и $\frac{3}{4} = \frac{3 \cdot 10^2}{4 \cdot 10^2} = \frac{3 \cdot 25}{10^2} = \frac{75}{100} =$ 0,75.

б) Так как $40 = 2^3 \cdot 5 \mid 10^3$, то умножим и разделим дробь $\frac{7}{40}$ на $10^3 : \frac{7}{40} = \frac{7 \cdot 10^3}{40 \cdot 10^3} = \frac{7 \cdot 25}{10^3} = \frac{175}{1000} = 0{,}175$.

2. Представим в виде 12-ичной дроби числа а) $\frac{5}{6}$ и б) $\frac{3}{8}$.

Р е ш е н и е. а) 6 делит q=12. Поэтому дробь $\frac{5}{6}$ умножаем и делим на 12: $\frac{5}{6} = \frac{5 \cdot 12}{6 \cdot 12} = \frac{10}{12} = (0, \mathrm{A})_{12}$ – конечная 12-ичная дробь длины 1, цифра А обозначает число 10.

б) $8 \mid 12^2$ и $\frac{3}{8} = \frac{3 \cdot 12^2}{8 \cdot 12^2} = \frac{3 \cdot 18}{12^2} = \frac{4 \cdot 12 + 6}{12^2} = (0, \overline{4}\overline{6})_{12}$. Здесь $\overline{4}, \overline{6}$ – цифры 12-ичной системы счисления и число $\frac{3}{8}$ представимо в виде конечной 12-ичной дроби длины 2. ◄

Чистой периодической q-ичной дробью с периодом s называется q-ичная дробь $(0, a_1 a_2 \ldots a_n \ldots)_q$, где для каждого $k \in N$ выполняется равенство $a_{s+k} = a_k$, которое сокращённо записывается в виде $0,(a_1 a_2 \ldots a_s)_q$. Причем s – наименьшее натуральное число с этим условием.

Например, $\frac{1}{3} = 0{,}33\ldots = 0,(3)_{10}$; $\frac{7}{11} = 0,(63)_{10}$. Равенства проверяются «делением уголком».

► Представим в виде обыкновенной дроби десятичную периодическую дробь 0,(30).

Р е ш е н и е. По определению десятичной дроби имеем $0,(30) = \frac{3}{10} + \frac{3}{10^3} + \frac{3}{10^5} + \ldots = \frac{3}{10} \cdot \left(1 + \frac{1}{10^2} + + \frac{1}{10^4} + \ldots\right) = \frac{3}{10} \cdot\cdot \frac{10^2}{10^2-1} = \frac{3 \cdot 10}{99} = = \frac{10}{33}$.

О т в е т. $(0,30) = \frac{10}{33}$. ◄

Предложение 5.6. Справедливо следующее тождество

$$0, (a_1 a_2 \ldots a_s)_q = \frac{a_1 q^{s-1} + a_2 q^{s-2} + \cdots + a_s}{q^s - 1}. \qquad (3)$$

■ По определению чистой периодической дроби имеем

$0,(a_1, a_2 \ldots a_s)_q = \left(\frac{a_1}{q} + \frac{a_2}{q^2} + \ldots + \frac{a_s}{q^s}\right) + \left(\frac{a_1}{q^{s+1}} + \frac{a_2}{q^{s+2}} + \cdots + \frac{a_s}{q^s}\right) + + \ldots = \left(\frac{a_1}{q} + \frac{a_2}{q^2} + \ldots + \frac{a_s}{q^s}\right) \cdot \left(1 + \frac{1}{q^s} + \frac{1}{q^{2s}} + \cdots\right) =$

$= \frac{a_1 q^{s-1} + a_2 q^{s-2} + \cdots + a_s}{q^s} \cdot \frac{q^s}{q^s - 1}$. ■

Теорема 5.7. Положительная правильная несократимая дробь $\frac{a}{b}$ представима в виде чистой периодической q-ичной дроби с периодом s тогда и только тогда, когда $(b, q) = 1$. Причем период равен порядку числа q по модулю b, т.е. $s = O(q \bmod b)$.

■ (⇒) Пусть $\frac{a}{b} = 0,(a_1 a_2 \ldots a_s)_q$ – чисто периодическая q-ичная дробь с периодом s. По предложению имеем $\frac{a}{b} = = \frac{a_1 q^{s-1} + a_2 q^{s-2} + \cdots + a_s}{q^s} \cdot \frac{q^s}{q^s - 1}$.

Откуда $a \cdot (q^{s-1}) = b \cdot (a_1 q^{s-1} + a_2 q^{s-2} + \cdots + a_s)$. Так как $(a, b) = 1$, то $b | (q^s - 1)$ и $(b, q) = 1$. Осталось показать, что s – порядок вычета q по модулю b. Пусть $O(q \bmod b) = t$. Тогда $q^t - 1 = c \cdot b$ для некоторого $c \in$N, $b = \frac{q^t - 1}{c}$ и $\frac{a}{b} = \frac{a \cdot (q^t - 1)}{b(q^t - 1)} = \frac{a \cdot c}{q^t - 1}$. Из $\frac{a}{b} < 1$ следует, что $a \cdot c < q^t$. Поэтому

число $a \cdot c$ можно представить в виде $a \cdot c = b_1 q^{t-1} + + b_2 q^{t-2} + \cdots + b_t$,

где $0 \leq b_k < q$. Следовательно, $\frac{a}{b} = \frac{b_1 q^{t-1} + b_2 q^{t-2} + \cdots + b_t}{q^t - 1}$. Но тогда по предложению 5.6 имеем $\frac{a}{b} = 0,(b_1 \ldots b_t)_q$ и $t = s$, ч.т.д.

($\Leftarrow$) Пусть $(b, q) = 1$ и $s = O(q \bmod b)$. Тогда по определению порядка числа q по модулю b следует, что $b \mid q^s - 1$ и s наименьшее натуральное с этим условием. Пусть $q^s - 1 = c \cdot b$. Тогда $\frac{a}{b} = \frac{a \cdot (q^s - 1)}{b(q^s - 1)} = \frac{a \cdot c}{q^s - 1}$. Число ac можно представить в виде $ac = b_1 q^{s-1} + b_2 q^{s-2} + \cdots + b_s$.

Но тогда $\frac{a}{b} = \frac{b_1 q^{s-1} + b_2 q^{s-2} + \cdots + b_t}{q^s - 1} = 0,(b_1 \ldots b_s)_q$. Из определения порядка $s = O(q \bmod b)$ следует, что s – период q-ичной дроби. ■

• ***Смешанной периодической дробью с периодом s и предпериодом m*** называется бесконечная систематическая дробь $0, a_1 \ldots a_m a_{m+1} \ldots$, если для каждого натурального $k > m$ выполняется равенство $a_{k+s} = a_k$, для $k = m+1, m+2, \ldots$ причем m, s – наименьшие натуральные с этим свойством.

Систематическая смешанная дробь **по основанию q** с периодом s и предпериодом m записывается в виде $0, a_1 \ldots a_m (a_{m+1} \ldots a_s)_q$.

Последовательность цифр $a_1 a_2 \ldots a_m$ называется **предпериодом**, а последовательность $a_{m+1} \ldots a_{m+s}$ – **периодом** q-ичной дроби.

► Применяя «деление уголком» получаем: $\frac{1}{6} = 0,166 \ldots = = 0,1(6)_{10}$. Предпериод $m = 1$, период $s = 1$. Можно дробь записать и в виде $\frac{1}{6} = 0,166(66)$. ◄

В дальнейшем нас будет интересовать предпериод m и период s правильной дроби.

Теорема 5.8. Положительная правильная несократимая дробь $\frac{a}{b}$ представима в виде смешанной периодической q-ичной дроби тогда и только тогда, когда $b = b_0 \cdot b_1$, *где* $b_0 > 1$, $b_1 > 1$, $(b_1,q)=1$ и каждое простое число, которое делит b_0 делит и основание q счисления. При этом предпериод равен наименьшему натуральному m, такому, что $b_0 \mid q^m$, а период s равен показателю числа q по модулю b_1: $s = O(q \bmod b_1)$.

■ ($\Leftarrow$) Пусть $b = b_0 \cdot b_1$, где $(b_1,q) = 1$, а все простые числа из канонического разложения числа $b_0 > 1$ делят основание счисления q. Пусть m – наименьшее натуральное с условием $b_0 \mid q^m$. Тогда $q^m = Mb_0$ для некоторого $M \in N$ и $\frac{a \cdot q^m}{b} = \frac{a \cdot M \cdot b_0}{b_0 \cdot b_1} = \frac{A}{b_1}$. Пусть $\frac{A}{b_1} = Q + \frac{c}{b_1}$, где $Q < q^m$ и $\frac{c}{b_1}$ – правильная несократимая дробь. Имеем $Q = c_1 q^{m-1} + + c_2 q^{m-2} + \cdots + c_m$ для некоторых $c_1,\ldots, c_m \in \{0, 1, 2, \ldots, q-1\}$. По теореме 5.7 $\frac{c}{b_1} = 0, (a_1 \ldots a_s)_q$, где $s = O(q \bmod b_1)$ – период. Следовательно, $\frac{a \cdot q^m}{b} = c_1 \ldots c_m, (a_1 \ldots a_s)_q$. Но тогда $\frac{a}{b} = 0, c_1 \ldots c_m (a_1 \ldots a_s)_q$. Покажем, что предпериод равен m. Действительно, предположим противное. Пусть $\frac{a}{b} = \frac{a}{b_0 \cdot b_1} = = 0, t_1 \ldots t_k (l_1 \ldots l_s)_q$, где $k < m$. Тогда $\frac{a}{b} \cdot q^k = t_1 \ldots t_k (l_1 \ldots l_s)_q = = (t_1 \ldots t_k)_q + 0, (l_1 \ldots l_s)_q = Q_1 + \frac{d}{b_2 \cdot b_1}$, где $\frac{d}{b_2 \cdot b_1}$ – правильная несократимая дробь, $b_2 \neq 1, b_2 | b_0$ и $\frac{d}{b_2 \cdot b_1} = 0, (l_1 \ldots l_s)_q$, что противоречит теореме 5.7, так как $(b_2, q) > 1$ в силу выбора m.

(⟹) Пусть несократимая правильная дробь $\frac{a}{b}$ представима смешанной периодической q-ичной дробью: $\frac{a}{b} = 0, c_1c_2 \dots c_m(a_1a_2 \dots a_s)_q$, где m предпериод, s – период дроби. В силу теоремы 5.5 и теоремы 5.7 знаменатель $b = b_0 \cdot b_1$, где $(b_1, q) = 1$, $b_0 > 1$, $b_1 > 1$ и каждое простое число, которое делит b_0, делит q.

Имеем $\frac{a}{b} \cdot q^m = c_1c_2 \dots c_m, (a_1a_2 \dots a_s)_q = Q + r$, где r – несократимая правильная дробь и $r = 0, (a_1a_2 \dots a_{s)_q}$. По теореме 5.7 знаменатель дроби r взаимно прост с q, а так как $(b_1, q) = 1$, то он равен b_1. Следовательно, $b_0 \mid q^m$ и $s = O(q \bmod b_1)$. Осталось показать, что m – наименьшее натуральное с условием $b_0 \mid q^m$.

Предположим, что существует натуральное $n < m$, такое, что $b_0 \mid q^n$, т.е. $q^n = b_0 \cdot A$ для некоторого $A \in N$. Умножив дробь $\frac{a}{b}$ на q^n, получим $\alpha = \frac{a}{b} \cdot q^n = \frac{a \cdot A \cdot b_0}{b_0 \cdot b_1} = \frac{a \cdot A}{b_1} =$ $= Q_1 + \frac{d}{b_1}$, где Q_1 – целая часть , $\frac{d}{b_1}$ – дробная часть числа α. Так как $b_1 \nmid q^n$, то $d \neq 0$, причём $\frac{d}{b_1}$ – несократимая дробь, ибо $(q, b_1) = 1$. По теореме 5.7 имеем $\frac{d}{b_1} = 0, (\gamma_1 \dots \gamma_{s)_q}$, где $s = O(q \bmod b_1)$. Далее заметим, что $Q_1 < q^n$, так как $\frac{a}{b} < 1$ и $\frac{a \cdot q^n}{b} < q^n$. Поэтому $Q_1 = b_1q^{n-1} + b_2q^{n-2} + \dots + b_n$ для некоторых чисел $b_1, \dots, b_n \in \{0,1, \dots, q-1\}$. Но тогда $\frac{a}{b} = \frac{aq^n}{b} \cdot \frac{1}{q^n} =$ $= 0, b_1, \dots, b_n(\gamma_1 \dots \gamma_{s)_q}$, что противоречит условию. Полученное противоречие доказывает, что m – наименьшее натуральное с условием $b_0 | q^m$. ■

Предложение 5.9. В одной и той же q-ичной системе счисления справедливо следующее равенство:

$$\left(0, b_1 \dots b_m(a_1 \dots a_s)\right)_q = \left(\frac{b_1 \dots b_m a_1 \dots a_s - b_1 \dots b_m}{10^m \cdot (10^s - 1)}\right)_q,$$

в частности $\left(0, (a_1 \dots a_s)\right)_q = \left(\frac{a_1 \dots a_s}{10^s - 1}\right)_q$. Здесь 10-я запись числа q в q-ичной системе счисления.

■ В q-ичной системе счисления число q записывается в виде 10, где 1,0 – цифры счисления, соответствующие натуральным числам 1 и 0. Поэтому в q-ичной системе счисления систематическая дробь запишется следующим образом: $\left(0, b_1 \dots b_m(a_1 \dots a_s)\right)_q = \left(\frac{b_1 \dots b_m}{10^m} + \frac{a_1 \dots a_s}{10^m \cdot 10^s} + \frac{a_1 \dots a_s}{10^m \cdot 10^{2s}} + \right.$

$$\left. + \cdots\right)_q + \left(\frac{b_1 \dots b_m}{10^m} + \frac{a_1 \dots a_s}{10^m \cdot 10^s} \cdot \left(1 + \frac{1}{10^s} + \frac{1}{10^{2s}} + \cdots\right)\right)_q =$$

$$= \left(\frac{b_1 \dots b_m}{10^m} + \frac{a_1 \dots a_s}{10^m \cdot 10^s} \cdot \frac{10^s}{10^s - 1}\right)_q = \left(\frac{(b_1 \dots b_m) \cdot (10^s - 1) + a_1 \dots a_s}{10^m \cdot (10^s - 1)}\right)_q =$$

$$= \left(\frac{b_1 \dots b_m a_1 \dots a_s - b_1 \dots b_m}{10^m \cdot (10^s - 1)}\right)_q, \text{ ч.т.д } ■$$

► 1. Запишем данные систематические дроби в виде обыкновенных в той же системе счисления: а) $0{,}1(4)_7$; б) $0{,}4(13)_5$; в) $0, (132)_4$

Р е ш е н и е. а) $0{,}1(4)_7 = \left(\frac{14-1}{10 \cdot (10-1)}\right)_7 = \left(\frac{13}{10 \cdot 6}\right)_7 =$

$$= \left(\frac{2 \cdot 5}{10 \cdot 2 \cdot 3}\right)_7 == \left(\frac{5}{30}\right)_7;$$

б) $0{,}4(13)_5 = \left(\frac{413-4}{10 \cdot (10^2-1)}\right)_5 = \left(\frac{404}{10 \cdot 44}\right)_5 = \left(\frac{404}{440}\right)_5 = \left(\frac{13 \cdot 23}{13 \cdot 30}\right)_5 =$

$$= \left(\frac{23}{30}\right)_5;$$

в) $0, (132)_4 = \left(\frac{132}{10^3-1}\right)_4 = \left(\frac{132}{333}\right)_4 = \left(\frac{3 \cdot 22}{111 \cdot 3}\right)_4 = \left(\frac{22}{111}\right)_4$. ◄

2. Определим длину периода при обращении в 10-ичную дробь обыкновенную дробь $\frac{1}{11 \cdot 41}$.

Р е ш е н и е. Так как (10,11·41) = 1, то число $\frac{1}{11\cdot 41}$ при обращении в 10-ичную дробь будет чисто периодической с периодом s = 0 (10 (*mod* 11 · 41) = НОК [0 (10 (*mod* 11), 0 (10 (*mod* 41)]. По таблицам индексов для модулей $p = 11$ и $p = 41$ находим индексы числа 10: $ind10 = 5(mod\ 10)$; $ind10 = 32(mod\ 40)$. Следовательно, $O(10\ mod\ 11) = \frac{10}{(5,10)} = 2$, $O(10\ mod\ 41) = \frac{40}{(32,40)} = 5$.

О т в е т. $s = НОК[2,5] = 10$.

3. Представим обыкновенную дробь $\frac{13}{44}$ в виде десятичной дроби.

Р е ш е н и е. $\frac{13}{44} = \frac{13}{2^2\cdot 11}$. Имеем $m = 2$, $s = O(10\ mod\ 11) = 2$.

Умножим дробь на 10^2: $\frac{13}{44}\cdot 10^2 = \frac{325}{11} = 29 + \frac{6}{11}$. Следовательно, предпериод равен 29. Найдём периодическую дробь $\frac{6}{11}$: $\frac{6}{11} = \frac{6}{11}\cdot\frac{10^2-1}{10^2-1} = \frac{54}{10^2-1} = 0,(54)$.

О т в е т. $\frac{13}{44} = 0,29(54)$.

4. Обратим в 12-ичные дроби следующие обыкновенные дроби: а) $\frac{1}{24}$, б) $\frac{1}{5}$.

Р е ш е н и е. Обозначим через $0, 1, 2, \dots, 9, A, B$ – цифры 12-ичной системы счисления, где $A = 10, B = 11$.

а) дробь $\frac{1}{24}$ обращается в конечную 12-ичную дробь, так как знаменатель делится только на простые числа, которые делят основание счисления $q = 12$. Длина дроби равна 2, так как $24 \nmid 12$ и $24 || 12^2$.

Умножим и разделим дробь на $q^2 = 12^2$: $\frac{1}{24} = \frac{12^2}{24\cdot 12^2} = \frac{18}{12^2}$.

Разложим числитель по степени 12: $\frac{18}{12^2} = \frac{1\cdot 12+6}{12^2} =$ $= (0,\overline{1\bar{6}})_{12}$.

О т в е т. $\frac{1}{24} = (0,\overline{1\bar{6}})_{12}$.

б) дробь $\frac{1}{5}$ обращается в чисто периодическую дробь с длиной периодом $s = O(12\ mod\ 5) = 4$. Преобразуем дробь $\frac{1}{5} = \frac{1}{5}\cdot\frac{(q^s-1)}{q^s-1} = \frac{12^4-1}{5\cdot(12^4-1)} = \frac{29\cdot 143}{12^4-1} = \frac{4147}{12^4-1}$. Разложим числитель по степеням $q = 12$: $4147 = 2\cdot 12^3 + 4\cdot 12^2 + 9\cdot 12 + 7 =$ $= (\overline{2}\overline{4}\overline{9}\overline{7})_{12}$. Знаменатель $12^4 - 1 = (10^4 - 1)_{12}$. В силу предложения 5.9 имеем, $\frac{1}{5} = \left(\frac{2497}{10^4-1}\right)_{12} = 0,(2497)_{12} = 0$.

О т в е т. $\frac{1}{5} = 0,(2497)_{12}$.

5. Обратим следующие обыкновенные дроби в десятичные: а) $\frac{1}{11}$, б) $\frac{1}{6}$.

а) знаменатель дроби $\frac{1}{11}$ взаимно прост с основанием счисления $q = 10$. Следовательно, соответствующая десятичная дробь будет чисто периодической с периодом $s = O(10\ mod\ 11) = 2$. Представим дробь в виде

$$\frac{1}{11} = \frac{10^s - 1}{11\cdot(10^s - 1)} = \frac{10^2 - 1}{11\cdot(10^2 - 1)} = \frac{9}{10^2 - 1} = 0{,}09.$$

О т в е т. $\frac{1}{11} = 0,(09)$;

б) так как знаменатель $6 = 2\cdot 3$, причём $(2,10) = 2$, $(3,10) = 1$, то соответствующая десятичная дробь будет смешанной с предпериодом $m = 1$, так как $2|10$ и периодом $s = O(10\ mod\ 3) = 1$. Умножим дробь на $10^m = 10$ и выделим целую и дробные части: $\frac{1}{6}\cdot 10 = \frac{5}{3} = 1 + \frac{2}{3}$. Найдём

период дроби $\frac{2}{3} : \frac{2}{3} \cdot \frac{10-1}{10-1} = \frac{6}{10-1} = 0,(6)$. Так как $\frac{1}{6} \cdot 10 = 1,(6)$, то $\frac{1}{6} = 0,1(6)$.

О т в е т. $\frac{1}{6} = 0,1(6)$.

ПРИЛОЖЕНИЕ

1. Индивидуальные задания к самостоятельной работе по теории чисел

Задача 1. Найти НОД трех чисел *a, b, c*, используя алгоритм Евклида.

№	*a*	*b*	*c*	№	*a*	*b*	*c*	№	*a*	*b*	*c*
1	2428	788	120	11	4262	842	106	21	1514	372	106
2	2916	944	106	12	386	186	120	22	5684	1122	102
3	780	376	104	13	1734	424	106	23	442	214	105
4	1714	422	106	14	3110	1490	106	24	1830	876	120
5	442	214	104	15	2938	484	120	25	3204	788	105
6	1636	532	120	16	2016	978	104	26	2886	474	105
7	2794	552	102	17	1298	318	106	27	1598	522	104
8	1220	584	120	18	4734	780	120	28	2526	618	104
9	808	114	106	19	536	174	102	29	8080	1330	106
10	1536	738	104	20	1058	174	102	30	1324	432	120

Задача 2. Найти линейные разложения НОД чисел *a* и *b*.

№	*a*	*b*	№	*a*	*b*	№	*a*	*b*
1	840	342	11	584	236	21	750	312
2	392	161	12	745	310	22	786	318
3	284	116	13	825	335	23	596	248
4	692	280	14	534	222	24	344	140
5	565	235	15	696	282	25	476	192
6	345	140	16	452	188	26	365	150
7	318	132	17	812	332	27	445	180
8	798	324	18	436	176	28	966	402
9	308	128	19	925	385	29	654	264
10	548	224	20	580	235	30	740	308

Задача 3. Найти НОК чисел *a* и *b*.

№	*a*	*b*	№	*a*	*b*	№	*a*	*b*
1	2348	462	11	867	282	21	3756	927
2	1374	660	12	2742	672	22	4250	468
3	2889	358	13	2676	870	23	3941	434
4	5686	628	14	3171	779	24	1219	201
5	2310	565	15	903	438	25	3698	912
6	860	211	16	1655	538	26	7929	876
7	1951	242	17	4698	519	27	2804	688
8	3636	892	18	2948	366	28	5910	972
9	6084	862	19	2064	675	29	2467	272
10	4722	586	20	5734	633	30	1812	592

Задача 4. Определить, является ли число *a* простым.

1	6947	7	6703	13	6557	19	5917	25	3337
2	7207	8	6961	14	6733	20	7979	26	4891
3	7489	9	7219	15	6977	21	6763	27	8611
4	2623	10	1271	16	7243	22	6997	28	6791
5	4087	11	3139	17	1643	23	7283	29	7019
6	7519	12	4819	18	2773	24	2077	30	7309

Задача 5. Найти НОД и НОК чисел *a* и *b* по их каноническому разложению.

№	*a*	*b*	№	*a*	*b*	№	*a*	*b*
1	3240	415800	11	11520	120960	21	864000	2520
2	10080	5040	12	7560	3240	22	99000	120960
3	37800	1209600	13	3240	1900800	23	201600	693000
4	70560	317520	14	172800	27000	24	1764000	95040
5	126000	7920	15	594000	564480	25	2910600	693000
6	864000	760320	16	69120	432000	26	504000	100800
7	11520	2419200	17	16200	5544000	27	108000	594000
8	17640	166320	18	32400	9072000	28	110880	693000
9	81000	5760	19	2494800	201600	29	3960	1036800
10	27720	14553000	20	12600	864000	30	211680	34560

Задача 6. Найти показатель степени простых чисел p в каноническом разложении чисел $n!$.

№	p	n	№	p	n	№	p	n
1	17	1253	11	23	1709	21	31	1438
2	19	2091	12	13	2149	22	23	1778
3	29	2501	13	19	2432	23	29	1032
4	31	1658	14	47	2102	24	37	1064
5	19	2413	15	41	2448	25	29	1922
6	17	2479	16	47	2386	26	41	2166
7	29	2772	17	41	1910	27	29	1324
8	13	1786	18	41	1824	28	41	1423
9	31	1872	19	47	1788	29	41	2689
10	11	2391	20	37	1148	30	31	2096

Задача 7. Найти остаток от деления числа a^k на b.

№	a	k	b	№	a	k	b	№	a	k	b
1	6652	28	12	11	5242	29	12	21	3892	28	18
2	4912	23	14	12	2812	23	12	22	3382	20	12
3	1282	28	12	13	1432	29	12	23	3772	23	12
4	5992	24	18	14	2572	30	14	24	4642	21	20
5	1432	29	18	15	3172	28	18	25	3742	24	14
6	1252	22	14	16	2062	28	18	26	5212	25	14
7	3742	30	12	17	3202	23	20	27	4222	26	20
8	1702	28	18	18	1882	22	20	28	7042	26	20
9	4102	23	18	19	3202	21	12	29	6622	27	12
10	2302	20	14	20	2872	20	20	30	4882	23	20

Задача 8. С помощью разложения в непрерывную дробь сократить дробь a/b.

№	a	b	№	a	b	№	a	b
1	5222	862	11	15021	7254	21	4188	688
2	1638	402	12	3860	634	22	6771	837
3	2048	668	13	29408	7224	23	11448	2799
4	3386	556	14	6892	1356	24	21264	3496
5	3030	993	15	14476	2051	25	7922	1568
6	4232	696	16	23694	3906	26	7450	1055
7	12309	1743	17	7680	1089	27	4791	594
8	4696	776	18	2245	550	28	2589	636
9	3537	873	19	3994	980	29	2112	687
10	8356	920	20	4250	835	30	2802	462

Задача 9. Решить в целых неотрицательных числах уравнение $ax + by = c$.

№	a	b	c	№	a	b	c	№	a	b	c
1	25	11	759	11	30	41	4819	21	40	31	3093
2	28	47	3971	12	36	37	4385	22	48	29	5327
3	35	41	4050	13	45	31	4532	23	14	23	1044
4	42	37	4927	14	12	29	869	24	18	19	1220
5	10	31	1045	15	16	23	940	25	24	17	918
6	15	29	1034	16	21	19	1259	26	28	13	1218
7	20	23	1757	17	27	17	1199	27	35	11	816
8	25	19	1430	18	32	13	1141	28	40	47	5058
9	30	17	1672	19	40	11	1468	29	48	41	6696
10	36	13	1575	20	45	47	6747	30	14	37	1774

Задача 10. Решить систему сравнений

$$a_1x \equiv b_1(mod m_1)$$
$$a_2x \equiv b_2(mod m_2)$$
$$a_3x \equiv b_3(mod m_3)$$

с коэффициентами $[a_1, b_1, m_1]$; $[a_2, b_2, m_2]$; $[a_3, b_3, m_3]$.

№	$[a_1, b_1, m_1]$	$[a_2, b_2, m_2]$	$[a_3, b_3, m_3]$	№	$[a_1, b_1, m_1]$	$[a_2, b_2, m_2]$	$[a_3, b_3, m_3]$
1	5, 1, 6	8, 2, 5	4, 10, 17	16	5, 5, 8	12, 4, 11	4, 2, 19
2	5, 1, 6	8, 1, 7	6, 4, 13	17	7, 1, 4	6, 3, 5	4, 16, 17
3	5, 1, 6	12, 1, 7	4, 6, 19	18	7, 1, 4	6, 2, 7	6, 1, 13
4	5, 1, 6	12, 4, 11	6, 5, 17	19	5, 5, 8	6, 6, 7	4, 6, 13
5	7, 5, 8	6, 4, 5	4, 10, 13	20	5, 3, 8	6, 5, 7	6, 3, 19
6	5, 1, 6	6, 4, 5	4, 10, 13	21	5, 1, 8	8, 1, 11	4, 16, 17
7	5, 1, 6	6, 1, 5	6, 5, 19	22	5, 3, 4	12, 4, 5	4, 1, 13
8	5, 5, 6	8, 4, 7	4, 9, 17	23	5, 1, 4	12, 4, 5	6, 2, 19
9	5, 1, 6	8, 2, 11	6, 8, 13	24	7, 1, 4	6, 5, 7	4, 3, 17
10	5, 5, 6	12, 7, 11	4, 6, 19	25	7, 3, 4	6, 4, 11	6, 12, 13
11	5, 5, 8	12, 4, 5	6, 5, 17	26	5, 3, 8	6, 8, 11	4, 11, 13
12	7, 3, 8	6, 6, 7	4, 7, 13	27	5, 7, 8	6, 9, 11	6, 17, 19
13	5, 1, 6	6, 6, 7	4, 1, 13	28	5, 1, 4	8, 1, 5	6, 6, 17
14	5, 1, 6	6, 2, 7	6, 2, 19	29	5, 1, 4	12, 4, 7	4, 5, 13
15	5, 5, 6	8, 9, 11	4, 12, 17	30	5, 3, 4	12, 3, 7	6, 10, 19

Задача 11. Разложить в цепную дробь и заменить подходящей дробью с точностью до 0,0001 числа $\sqrt{a}$.

1	$\sqrt{31}$	11	$\sqrt{79}$	21	$\sqrt{67}$
2	$\sqrt{48}$	12	$\sqrt{29}$	22	$\sqrt{19}$
3	$\sqrt{59}$	13	$\sqrt{33}$	23	$\sqrt{21}$
4	$\sqrt{61}$	14	$\sqrt{37}$	24	$\sqrt{113}$
5	$\sqrt{73}$	15	$\sqrt{43}$	25	$\sqrt{117}$
6	$\sqrt{13}$	16	$\sqrt{111}$	26	$\sqrt{109}$
7	$\sqrt{75}$	17	$\sqrt{113}$	27	$\sqrt{65}$
8	$\sqrt{77}$	18	$\sqrt{47}$	28	$\sqrt{43}$
9	$\sqrt{83}$	19	$\sqrt{57}$	29	$\sqrt{39}$
10	$\sqrt{91}$	20	$\sqrt{63}$	30	$\sqrt{51}$

Задача 12. Решить сравнение $ax \equiv b(mod\ m)$ с помощью цепных дробей.

№	*a*	*b*	*m*	№	*a*	*b*	*m*	№	*a*	*b*	*m*
1	251	28	1053	11	265	29	1097	21	231	31	949
2	394	23	1619	12	94	9	593	22	82	13	507
3	173	26	1071	13	127	14	779	23	463	30	2843
4	194	28	1185	14	38	36	277	24	128	34	937
5	71	22	510	15	251	6	1806	25	265	35	1892
6	406	11	2899	16	394	27	2801	26	94	28	875
7	59	30	253	17	203	28	877	27	253	30	1061
8	82	27	339	18	292	35	1209	28	284	7	1167
9	447	23	1837	19	117	17	739	29	131	10	811
10	222	17	1375	20	210	40	1289	30	142	17	867

Задача 13. С помощью таблицы индексов решить степенное сравнение $ax^k \equiv b(mod\ m)$.

№	*a*	*k*	*b*	*m*	№	*a*	*k*	*b*	*m*
1	38	137	37	79	16	48	163	38	53
2	61	101	3	67	17	5	139	28	31
3	7	171	5	11	18	25	101	5	31
4	12	119	3	19	19	8	163	12	17
5	28	149	14	31	20	6	137	51	67
6	29	139	15	37	21	2	155	3	19
7	10	103	8	13	22	8	135	2	23
8	25	129	44	53	23	3	185	42	59
9	5	169	4	19	24	3	133	5	13
10	17	151	20	61	25	16	107	24	59
11	22	163	3	79	26	4	109	3	37
12	2	157	8	17	27	36	101	50	71
13	3	187	1	13	28	20	103	52	79
14	10	151	8	11	29	6	101	9	19
15	34	129	40	59	30	27	113	25	71

Задача 14. С помощью таблицы индексов решить показательное сравнение $a \cdot b^x \equiv c \pmod m$.

№	a	b	c	m	№	a	b	c	m	№	a	b	c	m
1	12	45	20	73	11	21	7	38	41	21	34	8	17	53
2	21	19	16	23	12	23	7	34	41	22	26	30	4	43
3	24	67	44	71	13	11	77	24	79	23	8	7	22	23
4	36	15	35	41	14	78	58	14	83	24	9	11	5	13
5	61	48	62	67	15	8	10	11	17	25	7	14	15	29
6	8	17	13	61	16	11	28	9	41	26	43	22	14	71
7	10	38	59	89	17	63	77	26	79	27	7	2	12	13
8	44	11	22	59	18	12	34	16	53	28	57	11	14	67
9	13	39	74	79	19	39	46	38	67	29	13	24	1	31
10	4	14	12	19	20	35	51	24	53	30	38	53	13	83

Задача 15. Перевести число a из p-ичной системы счисления в q-ичную.

№	a	p	q	№	a	p	q	№	a	p	q
1	202002	3	5	11	111110011	2	5	21	33423	6	9
2	31100	4	7	12	10654	8	9	22	14202	5	6
3	104202	5	8	13	14415	7	8	23	10342	6	9
4	14531	6	8	14	10410	6	7	24	3102	6	8
5	31023	5	8	15	5255	6	7	25	10310	5	6
6	13020	5	8	16	112001	3	6	26	11011011	2	5
7	14100	5	7	17	202100	3	5	27	23011	4	6
8	10320	4	5	18	111331	5	8	28	11011000	2	5
9	10430	5	6	19	3462	8	9	29	121013	4	7
10	110023	4	7	20	14155	6	8	30	1001010000	2	5

Задача 16. Определить длину периода при обращении обыкновенной дроби $\frac{1}{m}$ в десятичную.

№	m	№	m	№	m
1	$3 \cdot 17$	11	$11 \cdot 17$	21	$11 \cdot 73$
2	$7 \cdot 13$	12	$11 \cdot 19$	22	$13 \cdot 67$
3	$3 \cdot 23$	13	$19 \cdot 23$	23	$19 \cdot 73$
4	$11 \cdot 41$	14	$19 \cdot 41$	24	$23 \cdot 67$
5	$17 \cdot 23$	15	$13 \cdot 19$	25	$29 \cdot 63$
6	$19 \cdot 23$	16	$13 \cdot 23$	26	$29 \cdot 37$
7	$17 \cdot 43$	17	$13 \cdot 41$	27	$37 \cdot 67$
8	$19 \cdot 47$	18	$23 \cdot 41$	28	$11 \cdot 63$
9	$41 \cdot 53$	19	$23 \cdot 57$	29	$19 \cdot 67$
10	$19 \cdot 37$	20	$19 \cdot 57$	30	$11 \cdot 79$

2. Таблица индексов

Таблица 1

Числа	Модули																						Числа
	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97	
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
2	1	3	4	3	7	14	7	12	17	24	11	14	27	18	49	15	31	17	6	8	4	79	16	34	2
3		1	5	4	4	1	1	8	1	1	34	25	1	20	1	54	6	3	26	6	1	30	1	70	3
4		2	2	6	2	12	14	2	6	18	22	28	12	36	46	30	2	34	12	16	8	76	32	68	4
5			1	2	3	5	4	17	10	20	1	18	25	1	15	32	22	57	28	1	62	1	70	1	5
6			3	7	11	15	8	20	18	25	9	39	28	38	50	11	37	20	32	14	5	27	17	8	6
7				1	5	11	6	15	8	28	28	1	35	32	10	38	19	61	1	33	53	58	81	31	7
8				9	9	10	3	14	23	12	33	2	39	8	43	45	33	51	18	24	12	73	48	6	8
9				8	8	2	2	16	2	2	32	10	2	40	2	50	12	6	52	12	2	60	2	44	9
10				5	10	3	11	7	27	14	12	32	10	19	12	47	53	8	34	9	66	80	86	35	10
11					1	7	12	21	5	23	6	37	30	7	34	27	45	13	31	55	68	10	84	6	11
12					6	13	15	10	7	19	20	13	13	10	47	26	8	37	38	22	9	24	33	42	12
13						4	17	18	26	11	13	9	32	11	32	37	40	59	39	59	34	15	23	25	13
14						9	13	5	25	22	3	15	20	4	7	53	50	12	7	41	57	55	9	65	14
15						6	5	3	11	21	35	3	26	21	16	28	28	60	54	7	63	31	71	71	15
16						8	10	4	12	6	8	16	24	26	40	2	4	2	24	32	16	70	64	40	16
17							16	9	21	7	5	7	38	16	22	20	17	32	49	21	21	78	6	89	17
18							9	6	19	26	7	24	29	12	51	7	43	23	58	20	6	57	18	78	18
19								13	13	4	25	31	19	45	45	48	26	38	16	62	32	23	35	81	19
20								19	16	8	23	6	37	37	9	4	24	25	40	17	70	77	14	69	20

Окончание таблицы 1

Числа	Модули																						Числа
	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97	
21								1	9	29	26	26	36	6	11	34	25	64	27	39	54	6	82	5	21
22								11	22	17	17	11	15	25	31	42	16	30	37	63	72	7	12	24	22
23									4	27	21	4	16	5	39	51	27	14	15	46	26	66	57	77	23
24									24	13	31	27	49	28	44	41	39	54	44	30	13	21	49	76	24
25									20	10	2	36	8	2	30	6	44	48	56	2	46	2	52	2	25
26									15	5	24	23	17	29	29	52	11	10	45	67	38	12	39	59	26
27									3	3	30	35	3	14	3	46	18	9	8	18	3	8	3	18	27
28									14	16	14	29	5	22	4	10	21	29	13	49	61	52	25	3	28
29										9	15	33	41	35	18	14	5	22	68	35	11	46	59	13	29
30										15	10	17	11	39	13	43	59	11	60	15	67	28	87	9	30
31											27	12	34	3	5	39	29	7	11	11	56	50	31	46	31
32											19	39	9	44	37	17	35	19	30	46	20	67	80	74	32
33											4	22	31	27	35	23	51	16	57	61	69	40	85	60	33
34											16	21	23	34	19	35	48	49	55	29	25	75	22	27	34
35											29	19	18	33	25	12	41	52	29	34	37	59	63	32	35
36											18	38	14	30	48	22	14	40	64	28	10	54	34	16	36
37												8	7	42	14	13	9	44	20	64	19	22	11	91	37
38												5	4	17	42	5	57	55	22	70	36	20	51	19	38
39												34	33	31	33	33	46	62	65	65	35	45	24	95	39
40												20	22	9	6	19	55	42	46	25	74	74	30	7	40

3. Простые числа <4070 и их наименьшие первообразные корни

Таблица 2

p	g	p	g	p	g	p	g	p	g	p	g	p	g
2	1	179	2	419	2	661	2	947	2	1229	2	1523	2
3	2	181	2	421	2	673	5	953	3	1231	3	1531	2
5	2	191	19	431	7	677	2	967	5	1237	2	1543	5
7	3	193	5	433	5	683	5	971	6	1249	7	1549	2
11	2	197	2	439	15	691	3	977	3	1259	2	1553	3
13	2	199	3	443	2	701	2	983	5	1277	2	1559	19
17	3	211	2	449	3	709	2	991	6	1279	3	1567	3
19	2	223	3	457	13	719	11	997	7	1283	2	1571	2
23	5	227	2	461	2	727	5	1009	11	1289	6	1579	3
29	2	229	6	463	3	733	6	1013	3	1291	2	1583	5
31	3	233	3	467	2	739	3	1019	2	1297	10	1597	11
37	2	239	7	479	13	743	5	1021	10	1301	2	1601	3
41	6	241	7	487	3	751	3	1031	14	1303	6	1607	5
43	3	251	6	491	2	757	2	1033	5	1307	2	1609	7
47	5	257	3	499	7	761	6	1039	3	1319	13	1613	3
53	2	263	5	503	5	769	11	1049	3	1321	13	1619	2
59	2	269	2	509	2	773	2	1051	7	1327	3	1621	2
61	2	271	6	521	3	787	2	1061	2	1361	3	1627	3
67	2	277	5	523	2	797	2	1063	3	1367	5	1637	2
71	7	281	3	541	2	809	3	1069	6	1373	2	1657	11
73	5	283	3	547	2	811	3	1087	3	1381	2	1663	3
79	3	293	2	557	2	821	2	1091	2	1399	13	1667	2
83	2	307	5	563	2	823	3	1093	5	1409	3	1669	2
89	3	311	17	569	3	827	2	1097	3	1423	3	1693	2
97	5	313	10	571	3	829	2	1103	5	1427	2	1697	3
101	2	317	2	577	5	839	11	1109	2	1429	6	1699	3
103	5	331	3	587	2	853	2	1117	2	1433	3	1709	3
107	2	337	10	593	3	857	3	1123	2	1439	7	1721	3
109	6	347	2	599	7	859	2	1129	11	1447	3	1723	3
113	3	349	2	601	7	863	5	1151	17	1451	2	1733	2
127	3	353	3	607	3	877	2	1153	5	1453	2	1741	2
131	2	359	7	613	2	881	3	1163	5	1459	5	1747	2
137	3	367	6	617	3	883	2	1171	2	1471	6	1753	7
139	2	373	2	619	2	887	5	1181	7	1481	3	1759	6
149	2	379	2	631	3	907	2	1187	2	1483	2	1777	5
151	6	383	5	641	3	911	17	1193	3	1487	5	1783	10
157	5	389	2	643	11	919	7	1201	11	1489	14	1787	2
163	2	397	5	647	5	929	3	1213	2	1493	2	1789	6
167	5	401	3	653	2	937	5	1217	3	1499	2	1801	11
173	2	409	21	659	2	941	2	1223	5	1511	11	1811	6

Окончание таблицы 2

p	g	p	g	p	g	p	g	p	g	p	g	p	g
1823	5	2131	2	2437	2	2749	6	3083	2	3433	5	3733	2
1831	3	2137	10	2441	6	2753	3	3089	3	3449	3	3739	7
1847	5	2141	2	2447	5	2767	3	3109	6	3457	7	3761	3
1861	2	2143	3	2459	2	2777	3	3119	7	3461	2	3767	5
1867	2	2153	3	2467	2	2789	2	3121	7	3463	3	3769	7
1871	14	2161	23	2473	5	2791	6	3137	3	3467	2	3779	2
1873	10	2179	7	2477	2	2797	2	3163	3	3469	2	3793	5
1877	2	2203	5	2503	3	2801	3	3167	5	3491	2	3797	2
1879	6	2207	5	2521	17	2803	2	3169	7	3499	2	3803	2
1889	3	2213	2	2531	2	2819	2	3181	7	3511	7	3821	3
1901	2	2221	2	2539	2	2833	5	3187	2	3517	2	3823	3
1907	2	2237	2	2543	5	2837	2	3191	11	3527	5	3833	3
1913	3	2239	5	2549	2	2843	2	3203	2	3529	17	3847	5
1931	2	2243	2	2551	6	2851	2	3209	3	3533	2	3851	2
1933	5	2251	7	2557	2	2857	11	3217	5	3539	2	3853	2
1949	2	2267	2	2579	2	2861	2	3221	10	3541	7	3863	5
1951	3	2269	2	2591	7	2879	7	3229	6	3547	2	3877	2
1973	2	2273	3	2593	7	2887	5	3251	6	3557	2	3881	13
1979	2	2281	7	2609	3	2897	3	3253	2	3559	3	3889	11
1987	2	2287	19	2617	5	2903	5	3257	3	3571	2	3907	2
1993	5	2293	2	2621	2	2909	2	3259	3	3581	2	3911	13
1997	2	2297	5	2633	3	2917	5	3271	3	3583	3	3917	2
1999	3	2309	2	2647	3	2927	5	3299	2	3593	3	3919	3
2003	5	2311	3	2657	3	2939	2	3301	6	3607	5	3923	2
2011	3	2333	2	2659	2	2953	13	3307	2	3613	2	3929	3
2017	5	2339	2	2663	5	2957	2	3313	10	3617	3	3931	2
2027	2	2341	7	2671	7	2963	2	3319	6	3623	5	3943	3
2029	2	2347	3	2677	2	2969	3	3323	2	3631	15	3947	2
2039	7	2351	13	2683	2	2971	10	3329	3	3637	2	3967	6
2053	2	2357	2	2687	5	2999	17	3331	3	3643	2	3989	2
2063	5	2371	2	2689	19	3001	14	3343	5	3659	2	4001	3
2069	2	2377	5	2693	2	3011	2	3347	2	3671	13	4003	2
2081	3	2381	3	2699	2	3019	2	3359	11	3673	5	4007	5
2083	2	2383	5	2707	2	3023	5	3361	22	3677	2	4013	2
2087	5	2389	2	2711	7	3037	2	3371	2	3691	2	4019	2
2089	7	2393	3	2713	5	3041	3	3373	5	3697	5	4021	2
2099	2	2399	11	2719	3	3049	11	3389	3	3701	2	4027	3
2111	7	2411	6	2729	3	3061	6	3391	3	3709	2	4049	3
2113	5	2417	3	2731	3	3067	2	3407	5	3719	7	4051	6
2129	3	2423	5	2741	2	3079	6	3413	2	3727	3	4057	5

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Виноградов И.М. Основы теории чисел / И.М. Виноградов. – М.: Наука, 1972.
2. Алгебра и теория чисел. Часть III: учебное пособие для студентов-заочников педагогических институтов / Н.А. Казачек, Г.Н. Перлатов, Н.Л. Виленкин, А.И. Бородин. – М.: Просвещение, 1984.
3. Грибанов В.У. Сборник упражнений по теории чисел / В.У. Грибанов, П.И. Титов. – М.: Просвещение, 1964.
4. Куликов Л.Я. Алгебра и теория чисел / Л.Я. Куликов. – М.: Высшая школа, 1979.
5. Кочева А.А. Задачник-практикум по алгебре и теории чисел. Часть III / А.А. Кочева. – М.: Просвещение, 1984.
6. Кудреватов Г.А. Сборник задач по теории чисел / Г.А. Кудреватов. – М.: Просвещение, 1970.
7. Ильиных А.П. Теория чисел: учебное пособие / Урал. гос. пед. Ун-т. – Екатеринбург, 2003.
8. Ситников В.М. Сравнения: методическое пособие / В.М. Ситников. – Челябинск: Издательство ЧГПУ, 2000.

ОГЛАВЛЕНИЕ

Учебное издание

Ситников Владимир Михайлович

Теория чисел

Учебное пособие

ISBN 978-5-906777-06-5

Работа рекомендована РИСом ЧГПУ
Протокол № 7 (пункт 4), 2014 г.

Редактор Е.М. Сапегина
Технический редактор А.Г. Петрова

Издательство ЧГПУ
454080 г. Челябинск, пр. Ленина, 69

Подписано в печать 15.08.2014 Тираж 100 экз.
Формат 60x84 1/16 Бумага типографская
Объем 4,2 уч.-изд.л. Заказ № ___.

Отпечатано с готового оригинал-макета
в типографии ЧГПУ
454080 г. Челябинск, пр. Ленина, 69