МГЗПИ

АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ

Московский государственный
заочный
педагогический институт

АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ

Учебное пособие для студентов-заочников II курса физико-математических факультетов педагогических институтов

Под редакцией **Н. Я. ВИЛЕНКИНА**

Издание второе

Рекомендовано Главным управлением высших и средних педагогических учебных заведений Министерства просвещения РСФСР

МОСКВА
«ПРОСВЕЩЕНИЕ»
1984

ББК 22—13
А45

Авторы:
**Н. А. КАЗАЧЕК, Г. Н. ПЕРЛАТОВ,
Н. Я. ВИЛЕНКИН, А. И. БОРОДИН**

Рецензенты:
кандидат физико-математических наук, доцент **А. А. Полянский**
(Куйбышевский пединститут)
кандидат физико-математических наук, доцент **Т. М. Федулова**
(Куйбышевский пединститут)

Редактор МГЗПИ О. А. Павлович

А45 **Алгебра** и теория чисел: Учеб. пособие для студентов-заочников II курса физ.-мат. фак. пед. ин-тов (Н. А. Казачек, Г. Н. Перлатов, Н. Я. Виленкин, А. И. Бородин; Под ред. Н. Я. Виленкина. — 2-е изд. — М.: Просвещение, 1984.— 192 с.

Наряду с теоретическим материалом пособие содержит большое количество подробно разобранных примеров, а также упражнения для самостоятельного решения.

А $\frac{4309020400—525}{103(03)—84}$ **заказное**

**ББК 22—13
517.1**

ПРЕДИСЛОВИЕ

Предлагаемое вниманию читателя учебное пособие предназначено для студентов-заочников физико-математических факультетов педагогических институтов. Оно написано в полном соответствии с новой программой курса «Алгебра и теория чисел» и является третьим в серии учебных пособий, охватывая материал, изучаемый в IV семестре.

Книга состоит из трех глав, причем каждая глава разбита на параграфы, а параграфы — на пункты. Нумерация определений, лемм и теорем единая в пределах одного параграфа, а нумерация формул единая внутри одного пункта. При ссылке на теорему указываются соответственно ее номер, номера параграфа и главы, причем при ссылке на теорему того же параграфа номера главы и параграфа опускаются, а при ссылке на теорему той же главы указываются лишь номера теоремы и параграфа. Аналогично производятся ссылки на формулы (например, ссылка на формулу (4) означает, что речь идет о формуле (4) данного пункта).

В первой главе изложена теория делимости в кольце целых чисел, т. е. дано теоретическое обоснование вопросов, изучаемых в V классе средней школы (и частично в VII классе). Здесь рассмотрены свойства отношения делимости, алгоритм Евклида для нахождения наибольшего общего делителя целых чисел, теория простых чисел, а также системы счисления, числовые функции и цепные дроби.

Вторая глава посвящена теории колец. В ней излагается теория делимости в коммутативных кольцах, в частности в кольцах главных идеалов, обобщающая изученную в первой главе теорию делимости в кольце целых чисел, рассматривается теория идеалов в кольцах, гомоморфизмов и фактор-колец, дающая алгебраическое обоснование изучаемой далее теории сравнений. Приводимое в этой главе доказательство теоремы о существовании и единственности разложения на простые множители в кольцах главных идеалов позволяет не рассматривать в дальнейшем этот вопрос для колец многочленов от одного переменного. Кроме того, в этой главе дано построение поля отношений для области целостности,

являющееся теоретической основой построения поля рациональных чисел и поля алгебраических дробей.

Третья глава содержит теорию сравнений и некоторые приложения теории чисел к школьной математике. Изложение теории сравнений ведется на основе понятий теории колец; широко используются понятия идеала, фактор-кольца, обратимого элемента и т. д. Такой подход позволяет, в частности, рассматривать решение сравнений как решение уравнений с коэффициентами из кольца вычетов. Поскольку общая теория уравнений изучается в следующих семестрах, мы сочли возможным опустить доказательство некоторых теорем о решении сравнений высших степеней по простому модулю (эти доказательства намечено дать в следующей части книги). Учитывая, что лектор может излагать материал в более традиционном духе, мы сочли полезным сделать «перевод» основных результатов на язык сравнений. Из приложений теории чисел к школьной математике рассмотрены признаки делимости, проверка результатов действий, обращение обыкновенных дробей в систематические.

Изложение теоретического материала сопровождается большим количеством примеров, раскрывающих суть вводимых понятий и определений.

Каждый параграф книги заканчивается вопросами для самопроверки и упражнениями, позволяющими студенту-заочнику проверить, насколько он овладел изложенным материалом. Наряду с этими задачами читатель может использовать «Задачник-практикум по алгебре и теории чисел» А. А. Кочевой («Просвещение», 1984).

Авторы просят присылать все замечания и пожелания читателей по адресу: 109004 Москва, Верхняя Радищевская ул., д. 18, МГЗПИ, редакционно-издательский отдел.

Глава I

ЦЕЛЫЕ ЧИСЛА И ОСНОВЫ ТЕОРИИ ДЕЛИМОСТИ

§ 1. ДЕЛИМОСТЬ

1. Отношение делимости и его свойства. В школьном курсе математики читатель ознакомился с натуральными и целыми числами. Обозначим множество натуральных чисел через **N**:

$$\mathbf{N} = \{1, 2, \ldots\},$$

а множество целых чисел — через **Z**:

$$\mathbf{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

Будем считать известными свойства операций над целыми числами (сложения, вычитания, умножения), понятие модуля целого числа и свойства этого понятия.

В этом параграфе мы рассмотрим свойства отношения делимости в множестве **Z**. Введем следующее определение:

Определение 1. Целое число a *делится* на целое число b, если существует такое целое число c, что $a = b \cdot c$.

Число a называется *делимым*, b — *делителем* и c — *частным*.

Если a делится на b, то пишут $a \vdots b$ (a *кратно* b).

Обратным к отношению $a \vdots b$ является отношение «b делит a», которое обозначают так: b/a.

Отношение делимости $a \vdots b$ является бинарным отношением в **Z**. Оно обладает следующими свойствами:

1) *Отношение делимости рефлексивно*, т. е. для любого $a \in \mathbf{Z}$ имеем $a \vdots a$.

Это следует из того, что $a = a \cdot 1$ и $1 \in \mathbf{Z}$.

2) *Отношение делимости транзитивно*, т. е. из $a \vdots b$ и $b \vdots c$ следует $a \vdots c$.

Действительно, так как $a \vdots b$ и $b \vdots c$, то существуют такие целые числа q и t, что $a = b \cdot q$ и $b = c \cdot t$. Но тогда $a = b \cdot q = (c \cdot t) \cdot q = c \cdot (t \cdot q)$. Так как произведение целых чисел — целое число, то $tq \in \mathbf{Z}$, и потому $a \vdots c$.

3) *Если* $a \vdots b$, *то* $(-a) \vdots b$, $a \vdots (-b)$ и $(-a) \vdots (-b)$, т. е. *отношение делимости сохраняется при изменении знаков делимого и делителя.*

В самом деле, если $a \vdots b$, то $a = bq$, где $q \in \mathbf{Z}$, а тогда $-a = b(-q)$, $a = (-b)(-q)$, $-a = (-b) \cdot q$.

4) *Если* $a \vdots c$ *и* $b \vdots c$, *то* $(a + b) \vdots c$.

В самом деле, так как $a \vdots c$ и $b \vdots c$, то существуют такие целые числа q и t, что $a = cq$ и $b = ct$. Но тогда $a + b = cq + ct = c(q + t)$. Так как $q + t$ — целое число, то $a + b$ делится на c.

Точно так же доказывается, что из $a \vdots c$, $b \vdots c$ следует $(a - b) \vdots c$.

5) *Если* $a \vdots c$ *и* $b \in \mathbf{Z}$, *то* $(ab) \vdots c$.

В самом деле, так как $a \vdots c$, то существует $q \in \mathbf{Z}$ такое, что $a = cq$. Но тогда $ab = (cq) \cdot b = c(qb)$. Так как $qb \in \mathbf{Z}$, то $(ab) \vdots c$.

Следствие 1. *Если* $a_1 \vdots c$, ..., $a_n \vdots c$, *то для любых целых чисел* r_1, ..., r_n *имеем* $(r_1a_1 + \ldots + r_na_n) \vdots c$.

В самом деле, в силу 5) числа r_1a_1, ..., r_na_n делятся на c, а тогда в силу 4) и сумма $r_1a_1 + \ldots + r_na_n$ делится на c.

Следствие 2. *Если числа* a_1, ..., a_n, b_1, ..., b_m *делятся на* c *и* r_1, ..., r_n, s_1, ..., s_m — *целые числа, то из* $r_1a_1 + \ldots + r_na_n = s_1b_1 + \ldots + s_mb_m + b_{m+1}$ *следует, что* $b_{m+1} \vdots c$.

Для доказательства достаточно заметить, что

$$b_{m+1} = r_1a_1 + \ldots + r_na_n - s_1b_1 - \ldots - s_mb_m,$$

и воспользоваться следствием 1.

Отметим, что утверждения, обратные 4) и 5), ложны: *из делимости суммы не вытекает делимость слагаемых, а из делимости произведения не вытекает делимость сомножителей.*

Например, $35 + 13 = 48$ делится на 12, но ни 35, ни 13 не делятся на 12; $3 \cdot 8 = 24$ делится на 12, но ни 3, ни 8 на 12 не делятся.

6) *Если* $a \vdots c$, а b *не делится на* c, *то* $a \pm b$ *не делится на* c.

В самом деле, если бы $(a + b) \vdots c$, то из $a \vdots c$ вопреки условию следовало бы, что и $b \vdots c$.

7) *Нуль делится на любое число* b.

В самом деле, $0 = b \cdot 0$. Частное от деления нуля на b при $b \neq 0$ равно нулю.

8) *Любое число* a *делится на* 1.

В самом деле, $a = 1 \cdot a$.

9) *Если* $a \neq 0$, *то не существует такого* q, *что* $0 \cdot q = a$.

Поэтому ни одно число $a \neq 0$ не делится на 0. С другой стороны, для любого $q \in \mathbf{Z}$ имеем: $0 \cdot q = 0$. Поэтому частное $0 : 0$ не определено однозначно. Кратко говорят: *деление на нуль невозможно.*

10) *Если* $a \vdots b$, *то* $|a| \geqslant |b|$.

В самом деле, $a = b \cdot q$, и потому $|a| = |b| \cdot |q| \geqslant |b|$.

Следствие 1. *Если* $1 \vdots a$, *то либо* $a = 1$, *либо* $a = -1$.

В самом деле, $1 \geqslant |a|$, но поскольку a — целое число, отличное от нуля, то $|a| \geqslant 1$. Значит, $|a| = 1$ и $a = \pm 1$.

Следствие 2. *Если* $a \vdots b$ *и* $b \vdots a$, *то либо* $a = b$, *либо* $a = -b$.

В самом деле, из $a \vdots b$ следует, что $|a| \geqslant |b|$, а из $b \vdots a$, что $|b| \geqslant |a|$. Значит, $|a| = |b|$ и $a = b$, или $a = -b$.

2. Деление с остатком. Определение 2. Разделить целое число a на целое число $b \neq 0$ с остатком — это значит найти два таких целых числа q и r, чтобы выполнялись условия:

а) $a = bq + r$,

б) $0 \leqslant r < |b|$.

Число q называется *неполным частным*, а r — *остатком*.

Теорема 1. *Каковы бы ни были целое число a и целое число $b \neq 0$, всегда возможно, и притом единственным способом, разделить a на b с остатком.*

Докажем сначала возможность деления с остатком.

Рассмотрим все случаи, которые здесь могут представиться.

1) a — любое целое число, $b > 0$.

Рассмотрим множество всех чисел, кратных b, и расположим его в порядке возрастания:

$$\ldots,\ b \cdot (-2),\ b \cdot (-1),\ b \cdot 0,\ b \cdot 1,\ b \cdot 2,\ \ldots$$

Пусть bq — наибольшее кратное числа b, не превышающее a. Тогда $a \geqslant bq$, но $a < b(q+1)$, т. е. $bq \leqslant a < b(q+1)$, откуда $0 \leqslant a - bq < b$.

Положив $a - bq = r$, получим:

$$a = bq + r,\ 0 \leqslant r + b.$$

2) a — целое число, $b < 0$.

Так как $b < 0$, то $-b > 0$ и согласно случаю 1) деление a на $-b$ возможно, а это означает существование таких целых чисел q и r, что $a = (-b) \cdot q + r$, $0 \leqslant r < |-b|$, или $a = b(-q) + r$, $0 \leqslant r < |b|$.

Возможность деления с остатком доказана.

Теперь докажем единственность деления с остатком.

Пусть деление a на b не единственно, т. е. пусть существуют два неполных частных q_1 и q_2 и два остатка r_1 и r_2 такие, что:

$$\begin{aligned} a &= bq_1 + r_1, & 0 \leqslant r_1 < |b|, \\ a &= bq_2 + r_2, & 0 \leqslant r_2 < |b|. \end{aligned}$$

Тогда

$$bq_1 + r_1 = bq_2 + r_2, \text{ или } b(q_1 - q_2) = r_2 - r_1. \qquad (*)$$

Так как $0 \leqslant r_1 < |b|$ и $0 \leqslant r_2 < |b|$, то

$$|r_2 - r_1| < |b|.$$

Но в этом случае равенство (*) возможно лишь при условии: $r_2 - r_1 = 0$, или $r_2 = r_1$, но тогда $q_1 - q_2 = 0$, или $q_1 = q_2$.

Итак, $q_1 = q_2$, $r_1 = r_2$. Единственность доказана.

Вопросы для самопроверки и упражнения

1. Что означает высказывание «целое число a делится на целое число b»? Истинно ли оно, если $a = 275$, $b = 1$? А если $b = 275$, $a = 1$? Сформулируйте отрицание этого высказывания.

2. Охарактеризуйте множество целых чисел b таких, что $a \vdots b$, где a — фиксированное число.

3. Каким условиям должен удовлетворять остаток от деления a на b? Может ли при делении на —142 получиться остаток 187? а остаток — 45? а остаток 56?

4. Докажите, что: а) из трех последовательных натуральных чисел одно делится на 3; б) из двух последовательных четных чисел одно делится на 4; в) из пяти последовательных натуральных чисел одно делится на 5.

5. Докажите, что: а) произведение трех последовательных натуральных чисел делится на 6; б) произведение пяти последовательных чисел делится на 120.

6. Пусть $a = -1284$, $b = 148$. Укажите такое q, что $b \cdot q \leqslant a < b \cdot (q + 1)$.

7. Пусть $a = -135$, $b = 14$. Укажите такое r, что $0 \leqslant r < |b|$ и $(a - r) \vdots b$.

8. Укажите частное и остаток от деления 5 на 7, 120 на 13, —529 на —23, —410 на 47, 256 на —15.

9. По делимому a и остатку r найдите делители b и соответствующие частные q, если:

а) $a = 100$, $r = 6$; б) $a = 148$, $r = 37$; в) $a = 497$, $r = 16$.

10. Число a при делении на некоторое целое положительное число b дает в частном q. Найдите делители b и соответствующие им остатки r, если: а) $a = 371$, $q = 14$; б) $a = 3129$, $q = 83$; в) $a = 13127$, $q = 121$; г) $a = 42157$, $q = 231$.

11. Докажите, что если $(mn + pq) \vdots (m - p)$, то $(mq + np) \vdots (m - p)$. (Здесь m, n, p, q — целые числа.)

§ 2. НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ. АЛГОРИТМ ЕВКЛИДА

1. Наибольший общий делитель. Введем следующие определения:

Определение 1. Целое число $\delta \neq 0$ называется *общим делителем целых чисел* $a_1, a_2, \ldots, a_n$, если каждое из этих чисел делится на δ.

Определение 2. Целое число d называется *наибольшим общим делителем* чисел $a_1, a_2, \ldots, a_n$, если:

1) d является общим делителем этих чисел;

2) d делится на любой общий делитель чисел $a_1, \ldots, a_n$*.

Теорема 1. *Наибольший общий делитель чисел* $a_1, \ldots, a_n$ *определен однозначно с точностью до знака* (иными словами, если

* Данное здесь определение отличается от школьного. Оно более удобно, поскольку допускает обобщение на весьма широкий класс объектов (см. § 2 главы II).

d_1 и d_2 — наибольшие общие делители чисел $a_1, \ldots, a_n$, то либо $d_1 = d_2$, либо $d_1 = -d_2$).

Доказательство. Пусть d_1 и d_2 — наибольшие общие делители чисел $a_1, \ldots, a_n$. Так как d_1 — наибольший общий делитель, то он делится на любой общий делитель этих чисел, а значит, делится на d_2, $d_1 \vdots d_2$. Точно так же доказываем, что $d_2 \vdots d_1$. Но отношения $d_1 \vdots d_2$ и $d_2 \vdots d_1$ могут иметь место лишь в случае, когда $d_1 = d_2$ или $d_1 = -d_2$ (следствие 2 к свойству 10, п. 1).

Условимся всегда брать положительное значение наибольшего общего делителя чисел $a_1, \ldots, a_n$. Это значение будем обозначать $d = (a_1, \ldots, a_n)$.

Пример. Наибольший общий делитель чисел 135 и —180 равен 45. В самом деле, множество положительных делителей числа 135 имеет вид:

$$A = \{1, 3, 5, 9, 15, 27, 45, 135\},$$

а для числа —180 — вид:

$$B = \{1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 20, 30, 36, 45, 60, 90, 180\}.$$

Пересечением этих множеств является

$$A \cap B = \{1, 3, 5, 9, 15, 45\}.$$

Число 45 является общим делителем чисел 135 и —180 и делится на все остальные общие делители этих чисел, т. е. на 1, 3, 5, 9, 15. Значит, (135, —180) = 45. Заметим, что 45 — наибольший по величине положительный общий делитель чисел 135 и —180. Позже мы докажем, что для любых целых чисел $a_1, \ldots, a_n$ их наибольший общий делитель является бо́льшим по величине положительным общим делителем.

2. Алгоритм Евклида. Из определения 1 еще не следует, что наибольший общий делитель любого конечного множества целых чисел существует. Чтобы доказать существование наибольшего общего делителя, опишем способ нахождения наибольшего общего делителя, предложенный великим древнегреческим математиком Евклидом. Этот способ называют *алгоритмом Евклида*. Он основан на следующих леммах:

Лемма 1. *Если* $a \vdots b$, *то* $(a, b) = b$.

Доказательство. Поскольку $a \vdots b$ и $b \vdots b$, то b — общий делитель a и b. С другой стороны, если c — любой общий делитель чисел a и b, то он является делителем b. Оба условия определения 2 выполнены, и потому $(a, b) = b$.

Лемма 2. *Если* $a = bq + r$, *где* a, b и r *отличны от нуля, то* $(a, b) = (b, r)$.

Доказательство. Пусть δ—общий делитель a и b; тогда $a \vdots \delta$, $b \vdots \delta$. Так как $a = bq + r$, то $r = a - bq$ и по следствию 2 свойства 5 из п. 1 § 1 $r \vdots \delta$. Поэтому любой общий делитель чисел a

и b является общим делителем b и r. Обратно, если $b \vdots \delta$ и $r \vdots \delta$, то $a = bq + r$ делится на δ, а потому любой общий делитель b и r является общим делителем a и b. Таким образом, множество A общих делителей a и b совпадает с множеством B общих делителей b и r, следовательно, $A = B$.

Пусть d — наибольший общий делитель чисел a и b. Тогда $d \in A$ и d делится на любое число из множества A (т. е. на любой общий делитель чисел a и b). Поскольку $A = B$, то $d \in B$ и d делится на любое число из множества B, т. е. d — наибольший общий делитель чисел b и r.

Равенство $(a, b) = (b, r)$ доказано.

Алгоритм Евклида для отыскания общего наибольшего делителя чисел a и b состоит в следующем. Сначала число a делят на число b, $a > b > 0$. Если $a \vdots b$, то по лемме 1 $(a, b) = b$. В противном случае получаем остаток $r_1 : a = bq_0 + r_1$. Делим b на r_1. Если $b \vdots r_1$, то $(b, r_1) = r_1$, а тогда $(a, b) = (b, r_1)$. Если же b не делится на r_1, то получится остаток r_2. Делим r_1 на r_2 и т. д. Поскольку остатки, получаемые в процессе деления, убывают и являются натуральными числами, то на каком-то шагу получим деление без остатка. Последний, не равный нулю остаток является наибольшим общим делителем чисел a и b*. Это утверждение можно сформулировать в виде следующей теоремы:

Т е о р е м а 2. *Если*

$$\begin{aligned} a &= bq_0 + r_1; \quad 0 \leqslant r_1 < b, \\ b &= r_1q_1 + r_2; \quad 0 \leqslant r_2 < r_1, \\ &\cdots\cdots\cdots\cdots \\ r_{n-2} &= r_{n-1} \cdot q_{n-1} + r_n; \quad 0 \leqslant r_n < r_{n-1}, \\ r_{n-1} &= r_n \cdot q_n, \end{aligned} \tag{1}$$

то $(a, b) = r_n$.

Д о к а з а т е л ь с т в о. В силу леммы 2 получаем: из первой строки $(a, b) = (b, r_1)$, из второй $(b, r_1) = (r_1, r_2)$ и т. д. Значит,

$$(a, b) = (r_{n-1}, r_n).$$

Но $r_{n-1} \vdots r_n$ и по лемме 1 $(r_{n-1}, r_n) = r_n$.

Поэтому $(a, b) = r_n$.

---

* Аналогичный алгоритм применяется при нахождении общей меры двух отрезков и общего наибольшего делителя двух многочленов от одного переменного.

Пример. Найдем (2585, 7975).

$$
\begin{array}{r|l}
7975 & 2585 \\
\cline{2-2}
7755 & 3 \\
\cline{1-1}
2585 & 220 \\
\cline{2-2}
220 & 11 \\
\cline{1-1}
385 & \\
\cline{1-1}
220 & \\
\cline{1-1}
220 & 165 \\
\cline{2-2}
165 & 1 \\
\cline{1-1}
165 & 55 \\
\cline{2-2}
165 & 3 \\
\cline{1-1}
0 &
\end{array}
$$

Последний, отличный от нуля остаток равен 55, следовательно, (2585, 7975) = 55.

Из алгоритма Евклида вытекает существование наибольшего общего делителя для любых двух целых чисел a и b*. Чтобы доказать существование наибольшего общего делителя любого конечного множества $\{a_1, \ldots, a_n\}$ целых чисел, нам понадобится следующая теорема.

Теорема 3. *Если* $(a_1, \ldots, a_{n-1}) = \delta$ *и* $d = (\delta, a_n)$, *то* $d = (a_1, \ldots, a_n)$.

Доказательство. Так как $d = (\delta, a_n)$, то $a_n \vdots d$ и $\delta \vdots d$. А так как $\delta = (a_1, \ldots, a_{n-1})$, то при всех k, $1 \leqslant k \leqslant n-1$, имеем $a_k \vdots \delta$, и потому $a_k \vdots d$. Значит, d — общий делитель всех чисел: $a_1, \ldots, a_n$.

С другой стороны, пусть d_1 — общий делитель чисел $a_1, \ldots, a_n$. Тогда d_1 — общий делитель чисел $a_1, \ldots, a_{n-1}$, и потому $\delta \vdots d_1$. Но и $a_n \vdots d_1$, а потому наибольший общий делитель чисел δ и a_n, т. е. число d, делится на d_1. Мы доказали, что d делится на любой общий делитель чисел $a_1, \ldots, a_n$, т. е. $d = (a_1, \ldots, a_n)$.

Следствие. *Если* $(a_1, a_2) = d_1$, $(d_1, a_3) = d_2, \ldots, (d_{n-2}, a_n) = d_{n-1}$, *то* $(a_1, \ldots, a_n) = d_{n-1}$.

Доказательство. Проведем доказательство с помощью математической индукции. При $n = 2$, т. е. для двух чисел a_1 и a_2, утверждение справедливо. Пусть оно уже доказано для $n = k \geqslant 2$. Тогда из $(a_1, a_2) = d_1, \ldots, (d_{k-2}, a_k) = d_{k-1}$ следует, что $(a_1, \ldots, a_k) = d_{k-1}$. Если $(d_{k-1}, a_{k+1}) = d_k$, то в силу теоремы 3 имеем $(a_1, \ldots, a_{k+1}) = d_k$. Значит, утверждение верно и при $n = k + 1$. В силу математической индукции утверждение верно для всех n.

Следствие из теоремы 3 указывает путь нахождения наибольшего общего делителя нескольких чисел $a_1, \ldots, a_n$: сначала находим $d_1 = (a_1, a_2)$, потом $d_2 = (d_1, a_3)$ и т. д. вплоть до $d_{n-1} =$

* Кроме пары (0, 0), для которой НОД не существует.

$= (d_{n-2}, a_n)$, который и является наибольшим общим делителем чисел $a_1, \ldots, a_n$. Таким образом, нахождение наибольшего общего делителя чисел $a_1, \ldots, a_n$ сводится к последовательному нахождению наибольшего общего делителя двух чисел. Поскольку для двух чисел наибольший общий делитель всегда существует, он существует и для любого конечного множества целых чисел.

Пример. Найдем (988, 2014, 42598, 6726).

Введем обозначения: $a_1 = 988$; $a_2 = 2014$; $a_3 = 42598$; $a_4 = 6726$.

Применяя алгоритм Евклида, последовательно находим:

$$d_1 = (a_1, a_2) = (988, 2014) = 26;$$
$$d_2 = (d_1, a_3) = (26, 42598) = 2;$$
$$d_3 = (d_2, a_4) = (2, 6726) = 2.$$

Итак, $d = (988, 2014, 42598, 6726) = 2$.

3. Свойства наибольшего общего делителя. Докажем следующее утверждение.

Теорема 4. *Наибольший по величине положительный общий делитель δ целых чисел $a_1, \ldots, a_n$ является наибольшим общим делителем этих чисел.*

Доказательство. Из условий теоремы вытекает, что $\delta > 0$ — общий делитель чисел $a_1, \ldots, a_n$. Поэтому $d = (a_1, \ldots, a_n)$ делится на δ. Но тогда $d \geqslant \delta$. Поскольку δ — наибольший по величине положительный общий делитель чисел $a_1, \ldots, a_n$, а d — один из таких делителей, то $\delta \geqslant d$. Из неравенств $d \geqslant \delta$ и $\delta \geqslant d$ следует, что $d = \delta$.

Теорема 4 указывает еще один путь нахождения наибольшего общего делителя чисел a и b: необходимо выписать общие положительные делители данных чисел и выбрать среди них наибольший по величине. Этот метод несложен, если у чисел a и b мало делителей.

Теорема 5. *Если каждое из чисел a и b умножить на одно и то же число $k \neq 0$, то их наибольший общий делитель умножится на k.*

Доказательство. Умножим обе части каждого из равенств (1) в п. 2 на k. После очевидных преобразований получаем:

$$ak = bkq_0 + r_1k,$$
$$\ldots\ldots\ldots\ldots$$
$$r_{n-2}k = r_{n-1}kq_{n-1} + r_nk,$$
$$r_{n-1}k = r_nkq_n.$$

Следовательно,

$$(ak, bk) = r_nk = (a, b) \cdot k.$$

Точно так же доказывается, что если числа a и b имеют общий делитель δ, то

$$\left(\frac{a}{\delta}, \frac{b}{\delta}\right) = \frac{1}{\delta}(a, b).$$

Фундаментальную роль в дальнейшем изложении играет следующее свойство наибольшего общего делителя.

Теорема 6. *Если d — наибольший общий делитель чисел a и b, то существуют такие целые числа x и y, что $ax + by = d$.*

Равенство $ax + by = d$ называется представлением наибольшего общего делителя в виде линейной комбинации чисел a и b.

Доказательство. Воспользуемся алгоритмом Евклида.

Из первого равенства (1) п. 2 находим:

$$r_1 = a - bq_0 = ax_1 + by_1, \text{ где } x_1 = 1,\ y_1 = -q_0.$$

Из второго равенства (1) п. 2 получаем:

$$r_2 = b - r_1q_1 = b - (ax_1 + by_1)\,q_1 = a\,(-q_1x_1) + b\,(1 - q_1y_1) =$$

$$= ax_2 + by_2, \text{ где } x_2 = -q_1x_1,\ y_2 = 1 - q_1y_1 \text{ — целые числа.}$$

Продолжая аналогичные рассуждения и выкладки, получим: $r_n = ax_n + by_n$, где x_n, y_n — целые числа. Но $r_n = d$. Значит, $d = ax + by$, где $x_n = x$, $y_n = y$.

Теорема доказана.

Пример. Найдем линейное представление наибольшего общего делителя чисел 90 и 35.

Применяя алгоритм Евклида к числам 90 и 35, получаем:

$$\begin{aligned} 90 &= 35 \cdot 2 + 20 \\ 35 &= 20 \cdot 1 + 15 \\ 20 &= 15 \cdot 1 + 5 \\ 15 &= 5 \cdot 3 \end{aligned}$$

Последний, отличный от нуля остаток равен 5, поэтому $(90, 35) = 5$. Заметим, что в силу первого равенства $20 = 90 - 35 \cdot 2$. Подставляя это значение в равенство $15 = 35 - 20 \cdot 1$, получаем: $15 = 35 - (90 - 35 \cdot 2) = 35 \cdot 3 - 90$. Наконец, в равенстве $5 = 20 - 15 \cdot 1$ заменим 20 на $90 - 35 \cdot 2$, а 15 на $35 \cdot 3 - 90$ и получим искомое линейное представление:

$$5 = 90 - 35 \cdot 2 - (35 \cdot 3 - 90) = 90 \cdot 2 - 35 \cdot 5 = 2 \cdot 90 + (-5) \cdot 35.$$

Здесь $x = 2$ и $y = -5$.

Теорема, аналогичная теореме 6, верна и для наибольшего общего делителя нескольких целых чисел: если $d = (a_1, \ldots, a_n)$, то найдутся такие целые числа $x_1, \ldots, x_n$, что $d = a_1x_1 + \ldots + a_nx_n$.

Вопросы для самопроверки и упражнения

1. Что называется наибольшим общим делителем (НОД) двух чисел?
2. Пользуясь определением, установите, чему равен НОД чисел 15 и 0.
3. Как найти наибольший общий делитель двух чисел? Каковы основные свойства НОД?
4. На основании какой теоремы написаны равенства (1) п. 2?

5. Что можно сказать о сравнительной величине остатков r_1, r_2, ..., r_n в этих равенствах?

6. Почему процесс последовательного деления в алгоритме Евклида конечен?

7. Проверьте на числовых примерах справедливость теорем 4, 5, 6.

8. Как понимать, что НОД двух чисел является их линейной комбинацией?

9. С помощью алгоритма Евклида найдите НОД каждой из следующих систем чисел: а) 42 628, 33 124; б) 71 004, 154 452; в) 469 459, 519 203; г) 179 370 199, 4 345 121; д) 299, 391, 667; е) 1955, 2431, 3111, 4862.

10. Докажите, что если $a = cq + r$ и $b = cq_1 + r_1$, где a, b, q, q_1, r_1 — целые неотрицательные числа и c — целое положительное число, то $(a, b, c) = (r, r_1, c)$. Сформулируйте вытекающее отсюда правило нахождения (a, b, c) путем «последовательного двойного деления». Обобщите это правило на случай n чисел.

§ 3. ВЗАИМНО ПРОСТЫЕ ЧИСЛА И ИХ ОСНОВНЫЕ СВОЙСТВА

Определение 1. Если $(a_1, \ldots, a_n) = 1$, то числа a_i, a_2, ..., a_n называются *взаимно простыми*.

Например, числа 30 и 77 взаимно просты, поскольку $(30, 77) = 1$, а числа 30 и 72 не являются взаимно простыми, так как $(30, 72) = 6$.

Рассмотрим некоторые свойства взаимно простых чисел.

Теорема 1. *Для того чтобы числа a и b были взаимно простыми, необходимо и достаточно, чтобы существовали такие целые числа x и y, что*

$$ax + by = 1. \tag{1}$$

Необходимость. Если числа a и b взаимно просты, то $(a, b) = 1$. Тогда (по теореме 6 § 2) существуют такие целые числа x и y, что имеет место равенство (1).

Достаточность. Пусть существуют такие целые числа x и y, что имеет место равенство (1), и пусть $(a, b) = d$. Тогда (согласно свойству 4 делимости) из (1) следует, что $1 \vdots d$. Значит, $d = 1$, т. е. числа a и b взаимно просты.

Следствие. *Если числа a и b взаимно просты и $a \vdots a_1$, $b \vdots b_1$, то числа a_1 и b_1 взаимно просты.*

В самом деле, так как $(a, b) = 1$, то найдутся такие целые числа x и y, что $ax + by = 1$. Но по условию $a = a_1q$, $b = b_1t$, а потому

$$a_1 (qx) + b_1 (ty) = 1.$$

Это равенство показывает, что a_1 и b_1 взаимно просты.

Теорема 2. *Частные от деления чисел a и b на (a, b) взаимно просты.*

Пусть $(a, b) = d$. Тогда существуют такие целые числа x и y, что $ax + by = d$. Разделив обе части этого равенства на d, получим:

$$\frac{a}{d}x + \frac{b}{d}y = 1.$$

Следовательно, по теореме 1 $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, т. е. числа $\frac{a}{d}$, $\frac{b}{d}$ взаимно просты.

Теорема 3. *Если произведение двух чисел $a \cdot b$ делится на c и a взаимно просто с c, то b делится на c.*

Так как $(a, c) = 1$, то существуют такие целые числа x и y, что

$$ax + cy = 1.$$

Умножая обе части этого равенства на b, получим: $abx + cby = b$. По условию $ab \vdots c$, следовательно, левая часть последнего равенства (согласно свойству 4 делимости) делится на c; тогда и правая часть тоже делится на c, т. е. $b \vdots c$.

Теорема 4. *Если числа a и b взаимно просты, то число c делится на ab тогда и только тогда, когда c делится на a и на b.*

Необходимость. Так как c делится на ab и ab делится на a и на b, то c делится на a и на b.

Достаточность. Если c делится на a, то $c = aq$. Но c делится на b, а числа a и b взаимно просты. В силу теоремы 3 получаем, что q делится на b. Но тогда $c = aq = abq_1$, т. е. c делится на ab.

Теорема может быть обобщена на случай любого конечного числа попарно взаимно простых чисел. В качестве следствий из нее можно получить признаки делимости на составные числа. Например, для того чтобы число N делилось на 6, необходимо и достаточно, чтобы оно делилось на 2 и на 3, поскольку $6 = 2 \cdot 3$ и $(2, 3) = 1$.

Примеры.

1. Число 876 делится на 6, так как оно делится на 2 и на 3; 876 — число четное и сумма его цифр делится на 3.

Для того чтобы число N делилось на 30, необходимо и достаточно, чтобы оно делилось на 2, на 3 и на 5.

В самом деле, $30 = 2 \cdot 3 \cdot 5$ и $(2, 3) = (3, 5) = (2, 5) = 1$.

2. Число 324 750 делится на 2 и на 5, так как оно оканчивается нулем и делится на 3, потому что сумма его цифр делится на 3. Следовательно, 324 750 делится на 30.

3. Число 123 530 не делится на 30, так как сумма его цифр не делится на 3 (хотя на 2 и на 5 данное число делится).

Теорема 5. *Если два числа a и b взаимно просты с третьим числом c, то и их произведение взаимно просто с c.*

Доказательство. Проведем доказательство от противного. Предположим, что $(ab, c) = d > 1$. Тогда $c \vdots d$. Так как по условию $(a, c) = 1$, то по следствию из теоремы 1 и $(a, d) = 1$. Поскольку $ab \vdots d$ и $(a, d) = 1$, то по теореме 3 $b \vdots d$. Значит, d является общим делителем чисел b и c, а это противоречит предположе-

нию о том, что эти числа взаимно просты. Полученное противоречие и доказывает, что $(ab, c) = 1$.

Эту теорему можно обобщить следующим образом: если каждое из чисел $a_1, \ldots, a_m$ взаимно просто с каждым из чисел $b_1, \ldots, b_n$, то и произведение $a_1 \cdot \ldots \cdot a_m$ взаимно просто с произведением $b_1 \cdot \ldots \cdot b_n$.

Действительно, имеем $(a_i, b_k) = 1$, где $i = 1, 2, \ldots, m$, $k = 1, 2, \ldots, n$. Тогда в силу доказанной теоремы $(a_1 \cdot a_2, b_k) = 1$, $(a_1 \cdot a_2 \cdot a_3, b_k) = 1$ и т. д.

В конце концов получим, что $(a_1 \cdot a_2, \ldots \cdot a_m, b_k) = 1$, т. е. произведение $a_1 \cdot a_2 \cdot \ldots \cdot a_m = A$ взаимно просто с b_k $(k = 1, 2, \ldots, n)$.

Точно так же будем иметь $(A, b_1) = (A, b_1 \cdot b_2) = \ldots = (A, b_1 \cdot b_2 \cdot \ldots \cdot b_n) = 1$, т. е. $a_1 \cdot a_2 \cdot \ldots \cdot a_m$ взаимно просто с $b_1 \cdot b_2 \cdot \ldots \cdot b_n$.

Следствие. *Если числа a и b взаимно просты, то любые их натуральные степени — взаимно простые числа.*

Действительно, положив $a_1 = a_2 = \ldots = a_m = a$ и $b_1 = b_2 = \ldots = b_n = b$, получим $(a^m, b^n) = 1$.

На основании этого следствия можно утверждать, что никакая натуральная степень несократимой дроби, знаменатель которой отличен от нуля, не может быть сократимой дробью и, в частности, натуральным числом.

Последнее означает, что корень n-й степени из натурального числа не может равняться несократимой дроби.

Замечание. *Из того, что $(a_1, a_2, \ldots, a_n) = 1$, еще не следует, что и числа, образующие некоторое подмножество множества $A = \{a_1, a_2, \ldots, a_n\}$, взаимно просты.* Вместе с тем нетрудно заметить, что если каждая пара чисел из множества A взаимно проста (т. е. $(a_i, a_j) = 1$, где $i, j = 1, 2, \ldots, n$), то $(a_1, a_2, \ldots, a_n) = 1$. Действительно, если допустить, что $(a_1, a_2, \ldots, a_n) = d > 1$, то наибольший общий делитель любой пары чисел из множества A был бы больше или равен $d > 1 : (a_i, a_j) \geqslant d > 1$. Получили противоречие.

Определение 2. Если любая пара чисел, составленная из чисел $a_1, \ldots, a_n$, взаимно проста, то числа $a_1, \ldots, a_n$ называют *попарно взаимно простыми*.

Например, числа 715, 96, 119 попарно взаимно просты, так как $(715, 96) = (715, 119) = (96, 119) = 1$.

Вопросы для самопроверки и упражнения

1. Какие числа называются взаимно простыми?
2. Каково условие взаимной простоты двух чисел a и b?
3. Перечислите свойства взаимно простых чисел.
4. Какая разница между понятиями: «взаимно простые числа» и «попарно взаимно простые числа»?
5. Какое из понятий «взаимно простые числа» и «попарно взаим-

но простые числа» является следствием другого? В каком случае эти два понятия совпадают?

6. Докажите, что $\sqrt[3]{5}$ — иррациональное число.

7. Существует ли такая пара целых чисел x и y, что $6x + 8y = 1$?

8. Для того чтобы делитель d чисел a и b был их наибольшим общим делителем, необходимо и достаточно, чтобы $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. Докажите.

9. Докажите, что алгебраическая сумма несократимых дробей, знаменатели которых попарно просты, не может быть целым числом.

10. Докажите, что целые решения уравнения $x^2 + y^2 = z^2$, где $x > 0$, $y > 0$, $z > 0$ и $(x, y, z) = 1$, получаются по формулам

$$x = uv,\ y = \frac{u^2 - v^2}{2},\ z = \frac{u^2 + v^2}{2},$$

при этом $u > v > 0$, $(u, v) = 1$, u и v нечетные.

§ 4. НАИМЕНЬШЕЕ ОБЩЕЕ КРАТНОЕ

Определение 1. Пусть $a_1, \ldots, a_n$ — целые числа, отличные от нуля. Целое число M называется *общим кратным* этих чисел, если оно делится на каждое из данных чисел.

Например, произведение $a_1, \ldots, a_n$ — общее кратное всех своих сомножителей.

Определение 2. Целое число m называется *наименьшим общим кратным* чисел $a_1, \ldots, a_n$, если оно является их общим кратным и если любое общее кратное этих чисел делится на m.

Покажем, что если наименьшее общее кратное чисел $a_1, \ldots, a_n$ существует, то оно однозначно определено с точностью до знака. В самом деле, пусть m_1 и m_2 — наименьшие общие кратные чисел $a_1, \ldots, a_n$. Тогда по определению 2 должны выполняться соотношения $m_1 \vdots m_2$ и $m_2 \vdots m_1$. Эти соотношения могут выполняться лишь при условии, что $m_1 = m_2$ или $m_1 = -m_2$.

В дальнейшем мы будем выбирать положительное значение наименьшего общего кратного и обозначать его так:

$$m = [a_1, \ldots, a_n].$$

Докажем следующую теорему:

Теорема 1. *Число* $\frac{ab}{(a, b)}$, *где* (a, b) — *наибольший общий делитель двух натуральных чисел* a *и* b, *является наименьшим общим кратным этих чисел.*

Доказательство. Пусть $(a, b) = d$, тогда $a = nd$ и $b = ld$, где $(n, l) = 1$. Следовательно,

$$\frac{ab}{(a, b)} = \frac{nd \cdot ld}{d} = nld = nb = al.$$

Это равенство показывает, что $\frac{ab}{(a, b)}$ делится на a и на b, т. е. является общим кратным чисел a и b.

Покажем теперь, что любое кратное $M > 0$ чисел a и b делится на $\frac{ab}{(a, b)}$. В самом деле, $M \vdots a$, и потому существует такое целое число s, что $M = as = nds$. Поскольку $M \vdots b$ и $b = ld$, то $nds \vdots ld$, и потому $ns \vdots l$. Но $(n, l) = 1$, и потому в силу теоремы 3 § 3 $s \vdots l$. Значит, существует такое натуральное число k, что $s = lk$. Но тогда $M = nds = ndlk$ и, поскольку $\frac{ab}{(a, b)} = nld$, число M делится на $\frac{ab}{(a, b)}$.

Мы доказали, что $m = \frac{ab}{(a, b)}$ — наименьшее общее кратное чисел a и b. Теорема доказана.

Следствие 1. *Любые два отличные от нуля целые числа имеют наименьшее общее кратное.*

В самом деле, этим наименьшим общим кратным является число $[a, b] = \frac{ab}{(a, b)}$.

Следствие 2. *Наименьшее общее кратное двух чисел a и b ($a \neq 0$, $b \neq 0$) является наименьшим по величине положительным общим кратным этих чисел.*

В самом деле, любое общее кратное $M > 0$ чисел a и b делится на $m = \frac{ab}{(a, b)}$, а потому $M \geqslant m$.

Пример 1. Найдем [364, 143]. Сначала находим (364, 143):

$$\begin{array}{r|l}
364 & 143 \\
\cline{2-2}
286 & 2 \\
\cline{2-2}
143 & 78 \\
\cline{2-2}
78 & 1 \\
\cline{2-2}
78 & 65 \\
\cline{2-2}
65 & 1 \\
\cline{2-2}
65 & 13 \\
\cline{2-2}
65 & 5 \\
\cline{2-2}
0 &
\end{array}$$

$(364, 143) = 13$.

Значит, $[364,\ 143] = \dfrac{364 \cdot 143}{13} = 28 \cdot 143 = 4004.$

Рассмотрим основные свойства наименьшего общего кратного.

Свойство 1. *Если каждое из чисел a и b умножить на одно и то же число $k \neq 0$, то их* НОК *умножится на k.*

Действительно:

$$[ak,\ bk] = \frac{ak \cdot bk}{(ak,\ bk)} = \frac{abk^2}{(a, b)\,k} = \frac{ab}{(a,\ b)} \cdot k = [a,\ b] \cdot k.$$

Свойство 2. *Если $a \vdots k$ и $b \vdots k$, то*

$$\left[\frac{a}{k}, \frac{b}{k}\right] = [a,\ b] \vdots k.$$

Доказательство аналогично доказательству свойства 1.

Пример 2. Найдем [5640, 2500].

Разделим каждое из данных чисел на 10 (очевидный делитель) и найдем [564, 250]. Поступая, как и в примере 1, находим $[564, 250] = \dfrac{564 \cdot 250}{(564,\ 250)} = \dfrac{564 \cdot 250}{2} = 564 \cdot 125 = 70\,500.$

Тогда $[5640,\ 2500] = 70\,500 \cdot 10 = 705\,000.$

Мы выяснили, как находят НОК двух чисел. Для нахождения НОК нескольких чисел имеет место правило, аналогичное рассмотренному выше правилу нахождения НОД нескольких чисел.

Теорема 2. *Если $[a_1, \ldots, a_{n-1}] = \mu$ и $[\mu, a_n] = m$, то $[a_1, \ldots, a_n] = m$.*

Доказательство. Число $m = [\mu, a_n]$ делится на a_n и на μ. Но μ делится на каждое из чисел $a_1, \ldots, a_{n-1}$. Поэтому m делится на любое из чисел $a_1, \ldots, a_n$, т. е. является их общим кратным.

Пусть M — общее кратное чисел $a_1, \ldots, a_n$. Тогда M делится на числа $a_1, \ldots, a_{n-1}$, а значит, и на $[a_1, \ldots, a_{n-1}] = \mu$. Так как M делится и на a_n, то M делится на $[\mu, a_n] = m$. Этим доказано, что m — наименьшее общее кратное чисел $a_1, \ldots, a_n$.

Из теоремы 2 точно так же, как и в случае наибольшего общего делителя, вытекает следующее утверждение:

Теорема 3. *Если $[a_1, a_2] = m_1$, $[m_1, a_3] = m_2$, $\ldots$, $[m_{n-2}, a_n] = m_{n-1}$, то $[a_1, \ldots, a_n] = m_{n-1}$.*

Иными словами, чтобы найти наименьшее общее кратное чисел $a_1, \ldots, a_n$, надо сначала найти $m_1 = [a_1, a_2]$, потом $m_2 = [m_1, a_3]$ и т. д. вплоть до $m_{n-1} = [m_{n-2}, a_n]$. Число m_{n-1} равно $[a_1, \ldots, a_n]$. На каждом шагу нам придется находить наименьшее общее кратное двух чисел, а это мы уже умеем делать.

Пример 3. Найдем [35, 77, 1141].

$$[35,\ 77] = \frac{35 \cdot 77}{(35,\ 77)} = \frac{35 \cdot 77}{7} = 35 \cdot 11 = 385,$$

$$[385,\ 1141] = \frac{385 \cdot 1141}{(385,\ 1141)} = \frac{385 \cdot 1141}{7} = 385 \cdot 163 = 62\,755.$$

Ответ. [35, 77, 1141] = 62 755.

Теорема 4. НОК *попарно взаимно простых чисел* $a_1, \ldots, a_n$ *равно их произведению.*

Действительно, пусть $(a_i, a_j) = 1$ $(i, j = 1, 2, \ldots, n)$, тогда

$$m_2 = [a_1,\ a_2] = \frac{a_1 a_2}{(a_1,\ a_2)} = \frac{a_1 a_2}{1} = a_1 a_2,$$

$$m_3 = [m_2 a_3] = \frac{m_2 a_3}{(m_2,\ a_3)} = \frac{a_1 a_2 a_3}{(a_1,\ a_2,\ a_3)} =$$

$$= \frac{a_1 a_2 a_3}{(1,\ a_3)} = \frac{a_1 a_2 a_3}{1} = a_1 a_2 a_3.$$

Аналогично рассуждая, дальше на $(n-1)$-м шаге получим:

$$m_n = [m_{n-1},\ a_n] = a_1 a_2 \ldots a_n.$$

Пример 4. Найдем [37, 43, 95].
Имеем (37, 43) = 1, (37, 95) = 1, (43, 95) = 1.
Следовательно, [37, 43, 95] = 37 · 43 · 95.

Вопросы для самопроверки и упражнения

1. Какое число называется общим кратным данных чисел?
2. Что называется наименьшим общим кратным двух чисел? нескольких чисел?
3. Чему равно НОК двух чисел?
4. НОК двух чисел a и b равно их произведению тогда и только тогда, когда a и b взаимно просты. Докажите.
5. Найдите НОК каждой из следующих систем чисел: а) 120, 96; б) 71 004, 154 452; в) 232, 460, 280; г) 67 283, 122 433, 221 703.
6. Докажите, что две положительные несократимые дроби равны тогда и только тогда, когда равны соответственно их числители и знаменатели.

§ 5. ПРОСТЫЕ И СОСТАВНЫЕ ЧИСЛА

1. Простые числа и их свойства. Определение 1. Натуральное число p называется *простым*, если оно больше 1 и не имеет положительных делителей, отличных от 1 и p.

Определение 2. Натуральное число n называется *составным*, если оно больше 1 и имеет по крайней мере один положительный делитель, отличный от 1 и n.

Согласно определению 2, если n — составное, то существует такой делитель δ, что $n = n_1\delta$, где $1 < n_1 < n$, $1 < \delta < n$.

Число 1 не относят ни к простым, ни к составным числам.

Первыми простыми числами в натуральном ряду чисел являются 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41...

Среди простых чисел имеется лишь одно четное число 2.

Итак, множество всех натуральных чисел разбивается на три подмножества: 1) простые числа, 2) составные числа, 3) число 1.

Основным результатом теории простых чисел является тот факт, что любое составное число разлагается (и притом единственным образом с точностью до порядка) в произведение простых чисел. Чтобы доказать эту теорему, рассмотрим сначала некоторые свойства простых чисел.

Теорема 1. *Если простое число p делится на некоторое натуральное число $n \neq 1$, то $p = n$.*

В самом деле, если бы $p \neq n$, то p имело бы три делителя: 1, p и n, а следовательно, не было бы простым.

Теорема 2. *Если p_1 и p_2 — различные простые числа, то p_2 не делится на p_1.*

Доказательство. Так как p_2 простое, то оно может делиться лишь на 1 и на p_2. По условию $p_1 \neq p_2$, а по определению $p_1 \neq 1$, следовательно, p_2 не делится на p_1.

Теорема 3. *Всякое натуральное число $n > 1$ делится хотя бы на одно простое число.*

Доказательство. Применим метод математической индукции.

1) Для натурального числа $n = 2$ теорема справедлива, т. е. 2 делится на простое число 2.

2) Предположим, что утверждение теоремы справедливо для всех натуральных чисел, больших 1 и меньших n, и докажем справедливость теоремы для числа n.

Если n простое, то n делится на простое число $p = n$, и теорема доказана.

Если же n составное, то $n = n_1 c$ $(1 < n_1 < n,\ 1 < c < n)$.

Так как $n_1 < n$, то по индуктивному предположению для n_1 теорема верна, т. е. n_1 делится хотя бы на одно простое число p. Но тогда и n делится на p. Теорема доказана.

Теорема 4. *Если n — натуральное число, а p — простое число, то либо n делится на p, либо n и p взаимно просты.*

Доказательство. Пусть d — наибольший общий делитель чисел n и p, т. е. $(n, p) = d$. Так как p — простое число, то либо $d = 1$, либо $d = p$. Если $d = 1$, то n и p взаимно просты. Если $d = p$, то $n \vdots p$. Теорема доказана.

Теорема 5. *Если произведение двух или нескольких натуральных чисел делится на простое число p, то хотя бы один из сомножителей делится на p.*

Доказательство. Воспользуемся методом математической индукции. Рассмотрим сначала произведение двух сомножителей. Пусть $a_1 a_2 \vdots p$. Здесь возможны два случая: $a_1 \vdots p$ или a_1 не делится на p. Если $a_1 \vdots p$, то утверждение доказано. Если a_1 не

делится на p, то согласно теореме 4 § 3 a_1 и p взаимно просты; тогда на основании теоремы 7 § 3 $a_2 \vdots p$.

Допустим далее, что теорема справедлива для случая, когда произведение содержит менее $k+1$ сомножителей, и докажем справедливость ее для случая $k+1$ сомножителей.

Рассмотрим произведение $k+1$ сомножителей:

$$n = a_1 a_2 \ldots a_k a_{k+1}. \qquad (1)$$

Представим выражение (1) в виде двух сомножителей, пользуясь сочетательным законом:

$$n = (a_1 \ldots a_k) \cdot a_{k+1} = m \cdot a_{k+1}.$$

Но для двух сомножителей теорема доказана; следовательно, одно из чисел m или a_{k+1} должно делиться на p. Если $a_{k+1} \vdots p$, то теорема доказана. Если $m \vdots p$, то в силу индуктивного предположения (m содержит k сомножителей) хотя бы одно из чисел a_1, a_2, ..., a_k должно делиться на p. Теорема доказана.

2. Разложение составных чисел на простые множители.

Теорема 6. *Если натуральное число n составное, а p — наименьший его простой делитель, то $p \leqslant \sqrt{n}$.*

Доказательство. Так как n — составное число, а p — его наименьший простой делитель, то $n = p \cdot n_1$, причем $p \leqslant n_1$. Умножая левую и правую части последнего неравенства на равные числа pn_1 и n, получим $p^2 n_1 \leqslant n_1 n$, откуда $p^2 \leqslant n$, или $p \leqslant \sqrt{n}$.

Из теоремы 6 следует, что если число n не делится ни на одно простое число, не превосходящее $\sqrt{n}$, то n — простое; в противном случае n — составное.

Пример. Пусть $n = 137$. $11 < \sqrt{137} < 12$. Рассмотрим простые числа 2, 3, 5, 7, 11. Число 137 не делится ни на одно из этих чисел, следовательно, 137 — простое число.

Теорема 7 (основная теорема арифметики). *Всякое натуральное число $n > 1$ либо просто, либо может быть представлено, и притом единственным образом, в виде произведения простых чисел.*

Два представления, отличающиеся только порядком расположения сомножителей, будем считать совпадающими.

Существование разложения. Пусть $n = 2$. Так как 2 — простое число, то для $n = 2$ утверждение доказано.

Предположим, что утверждение справедливо для всех натуральных чисел, больших или равных 2, но меньших n, и докажем справедливость его для числа n.

Рассмотрим натуральное число n. Если n — простое, то утверждение доказано. Если n — составное, то его можно представить в виде:

$$n = n_1 n_2,$$

где $1 < n_1 < n$, $1 < n_2 < n$.

Для чисел n_1 и n_2 согласно индуктивному предположению утверждение справедливо:

$$n_1 = p_1 \dots p_l, \quad n_2 = p_{l+1} \dots p_k.$$

Тогда

$$n = n_1 n_2 = p_1 \dots p_l \cdot p_{l+1} \dots p_k. \tag{1}$$

Существование разложения доказано.

Единственность разложения. Пусть $n = 2$. Число 2 простое, и его нельзя представить в виде произведения простых чисел.

Итак, для $n = 2$ утверждение справедливо.

Предположим, что утверждение справедливо для всех натуральных чисел, больших 2, но меньших n, и докажем справедливость его для числа n. Если n просто, то его нельзя представить в виде произведения простых чисел. Пусть теперь n — составное число и пусть число n представлено двумя способами в виде произведения простых чисел:

$$n = p_1 p_2 \dots p_k,$$
$$n = q_1 q_2 \dots q_s.$$

Тогда

$$p_1 p_2 \dots p_k = q_1 q_2 \dots q_s. \tag{2}$$

Левая часть равенства (2) делится на простое число p_1. Следовательно, и правая часть тоже делится на p_1. Согласно теореме 5 п. I хотя бы один из сомножителей произведения $q_1 q_2 \dots q_s$ должен делиться на p_1. Пусть $q_1 \vdots p_1$. Так как q_1 — простое число и $p_1 > 1$, то по теореме 1 п. 1 $q_1 = p_1$.

Разделив обе части равенства (2) на p_1, получим:

$$p_2 \dots p_k = q_2 \dots q_s. \tag{3}$$

Так как $p_2 \dots p_k$ и $q_2 \dots q_s$ меньше, чем n, то по индуктивному предположению из равенства (3) следует, что $k = s$, а числа $p_2, \dots, p_k$ отличаются от чисел $q_2, \dots, q_s$ лишь порядком.

Поэтому при соответствующей нумерации этих чисел имеем:

$$p_1 = q_1, \quad p_2 = q_2, \quad \dots, \quad p_k = q_s.$$

Разложение натурального числа n на простые множители единственно. Теорема доказана.

Итак, согласно основной теореме арифметики всякое составное число $n > 1$ может быть представлено в виде произведения простых чисел. Среди этих простых множителей могут встречаться одинаковые. Пусть, например, p_1 встречается α_1 раз, p_2 встречается α_2 раз, ..., p_k встречается α_k раз; тогда разложение числа n на простые множители можно записать следующим образом:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots p_k^{\alpha_k}, \tag{4}$$

Множители $p_1, p_2, \ldots, p_k$ обычно располагают в порядке возрастания.

Представление натурального числа n в форме (4) называется *каноническим*; это представление единственно. Представление (4) называют также *факторизацией* числа n.

Примеры. $1176 = 2^3 \cdot 3 \cdot 7^2$; $136\,125 = 5^3 \cdot 11^2$.

Из канонического представления числа вытекают следующие предложения.

Следствие 1. *Если* $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ — *каноническое разложение числа* a, *то все делители этого числа имеют вид*:

$$c = p_1^{\beta_1} \cdot p_2^{\beta_2} \ldots p_k^{\beta_k}, \tag{5}$$

где $0 \leqslant \beta_i \leqslant \alpha_i$ $(i = 1, 2, \ldots, k)$.

В самом деле, очевидно, что всякое c вида (5) делит a. Обратно, пусть c делит a, тогда $a=cq$, где c — целое число и, следовательно, все простые делители числа c входят в каноническое разложение числа a с показателями β_i, где $0 \leqslant \beta_i \leqslant \alpha_i$. Поэтому все делители δ числа a имеют вид (5).

Пусть даны натуральные числа a и b. Их канонические разложения всегда можно записать в виде:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}, \; b = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_s^{\gamma_s}.$$

Мы предполагаем здесь, что α_i и γ_i могут принимать и нулевые значения. Это позволит писать в обоих разложениях одни и те же простые числа $p_1, p_2, \ldots, p_s$, а именно простые числа, которые входят в разложение хотя бы одного из чисел a и b. Справедливы следующие утверждения.

Следствие 2. *Наибольший общий делитель чисел* a *и* b *имеет вид*:

$$(a, b) = p_1^{\lambda_1} p_2^{\lambda_2} \ldots p_s^{\lambda_s},$$
$$\text{где } \lambda_i = \min(\alpha_i, \gamma_i).$$

Следствие 3. *Наименьшее общее кратное чисел* a *и* b *имеет вид*:

$$[a, b] = p_1^{\mu_1} p_2^{\mu_2} \ldots p_s^{\mu_s},$$
$$\text{где } \mu_i = \max(\alpha_i, \gamma_i).$$

Эти утверждения очевидны. Из них непосредственно следует ранее доказанное тождество $[a, b] \cdot (a, b) = ab$. Эти утверждения переносятся и на случай более чем двух чисел.

3. Бесконечность множества простых чисел.

Теорема 8 (Евклида). *Множество простых чисел бесконечно.*

Доказательство (от противного). Предположим, что множество простых чисел конечно: пусть это будут числа $p_1 = 2$, $p_2, \ldots, p_k$, где p_k — наибольшее простое число.

Составим произведение $p_1 \cdot p_2 \cdot \ldots \cdot p_k$ всех простых чисел и рассмотрим натуральное число $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$. Так как $n > p_k$, то n должно быть составным. Следовательно, оно должно делиться на некоторое простое число. Но по предположению все простые числа принадлежат конечному множеству $\{p_1, \ldots, p_k\}$. Значит, n делится на одно из чисел $p_1, \ldots, p_k$, скажем на p_1. Поскольку произведение $p_1 \ldots p_k$ тоже делится на p_1 и $n = p_1 \ldots p_k + 1$, то и число 1 должно делиться на p_1. Но это невозможно, так как $1 < p_1$. Полученное противоречие доказывает теорему.

Таким образом, простых чисел бесконечно много. Вместе с тем оказывается, что простые числа составляют лишь небольшую часть чисел натурального ряда.

Теорема 9 (об интервалах). *В натуральном ряду существуют сколь угодно длинные интервалы, не содержащие ни одного простого числа.*

Доказательство. Возьмем произвольное натуральное число n и составим такую последовательность натуральных чисел:

$$(n+1)! + 2,\ (n+1)! + 3,\ \ldots,\ (n+1)! + n + 1.$$

Все эти числа составные. Мы получили n идущих подряд составных чисел.

Сопоставление фактов, вытекающих из теоремы Евклида и теоремы об интервалах, свидетельствует о сложном характере распределения простых чисел в натуральном ряду. Вопрос этот является одним из труднейших в математике (см. § 7).

4. Решето Эратосфена. Греческим математиком Эратосфеном (III в. до н. э.) был найден способ выделения простых чисел из любого отрезка 1, 2, 3, ..., n натурального ряда путем вычеркивания числа 1, затем всех чисел, кратных числу 2 (кроме 2), затем — кратных числу 3 (кроме 3), и т. д.

Таким образом, надо вычеркнуть все числа, кратные простым числам: $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ..., $p \leqslant \sqrt{n}$.

Практические советы

1) Каждое p_s-е число после p_s (считая и уже зачеркнутые ранее) кратно p_s и подлежит вычеркиванию.

2) Дойдя до невычеркнутого простого числа, большего или равного $\sqrt{n}$, следует остановиться, так как все числа, оставшиеся невычеркнутыми, уже простые (на основании теоремы 6).

Пример. Выделим простые числа из отрезка натурального ряда: 1, 2, 3, ..., 40.

Выписываем все натуральные числа от 2 до 40 и вычеркиваем указанным способом все составные числа (вычеркивание заменяем подчеркиванием).

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.

Числа 3, 5, 7, 11, 13, 19, 23, 29, 31, 37 простые.

Разложение натурального числа на простые множители, распознавание простых чисел является довольно трудоемким делом. Облегчить работу можно, используя теорему 6.

Примеры.

1. Установим, каким числом является натуральное число 919, простым или составным.

Если число 919 составное, то его наименьший простой делитель не должен превосходить $\sqrt{919}$. Таким образом, следует выяснить, нет ли делителей среди простых чисел, не превосходящих $\sqrt{919}$. Находим, что $30 < \sqrt{919} < 31$. Далее выпишем все простые числа, не превосходящие числа 30. Это будут числа 2, 3, 5, 7, 11, 13, 17, 19, 23, 29. Проверим каждое из них. Число 919 ни на одно из указанных чисел не делится, следовательно, 919 — простое число.

2. Является ли простым число 323? Находим, что $18 < \sqrt{323} < 19$. Проверяем простые числа 2, 3, 5, 7, 11, 13, 17. Устанавливаем, что 323 делится на 17, следовательно, 323 — число составное.

3. Разложим на простые множители число 7469. Находим, что $86 < \sqrt{7469} < 87$. Далее испытываем все простые числа, не превосходящие 86: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 71, 73, 79, 83. Устанавливаем, что 7469 не делится на 2, 3, 5, но на 7 делится: $7469 = 7 \cdot 1067$. Число 1067 не делится на 2, 3, 5.

Далее находим, что $32 < \sqrt{1067} < 33$. Проверяем теперь простые числа 7, 11, 13, 17, 19, 23, 29, 31. Устанавливаем, что 1067 не делится на 2, 3, 5, 7, но делится на 11: $1067 = 11 \cdot 97$, а 97 — простое число. Окончательно получаем разложение: $7469 = 7 \cdot 11 \cdot 97$.

Вопросы для самопроверки и упражнения

1. Какие числа называются простыми? составными?
2. Является ли 1 простым числом? составным числом?
3. Какие из простых чисел четные?
4. Может ли одно простое число делиться на другое простое число?
5. Число 30 не делится на простое число 13. Чему равно $(30, 13)$? Чему равно $[30, 13]$?
6. Докажите, что если ни одно из чисел $a_1, \ldots, a_n$ не делится на простое число p, то их произведение тоже не делится на p.
7. Исследуется вопрос: является ли простым число 1093? Уже проверено, что оно не делится ни на одно из чисел 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37. Следует ли продолжать проверку? Почему?
8. Напишите все разложения числа 30 на простые множители (считая различными разложения, отличающиеся порядком множителей). То же самое сделайте для числа 96.

9. Можно ли назвать самое большое простое число?

10. Могут ли в натуральном ряду чисел идти подряд 1 000 000 составных чисел?

11. С помощью решета Эратосфена найдите простые числа от 2 до 300.

12. Укажите пары простых чисел, меньших 300, разность которых равна двум (например, 3 и 5, 5 и 7, 11 и 13 и т. д.).

13. Определите, какие числа между 2680 и 2710 простые.

14. Какие из чисел $p = 2 \cdot 3 \cdot 5 \cdot \ldots \cdot p + 1$, где $p = 5, 7, 11, 13$, будут простыми, а какие составными? Найдите канонические разложения составных чисел.

15. С помощью канонического разложения найдите НОД каждой из следующих систем чисел: а) 349, 387; б) 12 606, 6494; в) 29 719, 76 501; г) 2737, 9163, 9639.

16. С помощью канонического разложения найдите НОК каждой из следующих систем чисел: а) 187, 533; б) 32 176, 162 891; в) 2737, 9163, 9639.

17. Найдите каноническое разложение чисел: а) 82 798 848; б) 4 497 552 259 200; в) 67 463 283 888 000.

18. Сколько существует способов разложения числа $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ в произведение двух взаимно простых множителей?

19. Пусть $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ — каноническое разложение натурального числа n. Докажите, что $\sqrt[m]{n}$ тогда и только тогда является целым числом, когда показатели $\alpha_1, \ldots, \alpha_k$ канонического разложения делятся на m.

20. Докажите, что сумма $\frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$ $(n > 1)$ не может быть целым числом.

21. Докажите, что сумма $\frac{1}{3} + \frac{1}{5} + \ldots + \frac{1}{2n+1}$ $(n > 0)$ не может быть целым числом.

22. Докажите, что если $2^n + 1$ — простое число, где n — целое положительное, то $n = 2^k$, где k — целое неотрицательное число.

23. Докажите, что если $(2^n - 1)$ — простое число, то и n — простое число.

24. Докажите, что существует бесконечное множество простых чисел вида $(6m - 1)$.

§ 6. ЧИСЛОВЫЕ ФУНКЦИИ

1. Число и сумма натуральных делителей. В этом параграфе мы рассмотрим некоторые функции, заданные на множестве натуральных чисел и связанные с арифметической природой этих чисел. Их называют *числовыми функциями*. Примерами таких функций могут служить:

1) число $\tau(n)$ всех натуральных делителей n;

2) сумма $\sigma(n)$ всех натуральных делителей числа n;

3) число $\varphi(n)$ натуральных чисел, меньших n и взаимно простых с n (функция Эйлера).

Выведем формулу, позволяющую вычислить $\tau(n)$, зная каноническое разложение n: $n = p_1^{k_1} \dots p_m^{k_m}$. Мы уже знаем, что любой делитель числа n имеет вид:

$$c = p_1^{l_1} \dots p_m^{l_m},$$

где для любого j, $1 \leqslant j \leqslant m$, выполняются неравенства $0 \leqslant l_j \leqslant k_j$. Поэтому показатель l_1 может принимать $k_1 + 1$ различных значений: 0, 1, ..., k_1, показатель l_2 принимает $k_2 + 1$ различное значение, ..., показатель l_m принимает $k_m + 1$ различных значений. Иными словами, в кортеже $(l_1, \dots, l_m)$ первая координата может принимать $(k_1 + 1)$ значений, вторая — $(k_2 + 1)$ значений, ..., m-я — $(k_m + 1)$ значений. Но в первой части курса «Алгебра и теория чисел» было показано, что число таких кортежей равно $(k_1 + 1)(k_2 + 1) \dots (k_m + 1)$.

Итак, мы доказали следующую теорему:

Теорема 1. *Если каноническая запись числа n имеет вид*:

$$n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}, \tag{1}$$

то число натуральных делителей n равно:

$$\tau(n) = (k_1 + 1)(k_2 + 1) \dots (k_m + 1). \tag{2}$$

Пример. Поскольку $60 = 2^2 \cdot 3 \cdot 5$, то

$$\tau(60) = (2 + 1)(1 + 1)(1 + 1) = 3 \cdot 2 \cdot 2 = 12.$$

Делителями числа 60 являются 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60. Их число действительно равно 12.

Теперь выведем формулу для $\sigma(n)$ — суммы всех натуральных делителей.

Пусть $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$. Рассмотрим произведение

$$(1 + p_1 + \dots + p_1^{k_1})(1 + p_2 + \dots + p_2^{k_2}) \dots (1 + p_m + \dots + p_m^{k_m}). \tag{2'}$$

Если раскрыть скобки, то получим сумму членов вида $p_1^{l_1} \dots p_m^{l_m}$, где при любом j, $1 \leqslant j \leqslant m$, выполняется неравенство $0 \leqslant l_j \leqslant k_j$. Но такие члены являются делителями n, причем каждый делитель входит в сумму только один раз. Поэтому произведение (2′) равно сумме всех делителей n, т. е. $\sigma(n)$. Итак,

$$\sigma(n) = (1 + p_1 + \dots + p_1^{k_1})(1 + p_2 + \dots + p_2^{k_2}) \dots (1 + p_m + \dots + p_m^{k_m}).$$

Но каждая сумма $1 + p_j + \dots + p_j^{k_j}$ является суммой геометри-

ческой прогрессии со знаменателем p_j. Применяя формулу суммирования геометрической прогрессии, получаем, что

$$\sigma(n) = \frac{p_1^{k_1+1}-1}{p_1-1} \cdot \frac{p_2^{k_2+1}-1}{p_2-1} \cdots \frac{p_m^{k_m+1}-1}{p_m-1}. \qquad (3)$$

Итак, мы доказали следующую теорему.

Т е о р е м а 2. *Если каноническая запись числа n имеет вид $n = p_1^{k_1} \ldots p_m^{k_m}$, то $\sigma(n)$ выражается формулой* (3).

П р и м е р. Найдем сумму натуральных делителей числа 360. Так как $360 = 2^3 \cdot 3^2 \cdot 5$, то

$$\delta(360) = \frac{2^4-1}{2-1} \cdot \frac{3^3-1}{3-1} \cdot \frac{5^2-1}{5-1} = 15 \cdot 13 \cdot 6 = 1170.$$

2. Мультипликативные числовые функции. Формулы для $\tau(n)$ и $\sigma(n)$ являются частными случаями более общей формулы, связанной с так называемыми мультипликативными числовыми функциями.

О п р е д е л е н и е 1. Числовая функция $\Theta(n)$ называется *мультипликативной*, если:

1) $\Theta(n)$ определена для всех натуральных n, причем $\Theta(1) = 1$;

2) для любых взаимно простых натуральных чисел n и m выполняется равенство

$$\Theta(mn) = \Theta(m) \cdot \Theta(n). \qquad (1)$$

Примером мультипликативной функции может служить функция $\Theta(n) = n^\lambda$, где λ — любое число, а $n \in \mathbf{N}$. В самом деле, $\Theta(1) = 1^\lambda = 1$ и для любых натуральных m и n (даже не взаимно простых) выполняется равенство:

$$\Theta(mn) = (mn)^\lambda = m^\lambda n^\lambda = \Theta(m)\Theta(n).$$

Докажем следующие свойства мультипликативных функций:

Т е о р е м а 3. *Если числа $n_1, \ldots, n_m$ попарно взаимно просты, а $\Theta(n)$ — мультипликативная функция, то*

$$\Theta(n_1 \ldots n_m) = \Theta(n_1) \ldots \Theta(n_m). \qquad (2)$$

Доказательство проведем с помощью математической индукции. При $m = 2$ равенство (2) справедливо по определению мультипликативности. Пусть уже доказано, что оно верно при $m = j$, и пусть $n_1, \ldots, n_j, n_{j+1}$ — любые попарно взаимно простые числа. Тогда числа $n_1 \ldots n_j$ и n_{j+1} взаимно просты, и потому

$$\Theta(n_1 \ldots n_j n_{j+1}) = \Theta(n_1 \ldots n_j) \cdot \Theta(n_{j+1}).$$

Но, поскольку равенство (2) верно при $m = j$, то $\Theta(n_1 \ldots n_j) = \Theta(n_1) \ldots \Theta(n_j)$, и потому

$$\Theta(n_1 \ldots n_j n_{j+1}) = \Theta(n_1) \ldots \Theta(n_j)\,\Theta(n_{j+1}).$$

Итак, равенство (2) верно при $m = 2$ и из его справедливости

при $m = j$ следует справедливость и при $m = j + 1$. Значит, равенство (2) верно для любого числа попарно взаимно простых сомножителей.

Следствие. *Если каноническая запись числа n имеет вид $n = p_1^{k_1} \dots p_m^{k_m}$, $\Theta(n)$ — мультипликативная функция, то*

$$\Theta(n) = \Theta(p_1^{k_1}) \dots \Theta(p_m^{k_m}).$$

Утверждение вытекает непосредственно из того, что числа $p_1^{k_1}, \dots, p_m^{k_m}$ попарно взаимно просты, и из теоремы 3.

Теорема 4. *Если каноническая запись числа n имеет вид $n = p_1^{k_1} \dots p_m^{k_m}$ и $\Theta(n)$ — мультипликативная функция, то*

$$\sum_{d/n} \Theta(n) = [1 + \Theta(p_1) + \dots + \Theta(p_1^{k_1})] \dots [1 + \Theta(p_m) + \dots + \Theta(p_m^{k_m})], \tag{3}$$

где слева сумма распространена на все делители числа d.

Доказательство. Для доказательства формулы (3) достаточно раскрыть скобки в правой части и принять во внимание, что по теореме 4

$$\Theta(p_1^{l_1}) \dots \Theta(p_m^{l_m}) = \Theta(p_1^{l_1} \dots p_m^{l_m}),$$

причем $p_1^{l_1} \dots p_m^{l_m}$ — делитель числа $n = p_1^{k_1} \dots p_m^{k_m}$.

Формулы для $\tau(n)$ и $\sigma(n)$, выведенные выше, являются частными случаями общей формулы (3). Чтобы вывести формулу для $\tau(n)$, надо положить $\Theta(n) = 1$. Тогда слева получится сумма единиц, причем число слагаемых равно числу делителей n, т. е. $\tau(n)$, а справа — произведение чисел $(k_1 + 1), \dots, (k_m + 1)$. А формула для $\sigma(n)$ получается, если положить $\Theta(n) = n$ (эта функция мультипликативна). Тогда слева получится сумма всех делителей n, т. е. $\sigma(n)$, а справа — произведение $(1 + p_1 + \dots + p_1^{k_1}) \dots (1 + p_m + \dots + p_m^{k_m})$.

С помощью формулы (3) можно получить и новые формулы. Например, полагая $\Theta(n) = n^\lambda$, выводим, что при $n = p_1^{k_1} \dots p_m^{k_m}$

$$\sum_{d/n} d^\lambda = (1 + p_1^\lambda + \dots + p_1^{\lambda k_1}) \dots (1 + p_m^\lambda + \dots + p_m^{\lambda k_m}) =$$

$$= \frac{p_1^{\lambda(k_1+1)} - 1}{p_1^\lambda - 1} \dots \frac{p_m^{\lambda(k_m+1)} - 1}{p_m^\lambda - 1}. \tag{4}$$

Теорема 5. *Если $\Theta_1(n)$ и $\Theta_2(n)$ — мультипликативные функции, то их произведение $\Theta_1(n) \cdot \Theta_2(n) = \Theta(n)$ тоже является мультипликативной функцией.*

Доказательство. Мы имеем $\Theta(1) = \Theta_1(1) \cdot \Theta_2(1) = 1 \cdot 1 = 1$, и если $(m, n) = 1$, то $\Theta(mn) = \Theta_1(mn) \cdot \Theta_2(mn) = \Theta_1(m) \cdot \Theta_1(n) \cdot \Theta_2(m) \times \times \Theta_2(n) = \Theta_1(m) \cdot \Theta_2(m) \cdot \Theta_1(n) \cdot \Theta_2(n) = \Theta(m) \cdot \Theta(n)$.

3. Функция $E(x)$ и ее применения в теории чисел. В курсе математического анализа рассматривалась функция $y = E(x)$ — целая часть x. Она определяется так: если $n \leqslant x < n + 1$, $n \in \mathbf{Z}$, то $E(x) = n$.

Например,

$$E(7{,}25) = 7,\ E(\pi) = 3,\ E(-4{,}75) = -5,\ E(0) = 0.$$

Разность $x - E(x)$ обозначают (x) и называют дробной частью числа x. Например, $(7{,}81) = 0{,}81$.

Пусть m и n — натуральные числа. Покажем, что количество натуральных чисел, кратных m и не превосходящих n, равно $E\left(\frac{n}{m}\right)$. В самом деле, если $n = mq + r$, где $0 \leqslant r < m$, то такими кратными являются числа m, $2m$, ..., mq. Их количество равно q. Но, с другой стороны, из $n = mq + r$ следует, что $\frac{n}{m} = q + \frac{r}{m}$. Так как $0 \leqslant \frac{r}{m} < 1$, то $E\left(\frac{n}{m}\right)$ тоже равно q. Утверждение доказано.

Теорема 6. *Показатель, с которым простое число p входит в каноническое представление числа $n! = 1 \cdot 2 \ldots \cdot n$, равен*

$$E\left(\frac{n}{p}\right) + E\left(\frac{n}{p^2}\right) + \ldots + E\left(\frac{n}{p^k}\right) + \ldots \qquad (1)$$

(в сумме (1) отличны от нуля лишь члены, для которых $n \geqslant p^k$, поэтому если $p^s \leqslant n < p^{s+1}$, то последним, отличным от нуля членом будет $E\left(\frac{n}{p^s}\right)$).

Доказательство. Среди чисел 1, 2, ..., n есть $E\left(\frac{n}{p}\right)$ чисел, кратных p, $E\left(\frac{n}{p^2}\right)$ — кратных p^2, ..., $E\left(\frac{n}{p^k}\right)$ — кратных p^k, и т. д. Поэтому количество чисел, кратных p, но не кратных p^2, равно $E\left(\frac{n}{p}\right) - E\left(\frac{n}{p^2}\right)$, чисел, кратных p^2, но не кратных p^3, равно $E\left(\frac{n}{p^2}\right) - E\left(\frac{n}{p^3}\right)$ и т. д.

Каждое число 1, 2, ..., n, кратное p, но не кратное p^2, дает в произведении $n! = 1 \cdot 2 \cdot \ldots \cdot n$ один простой множитель, равный p. Числа, кратные p^2, но не кратные p^3, дают два таких множителя и т. д. Поэтому общее число простых множителей, равных p, в каноническом выражении числа $n!$ таково:

$$c = E\left(\frac{n}{p}\right) - E\left(\frac{n}{p^2}\right) + 2\left[E\left(\frac{n}{p^2}\right) - E\left(\frac{n}{p^3}\right)\right] +$$
$$+ 3\left[E\left(\frac{n}{p^3}\right) - E\left(\frac{n}{p^4}\right)\right] + \ldots + k\left[E\left(\frac{n}{p^k}\right) - E\left(\frac{n}{p^{k+1}}\right)\right].$$

Раскрывая скобки и приводя подобные члены, получим сумму:

$$c = E\left(\frac{n}{p}\right) + E\left(\frac{n}{p^2}\right) + \ldots + E\left(\frac{n}{p^k}\right) + \ldots .$$

Вычисления удобно располагать следующим образом:

$$\begin{array}{l|l} n & p \\ \hline r_1 & q_1 \end{array} \quad \begin{array}{l|l} q_1 & p \\ \hline r_2 & q_2 \end{array} \quad \begin{array}{l|l} q_2 & p \\ \hline r_3 & \ldots \end{array} \quad \begin{array}{l|l} q_s & p \\ \hline 0 & \end{array}$$

Тогда

$$c = q_1 + q_2 + \ldots + q_s.$$

При этом деление ведется до тех пор, пока не получим частного, меньшего p.

Примеры.

1. На какую наивысшую степень 7 делится число 900!?

Решение. Здесь $n = 900$, $p = 7$. Поэтому

$$\begin{array}{r|l} 900 & 7 \\ \hline 7 & 128 \\ \hline 20 & 7 \\ \hline 14 & 58 \\ \hline 60 & 56 \\ \hline 56 & 2 \\ \hline 4 & \end{array} \quad \begin{array}{r|l} 128 & 7 \\ \hline 7 & 18 \\ \hline 58 & 14 \\ \hline 56 & 4 \\ \hline 2 & \end{array} \quad \begin{array}{r|l} 18 & 7 \\ \hline 14 & 2 \\ \hline 4 & \end{array}$$

Находим: $\alpha = 128 + 18 + 2 = 148$, а соответствующая степень 7^{148}.

2. Найдем каноническое разложение числа 20!

Решение. В каноническое разложение числа 20! входят только степени простых чисел, не превосходящих 20, т. е. степени чисел 2, 3, 5, 7, 11, 13, 17, 19. Найдем показатели, с которыми эти простые числа входят в разложение числа 20!

$$\begin{array}{r|l} 20 & 2 \\ \hline 20 & 10 \\ \hline 0 & 10 \\ \hline & 0 \end{array} \quad \begin{array}{r|l} 10 & 2 \\ \hline 5 & 2 \\ \hline 4 & 2 \\ \hline 1 & 2 \\ \hline & 0 \end{array} \quad \begin{array}{r|l} 2 & 2 \\ \hline 2 & 1 \\ \hline 0 & \end{array}$$

$$\begin{array}{r|l} 20 & 3 \\ \hline 18 & 6 \\ \hline 2 & 6 \\ \hline & 0 \end{array} \quad \begin{array}{r|l} 3 & 3 \\ \hline & 2 \end{array} \qquad \begin{array}{r|l} 20 & 5 \\ \hline 20 & 4 \\ \hline 0 & \end{array} \qquad \begin{array}{r|l} 20 & 7 \\ \hline 14 & 2 \\ \hline 6 & \end{array} \text{ и т. д.}$$

$$10 + 5 + 2 + 1 = 18;\ 6 + 2 = 8 \text{ и т. д.}$$

Окончательно находим: $20! = 2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11^1 \cdot 13^1 \cdot 17^1 \cdot 19^1$.

Вопросы для самопроверки и упражнения

1. Напишите формулу для количества делителей числа $n = p_1^{k_1} \ldots p_m^{k_m}$. Напишите формулу для суммы его делителей.

2. Напишите формулу для суммы кубов делителей числа n.

3. Какие числовые функции называются мультипликативными?

4. Приведите примеры мультипликативных числовых функций.

5. Функция Мебиуса $\mu(n)$ определяется так: если n делится на квадрат какого-нибудь простого числа, то $\mu(n) = 0$. Если же $n = p_1 p_2 \ldots p_m$, где все простые числа $p_1, p_2, \ldots, p_m$ различны, то $\mu(n) = (-1)^m$. Докажите, что $\mu(n)$ — мультипликативная числовая функция.

6. Напишите формулу, частными случаями которой являются формулы для $\tau(n)$ и $\sigma(n)$.

7. Перечислите свойства мультипликативных числовых функций.

8. На какую степень 7 делится 500!?

9. Найдите число натуральных чисел, не превосходящих 471,8 и делящихся на 7.

10. Найдите количество натуральных чисел на отрезке от 165 до 926,1, делящихся на 11.

11. Решите уравнение $E(2ax) = m$, где $a \neq 0$ и x — действительные числа.

12. Найдите, при каком целом положительном m выполняются соотношения: а) $E(32{,}6m) = 97$; б) $E(27{,}4\,m) = 140$.

13. Докажите, что $E(x) + E\left(x + \frac{1}{2}\right) = E(2x)$ для любого действительного x.

14. Найдите показатель, с которым простое число p входит в произведение $n!$, если: а) $p = 3$, $n = 100$; б) $p = 11$, $n = 1000$; в) $p = 7$, $n = 8156$.

15. Сколькими нулями оканчивается число $n!$, если: а) $n = 100$; б) $n = 325$; в) $n = 471$.

16. Найдите каноническое разложение чисел: а) 40!; б) 50!.

17. Докажите, что если $a, b, \ldots, l$ — натуральные числа и $n \geqslant a + b + \ldots + l$, то $\frac{n!}{a!b! \ldots l!}$ — натуральное число.

18. Докажите, что если $m < n$, то $\frac{n(n-1)\ldots(n-m+1)}{1 \cdot 2 \cdot 3 \ldots m} = C_n^m$ есть натуральное число.

19. Найдите количество делителей числа n, если: а) $n = 4520$; б) $n = 27\,504$; в) $n = 116\,424$; г) $n = 1\,002\,001$; д) $n = 1\,294\,700$.

20. Найдите сумму делителей для чисел задачи 19.

21. Найдите все натуральные делители чисел: а) 90; б) 4520.

22. Найдите наименьшее натуральное число, имеющее: а) 10 натуральных делителей; б) 15 натуральных делителей.

23. Найдите натуральное число, зная, что оно имеет только два простых делителя, что число всех делителей равно 6, а сумма всех делителей — 28.

§ 7. РАСПРЕДЕЛЕНИЕ ПРОСТЫХ ЧИСЕЛ

1. Доказательство бесконечности множества простых чисел (доказательство Эйлера). Достаточно взглянуть на таблицу простых чисел, чтобы убедиться в крайней нерегулярности их распределения в натуральном ряду. С одной стороны, встречаются пары простых чисел, отличающиеся друг от друга лишь на две единицы (например, 11 и 13, 17 и 19, 41 и 43). Такие пары простых чисел называются *близнецами*. Известны очень большие пары чисел-близнецов; вопрос о том, конечно ли их множество или нет (проблема близнецов), не решен до сих пор. С другой стороны, по теореме 9 § 5 в натуральном ряду есть сколь угодно длинные промежутки, свободные от простых чисел.

Поэтому уже давно математиков интересовал вопрос о распределении простых чисел в натуральном ряду. В XVIII веке новое доказательство бесконечности множества простых чисел было дано членом Петербургской Академии наук, выдающимся математиком своего времени Леонардом Эйлером. В основе этого доказательства лежит формула, которая приведена в § 6 настоящего пособия на с. 30.

Запишем эту формулу в несколько ином виде:

$$\sum_{d/n} d^{\lambda} = \frac{1 - p_1^{\lambda(k_1+1)}}{1 - p_1^{\lambda}} \cdots \frac{1 - p_m^{\lambda(k_m+1)}}{1 - p_m^{\lambda}}, \tag{1}$$

где $n = p_1^{k_1} \ldots p_m^{k_m}$.

Устремим показатели $k_1, \ldots, k_m$ к бесконечности. При $\lambda < 0$ имеем $\lim\limits_{k \to \infty} p^{\lambda k+1} = 0$, и потому в пределе получим:

$$\sum{}' d^{\lambda} = \frac{1}{1 - p_1^{\lambda}} \cdots \frac{1}{1 - p_m^{\lambda}}. \tag{2}$$

Здесь сумма левой части превратилась в бесконечный ряд, распространенный на все d, в каноническое разложение которых входят лишь числа $p_1, \ldots, p_m$. Заменяя λ на $-s$, а d на n, получаем, что при $s > 0$

$$\sum{}' \frac{1}{n^s} = \frac{1}{1 - \frac{1}{p_1^s}} \cdots \frac{1}{1 - \frac{1}{p_m^s}}, \tag{3}$$

где, напомним, сумма в левой части распространена лишь на числа n вида $n = p_1^{j_1} \ldots p_m^{j_m}$. В частности, при $s = 1$ имеем:

$$\sum{}' \frac{1}{n} = \frac{1}{1 - \frac{1}{p_1}} \cdots \frac{1}{1 - \frac{1}{p_m}}. \tag{4}$$

Если бы множество простых чисел было конечно, например состояло бы лишь из чисел $p_1, \ldots, p_m$, то лишь эти простые числа входили бы в каноническое разложение всех натуральных чисел, и потому левая часть равенства (4) имела бы вид $\sum\limits_{n=1}^{\infty} \frac{1}{n}$. Мы получили бы равенство:

$$\sum_{n=1}^{\infty} \frac{1}{n} = \frac{1}{1 - \frac{1}{p_1}} \cdots \frac{1}{1 - \frac{1}{p_m}},$$

которое невозможно, поскольку ряд $\sum_{n=1}^{\infty}\frac{1}{n}$ (гармонический ряд) расходится и сумма его не может равняться никакому числу. Значит, наше предположение неверно, и множество простых чисел бесконечно.

Если $s>1$, то ряд $\sum_{n=1}^{\infty}\frac{1}{n^s}$ сходится. Переходя в равенстве (3) к пределу при $m\to\infty$, получим:

$$\sum_{n=1}^{\infty}\frac{1}{n^s}=\frac{1}{1-\frac{1}{p_1^s}}\cdots\frac{1}{1-\frac{1}{p_m^s}}\cdots, \qquad (5)$$

где бесконечное произведение распространено на все простые числа $p_1, \ldots, p_m, \ldots$ Эта замечательная формула Эйлера позволяет преобразовать при $s>1$ ряд $\sum_{n=1}^{\infty}\frac{1}{n^s}$ в бесконечное произведение, распространенное на все простые числа. Когда $s\to 1$, обе части равенства (5) стремятся к бесконечности. Логарифмируя равенство (5), Эйлер вывел, что ряд $\sum_{n=1}^{\infty}\ln\left(1-\frac{1}{p_m}\right)$ расходится, а отсюда нетрудно получить, что расходится и ряд $\sum_{m=1}^{\infty}\frac{1}{p_m}$, где суммирование ведется по множеству всех простых чисел. Это утверждение означает, что простые числа распространены в натуральном ряду «не слишком редко», что члены вида $\frac{1}{p_m}$ составляют «весомую часть» в расходящемся гармоническом ряде $\sum_{n=1}^{\infty}\frac{1}{n}$. Однако сделать какие-кибо точные выводы о распределении простых чисел из расходимости ряда $\sum_{m=1}^{\infty}\frac{1}{p_m}$ невозможно.

2. Асимптотический закон распределения простых чисел. Математики конца XVIII и начала XIX века обратились к изучению таблиц простых чисел. Обозначим через $\pi(x)$ количество простых чисел на промежутке $[2, x)$. Поскольку из-за нерегулярности распределения простых чисел явного выражения для $\pi(x)$ получить не удавалось, математики попытались получить асимптотическое приближение для $\pi(x)$. Будем говорить, что функции $y=f(x)$ и $y=\varphi(x)$ асимптотически равны при $x\to+\infty$, если они бесконечно велики при $x\to+\infty$ и $\lim\limits_{x\to+\infty}\frac{f(x)}{\varphi(x)}=1$. В этом случае пишут $f(x)\sim\varphi(x)$.

В 1808 г. французский математик Лежандр опубликовал гипотезу, согласно которой

$$\pi(x)\approx\frac{x}{\ln x-1{,}08366\ldots}.$$

Еще ранее великий немецкий математик К. Гаусс (1777—1855) пришел к предположению, что

$$\pi(x)\approx\int_2^x\frac{dt}{\ln t}$$

(этот интеграл, называемый *интегральным логарифмом*, не выражается через элементарные функции. Его обозначают $\mathrm{li}\ x$).

Однако эти предположения не были доказаны (а гипотеза Гаусса не была и опубликована). Первым после Евклида, кто пошел верным путем в вопросе о распределении простых чисел и достиг важных результатов, был великий русский математик Пафнутий Львович Чебышев (1821—1894). В 1849 г. он доказал, что гипотеза Лежандра ложна и что если при некоторых A и B формула $\pi(x) = \dfrac{x}{A \ln x + B}$ верна с точностью до слагаемого порядка $\dfrac{x}{\ln^2 x}$, то $A = 1$, $B = -1$. Отсюда вытекает, что если существует $\lim\limits_{x \to \infty} \left[\pi(x) : \dfrac{x}{\ln x}\right]$, то этот предел должен равняться 1.

Утверждение

$$\pi(x) \sim \frac{x}{\ln x}$$

или равносильное ему утверждение

$$\pi(x) \sim \mathrm{li}\ x$$

называют *асимптотическим законом распределения простых чисел.*

П. Л. Чебышев глубоко изучил свойства функции

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

введенной Л. Эйлером. Он получил для этой функции выражение через интегралы и изучил характер ее стремления к бесконечности при $s \to 1$.

Получить окончательное доказательство асимптотического закона распределения простых чисел П. Л. Чебышеву не удалось — он не доказал существования предела $\lim\limits_{x \to \infty} \left[\pi(x) : \dfrac{x}{\ln x}\right]$. Иной подход к проблеме распределения простых чисел П. Л. Чебышев развил во втором мемуаре о простых числах, появившемся в 1850 г. В нем он доказал, что

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

(неравенства Чебышева). Отсюда он вывел следующую теорему, впервые высказанную без доказательства французским математиком Бертраном: между n ($n > 3$) и $2n - 2$ всегда есть хоть одно простое число.

В 1859 г. немецкий математик Б. Риман изучил функцию $\zeta(s)$ не только для действительных, но и для комплексных значений s. Это позволило применить к изучению $\zeta(s)$ весьма сильные теоремы, которые были доказаны для функций комплексного переменного (с теорией этих функций читатель ознакомится в курсе «Теория аналитических функций»). Используя идеи Римана, почти одновременно французский математик Ж. Адамар и бельгийский математик Ш. Валле-Пуссен доказали в 1896 г. асимптотический закон распределения простых чисел.

3. Простые числа в арифметической прогрессии. Натуральный ряд чисел является арифметической прогрессией с первым членом 1 и разностью 1. Поэтому естественно было использовать результаты, полученные при изучении распределения простых чисел в натуральном ряду, и при решении вопроса о распределении простых чисел в арифметических прогрессиях. Здесь достаточно ограничиться рассмотрением прогрессий, в которых первый член a и разность d взаимно просты. В противном случае все члены прогрессии будут делиться на наибольший общий делитель a и d и в прогрессии не будет простых чисел. Слу-

чай, когда $(a, d) = 1$, рассмотрел немецкий математик Л. Дирихле. Он доказал в 1837 г. следующее обобщение теоремы Евклида.

Теорема 1. *Если* $(a, d) = 1$, *то прогрессия*

$$a, a + d, \ldots, a + (n - 1)\, d, \ldots$$

содержит бесконечно много простых чисел.

Еще до этого теорема о бесконечности множества простых чисел в арифметических прогрессиях была доказана для некоторых частных случаев элементарными методами. Докажем для примера следующую теорему:

Теорема 2. *Множество простых чисел вида* $p = 4n - 1$ *бесконечно* (к нему относятся, например, простые числа 3, 7, 11, 19, 23, 31 и др.).

Доказательство. Из равенства $(4m + 1)(4n + 1) = 16mn + 4m + 4n + 1$ видно, что произведение двух чисел, каждое из которых при делении на 4 дает в остатке 1, имеет тот же остаток 1 при делении на 4. Отсюда вытекает, что ни одно число вида $4n - 1$ не может быть разложено в произведение множителей вида $4n + 1$.

Предположим, что множество простых чисел вида $4n - 1$ конечно и состоит из чисел $p_1, p_2, \ldots, p_k$. Обозначим через N произведение $N = p_1 p_2 \ldots p_k$ и положим $M = 4N - 1$.

По сделанному выше замечанию M не может раскладываться в произведение простых множителей вида $4m + 1$, т. е. имеет хотя бы один простой делитель p вида $4n - 1$. Так как по предположению $p_1, \ldots, p_k$ — простые числа вида $4n - 1$, то $M = 4N - 1$ должно делиться на одно из этих чисел, например на p_j. Это противоречит тому, что $4N = 4p_1 \ldots p_k$ делится на p_j, а -1 не делится на p_j. Полученное противоречие доказывает теорему.

Если обозначить через $\pi_a(k, x)$ число простых чисел в прогрессии (1), не превосходящих x, то теорема Дирихле может быть сформулирована следующим образом: если $(k, a) = 1$, то $\lim\limits_{x \to +\infty} \pi_a(k, x) = +\infty$. Асимптотический закон для $\pi_a(k, x)$ имеет вид:

$$\pi_a(k, x) \sim \frac{x}{\varphi(k) \ln x},$$

где $\varphi(k)$ — функция Эйлера.

Вопросы для самопроверки и упражнения

1. Напишите выражение $\sum\limits_{n=1}^{\infty} \frac{1}{n^s}$ в виде бесконечного произведения.

2. Какие пары простых чисел называются близнецами? В чем состоит проблема близнецов?

3. В чем заключается асимптотический закон распределения простых чисел?

4. Оцените с помощью асимптотического закона распределения простых чисел количество простых чисел среди первых 5 000 000 натуральных чисел.

5. Сформулируйте предположение Лежандра. Верно ли оно?

6. Сформулируйте предположение Гаусса.

7. Сформулируйте предположение Бертрана. Проверьте его при $n = 100$, $n = 1\,000$.

8. Какому условию должна удовлетворять разность d арифметической прогрессии, чтобы в ней содержалось бесконечное множество простых чисел?

9. Справедлива ли теорема Дирихле для арифметической прогрессии: а) 4, 12, 20, 28, ...; б) 5, 9, 13, 17, ...? Почему?

10. Можно ли утверждать, ссылаясь на теорему Дирихле, что множество чисел вида: а) $5t + 1$; б) $6t + 3$ бесконечно? Почему?

§ 8. СИСТЕМАТИЧЕСКИЕ ЧИСЛА

1. Непозиционные системы счисления. Для записи натуральных чисел применяются различные системы счисления, которые можно разбить на две группы: *непозиционные* и *позиционные*. В непозиционных системах счисления значение каждого применяемого знака не зависит от его места в записи числа. Из многочисленных непозиционных систем счисления некоторое значение сохранила в настоящее время лишь римская нумерация.

В этой системе счисления используют следующие знаки: I — единица, V — пять, X — десять, L — пятьдесят, C — сто, D — пятьсот, M — тысяча. Знак для единицы означает один палец, для пяти — раскрытую ладонь, для десяти — две ладони. Знаки для ста и тысячи — первые буквы латинских слов centum — сто и mille — тысяча.

Правила записи чисел в римской системе счисления таковы:

а) если знак, изображающий меньшее число, стоит после знака, изображающего большее число, то производится сложение:

VI = 5 + 1 = 6, XV = 10 + 5 = 15, CLV = 100 + 50 + 5 = = 155, MCCV = 1000 + 100 + 100 + 5 = 1205;

б) если знак, изображающий меньшее число, стоит перед знаком, изображающим большее число, то производится вычитание:

IV = 5 — 1 = 4; IX = 10 — 1 = 9; XL = 50 — 10 = 40; XC = 100 — 10 = 90; MCDXXIX = 1000 + 500 — 100 + 10 + + 10 + 10 — 1 = 1429.

Непозиционной была система счисления и у древних греков. Они обозначали числа 1, 2, 3, 4, 5, 6, 7, 8, 9 первыми девятью буквами греческого алфавита, например $\alpha = 1$, $\beta = 2$, $\gamma = 3$, $\delta = 4$ и т. д. Для обозначения чисел 10, 20, 30, 40, 50, 60, 70, 80, 90 применялись следующие девять букв (например, $\iota = 10$), а для обозначения чисел 100, 200, 300, 400, 500, 600, 700, 800, 900 — последние девять букв (например, $\sigma = 200$). По записи было невозможно усмотреть, что число σ (это — обозначение для 200) в 100 раз больше числа β (т. е. 2). Некоторые элементы позиционной записи встречаются у древних греков при обозначении чисел, больших 1000.

Культура древней Руси была тесно связана с византийской, т. е. греческой, культурой, поэтому и принцип обозначения чисел был похож на греческий: числа обозначались с помощью букв, над которыми ставился особой знак (титло). В славянском счислении применялись следующие названия для обозначения высших десятичных разрядов: 10 тысяч назывались тьмой, 10 тем — легионом, 10 легионов — леодром.

2. Позиционные системы счисления. В позиционных системах счисления значение применяемых символов зависит от места, которое этот символ занимает в записи числа. Чаще всего применяют позиционные системы счисления с фиксированным основанием. В этих системах для записи натуральных чисел достаточно конечного множества знаков (цифр). При этом сдвиг цифры на одно место влево влечет за собой увеличение ее числового значения в g раз, где g — некоторое натуральное число, большее 1. Число g называют *основанием* системы счисления. Чаще всего применяют десятичную систему счисления, в которой $g = 10$. Это связано с тем, что число пальцев на руках человека равно 10, а первоначально люди считали по пальцам.

Перейдем к более подробному описанию позиционной системы счисления с основанием g.

Определение 1. *Систематической записью* натурального числа N по основанию g называют представление этого числа в виде суммы:

$$N = a_n g^n + \ldots + a_1 g + a_0, \qquad (1)$$

где a_n, ..., a_1, a_0 — числа, принимающие значения 0, 1, ..., g —1, причем $a_n \neq 0$.

Позиционная система счисления с основанием g называется g-ичной (двоичная, троичная и т. д.). На практике чаще всего применяется десятичная система счисления ($g = 10$). В быстродействующих вычислительных машинах применяют двоичную и восьмеричную системы счисления.

Для обозначения чисел 0, 1, ..., $g - 1$ в g-ичной системе счисления используют особые знаки, называемые *цифрами*. Иногда для краткости сами эти числа называют цифрами (что, строго говоря, неверно, так как цифры — лишь знаки для обозначения некоторых чисел). Замечательным открытием древнеиндийских математиков было изобретение нуля — особого знака, который должен был показать отсутствие единиц определенного разряда.

Для g-ичной системы счисления нужно g цифр (для обозначения чисел от 0 до $g - 1$). Если $g < 10$, то применяют те же обозначения цифр, что и в десятичной системе счисления (только берут не все цифры), а если $g > 10$, то нужны особые обозначения для чисел от 10 до $g - 1$ (например, в двенадцатеричной системе счисления нужны еще две цифры, а в двадцатеричной — еще десять цифр).

В двоичной системе достаточно двух цифр: 0 и 1. Именно этим, в частности, объясняется широкое использование двоичной системы счисления в вычислительных машинах: основные элементы вычислительных машин — особые устройства, которые могут находиться в двух положениях (скажем, пропускать или не пропускать ток). Одно положение ставят в соответствие цифре 0, а другое — цифре 1.

Докажем следующую теорему о систематической записи чисел:

Теорема 1. *Всякое натуральное число N может быть единственным образом представлено в виде систематической записи по любому основанию $g > 1$.*

Доказательство. Докажем сначала, что если $0 \leqslant N < g^{n+1}$, то число N допускает g-ичную запись в виде:

$$N = a_n g^n + \ldots + a_1 g + a_0 \qquad (1)$$

(где a_n может равняться нулю). При этом если $g^n \leqslant N < g^{n+1}$, то $a_n \neq 0$. Доказательство проведем с помощью математической индукции по n. При $n = 0$ имеем $0 \leqslant N < g$. В этом случае g-ичная запись числа N состоит из одного слагаемого — самого этого числа ($N = a_0$).

Пусть для всех чисел, меньших g^n, доказано существование g-ичной записи и пусть $g^n \leqslant N < g^{n+1}$. Разделим N на g^n с остатком: $N = a_n g^n + N_1$, где $N_1 < g^n$. Так как $N_1 < g^n$, то N_1 имеет g-ичную запись вида:

$$N_1 = a_{n-1} g^{n-1} + \ldots + a_1 g + a_0$$

(где, быть может, $a_{n-1} = 0$). Но тогда

$$N = a_n g^n + N_1 = a_n g^n + a_{n-1} g^{n-1} + \ldots + a_0.$$

Поскольку для любого N найдется такое n, что $N < g^{n+1}$, то возможность g-ичного представления доказана для всех натуральных n.

Теперь докажем, что такое представление единственно.

Если $a \leqslant N < g$, то N может иметь лишь g-ичную запись вида $N = a_0$, поскольку при $n \geqslant 1$, $a_n \neq 0$ выполняется неравенство

$$a_n g^n + a_{n-1} g^{n-1} + \ldots + a_0 > a_n g^n > g > N.$$

Запись $N = a_0$ однозначно определена, поскольку все числа от 1 до $g - 1$ обозначаются различными цифрами.

Пусть уже доказано, что g-ичная запись для чисел N, таких, что $0 \leqslant N < g^n$, определена однозначно, и пусть $g^n \leqslant N < g^{n+1}$. Если

$$N = a_n g^n + a_{n-1} g^{n-1} + \ldots + a_0,$$

то a_n — частное от деления N на g^n, а $M = a_{n-1} g^{n-1} + \ldots + a_0$ — остаток при таком делении. Значит, a_n и M однозначно определены. Но по предположению индукции g-ичная запись числа M определена однозначно. Значит, и цифры a_{n-1}, ..., a_0 однозначно определены. Иными словами, g-ичная запись числа N однозначно определена. С помощью индукции по n получаем, что все натуральные числа имеют лишь одну g-ичную запись.

Выведем теперь явную формулу для цифр a_n, ..., a_0 в g-ичной записи числа N:

$$N = a_n g^n + a_{n-1} g^{n-1} + \ldots + a_k g^k + a_{k-1} g^{k-1} + \ldots + a_0. \qquad (2)$$

Для этого разделим обе части равенства (2) на g^k, $0 \leqslant k \leqslant n$.

$$\frac{N}{g^k} = a_n g^{n-k} + \ldots + a_k + \frac{a_{k-1}}{g} + \ldots + \frac{a_0}{g^k}.$$

Так как $a_{k-1}g^{k-1} + \ldots + a_0 < g^k$, то имеем:

$$\frac{a_{k-1}}{g} + \ldots + \frac{a_0}{g^k} < 1,$$

и потому

$$\mathrm{E}\left(\frac{N}{g^k}\right) = a_n g^{n-k} + \ldots + a_{k+1}g + a_k. \tag{3}$$

Точно так же устанавливаем, что

$$\mathrm{E}\left(\frac{N}{g^{k+1}}\right) = a_n g^{n-k-1} + \ldots + a_{k+1}. \tag{3'}$$

Из равенств (3) и (3') вытекает, что

$$a_k = \mathrm{E}\left(\frac{N}{g^k}\right) - g\mathrm{E}\left(\frac{N}{g^{k+1}}\right). \tag{4}$$

Вместо громоздкой записи

$$N = a_n g^n + \ldots + a_1 g + a_0$$

обычно пишут $N = \overline{a_n \ldots a_1 a_0}_g$. Черта сверху пишется для того, чтобы отличить эту запись от произведения чисел a_n, ..., a_1, a_0. Индекс g (справа внизу) указывает, по какому основанию записано число. При записи конкретного числа черта опускается. В десятичной системе счисления индекс 10 не ставится.

Примеры.

1. Запись $51\,306_7$ означает число

$$5 \cdot 7^4 + 1 \cdot 7^3 + 3 \cdot 7^2 + 0 \cdot 7 + 6.$$

2. Запись

$$4 \cdot 8^3 + 6 \cdot 8^2 + 3 \cdot 8 + 0$$

коротко пишут в виде 4630_8.

3. Запись

$$5 \cdot 10^4 + 0 \cdot 10^3 + 6 \cdot 10^2 + 3 \cdot 10 + 7$$

коротко пишут так: 50 637.

4. Найдем коэффициент при 6^4 в шестеричной записи числа 13 178. По формуле (4) имеем:

$$a_4 = \mathrm{E}\left(\frac{13178}{6^4}\right) - 6\mathrm{E}\left(\frac{13178}{6^5}\right) = \mathrm{E}\left(\frac{13178}{1296}\right) - 6\mathrm{E}\left(\frac{13178}{7776}\right) =$$
$$= 10 - 6 \cdot 1 = 4.$$

3. Переход от g-ичной системы счисления к десятичной и обратно. Натуральное число N можно записать в любой системе счисления. Поэтому возникает вопрос о переводе записи числа из

одной системы счисления в другую. Достаточно научиться решать этот вопрос в случае, когда одна из систем счисления десятичная (подобно тому как для перевода с одного языка на другой нам достаточно иметь словари для перевода с этих языков на русский и с русского на эти языки).

Итак, разберем две задачи:

1. Пусть дана g-ичная запись числа N:

$$N = a_n g^n + \ldots + a_0. \qquad (1)$$

Надо найти десятичную запись того же числа.

2. Дана десятичная запись числа N. Надо найти g-ичную запись того же числа.

Чтобы решить первую задачу, достаточно подставить в запись (1) вместо a_n, ..., a_0 и g десятичные записи этих чисел и выполнить указанные действия. Десятичная запись результата и будет искомым ответом.

Примеры.

1. Получим десятичную запись для числа 4602_7. Запись 4602_7 перепишем в виде:

$$4602_7 = 4 \cdot 7^3 + 6 \cdot 7^2 + 0 \cdot 7 + 2$$

и выполним указанные действия. Получаем 1668.

2. Получим десятичную запись для числа (10) 6 $(11)_{12}$, где (10) — новая цифра для 10 в двенадцатеричной системе счисления, а (11) — новая цифра для 11.

Имеем:

$$(10)\ 6\ (11)_{12} = 10 \cdot 12^2 + 6 \cdot 12 + 11 = 1523.$$

Теперь рассмотрим вторую задачу. Пусть g-ичная запись числа N имеет вид:

$$N = a_n g^n + \ldots + a_1 g + a_0.$$

Тогда

$$N = N\,(1)\, g + a_0,$$

где

$$N\,(1) = a_n g^{n-1} + \ldots + a_1. \qquad (2)$$

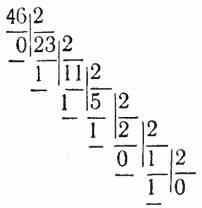
Поскольку $0 \leqslant a_0 < g$, то a_0 — остаток от деления N на g, а N (1) — частное от этого деления. Из равенства (2) видно, что a_1 — остаток от деления N (1) на g и т. д.

Таким образом, g-ичная запись числа N находится следующим образом. Число N делим (в десятичной системе счисления) на g. Остаток от деления даст последнюю цифру g-ичной записи N. Частное N (1) снова делим на g и новый остаток даст предпоследнюю цифру g-ичной записи N. Продолжая этот процесс деления, найдем все цифры g-ичной записи.

Примеры.

1. Найдем двоичную запись числа 46.

Расположим деление следующим образом:



Записывая остатки, начиная с последнего, получаем:

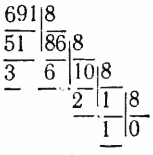
$$46 = 101\ 110_2.$$

Проверим ответ, переведя $101\ 110_2$ обратно в десятичную систему счисления:

$$101\ 110_2 = 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 0 =$$
$$= 32 + 8 + 4 + 2 = 46.$$

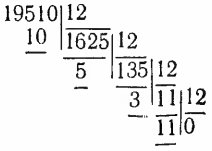
2. Найдем восьмеричную запись числа 691.

Последовательно деля число 691 и получающиеся частные на 8, получаем:



Значит, $691 = 1263_8$.

3. Найдем двенадцатеричную запись числа 19 510.



Для остатков 10 и 11 вводим новые цифры (10) и (11).
Тогда запись числа 19 510 имеет вид:

$$19\ 510 = (11)\ 35\ (10)_{12}.$$

4. Переведем число $32\ 014_5$ в восьмеричную систему счисления. Сначала переведем $32\ 014_5$ в десятичную систему счисления:

$$32\ 014_5 = 3 \cdot 5^4 + 2 \cdot 5^3 + 0 \cdot 5^2 + 1 \cdot 5 + 4 = 2134.$$

А теперь 2134 переведем в восьмеричную систему счисления:

$$\begin{array}{r|l} 2134 & 8 \\ \underline{6} & 266 \\ \quad \underline{2} & 33 \\ \quad\quad \underline{1} & 4 \\ \quad\quad\quad 4 & 0 \end{array} \quad \begin{array}{l|} 8 \\ 8 \\ 8 \\ \end{array}$$

Значит, $32014_5 = 4126_8$.

Мы видим, что при увеличении основания системы количество цифр в записи данного числа уменьшается, но приходится использовать большее число различных цифр.

Разумеется, возможен непосредственный перевод из p-ичной системы счисления в g-ичную. Но это требует навыка выполнения арифметических операций в этих системах счисления, и мы не будем пользоваться этим способом. Однако есть случай, когда перевод из p-ичной системы счисления в g-ичную и обратно не вызывает затруднений. Это случай, когда одно из чисел p, g является степенью другого, например $g = p^k$.

Пусть

$$N = a_n g^n + \ldots + a_1 g + a_0. \tag{3}$$

Здесь a_n, ..., a_1, a_0 — натуральные числа, меньшие g, т. е. меньшие, чем p^k. А тогда их можно представить в виде:

$$a_n = \alpha_{k-1} p^{k-1} + \ldots + \alpha_0,$$

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

$$a_0 = \lambda_{k-1} p^{k-1} + \ldots + \lambda_0,$$

и т. д. Подставляя эти записи в (3) и заменяя g на p^k, получим запись вида:

$$N = (\alpha_{k-1} p^{k-1} + \ldots + \alpha_0)\, p^{nk} + \ldots + \lambda_{k-1} p^{k-1} + \ldots + \lambda_0.$$

А теперь достаточно раскрыть скобки, чтобы получить p-ичную запись числа N.

Чтобы сделать обратный переход, достаточно разбить слагаемые в записи

$$N = b_s p^s + \ldots + p_0$$

справа налево на группы по k слагаемых (в самой левой группе может быть меньше слагаемых) и вывести за скобки p^k, p^{2k} и т. д. Заменяя p^k на g, p^{2k} на g^2 и т. д., получаем g-ичную запись числа N (выражения в скобках являются при этом g-ичными цифрами).

Примеры.

1. В практике работы быстродействующих вычислительных машин особо важную роль играет перевод из двоичной системы счисления в восьмеричную и обратно. Составим таблицу, показываю-

щую выражение каждого из чисел 0, 1, 2, 3, 4, 5, 6, 7 в двоичной системе счисления:

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

Чтобы перевести число $25\,420_8$ в двоичную систему счисления, достаточно заменить каждую цифру данного числа тремя соответствующими цифрами двоичной системы (триадой, состоящей из нуля и единиц). Получаем:

$$25\,420_8 = 10\,101\,100\,010\,000$$

(первую цифру 2 мы заменили на 10, а не на 010).

Переведем число $11\,010\,001\,101\,000\,111_2$ в восьмеричную систему счисления. Запись этого числа уже разбита на триады. Заменяя каждую триаду соответствующей цифрой по таблице, получаем, что это число равно $321\,507_8$.

Перевод десятичного числа в двоичное выполняется просто, если его сначала перевести в восьмеричное (а затем указанным способом — в двоичное). Этим приемом программисты пользуются при переходе $10 \to 2$.

2. $2567 = x_2$.

а) $2567 = y_8 = 5007_8$, б) $5007_8 = x_2 = 101\,000\,000\,111_2$.

$$\begin{array}{r|l} 2567 & 8 \\ \underline{24} & 320 \\ 16 & \\ \underline{16} & \\ 7 & \end{array} \qquad \begin{array}{r|l} 32 & 8 \\ \underline{0} & 40 \\ & \underline{40} \\ & 0 \end{array} \qquad \begin{array}{r|l} 8 & \\ \underline{8} & \\ 5 & 8 \\ \underline{5} & \\ 0 & \end{array}$$

Информацию, записываемую в ЭВМ, разбивают на восьмерки, состоящие из цифр 0 и 1 (например 00000000, 01010101 или 11001110). Число таких восьмерок равно $2^8 = 256$ и потому каждую из них можно рассматривать как «цифру» в 256-ричной системе счисления. Поскольку такая система счисления неудобна, разбивают каждую восьмерку на две четверки цифр (например, вместо 11001110 пишут 1100, 1110), после чего каждую четверку рассматривают как цифру в 16-ричной системе счисления (например, 1100 заменяют на $2^3 + 2^2 = 12$, а 1110 — на $2^3 + 2^2 + 2 = 14$). Пара «цифр» 16-ричной системы счисления и заменяет данную восьмерку.

4. Арифметические операции над систематическими числами. Сложение, вычитание, умножение и деление чисел в любой системе счисления производятся аналогично выполнению этих операций в привычной нам десятичной системе.

Для выполнения операций сложения и вычитания в системе счисления с основанием g надо знать таблицу сложения однозначных чисел в этой системе, а для выполнения операций умножения и деления — еще и таблицу умножения. Заметим, что роль «девятки» в двоичной системе выполняет цифра 1, в троичной — 2 и т. д., в g-ичной — цифра $g - 1$.

Рассмотрим примеры.

Сложение и вычитание

Примеры.

1. Пусть $g = 2$. Составим таблицу сложения: $1 + 0 = 1$, $1 + 1 = 10$.

$$\begin{array}{r} 110011_2 \\ +\ 11011_2 \\ \hline 1001110_2 \end{array} \qquad \begin{array}{r} \dot{1}\dot{0}0111\dot{0}_2 \\ -\ 110011_2 \\ \hline 11011_2 \end{array}$$

Сложение проверили вычитанием.

Точка, поставленная над цифрой в уменьшаемом, как и в десятичной системе, означает, что взята одна единица разряда и заменена соответствующим числом единиц низшего разряда. При $g = 2$ единица высшего разряда содержит 2 единицы соседнего с ним низшего разряда.

2. Пусть $g = 8$.

Составим таблицу сложения:

x \ y	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	10
2	2	3	4	5	6	7	10	11
3	3	4	5	6	7	10	11	12
4	4	5	6	7	10	11	12	13
5	5	6	7	10	11	12	13	14
6	6	7	10	11	12	13	14	15
7	7	10	11	12	13	14	15	16

$$\begin{array}{r} 430716_8 \\ +\ 54705_8 \\ \hline 505623_8 \end{array}$$

Проверим вычитанием.

$$\begin{array}{r} 505623_8 \\ -\ 430716_8 \\ \hline 54705_8 \end{array}$$

3. Пусть $g = 12$ (цифры: 0, 1, 2, ..., 8, 9, (10), (11)).

$$\begin{array}{r} 29\,(10)\;0\,(11)\;4_{12} \\ +\;\;6\;\;8\,(11)\;2\;\;7_{12} \\ \hline 34\;\;7\;\;0\;\;1\;\;(11)_{12} \end{array}$$

Проверим вычитанием.

$$\begin{array}{r} 34\;\;7\;\;0\;\;1\;\;(11)_{12} \\ -\,29\,(10)\;0\,(11)\;\;4_{12} \\ \hline 6\;\;8\,(11)\;2\;\;7_{12} \end{array}$$

Умножение и деление

4. Пусть $g = 2$. Составим таблицу умножения:

$$0 \cdot 0 = 0 \qquad 0 \cdot 1 = 0$$
$$1 \cdot 0 = 0 \qquad 1 \cdot 1 = 1$$

$$\begin{array}{r} \times\;10111_2 \\ \quad\;1011_2 \\ \hline \quad\;10111 \\ \quad\;10111 \\ \;\;10111 \\ \hline 11111101_2 \end{array}$$

Проверим делением.

$$\begin{array}{r|l} -\,11111101_2 & 10111_2 \\ \cline{2-2} \quad\;10111 & 1011_2 \\ \cline{1-1} \quad\;100010 & \\ -\;\;10111 & \\ \cline{1-1} \quad\;\;10111 & \\ -\;\;10111 & \\ \cline{1-1} \quad\;\;\;\;0 & \end{array}$$

5. Умножить 457_8 на 56_8.
Здесь $g = 8$. Составим таблицу умножения:

x \ y	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	10	12	14	16
3	0	3	6	11	14	17	22	25
4	0	4	10	14	20	24	30	34
5	0	5	12	17	24	31	36	43
6	0	6	14	22	30	36	44	52
7	0	7	16	25	34	43	52	61

(Таблица сложения при $g = 8$ была дана выше, в примере 2.)

$$\begin{array}{r} \times\;457_8 \\ \quad\;56_8 \\ \hline \quad\;3432 \\ +\;2753 \\ \hline 33162_8 \end{array}$$

Проверим делением.

$$\begin{array}{r|l} -\,33162_8 & 457_8 \\ \cline{2-2} \quad\;2753 & 56_8 \\ \cline{1-1} \quad\;3432 & \\ -\;\;3432 & \\ \cline{1-1} \quad\;\;\;0 & \end{array}$$

Вопросы для самопроверки и упражнения

1. В чем заключается сходство и различие между непозиционными и позиционными системами счисления?

2. Прочитайте числа LXIV, CLIX, DXCVI.

3. Запишите в римской нумерации числа: 26, 55, 93, 431, 2179, 3804.

4. Как изображается основание g в девятеричной, двенадцатеричной, шестнадцатеричной системах счисления?

5. Запишите все цифры шестнадцатеричной системы счисления. Сколько их?

6. При записи числа 4023 (10)7 (12)9_g использованы наименьшая и наибольшая цифры системы счисления. Чему равно основание g?

7. Верно ли записаны числа в семеричной системе счисления: 2360_7, $35\,721_7$, $608\,512_7$? Если нет, то почему?

8. Запишите первые 38 чисел в девятеричной, одиннадцатеричной и четырнадцатеричной системах счисления.

9. Запишите число 37 в восьмеричной, 54 — в девятеричной, 65 — в двенадцатеричной системах счисления.

10. Дайте теоретическое обоснование перехода от одной системы счисления к другой.

11. Чему равно основание системы счисления, в которой $26 = 101_x$?

Указание. $1 \cdot x^2 + 0 \cdot x + 1 = 26$.

12. Чему равно основание системы счисления, в которой $231_x = 123_7$?

13. Имеют ли место равенства:

а) $47056_8 = 100\ 111\ 000\ 101\ 110_2$, б) $101\ 001\ 100\ 011\ 101_2 = 51\ 465_8$?

14. Запишите числа $70\,532_8$ и $160\,346_8$ в двоичной системе.

15. Запишите числа $100\ 111\ 010\ 101_2$ и $1\ 100\ 010\ 010\ 110\ 111_2$ в восьмеричной системе.

16. Выполните действия в соответствующих системах счисления; после этого переведите числа в десятичную систему счисления, выполните действия в десятичной системе счисления и сравните полученные ответы:

а) $(1\ 001\ 101_2 + 1\ 110\ 001_2) \cdot (1\ 110\ 001_2 - 1\ 001\ 101_2)$.

б) $212\,012_3 \cdot 201_3 + 22020_3 \cdot 111_3$.

в) $767_8 \cdot 34_8 - 2\,055_8$.

г) 4 (10) $(11)5_{12} - 2$ (11) $(10)8_{12}$.

17. Докажите, что число, записанное в двенадцатеричной системе счисления, делится на 11 в том и только в том случае, когда сумма его цифр делится на 11.

18. Докажите, что число, записанное в двенадцатеричной системе счисления, делится на 4 в том и только в том случае, когда его последняя цифра делится на 4.

19. Выведите признак делимости на $g-1$ в g-ичной системе счисления.

20. Замените звездочки цифрами так, чтобы

а) число $7*8\,(10)\,5_{12}$ делилось на 11,
б) число $36*05_7$ делилось на 6,
в) число $51*2_6$ делилось на 4,
г) число $25**_8$ делилось на 32.

21. Осуществите переход:

а) $37\,051_8 = x_6$; б) $42\,013_5 = x_7$; в) $890\,721 = x_8$; г) $45\,261_7 = x_{10}$.

22. Число (11)(10)(10) записано в двенадцатеричной системе. Как оно запишется в десятичной системе счисления?

23. Запишите числа m и n в системе счисления с основанием g и разделите m на n с остатком:

а) $m = 54326_9$; $n = 35_7$; $g = 8$;
б) $m = 70\,463_8$; $n = 124_5$; $g = 7$;
в) $m = 23\,012_4$; $n = 158_9$; $g = 5$.

24. В какой системе счисления число 46 изобразится теми же цифрами, но в обратном порядке?

25. Найдите основание x системы счисления, в которой справедливо равенство:

а) $52_x = 32$; б) $400_x = 64$; в) $51 = 201_x$;
г) $45 = 231_x$; д) $10\,302_x = 2550$; е) $400_x = 32$.

26. В каких системах счисления возможны равенства:

а) $15 + 16 = 33$; $314 + 45 = 403$;
б) $236 - 145 = 61$; $263 - 214 = 46$;
в) $5 \cdot 7 = 38$; $13 \cdot 5 = 63$;
г) $66 : 9 = 8$; $347 : 12 = 28$?

27. Правильно ли выполнены действия:

а) $\begin{array}{r} 34807_9 \\ +\ 8765_9 \\ \hline 44573_9 \end{array}$ б) $\begin{array}{r} 40(10)8_{12} \\ +\ 31(11)9_{12} \\ \hline 72(10)5_{12} \end{array}$ в) $\begin{array}{r} 67(12)6_{15} \\ +\ 9\ \ 6\ 1_{15} \\ \hline 5(11)\,5(10)_{15} \end{array}$

28. Правильно ли выполнены действия:

а) $g = 5$, $\begin{array}{r} \times\ 243 \\ \hline 34 \\ \hline 2132 \\ +\ 1334 \\ \hline 20472 \end{array}$ б) $g = 12$, $\begin{array}{r} \times\ (11)26 \\ \hline 32 \\ \hline 1(10)\,5\,0 \\ +\ 2\,9\,7\,6 \\ \hline 2(11)\,5(11)0 \end{array}$

29. В каких системах счисления возможны равенства:

а) $14 + 12 = 30$; б) $3 \cdot 5 = 14$; в) $33 - 16 = 15$; г) $24 : 5 = 4$?

30. Составьте таблицы сложения и умножения однозначных чисел в системах с основаниями $g = 4$, $g = 7$, $g = 12$.

31. Выполните сложение чисел:

а) $1\,001\,010_2 + 1\,101\,001_2$; б) $1543_6 + 42_6$;

в) $65\,004_8 + 70\,645_8 + 132_8$; г) $7489(12)_{13} + 5762_{13}$;

д) $850(11)4_{12} + 706(10)_{12}$;

е) $43(10)(11)5_{12} + 3(10)6_{12} + 4(11)25_{12}$.

32. Выполните вычитание чисел:

а) $10\,101\,011_2 - 110\,111_2$; б) $2304_6 - 425_6$;

в) $783\,041_9 - 27\,605_9$; г) $46(10)37_{12} - 728(11)_{12}$;

д) $1(11)(10)(10)_{12} - 9(11)7_{12}$.

33. Выполните умножение чисел:

а) $1\,011\,111_2 \cdot 101_2$; б) $4203_5 \cdot 34_5$; в) $50\,624_7 \cdot 23_7$;

г) $42(11)_{12} \cdot 13_{12}$; д) $343\,224_7 \cdot 125_7$.

34. Выполните деление чисел:

а) $111\,100\,011_2 : 10\,101_2$; б) $1\,141\,043_5 : 23_5$;

в) $471\,222_8 : 27_8$; г) $51(10)3406_{11} : 548_{11}$.

35. Как изменится запись числа 214_5, если увеличить его в 25 раз, в 125 раз?

36. Найдите двузначное число, которое в системах с основаниями $g = 4$ и $g = 10$ записывается одними и теми же цифрами, но в обратном порядке.

37. Найдите двузначное число, которое в системах с основаниями $g = 7$ и $g = 9$ записывается одними и теми же цифрами, но в обратном порядке.

38. Найдите в десятичной системе счисления трехзначное число, которое, будучи записано в системе счисления с основанием 9, дает число, написанное теми же цифрами, что и искомое, но в обратном порядке.

39. Докажите, что в системе счисления, основание которой есть g, удвоенное число, предшествующее основанию, и квадрат числа, предшествующего основанию, записываются одними и теми же числами, но в обратном порядке.

40. Докажите, что число 144 будет квадратом натурального числа в системе счисления с любым основанием $g > 4$.

41. Докажите, что число 1331 будет кубом натурального числа в системе счисления с любым основанием $g > 3$.

42. Составьте таблицу умножения на 5 в шестеричной системе счисления; в девятеричной; в тринадцатеричной.

43. Что станет с цифрами числа 234_6, если это число увеличить в 6 раз?

44. Какие десятичные натуральные числа, записанные в семеричной системе, оканчиваются нулем? двумя нулями? тремя нулями? и т. д.?

§ 9. КОНЕЧНЫЕ ЦЕПНЫЕ ДРОБИ

1. Представление рациональных чисел конечными цепными дробями.

Пусть t — рациональное число: $t = \frac{a}{b}$, $b > 0$. Число t можно представить в виде дроби особого вида. Это представление тесно связано с алгоритмом Евклида. Применим алгоритм Евклида к числам a и b; последовательно получим:

$$\begin{aligned}
a &= bq_0 + r_1, & \frac{a}{b} &= q_0 + \frac{r_1}{b},\\
b &= r_1q_1 + r_2, & \frac{b}{r_1} &= q_1 + \frac{r_2}{r_1},\\
r_1 &= r_2q_2 + r_3, & \frac{r_1}{r_2} &= q_2 + \frac{r_3}{r_2},\\
&\ldots\ldots\ldots\ldots\ldots & &\\
r_{n-2} &= r_{n-1}q_{n-1} + r_n, & \frac{r_{n-2}}{r_{n-1}} &= q_{n-1} + \frac{r_n}{r_{n-1}},\\
r_{n-1} &= r_nq_n, & \frac{r_{n-1}}{r_n} &= q_n.
\end{aligned} \tag{1}$$

Из второго равенства получаем, что

$$\frac{r_1}{b} = \frac{1}{q_1 + \frac{r_2}{r_1}}. \tag{2}$$

Подставляя это выражение в первое равенство (1), получим:

$$\frac{a}{b} = q_0 + \frac{1}{q_1 + \frac{r_2}{r_1}}. \tag{3}$$

Но из третьего равенства (1) следует, что

$$\frac{r_2}{r_1} = \frac{1}{q_2 + \frac{r_3}{r_2}}.$$

Подставляя это выражение в (3), получим:

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \frac{r_3}{r_2}}}.$$

В конце концов получаем:

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ldots + \cfrac{1}{q_n}}}. \tag{4}$$

Сокращенно дробь вида (4) будем обозначать:

$$\frac{a}{b} = [q_0;\ q_1,\ q_2,\ \ldots,\ q_n].$$

О п р е д е л е н и е 1. Представление (4) рационального числа называется конечной *цепной или непрерывной дробью.*

Числа $q_0, q_1, \ldots, g_n$ называются *неполными частными числа* $\frac{a}{b}$; все q_l — целые, а начиная с q_1 — натуральные.

Если дробь $\frac{a}{b}$ положительная, то q_0 — натуральное при $a > b$ $\left(\text{тогда } \frac{a}{b} = [q_0;\ q_1,\ \ldots\ ,\ q_n]\right)$ и $q_0 = 0$ при $a < b$ $\left(\text{в этом случае } \frac{a}{b} = [0;\ q_1,\ q_2,\ \ldots,\ q_n]\right)$.

Если дробь $\frac{a}{b}$ отрицательная, то ее можно представить в виде $-l + \frac{a_1}{b_1}$ $\left(l,\ a_1,\ b_1 \text{ — натуральные; } \frac{a_1}{b_1} \text{ — правильная положительная дробь}\right)$.

Тогда $\frac{a}{b} = [-l;\ q_1,\ q_2,\ \ldots,\ q_n]$, $q_0 = -l$.

Здесь целое $q_0 < 0$; $q_1, q_2, \ldots, q_n$ — натуральные.

Если $\frac{a}{b} = c$ — целое, то $c = [c]$.

Нами доказана следующая теорема:

Т е о р е м а 1. *Всякое рациональное число может быть представлено в виде конечной цепной дроби.*

П р и м е р ы.

1. $\frac{37}{15} = 2 + \cfrac{1}{2 + \cfrac{1}{7}} = [2;\ 2,\ 7]$.

$$\begin{array}{r|l} 37 & 15 \\ \hline -30 & 2 \\ \hline 15 & 7 \\ \hline -14 & 2 \\ \hline 7 & 1 \\ \hline -7 & 7 \\ \hline 0 & \end{array}$$

2. $\frac{13}{141} = 0 + \cfrac{1}{10 + \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{1}{2}}}} = [0;\ 10,\ 1,\ 5,\ 2]$.

3. $-\frac{43}{15} = -2\frac{13}{15} = -3 + \frac{2}{15} = -3 + \cfrac{1}{7 + \cfrac{1}{2}} = [-3;\ 7,\ 2]$.

4. $\frac{-23}{29} = -1 + \frac{6}{29} = -1 + \cfrac{1}{4 + \cfrac{1}{1 + \frac{1}{5}}} = [-1;\ 4,\ 1,\ 5]$.

5. $\frac{1}{17} = 0 + \frac{1}{17} = [0;\ 17]$.

6. $9 = [9]$.

7. $-19 = [-19]$.

Если допустить, что последнее неполное частное может равняться 1, то для всякого рационального числа можно получить два представления в виде конечной цепной дроби.

Пример.

$$2 + \cfrac{1}{5 + \frac{1}{3}} = 2 + \cfrac{1}{5 + \cfrac{1}{2 + \frac{1}{1}}}.$$

Теорема 2. *Представление рационального числа в виде непрерывной дроби, такой, что последнее неполное частное отлично от* 1, *единственно.*

Доказательство (от противного). Пусть возможны два представления числа $\frac{a}{b}$ в виде конечной цепной дроби:

$$\frac{a}{b} = [a_0;\ a_1,\ a_2,\ \ldots,\ a_n];\quad \frac{a}{b} = [b_0;\ b_1,\ b_2,\ \ldots,\ b_k]. \tag{5}$$

Тогда $a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots + \frac{1}{a_n}}} = b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \ldots + \frac{1}{b_k}}}$.

Рассмотрим второе слагаемое левой части равенства, обозначив его через c:

$$c = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots + \frac{1}{a_n}}}.$$

Здесь все a_i — натуральные. Если $n > 1$, то $0 < c < 1$.

Если $n = 1$, $a_1 > 1$, то и в этом случае $0 < c < 1$. Если $n = 1$ и $a_1 = 1$, то $c = 1$. Поскольку этот случай исключается (по условию теоремы), то $0 < c < 1$ всегда, т. е. c — правильная дробь.

Тогда $\frac{a}{b} = a_0 + c$, где $0 < c < 1$.

Аналогично:

$$\frac{a}{b} = b_0 + l, \text{ где } 0 < l < 1.$$

Это значит, что a_0 и b_0 — целые части одного и того же числа $\frac{a}{b}$. Но так как целая часть числа определяется однозначно, то $a_0 = b_0$.

После вычитания a_0 и b_0 из обеих частей (5) получим равные дроби с равными числителями, но тогда и знаменатели этих дробей равны, т. е.

$$a_1 + \cfrac{1}{a_2 + \ldots + \cfrac{1}{a_n}} = b_1 + \cfrac{1}{b_2 + \ldots + \cfrac{1}{b_k}}.$$

Рассуждая аналогично, получим последовательно: $a_1 = b_1$, $a_2 = b_2$, ..., и т. д. Далее возможны три случая:

1) $n = k$; 2) $n < k$; 3) $n > k$.

1-й случай. $n = k$. Тогда получим: $a_0 = b_0$, $a_1 = b_1$, ..., $a_n = b_k$. Теорема доказана.

2-й случай. $n < k$. Тогда получим:

$$a_n = b_n + \cfrac{1}{b_{n+1} + \ldots + \cfrac{1}{b_k}}, \qquad (6)$$

a_n — целое число. Правая часть равенства (6) может быть целым лишь при $k = n + 1$ и $b_{n+1} = 1$, но это противоречит условию. Значит, случай $n < k$ невозможен.

Аналогично доказывается невозможность и случая $n > k$. Остается первый случай: $n = k$; $a_0 = b_0$, $a_1 = b_1$, ..., $a_n = b_k$. Теорема доказана.

Т е о р е м а 3. *Всякая конечная цепная дробь есть рациональное число.*

Д о к а з а т е л ь с т в о. Пусть дана цепная дробь (4). Если произвести указанные арифметические действия над целыми числами 1 и q_0, ..., q_n, то получим рациональное число.

2. Подходящие дроби и их свойства.

О п р е д е л е н и е 2. Дроби

$$\delta_0 = \frac{P_0}{Q_0} = \frac{q_0}{1},\ \delta_1 = \frac{P_1}{Q_1} = q_0 + \frac{1}{q_1},\ \delta_2 = \frac{P_2}{Q_2} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2}}$$

и т. д. называются *подходящими дробями* цепной дроби (4) или соответствующего ей числа $\frac{a}{b}$.

Очевидно, что последняя подходящая дробь $\delta_n = \frac{P_n}{Q_n}$ есть число $\frac{a}{b}$.

Каждая подходящая дробь есть некоторое рациональное число. Поставим задачу найти общую формулу для вычисления подходящей дроби любого порядка.

Заметим, что s-я подходящая дробь δ_s получается путем замены q_{s-1} на $q_{s-1} + \frac{1}{q_s}$.

Подходящие дроби последовательно можно представить в виде:

$$\delta_0 = \frac{q_0}{1} = \frac{P_0}{Q_0},\ \delta_1 = q_0 + \frac{1}{q_1} = \frac{q_0 q_1 + 1}{q_1} = \frac{P_1}{Q_1},$$

$$\delta_2 = q_0 + \frac{1}{q_1 + \frac{1}{q_2}} = q_0 + \frac{q_2}{q_1 q_2 + 1} = \frac{q_0 q_1 q_2 + q_0 + q_2}{q_1 q_2 + 1} =$$

$$= \frac{(q_0 q_1 + 1) q_2 + q_0}{q_1 q_2 + 1} = \frac{P_1 q_2 + P_0}{Q_1 q_2 + Q_0} = \frac{P_2}{Q_2}.$$

Откуда

$$\delta_2 = \frac{P_2}{Q_2} = \frac{P_1 q_2 + P_0}{Q_1 q_2 + Q_0}.$$

Предположим, что для s-й подходящей дроби имеет место формула:

$$\delta_s = \frac{P_s}{Q_s} = \frac{P_{s-1} q_s + P_{s-2}}{Q_{s-1} q_s + Q_{s-2}}, \qquad (1)$$

и докажем справедливость этой формулы для подходящей дроби δ_{s+1}.

Так как δ_{s+1} получается из δ_s заменой q_s на $q_s + \frac{1}{q_{s+1}}$, то получим:

$$\delta_{s+1} = \frac{P_{s+1}}{Q_{s+1}} = \frac{P_{s-1}\left(q_s + \frac{1}{q_{s+1}}\right) + P_{s-2}}{Q_{s-1}\left(q_s + \frac{1}{q_{s+1}}\right) + Q_{s-2}} =$$

$$= \frac{(q_s P_{s-1} + P_{s-2}) q_{s+1} + P_{s-1}}{(q_s Q_{s-1} + Q_{s-2}) q_{s+1} + Q_{s-1}} = \frac{P_s q_{s+1} + P_{s-1}}{Q_s q_{s+1} + Q_{s-1}}.$$

На основании принципа математической индукции заключаем, что формула (1) справедлива для любого s.

Выпишем рекуррентные формулы для вычисления числителей P_s и знаменателей Q_s подходящих дробей (закон составления подходящих дробей):

$P_0 = q_0$, $P_1 = q_0 q_1 + 1$, а при $s > 1$ $P_s = P_{s-1} q_s + P_{s-2}$,
$Q_0 = 1$, $Q_1 = q_1$, $Q_s = Q_{s-1} q_s + Q_{s-2}$.

Вычисления удобно проводить по схеме:

s		0	1	2	...	s	$s+1$	...	n
q_s		q_0	q_1	q_2	...	q_s	q_{s+1}	...	q_n
P_s	1	$P_0 = q_0$	$P_1 = q_0 q_1 + 1$	$P_2 = P_1 q_2 + P_0$	...	$P_s = P_{s-1} q_s + P_{s-2}$	...	...	P_n
Q_s	0	$Q_0 = 1$	$Q_1 = q_1$	$Q_2 = Q_1 q_2 + Q_0$	...	$Q_s = Q_{s-1} q_s + Q_{s-2}$	...	...	Q_n

Например, для получения P_{s+1} нужно стоящее над ним число q_{s+1} умножить на стоящее слева от клетки для P_{s+1} число P_s и к результату прибавить стоящее слева от P_s число P_{s-1}. Аналогично вычисляется и Q_{s+1}.

Правильность проделанных вычислений проверяется совпадением последних вычисленных выражений для P_n и Q_n с числителем a и знаменателем b дроби $\frac{a}{b}$ $\left(\text{если } \frac{a}{b} \text{ несократима}\right)$.

Пример. Разложим в непрерывную дробь число $\frac{105}{38}$ и найдем все подходящие дроби разложения.

С помощью алгоритма Евклида получаем:

$\frac{105}{38} = [2;\ 1,\ 3,\ 4,\ 2]$.

$$
\begin{array}{r|l}
105 & 38 \\
\hline
76 & 2 \\
\hline
38 & 29 \\
\hline
29 & 1 \\
\hline
29 & 9 \\
\hline
27 & 3 \\
\hline
9 & 2 \\
\hline
8 & 4 \\
\hline
2 & 1 \\
\hline
2 & 2 \\
\hline
0 &
\end{array}
$$

Подходящие дроби находим по схеме:

s		0	1	2	3	4
q_s		2	1	3	4	2
P_s	1	2	3	11	47	105
Q_s	0	1	1	4	17	38

Последовательные подходящие дроби:

$$\delta_0 = \frac{2}{1};\quad \delta_1 = \frac{3}{1};\quad \delta_2 = \frac{11}{4};\quad \delta_3 = \frac{47}{17};\quad \delta_4 = \frac{105}{38}.$$

3. Основные свойства подходящих дробей.

1) *Числители и знаменатели подходящих дробей — целые числа; знаменатели, кроме того, числа натуральные и образуют возрастающую последовательность.*

Доказательство. Первое утверждение очевидно, так как q_l — числа целые.

Докажем второе. Действительно, $Q_0 = 1$, $Q_1 = q_1 \geqslant 1$, а при $s \geqslant 2$

$$Q_s = Q_{s-1}q_s + Q_{s-2}, \text{ где } q_s \geqslant 1,\ Q_{s-1} \geqslant 1,\ Q_{s-2} \geqslant 1. \qquad (1)$$

Значит, $Q_s > Q_{s-1}$.

2) *Числители и знаменатели двух соседних подходящих дробей связаны соотношением:*

$$P_{s-1}Q_s - P_sQ_{s-1} = (-1)^s. \qquad (2)$$

Доказательство. Используем метод математической индукции.

а) При $s = 1$ имеем:

$$P_0 = q_0, \quad Q_0 = 1,$$
$$P_1 = q_0 q_1 + 1, \quad Q_1 = q_1$$

и $P_0 Q_1 - P_1 Q_0 = q_0 q_1 - (q_0 q_1 + 1) \cdot 1 = -1 = (-1)^1$,
т. е. при $s = 1$ соотношение (2) имеет место.

б) Предположим верность формулы (2) для $s = k$:

$$P_{k-1} Q_k - P_k Q_{k-1} = (-1)^k$$

и докажем верность ее для $s = k + 1$.

$$P_k Q_{k+1} - P_{k+1} Q_k = P_k (Q_k q_{k+1} + Q_{k-1}) - Q_k (P_k q_{k+1} + P_{k-1}) =$$
$$= P_k Q_k q_{k+1} + P_k Q_{k-1} - Q_k P_k q_{k+1} - Q_k P_{k-1} =$$
$$= -(P_{k-1} Q_k - P_k Q_{k-1}) = -(-1)^k = (-1)^{k+1}.$$

Итак, $P_k Q_{k+1} - P_{k+1} Q_k = (-1)^{k+1}$.

Тогда согласно принципу математической индукции формула (2) верна для любого натурального s.

3) *Подходящие дроби* $\frac{P_s}{Q_s}$ *несократимы, т. е.* $(P_s, Q_s) = 1$.

Доказательство. Действительно, согласно свойству 2) подходящих дробей имеем:

$$P_{s-1} Q_s - P_s Q_{s-1} = (-1)^s.$$

Если допустить, что $(P_s, Q_s) \neq 1$, т. е. что $(P_s, Q_s) = d > 1$, то из равенства (1) п. 2 следует, что $(-1)^s$ делится на $d > 1$, что невозможно. Следовательно, $(P_s, Q_s) = 1$.

Замечание. Если рациональное число $\frac{a}{b}$ разложить в цепную дробь, то последняя подходящая дробь δ_n в этом разложении несократима и равна $\frac{a}{b}$. Таким образом, разложение в цепную дробь позволяет сокращать дроби.

4) *Подходящие дроби четного порядка образуют возрастающую, а нечетного — убывающую последовательность.*

Доказательство. Пользуясь формулами (1) и (2), получим:

$$\frac{P_{k-2}}{Q_{k-2}} - \frac{P_k}{Q_k} = \frac{P_{k-2} Q_k - P_k Q_{k-2}}{Q_{k-2} Q_k} =$$
$$= \frac{P_{k-2}(Q_{k-1} q_k + Q_{k-2}) - (P_{k-1} q_k + P_{k-2}) Q_{k-2}}{Q_{k-2} Q_k} = \frac{q_k (P_{k-2} Q_{k-1} - P_{k-1} Q_{k-2})}{Q_{k-2} Q_k} =$$
$$= \frac{-q_k (P_{k-1} Q_{k-2} - P_{k-2} Q_{k-1})}{Q_{k-2} Q_k} = \frac{(-1)^{k-1} q_k}{Q_{k-2} Q_k}.$$

Итак, $\frac{P_{k-2}}{Q_{k-2}} - \frac{P_k}{Q_k} = \frac{(-1)^{k-1} q_k}{Q_{k-2} Q_k}$.

Если k — четное, то $\frac{P_{k-2}}{Q_{k-2}} - \frac{P_k}{Q_k} < 0$, или $\frac{P_{k-2}}{Q_{k-2}} < \frac{P_k}{Q_n}$,

т. е. подходящие дроби четного порядка образуют возрастающую последовательность.

Если k — нечетное, то

$$\frac{P_{k-2}}{Q_{k-2}} - \frac{P_k}{Q_k} > 0, \text{ или } \frac{P_{k-2}}{Q_{k-2}} > \frac{P_k}{Q_k},$$

т. е. подходящие дроби нечетного порядка образуют убывающую последовательность.

5) *Каждая подходящая дробь* $\frac{P_k}{Q_k}$ *четного порядка меньше подходящих дробей* $\frac{P_{k-1}}{Q_{k-1}}$ и $\frac{P_{k+1}}{Q_{k+1}}$.

Доказательство. Используя свойство 2 подходящих дробей, находим:

$$\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{P_kQ_{k-1} - P_{k-1}Q_k}{Q_kQ_{k-1}} = \frac{-(P_{k-1}Q_k - P_kQ_{k-1})}{Q_{k-1}Q_k} =$$

$$= \frac{-(-1)^k}{Q_{k-1}Q_k} = \frac{(-1)^{k+1}}{Q_{k-1}Q_k}.$$

Заменяя k на $k+1$, получим:

$$\frac{P_{k+1}}{Q_{k+1}} - \frac{P_k}{Q_k} = \frac{(-1)^{k+2}}{Q_kQ_{k+1}}.$$

Если k — четно, то $(-1)^{k+1} = -1 < 0$, а $(-1)^{k+2} = 1 > 0$. Значит, при четном k

$$\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} < 0, \quad \frac{P_{k+1}}{Q_{k+1}} - \frac{P_k}{Q_k} > 0.$$

Это и показывает, что

$$\frac{P_k}{Q_k} < \frac{P_{k-1}}{Q_{k-1}} \text{ и } \frac{P_k}{Q_k} < \frac{P_{k+1}}{Q_{k+1}}.$$

Следствие. *Каждая подходящая дробь* $\frac{P_k}{Q_k}$ *нечетного порядка больше подходящих дробей* $\frac{P_{k-1}}{Q_{k-1}}$ *и* $\frac{P_{k+1}}{Q_{k+1}}$.

6) *Любая подходящая дробь четного порядка меньше любой подходящей дроби нечетного порядка.*

Доказательство. На основании четвертого и пятого свойства при $l \geqslant k$ получаем:

$$\frac{P_{2l+2}}{Q_{2l+2}} < \frac{P_{2l+1}}{Q_{2l+1}} \leqslant \frac{P_{2k+1}}{Q_{2k+1}}.$$

При $l < k$ получаем:

$$\frac{P_{2l+2}}{Q_{2l+2}} < \frac{P_{2k+2}}{Q_{2k+2}} < \frac{P_{2k+1}}{Q_{2k+1}}.$$

Следовательно, при любых соотношениях между l и k выполняется неравенство:

$$\frac{P_{2l+2}}{Q_{2l+2}} > \frac{P_{2k+1}}{Q_{2k+1}},$$

которое доказывает свойство 6.

7) *Если t — положительное рациональное число, то при его разложении в цепную дробь четные подходящие дроби — приближения по недостатку, а нечетные — по избытку (за исключением последней дроби, совпадающей с t).*

Доказательство. Если последняя подходящая дробь, совпадающая с числом t, четного порядка, то она (по свойству 4) больше остальных подходящих дробей четного порядка, которые дают, таким образом, приближения t по недостатку. Вместе с тем число t как подходящая дробь четного порядка меньше любой подходящей дроби нечетного порядка (по свойству 6), а потому подходящие дроби нечетного порядка дают для t приближение с избытком. Аналогично рассматривается случай, когда последняя подходящая дробь, совпадающая с t, является дробью нечетного порядка (читателю рекомендуется рассмотреть этот случай самостоятельно).

8) *Если t — положительное рациональное число и $\frac{P_k}{Q_k}$ — подходящая дробь k-го порядка в разложении t в непрерывную дробь, то*

$$\left|t-\frac{P_k}{Q_k}\right| \leqslant \frac{1}{Q_kQ_{k+1}} < \frac{1}{Q_k^2}. \tag{3}$$

Доказательство. Так как на основании свойства 7 число t заключено между любыми двумя своими соседними подходящими дробями, то

$$\left|t-\frac{P_k}{Q_k}\right| \leqslant \left|\frac{P_k}{Q_k}-\frac{P_{k+1}}{Q_{k+1}}\right|. \tag{4}$$

Но

$$\left|\frac{P_k}{Q_k}-\frac{P_{k+1}}{Q_{k+1}}\right| = \left|\frac{(-1)^{k+1}}{Q_{k+1}Q_k}\right| = \frac{1}{Q_{k+1}Q_k} \tag{5}$$

(см. доказательство свойства 5).

Тогда из (3) и (5) следует:

$$\left|t-\frac{P_k}{Q_k}\right| \leqslant \frac{1}{Q_kQ_{k+1}}.$$

Так как $Q_{k+1} = Q_kq_{k+1} + Q_{k-1}$, то $Q_{k+1} > Q_k$, а потому $\frac{1}{Q_kQ_{k+1}} < \frac{1}{Q_k^2}$.

Следовательно,

$$\left|t-\frac{P_k}{Q_k}\right| \leqslant \frac{1}{Q_kQ_{k+1}} < \frac{1}{Q_k^2}.$$

Примеры.

1. В предыдущем примере (см. с. 56) оцените приближение числа $t = \frac{105}{38}$ подходящей дробью $\delta_2 = \frac{11}{4}$.

На основании неравенства (3) получаем:

$$\left|t - \frac{11}{4}\right| < \frac{1}{Q_2 Q_3} = \frac{1}{4 \cdot 17} = \frac{1}{68}.$$

2. Заменим число $\frac{245}{83}$ такой подходящей дробью, чтобы полученная при этом погрешность не превышала 0,001.

Решение. Разлагаем данное число в цепную дробь:

$$\begin{array}{r|l} 245 & 83 \\ \hline 166 & 2 \\ \hline 83 & 79 \\ \hline 79 & 1 \\ \hline 4 & 19 \\ \hline 39 & \\ \hline 36 & \\ \hline 4 & 3 \\ \hline 3 & 1 \\ \hline 3 & 3 \\ \hline 0 & \end{array}$$

Получим:

$$\frac{245}{83} = [2;\ 1,\ 19,\ 1,\ 3].$$

Находим подходящие дроби:

s		0	1	2	3	4
q_s		2	1	19	1	3
P_s	1	2	3	59	62	245
Q_s	0	1	1	20	21	83

$$\left|\frac{245}{83} - \frac{59}{20}\right| < \frac{1}{20 \cdot 21} > \frac{1}{1000}.$$

Следовательно, дробь δ_2 не подходит.

$$\left|\frac{245}{83} - \frac{62}{21}\right| < \frac{1}{21 \cdot 83} < \frac{1}{1000}.$$

Ответ. Искомая подходящая дробь $\delta_3 = \frac{62}{21}$.

Вопросы для самопроверки и упражнения

1. Как связан алгоритм Евклида с цепными дробями?
2. Какими числами являются q_0, q_1, q_2, ..., q_n? Как они называются?
3. В каком случае разложение рационального числа в конечную цепную дробь является единственным?
4. Каким числом является конечная цепная дробь $[q_0; q_1, \ldots, q_n]$?
5. Какие дроби называются подходящими к цепной дроби?
6. По какому закону составляются подходящие дроби? Примените его к нахождению подходящих дробей цепной дроби [1; 2, 3, 4, 1, 3]. Для чего в таблице для нахождения подходящих цепных дробей в столбце перед P_0 и Q_0 ставятся числа 1 и 0?
7. Какой характерной особенностью обладают знаменатели подходящих дробей?
8. Какова связь между числителями и знаменателями двух соседних подходящих дробей?
9. Какой характерной особенностью обладают подходящие дроби с четными номерами? с нечетными номерами?
10. Почему любая подходящая дробь с четным номером меньше любой подходящей дроби с нечетным номером?
11. Может ли быть сократимой какая-либо подходящая дробь цепной дроби $[q_0; q_1, \ldots, q_n]$? Почему?
12. Какие приближения к числу $\frac{a}{b}$ дают подходящие дроби с четными номерами? с нечетными?
13. Верно ли утверждение: все подходящие дроби числа $\frac{a}{b}$ с четными номерами дают приближения к $\frac{a}{b}$ по недостатку, а с нечетными — по избытку? Почему?
14. Чему равна погрешность, допускаемая при замене рационального числа $\frac{a}{b}$ подходящей дробью δ_k?

Оцените погрешность, которая получится при замене числа $\frac{48}{17}$ подходящей дробью δ_3.

15. Приведите к общему знаменателю следующие дроби:

а) $\frac{1}{750}, \frac{1}{1240}, \frac{1}{1675}$; б) $\frac{1}{875}, \frac{1}{1640}, \frac{1}{1975}$;

в) $\frac{1}{173}, \frac{1}{1201}, \frac{1}{101}$.

16. Разложите в непрерывные дроби:

а) $\frac{37}{81}$; б) $\frac{1811}{691}$; в) $\frac{1723}{1447}$; г) $\frac{3203}{1289}$; д) $\frac{4513}{18355}$; е) 2,98976;

ж) 2,71828; з) 3,14159.

17. Разложите в непрерывные дроби:

а) $\frac{343}{221}$ и $\frac{226}{343}$; б) $\frac{117}{343}$ и $\frac{-343}{117}$.

Сравните подходящие дроби в этих разложениях.

18. Преобразуйте в обыкновенную дробь следующие непрерывные дроби:

а) [2; 3, 1, 4]; б) [2; 1, 1, 2, 1, 6, 2, 5]; в) [0; 1, 2, 3, 4, 5]; г) [—2; 3, 1, 5, 4, 2]; д) [0; 13, 2, 2, 2, 1, 1, 7].

19. Разложите 0,429 в непрерывную дробь и найдите третье приближение.

20. Сократите с помощью разложения в непрерывную дробь:

а) $\frac{1043}{3427}$; б) $\frac{3587}{2743}$; в) $\frac{1857}{9153}$; г) $\frac{70757}{491209}$; д) $\frac{326129}{3270977}$; е) $\frac{798551}{858819}$.

21. Найдите x, если: а) $[2;\ 1,\ 2,\ x] = \left|\frac{19}{7}\right|$.

22. С помощью подходящих дробей найдите приближение к дроби $\alpha = \frac{13891}{5065}$ с точностью до а) 0,001; б) 0,0001.

Глава II

КОЛЬЦА И ИДЕАЛЫ

§ 1. ДЕЛИМОСТЬ В КОЛЬЦАХ

1. Отношение делимости в кольцах. В главе I была рассмотрена теория делимости в кольце $\mathbf{Z}$ целых чисел. Отношение делимости можно ввести не только для целых чисел, но и для целых гауссовских чисел, т. е. для комплексных чисел вида $a + bi$, где $a, b \in \mathbf{Z}$, для чисел вида $a + b\sqrt{2}$, где $a, b \in \mathbf{Z}$, для многочленов с действительными (или комплексными) коэффициентами и т. д. Для современной математики характерно стремление заменять изучение отдельных примеров изучением общих структур, частными случаями которых являются эти примеры. Для отношения делимости естественной областью изучения является структура коммутативного ассоциативного кольца с единицей (с определением и простейшими свойствами колец читатель знаком по книге Ф. Л. Варпаховского и А. С. Солодовникова «Алгебра». М.,«Просвещение», 1978, на которую мы и будем опираться в дальнейшем изложении)*. Поскольку колец иного вида мы не будем рассматривать, в этом параграфе слово «кольцо» будет обозначать коммутативные ассоциативные кольца с единицей.

Определим сначала отношение делимости в таких кольцах.

О п р е д е л е н и е 1. *Элемент a кольца R делится на элемент b* того же кольца, если существует такой элемент $q \in R$, что $a = bq$. В этом случае пишут $a \vdots b$. Элемент b называется *делителем* элемента a.

П р и м е р ы.

1. В кольце $\mathbf{R}[x]$ многочленов с действительными коэффициентами отношение делимости совпадает с обычным отношением делимости для многочленов: многочлен $f(x)$ делится на многочлен $\varphi(x)$, если существует такой многочлен $q(x)$, что $f(x) = \varphi(x) \cdot q(x)$. Например, $x^4 - 16$ делится на $x^2 - 4$, так как $x^4 - 16 = (x^2 - 4) \times (x^2 + 4)$.

2. В кольце $\mathbf{Z}[i]$ целых гауссовых чисел $23 + 2i$ делится на $2 + 3i$. В самом деле,

$$\frac{23 + 2i}{2 + 3i} = \frac{(23 + 2i)(2 - 3i)}{(2 + 3i)(2 - 3i)} = \frac{52 - 65i}{13} = 4 - 5i,$$

а $4 - 5i \in \mathbf{Z}[i]$.

* В дальнейшем при ссылке на эту книгу мы будем писать просто «Алгебра».

3. Точно так же доказывается, что в кольце $\mathbf{Z}[\sqrt{3}]$ число $-7+18\sqrt{3}$ делится на $4-\sqrt{3}$:

$$\frac{-7+18\sqrt{3}}{4-\sqrt{3}}=\frac{(-7+18\sqrt{3})(4+\sqrt{3})}{(4-\sqrt{3})(4+\sqrt{3})}=\frac{26+65\sqrt{3}}{13}=$$
$$=2+5\sqrt{3}\in\mathbf{Z}[\sqrt{3}].$$

4. Докажем, что в кольце $\mathbf{Z}[\sqrt[3]{2}]$, состоящем из чисел вида $a+b\sqrt[3]{2}+c\sqrt[3]{4}$, где a, b, c — целые числа, $-19+10\sqrt[3]{2}+20\sqrt[3]{4}$ делится на $1-3\sqrt[3]{2}+5\sqrt[3]{4}$. Для этого надо найти число $x+y\sqrt[3]{2}+z\sqrt[3]{4}$ из $\mathbf{Z}[\sqrt[3]{2}]$, такое, что
$(1-3\sqrt[3]{2}+5\sqrt[3]{4})(x+y\sqrt[3]{2}+z\sqrt[3]{4})=-19+10\sqrt[3]{2}+20\sqrt[3]{4}$.
Раскрывая скобки, получаем, что

$$x+10y-6z+(-3x+y+10z)\sqrt[3]{2}+$$
$$+(5x-3y+z)\sqrt[3]{4}=-19+10\sqrt[3]{2}+20\sqrt[3]{4}.$$

Это равенство может иметь место лишь при условии, что x, y, z удовлетворяют системе уравнений:

$$\begin{cases} x+10y-6z=-19, \\ -3x+y+10z=10, \\ 5x-3y+z=20. \end{cases}$$

Решая эту систему, получаем, что $x=3$, $y=-1$, $z=2$. Значит, $-19+10\sqrt[3]{2}+20\sqrt[3]{4}=(1-3\sqrt[3]{2}+5\sqrt[3]{4})(3-\sqrt[3]{2}+2\sqrt[3]{4})$. А число $-18+10\sqrt[3]{2}+20\sqrt[3]{4}$ не делится на $1-3\sqrt[3]{2}+5\sqrt[3]{4}$. В этом случае мы получили бы систему уравнений:

$$\begin{cases} x+10y-6z=-18, \\ -3x+y+10z=10, \\ 5x-3y+z=20, \end{cases}$$

имеющую дробные решения.

5. В поле P любой элемент a делится на любой отличный от нуля элемент b. В самом деле, если $b\neq 0$, то существует элемент b^{-1}, обратный b, т. е. такой, что $b\cdot b^{-1}=e$. А тогда имеем: $a=b(a\cdot b^{-1})$. Так как $a\cdot b^{-1}\in P$, то $a\vdots b$.

Многие свойства отношения делимости в кольце целых чисел $\mathbf{Z}$ сохраняются для любых колец (напомним еще раз, что мы рассмат-

риваем лишь ассоциативные и коммутативные кольца с единицей). Именно, справедливы следующие утверждения:

1) *Отношение делимости рефлексивно*, т. е. для любого $a \in R$ имеем $a \vdots a$.

В самом деле, $a = ae$ (по условию $e \in R$).

2) *Отношение делимости транзитивно*: если $a \vdots b$ и $b \vdots c$, то $a \vdots c$.

В самом деле, если $a \vdots b$, то существует такое $q \in R$, что $a = bq$. А так как $b \vdots c$, то существует такое $s \in R$, что $b = cs$. Но тогда мы имеем:

$$a = bq = (cs)\, q.$$

В силу ассоциативности кольца R получаем, что $a = c\,(sq)$. А это и означает, что $a \vdots c$.

3) *Если* $a \vdots c$ *и* $b \in R$, *то* $ab \vdots c$.

В самом деле, так как $a \vdots c$, то существует такое $q \in R$, что $a = cq$. А тогда имеем: $ab = (cq)\, b$. В силу ассоциативности кольца R получаем, что

$$ab = c\,(qb).$$

Так как $qb \in R$, то $ab \vdots c$.

4) *Если* $a \vdots c$ *и* $b \vdots c$, *то* $(a \pm b) \vdots c$.

В самом деле, $a = cq$, $b = cs$, где $q \in R$ и $s \in R$. А тогда имеем:

$$a \pm b = cq \pm cs = c\,(q \pm s).$$

Так как $(q \pm s) \in R$, то $(a \pm b) \vdots c$.

5) *Если* $a \vdots c$, а b *не делится на* c, *то* $a \pm b$ *не делится на* c.

6) *Нуль делится на любой элемент* b *кольца* R.

В самом деле, $0 = b \cdot 0$.

7) *Любой элемент* a *кольца* R *делится на единицу* e.

В самом деле, $a = e \cdot a$.

2. Обратимые элементы. Чтобы сформулировать дальнейшие свойства отношения делимости в кольцах, введем понятие обратимого элемента.

Определение 2. Элемент ε кольца R называется *обратимым*, если в R существует такой элемент ε_1, что $\varepsilon\varepsilon_1 = e$.

Примеры.

1. В кольце $\mathbf{Z}$ целых чисел обратимыми являются числа 1 и -1. Других обратимых чисел в $\mathbf{Z}$ нет, так как единственными делителями числа 1 являются 1 и -1.

2. В кольце $\mathbf{Z}[i]$ целых гауссовых чисел 4 обратимых элемента: 1, -1, i и $-i$. Других обратимых элементов в $\mathbf{Z}[i]$ нет. В самом деле, если элемент $(a + bi) \in \mathbf{Z}[i]$ обратим, то найдется число

$(c + di) \in \mathbf{Z}[i]$, такое, что $(a + bi)(c + di) = 1$. Но тогда и $|a + bi|^2 \cdot |c + di|^2 = 1$, т. е.

$$(a^2 + b^2)(c^2 + d^2) = 1. \qquad (1)$$

Так как a, b, c, d — целые числа и $a^2 + b^2 > 0$, то равенство (1) может иметь место лишь при условии, что $a^2 + b^2 = 1$, т. е. в одном из четырех случаев: $a = 1$, $b = 0$; $a = -1$, $b = 0$; $a = 0$, $b = 1$; $a = 0$, $b = -1$. Это и означает, что $a + bi$ может иметь лишь четыре значения: 1, -1, i и $-i$.

3. Аналогичным образом ищут обратимые элементы в кольце $\mathbf{Z}[\sqrt{3}]$ чисел вида $a + b\sqrt{3}$, где a и b — целые числа. Если число $a + b\sqrt{3}$ обратимо, то

$$(a + b\sqrt{3})(c + d\sqrt{3}) = 1. \qquad (2)$$

Раскрывая скобки, получаем, что $ac + 3d^2 = 1$ и $ad + bc = 0$. Но тогда и

$$(a - b\sqrt{3})(c - d\sqrt{3}) = (ac + 3d^2) - (ad + bc)\sqrt{3} = 1. \qquad (3)$$

Перемножая равенства (2) и (3), получаем, что

$$(a^2 - 3b^2)(c^2 - 3d^2) = 1.$$

Значит, $a^2 - 3b^2$ является целым делителем единицы, и потому $a^2 - 3b^2 = \pm 1$. Четыре решения этого уравнения находятся сразу: $a = 2$, $b = 1$; $a = 2$, $b = -1$; $a = -2$, $b = 1$; $a = -2$, $b = -1$. Значит, числа $\pm(2 + \sqrt{3})$, $\pm(2 - \sqrt{3})$ обратимы в $\mathbf{Z}[\sqrt{3}]$. Но числа $(2 + \sqrt{3})^n$ и $(2 - \sqrt{3})^n$ при любом натуральном значении n тоже обратимы в $\mathbf{Z}[\sqrt{3}]$, так как

$$(2 + \sqrt{3})^n \cdot (2 - \sqrt{3})^n = (4 - 3)^n = 1.$$

Можно показать, что множество всех обратимых чисел кольца $\mathbf{Z}[\sqrt{3}]$ состоит из элементов вида $\pm(2 + \sqrt{3})^n$, где n — целое число (в частности, при $n = 0$ получаем число 1, а при $n = -1$ — число $2 - \sqrt{3}$).

4. В кольце $\mathbf{R}[x]$ многочленов с действительными коэффициентами обратимыми являются многочлены нулевой степени, т. е. отличные от нуля действительные числа.

Выясним теперь роль обратимых элементов при делении элементов кольца. В кольце $\mathbf{Z}$ целых чисел отношение делимости не нарушилось при умножении делителя на -1, т. е. на обратимый элемент. Аналогичное утверждение верно в любом кольце.

Если $a \vdots b$ и элемент ε обратим в R, то $a \vdots b\varepsilon$.

В самом деле, так как $a \vdots b$, то существует такой элемент q, что $a = bq$. А так как ε обратим в R, то существует такой элемент $\varepsilon_1 \in R$, что $\varepsilon \cdot \varepsilon_1 = e$. А тогда имеем:

$$a = (b\varepsilon\varepsilon_1)q = (b\varepsilon)(\varepsilon_1 q).$$

Это равенство показывает, что $a \vdots b\varepsilon$. Утверждение доказано.

Заметим, что (в силу свойства 3 отношения делимости в кольцах) если $a \vdots b$, то и $a\varepsilon \vdots b$.

Докажем следующую теорему об обратимых элементах любого кольца.

Теорема 1. *Множество $\widetilde{R}$ обратимых элементов кольца R образует коммутативную группу относительно умножения.*

Доказательство. Так как по условию кольцо R коммутативно, ассоциативно и обладает единицей, то для доказательства теоремы нам достаточно показать справедливость двух утверждений:

а) произведение двух обратимых элементов обратимо в R;

б) если ε — обратимый элемент в R, то и ε^{-1} обратимо в R.

Пусть δ и ε обратимы в R. Тогда существуют такие элементы δ_1 и ε_1 в R, что $\delta\delta_1 = e$ и $\varepsilon\varepsilon_1 = e$. Но тогда имеем:

$$(\delta\varepsilon)(\delta_1\varepsilon_1) = (\delta\delta_1)(\varepsilon\varepsilon_1) = e \cdot e = e.$$

Значит, $\delta\varepsilon$ тоже обратимо в R. Этим доказано утверждение а). Утверждение же б) сразу следует из того, что если $\varepsilon\varepsilon_1 = e$, то не только ε, но и $\varepsilon_1 = \varepsilon^{-1}$ обратимо в R.

Группу $\widetilde{R}$ называют *группой обратимых элементов* кольца R. Единичным элементом группы $\widetilde{R}$ является единица e кольца R. Предоставляем читателю проверить, что во всех разобранных выше примерах множество обратимых элементов действительно является коммутативной группой относительно операции умножения.

3. Области целостности. Мы видели, что многие свойства отношения делимости в кольце целых чисел сохраняются и для отношения делимости в любом кольце. Но в произвольном кольце нельзя говорить о частном двух элементов даже в случае, когда a делится на b. Дело в том, что в некоторых кольцах деление неоднозначно, т. е. для некоторых элементов $a \in R$, $b \in R$ можно найти несколько элементов q, таких, что $a = bq$. Мы хотим выделить класс колец, в которых имеет смысл говорить и о частном двух элементов. Введем следующие определения:

Определение 3. Отличный от нуля элемент a кольца R называется *делителем нуля* в R, если в R существует отличный от нуля элемент b, такой, что $ab = 0$ (разумеется, в этом случае и элемент b является делителем нуля в R).

Определение 4. Кольцо R называется *областью целостности*, если в нем нет делителей нуля*

Иными словами, кольцо R является областью целостности, если из $ab = 0$ следует, что $a = 0$ или $b = 0$:

$$ab = 0 \rightarrow a = 0 \vee b = 0.$$

---

* Мы условились рассматривать лишь ассоциативные и коммутативные кольца с единицей.

Примеры.

1. Пусть $\mathbf{R}^2$ — кольцо, состоящее из пар (a, b) действительных чисел, в котором сложение и умножение определяются «покоординатно»:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

и

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2).$$

Элементы $(1, 0)$ и $(0, 1)$ кольца $\mathbf{R}^2$ отличны от нулевого элемента $(0, 0)$, но $(1, 0) \cdot (0, 1) = (0, 0)$. Значит, эти элементы—делители нуля в $\mathbf{R}^2$, и потому $\mathbf{R}^2$ не является областью целостности.

2. *Любое поле является областью целостности.* В самом деле, если P — поле и $a \in P$, $a \neq 0$, то существует элемент a^{-1}, обратный a. Если $ab = 0$, то $a^{-1}(ab) = 0$, т. е. $b = 0$. Значит, равенство $a \cdot b = 0$ может выполняться лишь при условии, что $a = 0$ или $b = 0$. Это и значит, что P — область целостности.

3. Так как множество $\mathbf{C}$ комплексных чисел является полем, то в $\mathbf{C}$ нет делителей нуля. А тогда их нет и ни в каком числовом кольце. Значит, *любое числовое кольцо является областью целостности.* В частности, областями целостности являются кольцо $\mathbf{Z}[i]$ целых гауссовых чисел, кольцо $\mathbf{Z}[\sqrt{2}]$ чисел вида $a + b\sqrt{2}$, $a, b, \in \mathbf{Z}$ и т. д. Разумеется, областью целостности является и кольцо $\mathbf{Z}$ целых чисел.

4. Кольцо многочленов $P[x]$ с коэффициентами из числового поля P является областью целостности. Это вытекает из того, что при умножении многочленов их степени складываются, а потому произведение двух отличных от нуля многочленов не может равняться нулю.

5. Кольцо $C[a, b]$ функций, непрерывных на отрезке $[a, b]$, не является областью целостности. В самом деле, если функция $f(x)$ отлична от нуля лишь на промежутке (a, c), а функция $\varphi(x)$ — лишь на промежутке (c, b), то их произведение $f(x) \cdot \varphi(x)$ равно нулю на всем отрезке $[a, b]$. Например, можно положить

$$f(x) = \begin{cases} (x - a)(c - x), & a \leqslant x \leqslant c, \\ 0, & c < x \leqslant b; \end{cases}$$

$$\varphi(x) = \begin{cases} 0, & a \leqslant x \leqslant c, \\ (x - c)(b - x), & c < x \leqslant b. \end{cases}$$

4. Свойства отношения делимости в областях целостности. Докажем следующую теорему:

Теорема 2. *Если a — отличный от нуля элемент области целостности R, то из равенства $ab = ac$, где $b, c \in R$, следует, что $b = c$.*

Иными словами, в областях целостности можно сокращать обе части равенства на отличный от нуля элемент.

Доказательство. Из равенства $ab = ac$ следует, что $a(b - c) = 0$. Поскольку по условию $a \neq 0$, а R не содержит де-

лителей нуля, то равенство $a(b-c)=0$ может иметь место лишь при условии, что $b-c=0$, т. е. $b=c$. Теорема доказана.

Из теоремы 2 вытекает, что если a и $b\neq 0$ — элементы области целостности R, причем $a \vdots b$, то в R существует единственный элемент q, такой, что $a=bq$. В самом деле, если $a=bq$ и $a=bs$, то $bq=bs$ и поскольку $b\neq 0$, то $q=s$.

Определение 5. Если R — область целостности и $a \vdots b$, $b\neq 0$, то элемент $q\in R$, такой, что $a=bq$, называют *частным от деления* a на b.

В кольце целых чисел $\mathbf{Z}$ из отношений $a \vdots b$, $b \vdots a$ следует, что $a=b$ или $a=-b$, т. е. a и b отличаются друг от друга лишь обратимым множителем. По аналогии введем следующее определение:

Определение 6. Элементы a и b области целостности R называются *ассоциированными* в R, если существует обратимый элемент $\varepsilon\in R$, такой, что $a=b\varepsilon$.

Например, числа 5 и -5 ассоциированы в кольце $\mathbf{Z}$ целых чисел. А числа $5+2\sqrt{3}$ и $4-\sqrt{3}$ ассоциированы в кольце $\mathbf{Z}[\sqrt{3}]$ чисел вида $a+b\sqrt{3}$, $a, b\in\mathbf{Z}$. В самом деле, мы видели (см. с. 66), что $2-\sqrt{3}$ обратимо в $\mathbf{Z}[\sqrt{3}]$, а $4-\sqrt{3}=(5+2\sqrt{3})(2-\sqrt{3})$.

Бинарное отношение «элемент a ассоциирован с элементом b в кольце целостности R» является отношением эквивалентности — оно рефлексивно, симметрично и транзитивно. В самом деле, a ассоциировано с a, так как $a=ae$, а e обратимо в R. Далее, пусть a ассоциировано с b. Тогда есть такой обратимый элемент ε, что $a=b\varepsilon$. Но в R есть такой обратимый элемент ε_1, что $\varepsilon\varepsilon_1=e$. Умножая обе части равенства $a=b\varepsilon$ на ε_1, получаем, что $a\varepsilon_1=b$. Это показывает, что b ассоциировано с a. Значит, отношение ассоциированности симметрично. Наконец, если a ассоциировано с b, а b ассоциировано с a, то $a=b\delta$, $b=c\varepsilon$, где δ и ε — обратимые в R. А тогда

$$a=b\delta=(c\varepsilon)b=c(\varepsilon\delta).$$

Но элемент $\varepsilon\delta$ обратим в силу теоремы 1 п. 2. Значит, a ассоциировано с c. Этим доказана транзитивность отношения ассоциированности.

В п. 2 было доказано, что если $a \vdots b$ и элемент ε обратим в R, то $a \vdots b\varepsilon$ и $a\varepsilon \vdots b$. Отсюда вытекает следующее утверждение:

Если a ассоциировано с a_1, b с b_1 и $a \vdots b$, то $a_1 \vdots b_1$.

В самом деле, $a_1=a\delta$, $b_1=b\varepsilon$, где δ и ε — обратимые элементы, а из $a \vdots b$ следует, что $a\delta \vdots b\varepsilon$, т. е. что $a_1 \vdots b_1$.

Докажем теперь следующую теорему:

Теорема 3. *Для того чтобы в области целостности R выполнялись отношения $a \vdots b$ и $b \vdots a$, необходимо и достаточно, чтобы элементы a и b были ассоциированы в R.*

Доказательство. Сначала докажем достаточность условий. Пусть элементы a и b ассоциированы. Так как $a \vdots a$, то из ассоциированности a и b следует в силу доказанного выше, что $a \vdots b$. Точно так же из $a \vdots a$ и ассоциированности b и a следует, что $b \vdots a$.

Значит, из ассоциированности a и b вытекают оба отношения делимости: $a \mid b$ и $b \mid a$.

Теперь докажем необходимость этого условия, т. е. докажем, что из $a \mid b$ и $b \mid a$ вытекает ассоциированность элементов a и b в R. Так как $a \mid b$, то в R найдется такой элемент δ, что $a = b\delta$, а так как $b \mid a$, то в R найдется такой элемент ε, что $b = a\varepsilon$. Для доказательства ассоциированности a и b осталось показать, что элементы δ и ε обратимы в R. Для этого перемножим почленно равенства $a = b\delta$ и $b = a\varepsilon$. Мы получим $ab = ab\delta\varepsilon$, откуда следует, что $ab(e - \delta\varepsilon) = 0$. Так как по условию R — область целостности и $a \neq 0$, $b \neq 0$, то $ab \neq 0$, а тогда из $ab(e - \delta\varepsilon) = 0$ следует, что $e - \delta\varepsilon = 0$, т. е. $\delta\varepsilon = e$. Это и показывает, что δ и ε обратимы в R. Теорема доказана.

5. Простые и составные элементы области целостности. Введем теперь понятия простых и составных элементов области целостности.

Определение 7. Элемент a области целостности R называется *простым* в R, если он не обратим в R, а любой делитель b элемента a либо обратим в R, либо ассоциирован с a.

Это определение можно сформулировать так: элемент a области целостности R является простым, если он не обратим в R, а любое разложение a на два множителя имеет вид $a = bc$, где один из элементов b, c обратим в R, а второй ассоциирован с a.

Определение 8. Элемент a области целостности R называется *составным*, если он допускает разложение на множители $a = bc$, причем ни b, ни c не обратимы в R.

Таким образом, все элементы области целостности R распадаются на четыре класса: нуль, обратимые элементы, простые элементы и составные элементы.

Ясно, что элемент, ассоциированный с простым элементом a, является простым, а ассоциированный с составным элементом — составным (напомним, что умножение на обратимые элементы не изменяет отношения делимости).

Одно и то же число может оказаться простым в одном кольце и составным в другом кольце. Например, число 5 просто в кольце $\mathbf{Z}$ целых чисел. А в кольце $\mathbf{Z}[i]$ целых гауссовых чисел оно является составным, так как $5 = (1 + 2i)(1 - 2i)$.

Одной из задач, вызвавших построение теории колец, была задача о разложении на простые множители в числовых кольцах. Оказалось, что в некоторых числовых кольцах дело обстоит примерно так же, как в кольце целых чисел, т. е. любое составное число разлагается на простые множители, причем это разложение по сути дела однозначно определено (смысл этих слов будет уточнен ниже), в других числовых кольцах разложение на простые множители существует, но некоторые числа могут иметь несколько существенно различных разложений, а в третьих кольцах есть числа, не имеющие разложений на простые множители.

Уточним, что мы будем понимать под словами «разложение эле-

мента a области целостности R на простые множители однозначно определено». Во-первых, мы знаем, что эти множители можно переставлять друг с другом. Но, кроме того, можно умножить один из простых множителей на какой-нибудь обратимый элемент ε, а другой — на такой обратимый элемент ε_1, что $\varepsilon\varepsilon_1 = e$. Тогда оба множителя останутся простыми, произведение же не изменится. Ясно, что полученное разложение не следует считать отличающимся от исходного. Итак, введем следующее определение:

Определение 9. Два разложения

$$a = p_1 \dots p_n$$

и

$$a = s_1 \dots s_m$$

элемента a области целостности R на простые множители по существу *одинаковы*, если они содержат одинаковое число множителей и могут быть переведены друг в друга перестановкой множителей и умножением их на обратимые элементы.

Примеры.

1. В кольце $\mathbf{Z}[i]$ целых гауссовых чисел существуют такие разложения для 5 на простые множители:

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

и

$$5 = (-2 + i)(-2 - i).$$

Эти разложения по существу одинаковы, так как второе разложение получается из первого умножением первого множителя на обратимый элемент i, а второго на обратимый элемент $-i$.

2. В кольце $\mathbf{Z}[\sqrt{3}]$ чисел вида $a + b\sqrt{3}$, $a, b \in \mathbf{Z}$, разложения

$$13 = (4 - \sqrt{3})(4 + \sqrt{3})$$

и

$$13 = (5 - 2\sqrt{3})(5 + 2\sqrt{3})$$

по существу одинаковы, так как второе разложение получается из первого следующим образом: первый множитель умножается на обратимый элемент $2 + \sqrt{3}$, второй — на обратимый элемент $2 - \sqrt{3}$, после чего множители переставляются.

3. В кольце $\mathbf{Z}[\sqrt{-3}]$ чисел вида $a + b\sqrt{-3}$, $a, b \in \mathbf{Z}$, число 4 разлагается на множители следующими способами:

$$4 = 2 \cdot 2$$

и

$$4 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

Можно доказать (мы опускаем здесь это доказательство), что числа 2, $1 + \sqrt{-3}$, $1 - \sqrt{-3}$ просты в $\mathbf{Z}[\sqrt{-3}]$, причем 2 и $1 + \sqrt{-3}$

не являются ассоциированными. Значит, в кольце $\mathbf{Z}[\sqrt{-3}]$ число 4 допускает два существенно различных разложения на простые множители.

4. Обозначим через R числовое кольцо, состоящее из конечных сумм вида $\Sigma a_r 2^r$, где a_r — целые числа и r — неотрицательные рациональные числа (при этом, например, $3 \cdot 2^{\frac{3}{2}} - 4 \cdot 2^{\frac{1}{2}}$ и $2 \cdot 2^{\frac{1}{2}}$ — один и тот же элемент кольца, поскольку $2^{\frac{3}{2}} = 2 \cdot 2^{\frac{1}{2}}$, и потому $3 \cdot 2^{\frac{3}{2}} - 4 \cdot 2^{\frac{1}{2}} = 2 \cdot 2^{\frac{1}{2}}$). Так как R — числовое кольцо, оно является областью целостности. В этом кольце для числа 2 имеем бесконечную последовательность разложений:

$$2 = 2^{\frac{1}{2}} \cdot 2^{\frac{1}{2}} = 2^{\frac{1}{2}} \cdot 2^{\frac{1}{4}} \cdot 2^{\frac{1}{4}} = 2^{\frac{1}{2}} \cdot 2^{\frac{1}{4}} \cdot 2^{\frac{1}{8}} \cdot 2^{\frac{1}{8}} = \ldots$$

Значит, число 2 не имеет в R разложения на простые множители.

Разобранные примеры показывают, что вопрос о разложении на простые множители в произвольных числовых кольцах сложнее, чем в кольце $\mathbf{Z}$ целых чисел. Причиной этого является то, что в произвольных числовых кольцах два элемента a и b могут не иметь наибольшего общего делителя, т. е. такого общего делителя a и b, который бы делился на все общие делители этих чисел. Чтобы найти выход из создавшегося положения, обобщили понятие делимости элементов. Это привело к созданию теории идеалов, которая и будет рассмотрена в следующем параграфе. С помощью теории идеалов удалось выяснить, в каких кольцах имеет место теорема о существовании и однозначности разложения на простые множители.

Вопросы для самопроверки и упражнения

1. Какими свойствами обладает отношение $a : b$ в любом кольце? Является ли оно рефлексивным? симметричным? транзитивным?

2. Какие элементы кольца называются делителями нуля? Могут ли быть делители нуля в числовых кольцах?

3. Какие элементы кольца называются обратимыми? Найдите обратимые элементы в кольцах $\mathbf{Z}[\sqrt{2}]$ чисел вида $a + b\sqrt{2}$, $a, b \in \mathbf{Z}$, и $\mathbf{Z}[-\sqrt{2}]$.

4. Может ли в кольце быть бесконечно много обратимых элементов?

5. Делится ли число $3 - 5\sqrt{2}$ на число $2 + 3\sqrt{2}$ в кольце $\mathbf{Z}[\sqrt{2}]$? а число $7 + 17\sqrt{2}$ на число $3 + 4\sqrt{2}$?

6. Какие элементы поля $\mathbf{Q}$ рациональных чисел делятся на число $\frac{7}{9}$?

7. Делится ли в кольце $\mathbf{Z}[\sqrt[3]{3}]$ число $9 + 3\sqrt[3]{3} + 2\sqrt[3]{9}$ на число $2 + \sqrt[3]{3}$?

8. Какими дополнительными свойствами обладает отношение делимости в области целостности?

9. Докажите, что если a — делитель нуля в кольце R, то все элементы вида ab, где $b \in R$, тоже являются делителями нуля.

10. Докажите, что область целостности R, состоящая из конечного числа элементов, является полем.

11. Пусть R — область целостности. Является ли областью целостности R^n? Рассмотрите произведение $(a, 0)\,(0, b)$.

12. Докажите, что кольцо $C(a, b)$ функций, непрерывных на отрезке $[a, b]$, не является областью целостности. Докажите, что если функция $y = f(x)$ из $C(a, b)$ не принимает на отрезке $[a, b]$ нулевого значения, то она обратима.

13. Функция $y = f(x)$ принадлежит кольцу $C(a, b)$ и принимает в точках a и b значения различных знаков: $f(a) f(b) < 0$. Обратима ли эта функция в $C(a, b)$?

14. Какие элементы области целостности R называются ассоциированными?

15. Докажите, что элементы $1 + 2\sqrt{5}$, $-8 + 3\sqrt{5}$ кольца $\mathbf{Z}[\sqrt{5}]$ ассоциированы.

16. Какие элементы области целостности R называются простыми, а какие составными? Является ли область целостности объединением множества простых и множества составных элементов?

17. Докажите, что числа 7 и 3 простые в кольце $\mathbf{Z}[i]$ и числа 13 и 17 составные в кольце $\mathbf{Z}[i]$.

§ 2. ИДЕАЛЫ

В этом параграфе будет изучено важное понятие идеала кольца. Как и ранее, мы ограничимся рассмотрением коммутативных и ассоциативных колец с единицей.

1. Главные идеалы. Сначала рассмотрим частный случай общего понятия идеала — главные идеалы.

Определение 1. *Главным идеалом* кольца R, порожденным элементом a этого кольца, называют множество элементов кольца R, кратных a.

Главный идеал, порожденный элементом a, обозначают (a). Таким образом, (a) — множество всех элементов, имеющих вид ra, где $r \in R$:

$$(a) = \{ra,\ r \in R\}.$$

Иными словами, $b \in (a)$ в том и только в том случае, когда $b \vdots a$.

Примеры.

1. Число 2 в кольце $\mathbf{Z}$ целых чисел порождает главный идеал (2), состоящий из четных чисел. Число -2 порождает в $\mathbf{Z}$ тот же самый идеал, что и число 2, $(-2) = (2)$. Вообще, числа n и $-n$ порождают в $\mathbf{Z}$ один и тот же главный идеал, состоящий из чисел, делящихся на n.

2. В кольце $\mathbf{Z}[x]$ многочленов с целыми коэффициентами число 2 порождает главный идеал, состоящий из всех многочленов с четными коэффициентами.

3. В кольце $\mathbf{R}[x]$ многочленов с действительными коэффициентами число 2 порождает главный идеал, совпадающий со всем кольцом $\mathbf{R}[x]$, так как любой многочлен с действительными коэффициентами после деления на 2 дает многочлен того же вида.

4. В кольце $\mathbf{R}[x]$ элемент x порождает главный идеал (x), состоящий из многочленов, делящихся на x, т. е. из многочленов, свободный член которых равен нулю.

Свойства главных идеалов:

1) *Любой элемент a кольца R принадлежит порожденному им главному идеалу*: $a \in (a)$.

В самом деле, поскольку R содержит единичный элемент e, то $a = ae \in (a)$.

2) *Главный идеал, порожденный нулевым элементом* 0, *состоит лишь из этого элемента, а главный идеал, порожденный единичным элементом e, совпадает со всем кольцом R*:

$$(0) = \{0\}, \quad (e) = R.$$

В самом деле, для всех $r \in R$ имеем $r \cdot 0 = 0$. Значит, $(0) = \{0\}$. С другой стороны, любой элемент $r \in R$ принадлежит идеалу (e), так как $r = re$. Значит, $(e) = R$.

3) *Если элементы b и c кольца R принадлежат главному идеалу (a), то и $b - c \in (a)$*:

$$b \in (a) \wedge c \in (a) \to b - c \in (a).$$

В самом деле, так как $b \in (a)$ и $c \in (a)$, то $b \vdots a$ и $c \vdots a$. А тогда $(b - c) \vdots a$ (см. п. 1 § 1), и потому $b - c \in (a)$.

4) *Если элемент b принадлежит главному идеалу (a), то все элементы вида rb, $r \in R$, также принадлежат (a)*.

В самом деле, из $b \in (a)$ следует, что $b \vdots a$. А тогда $rb \vdots a$, т. е. $rb \in (a)$.

Следующее свойство главных идеалов позволяет свести отношение делимости элементов кольца R к отношению включения соответствующих главных идеалов.

5) *Элемент a кольца R делится на элемент b того же кольца в том и только в том случае, когда $(a) \subset (b)$*:

$$a \vdots b \leftrightarrow (a) \subset (b).$$

В самом деле, пусть $a \vdots b$. Тогда в силу транзитивности отношения делимости в кольце (см. п. 1 § 1) из $x \vdots a$ следует, что $x \vdots b$. Иными словами, из $x \in (a)$ следует, что $x \in (b)$. А это и значит, что $(a) \subset (b)$.

Обратно, пусть $(a) \subset (b)$. Тогда $a \in (b)$, поскольку $a \in (a) \subset (b)$. Но из $a \in (b)$ следует, что $a \vdots b$.

Пользуясь свойством 5, можно переформулировать свойства делимости для элементов кольца на языке включения главных идеалов. Например, справедливо следующее утверждение:

6) *Ассоциированные элементы кольца R порождают один и тот же главный идеал.*

В самом деле, пусть элементы a и b кольца ассоциированы (т. е. пусть $a = b\varepsilon$, где ε — обратимый элемент в R). Тогда $x \vdots a \leftrightarrow x \vdots b$ (см. п. 2 § 1). Значит, $x \in (a) \leftrightarrow x \in (b)$, и потому $(a) = (b)$.

Частным случаем свойства 6 является следующее свойство:

7) *Главный идеал, порожденный обратимым элементом ε кольца R, совпадает с R,* $(\varepsilon) = R$.

В самом деле, по свойству 2 имеем: $(e) = R$. Так как e и ε ассоциированы, то и $(\varepsilon) = R$.

В областях целостности верно и обращение свойства 6:

8) *Если главные идеалы, порожденные элементами a и b области целостности R, совпадают,* $(a) = (b)$, *то элементы a и b ассоциированы в R.*

В самом деле, из $(a) = (b)$ следует, что $a \vdots b$ и $b \vdots a$. А тогда элементы a и b области целостности R ассоциированы (см. п. 4 § 1, теорему 3).

2. Идеалы кольца. Введем теперь общее понятие идеала кольца.

Определение 2. Подмножество I кольца R называется *идеалом* в R, если:

1) с любыми двумя элементами a и b подмножество I содержит их разность:

$$a \in I \wedge b \in I \to a - b \in I;$$

2) вместе с каждым элементом a подмножество I содержит все кратные этого элемента:

$$a \in I \wedge r \in R \to ra \in I.$$

Свойства 3 и 4 п. 1 показывают, что каждый главный идеал кольца R является идеалом этого кольца.

Так как кольцо R содержит элемент $-e$, то вместе с любым элементом b идеал I содержит и противоположный ему элемент $-b = b(-e)$. Значит, вместе с любыми двумя элементами a и b идеал I содержит их сумму:

$$a + b = a - (-b) \in I.$$

Вспоминая определение подкольца, мы видим, что *всякий идеал кольца R является подкольцом в R* (не содержащим, вообще говоря, единичного элемента e). Однако не всякое подкольцо является идеалом (см. ниже, пример 1).

Примеры.

1. Кольцо $\mathbf{Z}[x]$ многочленов с целыми коэффициентами является подкольцом в кольце $\mathbf{R}[x]$ многочленов с действительными коэф-

фициентами. Но $\mathbf{Z}[x]$ не является идеалом в $\mathbf{R}[x]$. Например, многочлен $2 + 3x$ принадлежит $\mathbf{Z}[x]$, а кратный ему многочлен

$$(2 + 3x)\left(\frac{1}{3} - \frac{x}{2}\right) = \frac{2}{3} - \frac{3}{2}x^2$$

имеет дробные коэффициенты и потому не принадлежит $\mathbf{Z}[x]$.

2. Множество I многочленов с нулевым свободным членом является идеалом в кольце $\mathbf{R}[x, y]$ многочленов от x и y с действительными коэффициентами. В самом деле, если свободные члены многочленов $\varphi(x, y)$ и $\psi(x, y)$ равны нулю, то то же самое верно и для многочлена $\varphi - \psi$, а также для любого многочлена вида $f(x, y)$, $\varphi(x, y)$, где $f(x, y) \in \mathbf{R}[x, y]$. Иными словами, если $\varphi \in I$ и $\psi \in I$, то $\varphi - \psi \in I$, а если $\varphi \in I$ и $f \in \mathbf{R}[x, y]$, то $f\varphi \in I$. Значит, I — идеал в кольце $\mathbf{R}[x, y]$. Этот идеал не является главным. В самом деле, многочлены x и y принадлежат I, но в I нет ни одного многочлена, которому были бы кратны и x и y.

Докажем теперь следующую теорему:

Теорема 1. *Пусть $a_1, \ldots, a_n$ — некоторые элементы кольца R. Тогда множество I всех элементов вида*

$$r_1a_1 + \ldots + r_na_n, \tag{1}$$

где $r_k \in R$, $k = 1, 2, \ldots, n$, образует идеал в кольце R.

Доказательство. Пусть

$$x = r_1'a_1 + \ldots + r_n'a_n$$

и

$$y = r_1''a_1 + \ldots + r_n''a_n$$

элементы множества I. Их разность можно записать так:

$$x - y = (r_1'a_1 + \ldots + r_n'a_n) - (r_1''a_1 + \ldots + r_n''a_n) =$$
$$= (r_1' - r_1'')a_1 + \ldots + (r_n' - r_n'')a_n.$$

Так как $r_k' - r_k''$, $k = 1, \ldots, n$ — элементы из R, то $x - y$ имеет вид (1), т. е. принадлежит I. Итак,

$$x \in I \wedge y \in I \to x - y \in I. \tag{2}$$

Далее, пусть $x \in I$, $x = r_1a_1 + \ldots + r_na_n$ и $r \in R$. Тогда $rx = rr_1a_1 + \ldots + rr_na_n$. Так как rr_k, $1 \leqslant k \leqslant n$ — элементы кольца R, то $rx \in I$. Итак,

$$x \in I \wedge r \in R \to rx \in I. \tag{3}$$

Из соотношений (2) и (3) следует, что I — идеал в R. Теорема доказана.

Точно так же, как теорема 1, доказывается более общее утверждение:

Теорема 1′. *Пусть A — любое подмножество кольца R. Множество I всех элементов вида*

$$r_1a_1 + \ldots + r_na_n, \tag{4}$$

где $a_1, \ldots, a_n$ — некоторые элементы из A, а $r_1, \ldots, r_n$ — некоторые элементы из R, является идеалом в R.

Идеал I, состоящий из всех элементов вида (4), называют *идеалом, порожденным множеством A*, и обозначают (A). В частности, если A состоит из одного элемента a, $A = \{a\}$, то порожденный множеством A идеал — это главный идеал, порожденный элементом a.

Поскольку кольцо R содержит единичный элемент e, то любой элемент a из A принадлежит (A). В самом деле, $a = ea$, а потому имеет вид (4). Значит, $a \in (A)$.

Понятие идеала, порожденного множеством A, можно определить иначе. Мы увидим ниже, что (A) является наименьшим идеалом в R, содержащим множество A. Сначала докажем следующую теорему:

Теорема 2. *Пересечение $I_1 \cap I_2$ двух идеалов I_1 и I_2 кольца R является идеалом того же кольца.*

Доказательство. Пусть $a \in I_1 \cap I_2$ и $b \in I_1 \cap I_2$. Тогда $a \in I_1$ и $b \in I_2$. Поскольку I_1 — идеал в R, то $a - b \in I_1$. Точно так же доказывают, что $a - b \in I_2$. А тогда $a - b \in I_1 \cap I_2$. Итак, $I_1 \cap I_2$ вместе с любыми двумя элементами содержит их разность.

Далее, пусть $a \in I_1 \cap I_2$ и $r \in R$. Тогда $a \in I_1$, и поскольку I_1 — идеал в R, то $ra \in I_1$. Точно так же доказывается, что $ra \in I_2$. А тогда $ra \in I_1 \cap I_2$. Итак, $I_1 \cap I_2$ вместе с любым элементом содержит все его кратные. Из доказанных утверждений вытекает, что $I_1 \cap I_2$ — идеал в R.

Теорема 2 обобщается на любое множество идеалов.

Теорема 2′. *Пересечение любого множества идеалов кольца R является идеалом в R.*

Пусть A — некоторое подмножество кольца R. Обозначим через $I(A)$ пересечение всех идеалов кольца R, содержащих подмножество A. По теореме 2′ это пересечение само является идеалом в R.

Так как $I(A)$ является подмножеством любого идеала, содержащего A, то $I(A)$ — наименьший из таких идеалов. Итак, мы доказали, что *наименьшим идеалом, содержащим множество A, является пересечение всех идеалов, содержащих это множество.*

Теорема 3. *Наименьший идеал $I(A)$ кольца R, содержащий подмножество A этого кольца, совпадает с идеалом (A), порожденным подмножеством A.*

Доказательство. Так как $A \subset (A)$, то (A) — один из идеалов, содержащих A, а потому $I(A) \subset (A)$ ($I(A)$ — наименьший из идеалов, содержащих A). С другой стороны, пусть

$a_1, \ldots, a_n$ — некоторые элементы множества A, а $r_1, \ldots, r_n$ — элементы кольца R. Поскольку $A \subset I(A)$, то элементы $a_1, \ldots, a_n$ принадлежат идеалу $I(A)$, а тогда и элементы $r_1a_1, \ldots, r_na_n$ принадлежат этому идеалу. Следовательно, и их сумма $r_1a_1 + \ldots + r_na_n$ принадлежит $I(A)$. Поскольку (A) состоит из сумм вида $r_1a_1 + \ldots + r_na_n$, то мы доказали, что любой элемент из (A) принадлежит $I(A)$, т. е. что $(A) \subset I(A)$. Из соотношений $I(A) \subset (A)$ и $(A) \subset I(A)$ вытекает, что $I(A) = (A)$. Теорема доказана.

3. Делимость идеалов. Мы видели (свойство 5 в п. 1), что элемент a кольца R делится на элемент $b \in R$ в том и только в том случае, когда $(a) \subset (b)$. По аналогии с этим определим отношение делимости для любых идеалов следующим образом:

Определение 3. *Идеал I_1 кольца R делится на идеал I_2* того же кольца, если $I_1 \subset I_2$.

Если I_1 делится на I_2, то пишут $I_1 \vdots I_2$ и говорят, что I_1 кратно I_2, а I_2 — делитель I_1. Таким образом,

$$I_1 \vdots I_2 \leftrightarrow I_1 \subset I_2.$$

Как и для элементов кольца, *отношение делимости идеалов транзитивно*: если $I_1 \vdots I_2$ и $I_2 \vdots I_3$, то $I_1 \vdots I_3$. В самом деле, если $I_1 \subset I_2$ и $I_2 \subset I_3$, то $I_1 \subset I_3$.

Поскольку любой идеал I содержит нулевой идеал (0) и содержится в кольце R, $(0) \subset I \subset R$, то для любого идеала I имеем $(0) \vdots I$, $I \vdots R$. Так как $R = (e)$, то получаем, что $I \vdots (e)$.

Чтобы построить теорию делимости для идеалов, введем понятие наибольшего общего делителя двух идеалов.

Определение 4. Идеал I кольца R называется *наибольшим общим делителем идеалов I_1 и I_2* этого кольца, если:

а) I является делителем I_1 и I_2;

б) I делится на любой общий делитель I_1 и I_2.

Теорема 4. *Любые два идеала I_1 и I_2 кольца R имеют наибольший общий делитель. Им является идеал, порожденный множеством $I_1 \cup I_2$, т. е. наименьший идеал, содержащий идеалы I_1 и I_2.*

Доказательство. Пусть I — наименьший идеал в R, содержащий идеалы I_1 и I_2. Так как $I_1 \subset I$ и $I_2 \subset I$, то $I_1 \vdots I$ и $I_2 \vdots I$, т. е. I — общий делитель для I_1 и I_2. С другой стороны, пусть I^* — любой общий делитель I_1 и I_2, т. е. пусть $I_1 \subset I^*$ и $I_2 \subset I^*$. Тогда I^* содержит и объединение $I_1 \cup I_2$ идеалов I_1 и I_2. Поскольку наименьшим идеалом в R, содержащим $I_1 \cup I_2$, является I, то $I \subset I^*$, т. е. $I \vdots I^*$. Итак, мы доказали, что I делится на любой общий делитель I_1 и I_2. Значит, I — наибольший общий делитель I_1 и I_2.

Наибольший общий делитель идеалов I_1 и I_2 обозначают (I_1, I_2). Из теоремы 4 вытекает, что

$$(I_1, I_2) = (I_1 \cup I_2).$$

Теорема 4 и является оправданием введения понятия идеала. В то время как два элемента a и b кольца R могут, вообще говоря, не

иметь наибольшего общего делителя, порожденные ими главные идеалы (a) и (b) всегда имеют наибольший общий делитель.

Идеал, порожденный идеалами I_1 и I_2, состоит из элементов вида $r_1x + r_2y$, где $r_1, r_2 \in R$, $x \in I_1$, $y \in I_2$ (см. п. 2). Если идеалы I_1 и I_2 главные, $I_1 = (a)$, $I_2 = (b)$, то любой элемент $x \in I_1$ имеет вид $x = s_1a$, $s_1 \in R$, а любой элемент $y \in I_2$ — вид $y = s_2b$, $s_2 \in R$. Значит, любой элемент из идеала (I_1, I_2) имеет вид $r_1s_1a + r_2s_2b$. Но r_1s_1 и r_2s_2 — элементы кольца R. Их можно обозначить $r_1s_1 = r$, $r_2s_2 = s$. Мы получили такое следствие:

Следствие. *Наибольший общий делитель главных идеалов (a) и (b) кольца R состоит из элементов вида $ra + sb$, где $r \in R$, $s \in R$.*

Примеры.

1. В кольце $\mathbf{Z}$ целых чисел наибольший общий делитель главных идеалов (24) и (40) — множество (24, 40) чисел вида $24m + 40n$, где m и n — целые числа. Любое число из этого множества делится на 8. С другой стороны, $8 = 24(-3) + 40 \cdot 2 \in (24, 40)$. Поэтому $(24, 40) = (8)$. Иными словами, наибольший общий делитель идеалов (24) и (40) является главным идеалом (8).

2. В кольце $\mathbf{Z}[\sqrt{-5}]$ наибольшим общим делителем главных идеалов (3) и $(1 + 2\sqrt{-5})$ является множество $(3, 1 + 2\sqrt{-5})$ элементов вида

$$3(a + b\sqrt{-5}) + (1 + 2\sqrt{-5})(c + d\sqrt{-5}),$$

где a, b, c, d — целые числа. Этот идеал не является главным.

3. В кольце $\mathbf{R}[x, y]$ многочленов от x и y с действительными коэффициентами наибольшим общим делителем главных идеалов (x) и (y) является идеал (x, y), состоящий из многочленов вида $x\varphi(x, y) + y\psi(x, y)$, где $\varphi(x, y)$ и $\psi(x, y)$ принадлежат $\mathbf{R}[x, y]$. В таком виде можно представить любой многочлен от x и y с нулевым членом. Таким образом (x, y) — идеал, состоящий из многочленов с нулевым свободным членом. Этот идеал не является главным.

Наименьшим общим кратным идеалов I_1 и I_2 кольца R называют такой идеал I этого кольца, что $I \vdots I_1$, $I \vdots I_2$, и любой идеал, кратный I_1 и I_2, делится на I.

Предоставим читателю показать, что наименьшим общим кратным идеалов I_1 и I_2 является их пересечение $I_1 \cap I_2$.

В заключение докажем следующую теорему об объединении возрастающей цепочки идеалов:

Теорема 5. *Объединение возрастающей цепочки*

$$I_1 \subset I_2 \subset \ldots \subset I_n \subset \ldots$$

идеалов кольца R является идеалом этого кольца.

Доказательство. Обозначим объединение всех идеалов $I_1, I_2, \ldots, I_n, \ldots$ через $I = \bigcup_{n=1}^{\infty} I_n$. Пусть $a \in I$ и $b \in I$. Тогда a

принадлежит одному из идеалов $I_1, \ldots, I_n, \ldots$, например $a \in I_k$. Точно так же найдется такое l, что $b \in I_l$. Пусть $k \leqslant l$. Тогда $I_k \subset I_l$ и $a \in I_k \subset I_l$. Значит, и a и b принадлежат идеалу I_l. А тогда и их разность $a - b$ принадлежит тому же идеалу, $a - b \in I_l$. Но $I_l \subset I$, и потому $a - b \in I$. Мы доказали, то I содержит вместе с любыми двумя элементами их разность $a - b$.

Пусть теперь $a \in I$ и $r \in R$. Найдется такое k, что $a \in I_k$, а тогда, поскольку I_k — идеал в R, и $ra \in I_k$. Но $I_k \subset I$ и, значит, $ra \in I$. Таким образом, I содержит вместе с любым элементом a его произведение на любой элемент $r \in R$. Этим доказано, что I — идеал в R.

4. Кольца главных идеалов. Наибольший общий делитель двух главных идеалов, вообще говоря, не является главным идеалом (см. примеры 2 и 3 п. 3). Полная теория делимости строится в кольцах, для которых наибольший общий делитель двух главных идеалов — главный идеал. Введем следующие определения.

Определение 5. Область целостности R (т. е. кольцо без делителей нуля) называется *кольцом главных идеалов*, если любой идеал I в R является главным (т. е. если для любого идеала I найдется такой элемент a в R, что $I = (a)$).

Определение 6. Элемент d области целостности R называется *наибольшим общим делителем элементов* a и b из R, если:

1) $a \vdots d$ и $b \vdots d$;

2) d делится на любой общий делитель δ элементов a и b.

Следующая теорема показывает, что в кольцах главных идеалов справедливы все утверждения о наибольших общих делителях, доказанные для кольца $\mathbf{Z}$ целых чисел.

Теорема 6. *Пусть R — кольцо главных идеалов. Тогда:*

а) *любые два элемента a и b этого кольца имеют хотя бы один наибольший общий делитель;*

б) *все наибольшие делители элементов a и b ассоциированы друг с другом* (т. е. отличаются друг от друга на обратимый множитель);

в) *если d — наибольший общий делитель элементов a и b, то в R найдутся такие элементы r и s, что $d = ra + sb$.*

Доказательство.

а) Пусть $a \in R$, $b \in R$. Обозначим через I наибольший общий делитель главных идеалов (a) и (b). Так как R — кольцо главных идеалов, то I — главный идеал, т. е. в R содержится такой элемент d, что $I = (d)$. Докажем, что d — наибольший общий делитель элементов a и b.

В самом деле, так как $(a) \vdots (d)$, то $(a) \subset (d)$, а потому $a \in (a) \subset (d)$, т. е. $a \vdots d$. Точно так же доказывается, что $b \vdots d$. Значит, d — общий делитель a и b. С другой стороны, если δ — общий делитель a и b, т. е. $a \vdots \delta$ и $b \vdots \delta$, то $(a) \subset (\delta)$, $(b) \subset (\delta)$. Но $(d) = I$ — наименьший идеал, содержащий (a) и (b), а потому из $(a) \subset (\delta)$, $(b) \subset (\delta)$ вытекает, что $(d) \subset (\delta)$, т. е. что $d \vdots \delta$. Значит, d делится

на любой общий делитель a и b, т. е. d — наибольший общий делитель элементов a и b.

б) Пусть d_1 и d_2 — два наибольших делителя (a) и (b). Тогда $d_1 \vdots d_2$ и $d_2 \vdots d_1$, а потому d_1 и d_2 — ассоциированные элементы в R (см. п. 1).

в) По следствию к теореме 4 любой элемент наибольшего общего делителя главных идеалов (a) и (b) имеет вид $ra + sb$. В частности, $d = ra + sb$, где $r, s \in R$. Теорема 6 доказана.

Из теоремы 6 следует, что наибольший общий делитель элементов a и b определен лишь с точностью до обратимого множителя. Поэтому запись $d = (a, b)$ мы будем понимать так: элемент d является одним из наибольших общих делителей элементов a и b.

Определение 7. Элементы a и b кольца главных идеалов R называются *взаимно простыми*, если (a, b) — обратимый элемент.

Из теоремы 6 следует, что если a и b — взаимно простые элементы в R, то найдутся такие элементы r и s кольца R, что $ra + sb = e$.

5. Разложение элементов на простые множители в кольцах главных идеалов. Мы уже говорили, что существование наибольшего общего делителя для любой пары элементов позволяет строить в кольцах главных идеалов полную теорию делимости точно так же, как она строилась в кольце $\mathbf{Z}$ целых чисел.

Теорема 7. *Если $ab \vdots c$, причем элементы a и c взаимно просты, то $b \vdots c$.*

Доказательство. По теореме 6 существуют такие элементы r и s в R, что $ar + cs = e$. Умножая обе части этого равенства на b, получим:

$$abr + bcs = b. \qquad (1)$$

В левой части равенства (1) оба слагаемых делятся на c, а потому и b делится на c, т. е. $b \vdots c$. Теорема доказана.

Одно и то же число в различных кольцах может быть либо простым, либо составным. Например, число 7 — простое в кольце целых чисел. Но в кольце $\mathbf{Z}[\sqrt{2}]$ чисел вида $a + b\sqrt{2}$, где a и b — целые числа, число 7 составное, так как $7 = (3 + \sqrt{2})(3 - \sqrt{2})$, а ни $3 + \sqrt{2}$, ни $3 - \sqrt{2}$ не являются обратимыми в $\mathbf{Z}[\sqrt{2}]$.

Теорема 8. *Если элемент a кольца главных идеалов R не делится на простой элемент p того же кольца, то a и p взаимно просты.*

Доказательство. Пусть $(a, p) = d$. Тогда $p \vdots d$, $p = dr$ и, поскольку p — простой элемент, либо d, либо r обратимы. Если r — обратимый элемент, то из $a \vdots d$ следует $a \vdots p$ вопреки предположению. Значит, обратимым элементом является d, а тогда a и p взаимно просты.

Теорема 9. *Если произведение ab делится на простой элемент p кольца главных идеалов, то $a \vdots p$ или $b \vdots p$.*

Доказательство. Если a делится на p, то теорема дока-

зана. Если a не делится на p, то a и p взаимно просты. А тогда из $ab \vdots p$ следует, что $b \vdots p$ (см. теорему 7).

С помощью метода математической индукции делаем следующий вывод: из делимости произведения $a_1 \dots a_n$ на простой элемент p вытекает делимость хотя бы одного сомножителя на p.

Теорема 10 (об обрыве цепочек). *В кольце главных идеалов R последовательность элементов $a_1, \dots, a_n, \dots$, в которой каждый элемент является собственным делителем предыдущего*, может содержать лишь конечное число элементов.*

Доказательство. Обозначим через (a_k) главный идеал, порожденный элементом a_k. Так как по условию a_{k+1} — собственный делитель a_k, то для любого k имеем $(a_k) \subset (a_{k+1})$, причем $(a_k) \neq (a_{k+1})$.

Мы получили возрастающую цепочку идеалов

$$(a_1) \subset (a_2) \subset \dots \subset (a_n) \subset \dots$$

По теореме 5 п. 3 объединение всех этих идеалов снова является идеалом. Но так как R — кольцо главных идеалов, то $I = \bigcup_{n=1}^{\infty} (a_n)$ — главный идеал, $I = (d)$.

Найдется такое k, что $d \in (a_k)$, т. е. d делится на a_k.

В таком случае a_k есть последний элемент последовательности $\{a_n\}$, так как, если бы существовал a_{n+1}, являющийся собственным делителем a_k, то мы бы имели:

$$a_k = a_{k+1} \cdot q; \tag{2}$$

$$a_{k+1} = d \cdot q_1; \tag{3}$$

$$d = a_k \cdot q_2. \tag{4}$$

Подставляя (3) и (4) в (2), мы бы имели:

$$a_k = a_k \cdot q \cdot q_1 \cdot q_2 \text{ и } e = qq_1q_2. \tag{5}$$

Но равенство (5) невозможно, так как по условию q не является обратимым элементом, ибо a_{k+1} — собственный делитель a_k. Теорема доказана.

Теорема 11. *Любой элемент a кольца главных идеалов R, отличный от нуля и обратимых элементов, либо является простым, либо представляется в виде произведения простых элементов и притом единственным способом с точностью до порядка сомножителей и до умножения их на обратимые элементы.*

Доказательство. Докажем сначала существование разложения элемента $a \in R$ на простые сомножители. Пусть $a \in R$. Если элемент a простой, то теорема доказана.

---

* То есть $a_{n+1} = a_n \cdot b$, причем b не является обратимым элементом.

Пусть a — составной элемент. Тогда $a = b_1 \cdot c_1$, где b_1 и c_1 — собственные делители a. Если оба элемента b_1 и c_1 простые, то теорема доказана. Пусть по крайней мере один из этих элементов, например b_1, составной. Тогда $b_1 = b_2 \cdot c_2$, где b_2 и c_2 — собственные делители b_1. Если b_2, c_2 и c_1 простые, то $a = b_2c_2c_1$ и теорема доказана. Если один из этих сомножителей составной, то разлагаем его на сомножители, являющиеся собственными делителями этого составного элемента. Тогда возможно одно из двух: либо через конечное число шагов мы получим разложение элемента a на простые сомножители, либо мы получим бесконечную последовательность элементов, из которых каждый последующий является собственным делителем предыдущего. Но последний вариант исключается предыдущей теоремой. Возможность разложения a на простые сомножители доказана.

Докажем единственность разложения элемента a на простые сомножители. Допустим, что

$$a = p_1p_2 \dots p_r = q_1q_2 \dots q_s, \tag{6}$$

где p_i и q_j — простые элементы. Без ограничения общности можем предположить, что $r \leqslant s$. Так как произведение $q_1 \cdot q_2 \dots q_s$ делится на простой элемент p_1, то по теореме 9 хотя бы один из сомножителей должен делиться на p_1. Изменив в случае необходимости нумерацию множителей q, можем считать, что q_1 делится на p_1. Так как q_1 — простой элемент, то $q_1 = c_1p_1$, где c_1 — обратимый элемент. Заменяя q_1 на c_1p_1, деля обе части равенства (6) на p_1 (что можно делать в области целостности), приходим к равенству:

$$p_2 \dots p_r = c_1q_2 \dots q_s. \tag{7}$$

Аналогично получим, что $q_2 = c_2p_2$. Подставляя вместо q_2 в правую часть (7) c_2p_2 и деля обе части равенства (7) на p_2, получим:

$$p_3 \dots p_r = c_1c_2q_3 \dots q_s. \tag{8}$$

Продолжая деление на элементы p_i, мы через r шагов получим в итоге равенство:

$$e = c_1 \dots c_rq_{r+1} \dots q_s. \tag{9}$$

Но равенство (9) невозможно, если $q_{r+1}, \dots, q_s$ — простые элементы, так как простые элементы не являются обратимыми. Значит $s = r$, в левой и правой частях равенства (6) мы имеем одинаковое число одинаковых простых элементов с точностью до обратимых множителей c_i. Теорема доказана.

Таким образом, однозначность разложения на простые множители произвольного элемента $a \in R$ есть необходимый признак кольца главных идеалов. И если в каком-то кольце R нарушается возможность разложения какого-либо элемента a на простые множители или однозначность такого разложения, то кольцо R заведомо не будет уже кольцом главных идеалов. Примеры подобных колец будут даны ниже.

6. Евклидовы кольца. Представляет интерес задача определения достаточного признака того, что некоторая область целостности R является кольцом главных идеалов.

Определение 8. *Евклидовым кольцом* называется область целостности R, в которой:

1) каждому элементу a, отличному от нуля, поставлено в соответствие неотрицательное целое число $N(a)$;

2) для любых $a, b \in R$, где $b \neq 0$, существуют такие $q, r \in R$, что

$$a = bq + r, \tag{1}$$

причем либо $r = 0$, либо $N(r) < N(b)$.

Иными словами, в евклидовых кольцах есть аналог операции деления с остатком.

Простейшими примерами евклидовых колец являются кольцо $\mathbf{Z}$ целых чисел и кольцо $\mathbf{R}[x]$ многочленов от одного переменного x с действительными коэффициентами. В кольце $\mathbf{Z}$ надо положить $N(a) = |a|$, в кольце $\mathbf{R}[x]$ за $N(\varphi(x))$ примем степень многочлена $\varphi(x)$.

Теорема 12. *Любое евклидово кольцо R является кольцом главных идеалов.*

Доказательство. Пусть I — ненулевой идеал кольца R. Выберем в I элемент a, для которого $N(a)$ принимает наименьшее положительное значение (такой элемент существует, так как все значения $N(a)$ — целые неотрицательные числа). Тогда все элементы из I можно представить в виде $b = qa$, $q \in R$. В самом деле, в противном случае мы имели бы $b = qa + r$, где $0 < N(r) < N(a)$. При этом поскольку $b \in I$ и $qa \in I$, то $r = b - qa \in I$. Мы нашли в I элемент r, такой, что $0 < N(r) < N(a)$, а это противоречит выбору a. Значит, b можно представить в виде $b = aq$. Итак, $I = \{aq\}$, где q пробегает кольцо R. Итак, идеал I является главным. Теорема доказана.

Из теоремы 12 следует, что кольца $\mathbf{Z}$ и $\mathbf{R}[x]$ являются кольцами главных идеалов.

Примеры.

1. Докажем, что кольцо $\mathbf{Z}[i]$ целых гауссовых чисел евклидово. Это кольцо является областью целостности, так как оно — подкольцо поля $\mathbf{C}$ комплексных чисел, и потому $zw = 0$ лишь в случае, когда $z = 0$ или $w = 0$.

Положим при $z = a + bi$

$$N(z) = (a + bi)(a - bi) = a^2 + b^2.$$

Ясно, что $N(z) \geqslant 0$ и

$$N(zw) = N(z) \cdot N(w).$$

Докажем, что $N(z)$ удовлетворяет и второму условию определения. Пусть $z = a + bi \in \mathbf{Z}[i]$ и

$$w = c + di \in \mathbf{Z}[i], \quad w \neq 0.$$

Докажем, что существует такое число $q \in \mathbf{Z}[i]$, что $N(z - qw) < N(w)$. Сначала разделим z на w:

$$\frac{z}{w} = \frac{a+bi}{c+di} = \alpha + \beta i.$$

Обозначим через x и y целые числа, ближайшие к числам α и β, т. е. такие, что $|\alpha - x| \leqslant \frac{1}{2}$ и $|\beta - y| \leqslant \frac{1}{2}$, и положим $q = x + iy$.

Разность $\frac{z}{w} - q$ обозначим через t:

$$t = (\alpha + \beta i) - (x + iy) = (\alpha - x) + (\beta - y)\, i.$$

По выбору x и y имеем:

$$N(t) = (\alpha - x)^2 + (\beta - y)^2 \leqslant \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}.$$

Так как $z - qw = \left(\frac{z}{w} - q\right) w = tw$, то

$$N(z - qw) = N(tw) = N(t) \cdot N(w) \leqslant \frac{1}{2} N(w).$$

Значит, $z = qw + r$, где

$$N(r) = N(z - qw) \leqslant \frac{1}{2} N(w) < N(w).$$

Значит, $\mathbf{Z}[i]$ — евклидово кольцо (а тем самым и кольцо главных идеалов).

Аналогично доказывается, что кольцо $\mathbf{Z}[\sqrt{2}]$, состоящее из чисел вида $a + b\sqrt{2}$, $a, b \in \mathbf{Z}$, — евклидово.

2. Кольцо $\mathbf{R}[x, y]$ многочленов от x и y с действительными коэффициентами не является кольцом главных идеалов (см. пример 3 п. 3). Значит, оно не является и евклидовым.

3. Кольцо $\mathbf{Z}[\sqrt{-19}]$ неевклидово, но является кольцом главных идеалов.

Вопросы для самопроверки и упражнения

1. Что такое главный идеал? Какой главный идеал порождается в кольце $\mathbf{Z}$ числом 7?

2. В каком случае элементы a и b кольца R порождают один и тот же главный идеал?

3. В каком случае главный идеал, порожденный элементом a, совпадает со всем кольцом R? Какой главный идеал порождает элемент $2 - \sqrt{5}$ в кольце $\mathbf{Z}[\sqrt{5}]$?

4. Как выразить на «языке идеалов» утверждение: элемент a делится на элемент b?

5. Всякое ли подкольцо является идеалом? Какому дополнительному условию оно должно удовлетворять?

6. Является ли идеалом в $\mathbf{Z}[x]$ подкольцо, состоящее из многочленов с делящимся на 3 свободным членом?

7. Является ли подкольцом в $\mathbf{Z}[x]$ множество многочленов с положительным свободным членом?

8. В кольце $\mathbf{Z}[\sqrt{3}]$ элемент $2+\sqrt{3}$ обратим (так как $(2+\sqrt{3})(2-\sqrt{3})=1$). Какой идеал порождает в $\mathbf{Z}[\sqrt{3}]$ этот элемент?

9. Что означает утверждение «идеал I_1 делится на идеал I_2»?

10. Найдите в кольце $\mathbf{Z}$ идеалы, порожденные следующими множествами элементов: $\{2; 5\}$, $\{4; 6\}$, $\{6; 15\}$. Найдите пересечение этих трех идеалов.

11. Найдите идеал в кольце $\mathbf{Z}[x]$ многочленов с целыми коэффициентами, порожденный элементами x^2 и 4.

12. Какой идеал называется наибольшим общим делителем идеалов I_1 и I_2? Какими свойствами он обладает?

13. Какие идеалы называют взаимно простыми?

14. Дайте определение кольца главных идеалов.

15. Какие известные вам кольца являются кольцами главных идеалов?

16. В каких кольцах два элемента заведомо имеют наибольший общий делитель?

17. В каком виде можно представить наибольший общий делитель двух элементов в кольце главных идеалов?

18. Докажите, что кольцо $\mathbf{Z}[\sqrt{2}]$ является кольцом главных идеалов.

19. Найдите наибольший общий делитель чисел $7+\sqrt{2}$ и $-5-5\sqrt{2}$ в кольце $\mathbf{Z}[\sqrt{2}]$ (примените алгоритм Евклида). Выразите НОД $[7+\sqrt{2}, -5-5\sqrt{2}]$ линейным образом через $7+\sqrt{2}$ и $-5-5\sqrt{2}$.

20. В каких кольцах заведомо справедлива теорема об однозначности разложения на простые множители? С точностью до каких преобразований имеет место эта однозначность?

21. В кольце $\mathbf{Z}[\sqrt{2}]$ число 5 имеет такие разложения на множители:

$$5 = 5 \cdot 1 = (3+2\sqrt{2})(15-10\sqrt{2}).$$

Следует ли отсюда, что в $\mathbf{Z}[\sqrt{2}]$ неверна теорема об однозначности разложения на простые множители?

§ 3. ГОМОМОРФИЗМЫ КОЛЕЦ

1. Гомоморфизм колец. Пусть M и M' — множества, в которых определены две бинарные операции. Мы обозначим эти операции в обоих множествах так: $a+b$ и ab (соответственно $a'+b'$ и $a'b'$).

Определение 1. *Гомоморфизмом* множества M в множе-

ство M' называется такое отображение $f\colon a \to a'$ множества M в M', что $f(a+b) = f(a) + f(b)$ и $f(ab) = f(a)\,f(b)$.

Иными словами, отображение $a \to f(a)$ является гомоморфизмом, если для любых двух элементов a и b из M следующие действия дают одинаковые результаты:

а) сложение (соответственно умножение) этих элементов, а затем отображение результата в M';

б) отображение этих элементов a и b в M', а затем сложение (соответственно умножение) их образов.

Если образом множества M при гомоморфизме является все множество M', то говорят о гомоморфном отображении M на M'.

Определение 2. Гомоморфное взаимно-однозначное отображение M на M' называют *изоморфизмом* M на M'.

Примеры.

1. Пусть $\mathbf{R}[x]$ — кольцо многочленов с действительными коэффициентами, а $\mathbf{R}$ — поле действительных чисел. Поставим в соответствие каждому многочлену его свободный член:

$$\varphi(x) = a_0x^n + \ldots + a_n \to a_n. \tag{1}$$

Известно, что при сложении многочленов их свободные члены складываются, а при умножении многочленов свободные члены перемножаются. Поэтому отображение (1) является гомоморфизмом: если $\varphi(x) \to a$ и $\psi(x) \to b$, то

$$\varphi(x) + \psi(x) \to a + b \text{ и } \varphi(x)\,\psi(x) \to ab.$$

2. Обозначим через $\mathbf{Z}_2$ множество, состоящее из двух элементов $Ч$ и $Н$. Операции сложения и умножения в этом множестве определим так:

$$Ч + Ч = Н + Н = Ч,\ Ч + Н = Н + Ч = Н,$$
$$Ч \cdot Ч = Ч \cdot Н = Н \cdot Ч = Ч,\ Н \cdot Н = Н.$$

Отобразим кольцо $\mathbf{Z}$ целых чисел на множество $\mathbf{Z}_2$ по следующему правилу: если a — четное целое число, то $f(a) = Ч$, а если a — нечетное целое число, то $f(a) = Н$ (теперь ясен смысл обозначений $Ч$ и $Н$). Покажем, что это отображение является гомоморфизмом $\mathbf{Z}$ на $\mathbf{Z}_2$. Пусть числа a и b четные. Тогда $f(a) = Ч$ и $f(b) = Ч$. Поскольку сумма четных чисел четна, то и $f(a+b) = Ч$. Так как $Ч + Ч = Ч$, то получаем, что

$$f(a) + f(b) = f(a+b) \tag{2}$$

(и левая и правая части этого равенства равны $Ч$). Точно так же доказывается, что равенство (2) верно и в случае, когда a — четное число, а b — нечетное число. В этом случае $f(a) = Ч$, $f(b) = Н$ и $f(a+b) = Н$, поскольку $Н$ нечетно. Равенство (2) верно, поскольку $Ч + Н = Н$. Предоставляем читателю разобрать случаи, когда a нечетно, а b четно и когда a и b — нечетные числа.

Далее, для любых целых чисел a и b верно равенство

$$f(a) \cdot f(b) = f(a,\ b). \tag{3}$$

Если a и b — четные числа, то ab тоже четное число, и потому $f(ab) = Ч$. Равенство (3) верно, поскольку $Ч \cdot Ч = Ч$. Предоставляем читателю разобрать остальные случаи.

Легко проверить, что множество $\mathbf{Z}_2$ является кольцом. Нулем этого кольца является $Ч$, а единицей — $Н$. Можно было бы обозначить элементы этого кольца не $Ч$ и $Н$, а $\overline{0}$ и $\overline{1}$. Таблицы сложения и умножения выглядели бы тогда так:

$$\overline{0} + \overline{0} = \overline{1} + \overline{1} = \overline{0},\ \overline{0} + \overline{1} = \overline{1} + \overline{0} = \overline{1},$$
$$\overline{0} \cdot \overline{0} = \overline{0} \cdot \overline{1} = \overline{1} \cdot \overline{0} = \overline{0},\ \overline{1} \cdot \overline{1} = \overline{1}.$$

3. Пусть $\mathbf{C}$ — поле комплексных чисел. Поставим в соответствие каждому числу $z = x + iy$ сопряженное с ним число $z = x - iy$. Так как $\overline{z + w} = \overline{z} + \overline{w}$ и $\overline{zw} = \overline{z} \cdot \overline{w}$, то отображение $z \to \overline{z}$ является изоморфным отображением $\mathbf{C}$ на себя. В математике изоморфные отображения множества M на себя называют *автоморфизмами*.

4. Определим отображение кольца $\mathbf{R}[x]$ многочленов с действительными коэффициентами на поле $\mathbf{C}$ комплексных чисел по следующему правилу: многочлен $f(x)$ делят на $x^2 + 1$; если остаток от деления равен $a + bx$, то многочлену $f(x)$ ставят в соответствие комплексное число $a + bi$. Проверка, детали которой мы опускаем, показывает, что это отображение является гомоморфизмом $\mathbf{R}[x]$ на $\mathbf{C}$.

5. Обозначим через $\mathbf{Z}[\sqrt[3]{2}]$ множество чисел вида $a + b\sqrt[3]{2} + c\sqrt[3]{4}$, где a, b, c — целые числа. Это множество является кольцом. Можно показать, что отображение

$$a + b\sqrt[3]{2} + c\sqrt[3]{4} \to a + b\sqrt[3]{4} + 2c\sqrt[3]{2}$$

является автоморфизмом кольца $\mathbf{Z}[\sqrt[3]{2}]$.

Нам понадобится в дальнейшем следующая теорема:

Теорема 1. *Пусть M и M' — множества с бинарными операциями сложения и умножения. Если существует гомоморфное отображение f множества M на M' и если M является кольцом, то и M' — кольцо.*

Доказательство. Мы покажем, что сложение в M' коммутативно. Пусть a' и b' — два элемента из M'. Так как f отображает M на все множество M', найдутся такие элементы a и b в M, что $f(a) = a'$, $f(b) = b'$. Но M является по условию кольцом, и потому сложение в M коммутативно. Поэтому $a + b = b + a$. Но тогда и $f(a + b) = f(b + a)$. Поскольку отображение f гомоморфно, то

$$f(a + b) = f(a) + f(b) = a' + b'$$

и

$$f(b + a) = f(b) + f(a) = b' + a'.$$

Значит, $a' + b' = b' + a'$.

Совершенно так же доказывается ассоциативность сложения в M', а также дистрибутивность умножения в M' относительно сложения. Нулевым элементом в M' является образ нулевого элемента кольца M: $0' = f(0)$. Если $f(a) = a'$, то противоположным к a' является образ элемента $-a$: $-f(a) = f(-a)$. Мы опускаем несложные доказательства этих утверждений.

Итак, в M' выполняются все аксиомы кольца, а потому M' — кольцо.

Замечания.

1) Если M — ассоциативное кольцо, то и гомоморфный образ M' — ассоциативное кольцо.

2) Если кольцо M коммутативно, то и M' — коммутативное кольцо.

3) Если в кольце M есть единица e, то и в M' есть единица — образ e.

4) Гомоморфный образ области целостности может содержать делители нуля, т. е. не быть областью целостности. Примером является гомоморфное отображение $\mathbf{Z} \to \mathbf{Z}_n$ при составном n: при составном n в $\mathbf{Z}_n$ есть делители нуля, а в $\mathbf{Z}$ их нет.

2. Ядро гомоморфизма. С каждым гомоморфизмом f кольца R в кольцо R' связано подмножество в R, которое состоит из всех элементов $a \in R$, переходящих при этом гомоморфизме в нуль кольца R'.

Определение 3. Множество I элементов кольца R, переходящих при гомоморфизме $f: R \to R'$ в нуль кольца R', называется *ядром гомоморфизма* f.

Теорема 2. *Если множество I кольца R является ядром гомоморфизма $f: R \to R'$ кольца R в кольцо R', то I — идеал в R.*

Доказательство. Пусть a и b принадлежат множеству I. Тогда $f(a) = 0$, $f(b) = 0$, а потому

$$f(a - b) = f(a) - f(b) = 0 - 0 = 0.$$

Значит, и $a - b \in I$. Далее, пусть $a \in I$ и $r \in R$. Тогда $f(a) = 0$ и $f(ar) = f(a) \cdot f(r) = 0 \cdot f(r) = 0$. Значит, $ar \in I$. Итак, множество I вместе с любыми двумя элементами a и b содержит их разность, а вместе с любым элементом a — произведение ar этого элемента на любой элемент r кольца R. Это и означает, что I — идеал кольца R.

В п. 4 будет доказана теорема, обратная теореме 2, т. е. будет показано, что любой идеал является ядром некоторого гомоморфизма кольца R. Эти две теоремы и дают исчерпывающее описание всех ядер гомоморфизмов колец.

Примеры.

1. Элемент 0 образует идеал в кольце R (нулевой идеал). Он является ядром автоморфизма кольца R, при котором каждый

элемент переходит сам в себя: $f(x) = x$. Такой автоморфизм называют *тождественным*.

2. В п. 1 мы рассмотрели гомоморфное отображение кольца $\mathbf{R}[x]$ на поле $\mathbf{R}$, при котором каждому многочлену ставится в соответствие его свободный член. Ясно, что при этом отображении в нуль переходят все многочлены с нулевым свободным членом. Они образуют идеал (x) в $\mathbf{R}[x]$.

3. В п. 1 мы рассмотрели гомоморфное отображение кольца $\mathbf{Z}$ на кольцо $\mathbf{Z}_2$, состоящее из элементов $Ч$ и $Н$. Нулем кольца $\mathbf{Z}_2$ является элемент $Ч$. В этот элемент переходят четные числа. Множество четных чисел является идеалом в $\mathbf{Z}$.

4. Обозначим через $C(a, b)$ кольцо функций, непрерывных на отрезке $[a, b]$. Пусть c — точка этого отрезка. Отображение $\varphi(x) \to \varphi(c)$ является гомоморфизмом кольца $C(a, b)$ в поле действительных чисел. Ядро $I(c)$ этого гомоморфизма (т. е. множество функций, переходящих при этом гомоморфизме в нуль) состоит из таких функций $\varphi(x)$, что $\varphi(c) = 0$. В п. 2 § 2 было показано, что $I(c)$ — идеал в $C(a, b)$.

3. Сравнения и классы вычетов по идеалу. Пусть I — идеал кольца R. Введем в кольцо R бинарное отношение

$$a \equiv b \pmod{I}, \tag{1}$$

означающее, что $a - b \in I$ (читается: «a сравнимо с b по модулю идеала I»).

Теорема 3. *Для любого идеала I в кольце R отношение «a сравнимо с b по модулю идеала I» является эквивалентностью.*

Доказательство. Нам надо доказать, что для любого идеала $I \subset R$ отношение $a \equiv b \pmod{I}$ рефлексивно, симметрично и транзитивно.

а) Для любого элемента $a \in R$ имеем $a - a = 0 \in I$, а потому $a \equiv a \pmod{I}$. Значит, отношение (1) рефлексивно.

б) Пусть $a \equiv b \pmod{I}$. Это значит, что $a - b \in I$. Но тогда и $b - a = -(a - b) \in I$, а потому $b \equiv a \pmod{I}$. Значит, из $a \equiv b \pmod{I}$ вытекает $b \equiv a \pmod{I}$, и потому отношение (1) симметрично.

в) Наконец, пусть $a \equiv b \pmod{I}$ и $b \equiv c \pmod{I}$. Тогда $a - b \in I$ и $b - c \in I$, а значит,

$$a - c = (a - b) + (b - c) \in I.$$

Но тогда $a \equiv c \pmod{I}$. Итак, из $a \equiv b \pmod{I}$ и $b \equiv c \pmod{I}$ следует, что $a \equiv c \pmod{I}$. Значит, отношение (1) транзитивно. Теорема доказана.

Замечание. По сути дела, мы использовали в доказательстве теоремы 3 лишь тот факт, что I является подгруппой аддитивной группы кольца R. Поэтому отношение $a \equiv b \pmod{I}$ можно ввести для любой коммутативной группы R и ее подгруппы I.

Любое отношение эквивалентности в множестве M определяет разбиение этого множества на классы эквивалентности. При этом

каждый класс состоит из попарно эквивалентных элементов. Поэтому из теоремы 3 вытекает такое следствие:

Следствие. *Каждый идеал I в кольце R определяет разбиение этого кольца на классы эквивалентности. Два элемента попадают в один класс в том и только в том случае, когда $a \equiv b \pmod I$, т. е. когда $a - b \in I$.*

Определение 4. Классы эквивалентности для бинарного отношения $a \equiv b \pmod I$ называются *классами вычетов по идеалу I.*

Таким образом, любые два элемента a и b, принадлежащие одному и тому же классу вычетов по идеалу I, сравнимы по модулю I:

$$a \equiv b \pmod I.$$

Из определения отношения $a \equiv b \pmod I$ следует, что если $j \in I$, то $a + j \equiv a \pmod I$. В самом деле, $(a + j) - a = j \in I$. Обратно, если $a \equiv b \pmod I$, то $b - a \in I$. Обозначим $b - a = j$. Тогда $b = a + j$, где $j \in I$.

Итак, *если A — класс вычетов по идеалу I и $a \in A$, то A состоит из всех элементов вида $a + j$, где $j \in I$.* Поэтому часто класс вычетов по идеалу I, содержащий элемент a, обозначают $a + I$. В частности, сам идеал I является одним из классов вычетов, а именно классом $0 + I$.

В качестве элемента a может быть выбран любой элемент класса вычетов A. Иными словами, если $a \equiv b \pmod I$, то $a + I = b + I$.

Примеры.

1. Множество $Ч$ четных чисел образует идеал в кольце $\mathbf{Z}$ целых чисел. Отношение $a \equiv b \pmod Ч$ означает, что разность чисел a и b четна, т. е. что либо оба числа четны, либо оба нечетны. Таким образом, классы вычетов по $Ч$ состоят из чисел одинаковой четности. Все кольцо $\mathbf{Z}$ распадается на два класса вычетов: один состоит из четных чисел, второй — из нечетных.

2. Многочлены с нулевым свободным членом образуют идеал I в кольце многочленов $\mathbf{R}[x]$. Отношение $\varphi(x) \equiv \psi(x) \pmod I$ означает, что $\varphi(x) - \psi(x) \in I$, т. е. что свободный член разности $\varphi(x) - \psi(x)$ равен нулю. Но тогда свободные члены многочленов $\varphi(x)$ и $\psi(x)$ равны друг другу. Обратно, если свободные члены у $\varphi(x)$ и $\psi(x)$ одинаковы, то свободный член разности $\varphi(x) - \psi(x)$ равен нулю, а потому $\varphi(x) - \psi(x) \in I$.

Итак, классы вычетов кольца $\mathbf{R}[x]$ по идеалу I состоят из многочленов $\varphi(x)$, имеющих одинаковые свободные члены. Каждый из этих классов можно задать значением свободного члена.

Докажем следующую теорему об операциях над сравнениями по идеалу:

Теорема 4. *Пусть I — идеал в кольце R и пусть*

$$a_1 \equiv a_2 \pmod I, \quad b_1 \equiv b_2 \pmod I$$

Тогда

$$a_1 + b_1 \equiv a_2 + b_2 \pmod I \tag{2}$$

и

$$a_1 \cdot b_1 \equiv a_2 b_2 \pmod I. \tag{3}$$

Доказательство. Так как $a_1 \equiv a_2 \pmod{I}$, то $a_1 = a_2 + j_1$, где $j_1 \in I$. Точно так же получаем, что $b_1 = b_2 + j_2$, где $j_2 \in I$. Но тогда

$$a_1 + b_1 = (a_2 + j_1) + (b_2 + j_2) = a_2 + b_2 + (j_1 + j_2).$$

Так как $j_1 \in I$ и $j_2 \in I$, то по определению идеала и $j_1 + j_2 \in I$. А это значит, что $a_1 + b_1 \equiv a_2 + b_2 \pmod{I}$. Соотношение (2) доказано.

Теперь докажем соотношение (3). Так как

$$a_1 = a_2 + j_1,\ b_1 = b_2 + j_2,\ \text{где } j_1,\ j_2 \in I,$$

то

$$a_1 \cdot b_1 = (a_2 + j_1) \cdot (b_2 + j_2) = a_2b_2 + a_2j_2 + j_1b_2 + j_1j_2.$$

Но по определению идеала из $j_1 \in I$, $j_2 \in I$ следует, что $a_2j_2 \in I$, $j_1b_2 \in I$, $j_1\ j_2 \in I$, а тогда и $a_2j_2 + j_1b_2 + j_1j_2 \in I$. Значит,

$$a_1b_1 - a_2b_2 = a_2j_2 + j_1b_2 + j_1j_2 \in I,$$

и потому $a_1b_1 \equiv a_2b_2 \pmod{I}$. Теорема доказана.

4. Фактор-кольцо. Теорема о гомоморфизмах. Пусть R — кольцо и I — идеал этого кольца. Образуем новое множество R/I, элементами которого являются классы вычетов кольца R по идеалу I. Возьмем классы вычетов $A = a + I$ и $B = b + I$ и назовем их *суммой* класс вычетов $A + B = a + b + I$, а *произведением* — класс вычетов $A \cdot B = ab + I$. Иными словами, для того чтобы сложить (соответственно умножить) два класса вычетов A и B, мы выбираем в классе A элемент a, в классе B элемент b и складываем (соответственно умножаем) эти элементы. Класс вычетов, которому принадлежит сумма (соответственно произведение) a и b и является суммой (соответственно произведением) классов вычетов A и B.

Нам надо показать теперь, что данное выше определение суммы и произведения классов вычетов позволяет находить по заданным двум классам однозначно определенные классы $A + B$ и AB, т. е. что результат операций над классами не зависит от выбора элементов a и b в этих классах. Пусть в классе вычетов A выбран элемент a_1, а в классе B — элемент b_1. Так как a и a_1 лежат в одном классе вычетов A, то $a \equiv a_1 \pmod{I}$. Точно так же получаем, что $b \equiv b_1 \pmod{I}$. Но тогда по теореме 4 п. 3 имеем:

$$a + b = a_1 + b_1 \pmod{I},$$

т. е.

$$a + b + I = a_1 + b_1 + I.$$

Это равенство и показывает, что сумма $A + B$ классов вычетов не зависит от того, какие элементы a и b мы выбираем в этих классах.

Точно так же доказывается, что произведение AB классов вычетов не зависит от выбора элементов a и b в этих классах.

Формулы, определяющие сложение и умножение классов вычетов, можно записать следующим образом:

$$(a + I) + (b + I) = a + b + I \tag{1}$$

и

$$(a + I)(b + I) = ab + I. \tag{2}$$

Итак, в множестве R/I классов вычетов определены операции сложения и умножения. Зададим теперь отображение f кольца R на множество R/I следующим образом: каждому элементу $a \in R$ ставится в соответствие содержащий его класс вычетов. Иными словами, мы полагаем:

$$f(a) = a + I.$$

Теорема 5. *Пусть I — идеал в кольце R. Отображение f: $a \to a + I$, ставящее в соответствие каждому элементу $a \in R$ содержащий его класс вычетов $A = a + I$, является гомоморфным отображением R на R/I.*

Доказательство. Если $f(a) = A$ и $f(b) = B$, то $A = a + I$ и $B = b + I$. А тогда по определению суммы классов вычетов $A + B = a + b + I$, и потому $f(a + b) = A + B = f(a) + f(b)$. Мы доказали, что

$$f(a) + f(b) = f(a + b).$$

Точно так же доказывается, что

$$f(a) \cdot f(b) = f(a \cdot b).$$

А это и значит, что отображение f является гомоморфным отображением R в R/I. При этом f — отображение R на R/I, поскольку любой класс вычетов содержит хотя бы один элемент $a \in R$ и потому $f(a) = A$. Теорема доказана.

Мы доказали, что f — гомоморфное отображение R на R/I. Из теоремы 1 вытекает, что R/I тоже является кольцом. Кольцо R/I называют *фактор-кольцом* кольца R по идеалу I.

Так как $0 \in I$, то нулем кольца R/I является класс вычетов $0 + I$, т. е. сам идеал I. Элементы этого идеала и только они переходят при гомоморфизме в нуль кольца R/I. Значит, I является ядром гомоморфизма R. Мы доказали следующую теорему:

Теорема 6. *Любой идеал I кольца R является ядром гомоморфизма при отображении кольца R на фактор-кольцо R/I.*

Выше (см. с. 89) было показано, что ядро любого гомоморфизма кольца R на кольцо R' является идеалом. Из этого утверждения и теоремы 6 вытекает следующее утверждение:

Теорема 7. *Для того чтобы подмножество I кольца R было ядром гомоморфизма этого кольца на некоторое кольцо R', необходимо и достаточно, чтобы I было идеалом кольца R.*

Следствие. *Все кольца, гомоморфные кольцу R, изоморфны фактор-кольцам этого кольца.*

Примеры.

1. Пусть I — идеал кольца $\mathbf{Z}$ целых чисел, состоящий из четных чисел. Мы видели, что $\mathbf{Z}$ распадается на два класса вычетов — четных чисел и нечетных чисел. Первый класс вычетов обозначим $Ч$, а второй — $Н$. Отображение, ставящее в соответствие каждому четному числу x класс $Ч$, а каждому нечетному — класс $Н$, является гомоморфным отображением $\mathbf{Z}$ на $\mathbf{Z}/I$. Мы рассмотрели это отображение в п. 1.

2. Пусть I — идеал кольца $\mathbf{R}[x]$, состоящий из многочленов с нулевым свободным членом. Мы видели в п. 3, что каждый класс вычетов по I состоит из многочленов с одним и тем же свободным членом и потому однозначно определяется значением свободного члена. Отображение, ставящее в соответствие каждому многочлену $\varphi(x)$ его свободный член, задает гомоморфное отображение $\mathbf{R}[x]$ на $\mathbf{R}[x]/I$, при котором каждому многочлену сопоставляется множество всех многочленов с тем же свободным членом.

5. Поле отношений. Пусть R — ненулевое подкольцо поля S. Тогда R — область целостности, т. е. коммутативное ассоциативное кольцо без делителей нуля. Это вытекает из того, что S коммутативно, ассоциативно и не имеет делителя нуля.

Поставим в соответствие каждой паре элементов (a, b) из R, такой, что $b \neq 0$, элемент $a \cdot b^{-1}$ поля S. По аналогии со школьной арифметикой будем записывать этот элемент в виде дроби $\frac{a}{b}$ и называть $\frac{a}{b}$ *дробью с числителем* a *и знаменателем* b.

Пусть S_1 — некоторое подполе в S, содержащее кольцо R, $R \subset S_1 \subset S$. Поле S_1 вместе с любыми двумя элементами a и b, $b \neq 0$, содержит элемент ab^{-1}. В частности, поскольку $R \subset S_1$, то S_1 содержит все дроби $\frac{a}{b}$, где $a \in R$, $b \in R$, $b \neq 0$.

Итак, нами доказана следующая лемма:

Лемма 1. *Любое подполе* S_1 *поля* S, *содержащее ненулевое подкольцо* R, *содержит все дроби* $\frac{a}{b}$, *где* $a \in R$, $b \in R$, $b \neq 0$ (точнее говоря, все элементы x из S такие, что $x = \frac{a}{b}$).

Обозначим через P множество всех элементов поля S, представимых в виде $x = \frac{a}{b}$. Мы докажем сейчас, что P — подполе в S. Так как любое подполе, содержащее R, содержит и P, то отсюда будет следовать, что P — наименьшее подполе в S, содержащее кольцо R. Это поле называют *полем отношений кольца* R *в поле* S.

Пример. Если $S = \mathbf{R}$ и $R = \mathbf{Z}$, то поле отношений — это поле $\mathbf{Q}$ всех рациональных чисел.

Лемма 2. *Пусть* R — *ненулевое подкольцо поля* S. *Подмно-*

жество P в S, состоящее из элементов, представимых в виде дробей $x = \frac{a}{b}$, $a \in R$, $b \in R$, $b \neq 0$, является полем.

Доказательство. Пусть $x = \frac{a}{b}$, $y = \frac{c}{d}$, причем $b \neq 0$, $d \neq 0$. Покажем, что тогда

$$x \pm y = \frac{ad \pm bc}{bd}$$

и

$$x \cdot y = \frac{ac}{bd}.$$

Если $x \neq 0$, то $x^{-1} = \frac{b}{a}$.

Иными словами, в S справедливы следующие правила действий над дробями:

$$\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd} \quad (b,\ d \neq 0), \tag{1}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \quad (b,\ d \neq 0), \tag{2}$$

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a} \quad (a,\ b \neq 0). \tag{3}$$

В самом деле,

$$\frac{ad \pm bc}{bd} = (ad \pm bc) \cdot (bd)^{-1} = ad\,(b^{-1} \cdot d^{-1}) \pm bc\,(b^{-1} \cdot d^{-1}).$$

Так как $d \cdot d^{-1} = b \cdot b^{-1} = e$, то

$$\frac{ad \pm bc}{bd} = a \cdot b^{-1} \pm cd^{-1} = \frac{a}{b} \pm \frac{c}{d} = x \pm y.$$

Равенство (1) доказано.

Равенство (2) вытекает из того, что

$$\frac{ac}{bd} = (ac)\,(b \cdot d)^{-1} = acb^{-1} \cdot d^{-1} = ab^{-1} \cdot cd^{-1} = \frac{a}{b} \cdot \frac{c}{d}.$$

Пусть $x = \frac{a}{b} \neq 0$. Тогда $a \neq 0$, и потому $\frac{b}{a}$ тоже дробь. При этом $\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = ab\,(ab)^{-1} = e$. Итак, операции сложения, умножения, а также деления на отличный от нуля элемент не выводят за пределы множества P, и потому P — поле.

Выясним теперь, при каком условии дроби $\frac{a}{b}$ и $\frac{c}{d}$ выражают один и тот же элемент поля P, т. е. при каком условии $\frac{a}{b} = \frac{c}{d}$. Для этого заметим, что

$$\frac{a}{b} = a \cdot b^{-1} = ad\,(b^{-1} \cdot d^{-1}) = \frac{ad}{bd}$$

и

$$\frac{c}{d} = c \cdot d^{-1} = bc\,(b^{-1} \cdot d^{-1}) = \frac{bc}{bd},$$

а потому равенство $\frac{a}{b} = \frac{c}{d}$ имеет место тогда и только тогда, когда

$$\frac{ad}{bd} = \frac{bc}{bd}.$$

Но это равенство равносильно равенству $ad = bc$. Итак, $\frac{a}{b} = \frac{c}{d}$ в том и только том случае, когда $ad = bc$ ($b \neq 0$, $d \neq 0$). В частности, для любого $c \in R$, $c \neq 0$ и любой дроби $\frac{a}{b}$ имеем $\frac{a}{b} = \frac{ac}{bc}$ (так как $a \cdot bc = b \cdot ac$).

Итак, мы доказали следующую теорему:

Теорема 8. *Если R — подкольцо поля S, то наименьшее подполе в S, содержащее R, состоит из дробей $\frac{a}{b}$, $a \in R$, $b \in R$, $b \neq 0$. Дроби $\frac{a}{b}$ и $\frac{c}{d}$ равны в том и только том случае, когда $ad = bc$.*

В теореме 8 мы предполагали, что кольцо R является подкольцом поля S. Это условие на самом деле излишне. Мы докажем сейчас, что любая область целостности является подкольцом некоторого поля.

Теорема 9. *Любая область целостности R с единицей является подкольцом некоторого поля P*.*

Доказательство. Обозначим через M множество всех дробей, т. е. символов вида $\frac{a}{b}$, где $a, b \in R$, $b \neq 0$ (здесь черта уже не является знаком деления, поскольку в R деление, вообще говоря, не определено).

В множестве таких дробей введем операции сложения и умножения по формулам, соответствующим формулам (1) и (2):

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd},$$

и положим при $a \neq 0$

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}.$$

---

* Предположение, что R содержит единицу, на самом деле излишне и введено для упрощения доказательства.

Введем в множество дробей отношение эквивалентности, положив $\frac{a}{b} \sim \frac{c}{d}$, если $ad = bc$. Покажем, что это отношение рефлексивно, симметрично и транзитивно.

а) Рефлексивность отношения вытекает из того, что $ab = ba$, и потому $\frac{a}{b} \sim \frac{a}{b}$.

б) Если $\frac{a}{b} \sim \frac{c}{d}$, то $ad = bc$. Но тогда $cb = da$, и потому $\frac{c}{d} \sim \frac{a}{b}$. Значит, отношение $\sim$ симметрично.

в) Докажем, что отношение $\sim$ транзитивно. Пусть $\frac{a}{b} \sim \frac{c}{d}$ и $\frac{c}{d} \sim \frac{f}{g}$. Тогда $ad = bc$ и $cg = df$. Умножим обе части равенства $ad = bc$ на g. Получим $adg = bcg$. Так как $cg = df$, то отсюда следует, что $adg = bdf$, $d(ag - bf) = 0$. Но R — область целостности, и $d \neq 0$. Значит, $ag - cf = 0$, т. е. $\frac{a}{b} \sim \frac{f}{g}$. Итак, из $\frac{a}{b} \sim \frac{c}{d}$ и $\frac{c}{d} \sim \frac{f}{g}$ следует, что $\frac{a}{b} \sim \frac{f}{g}$, т. е. отношение $\sim$ транзитивно.

Мы доказали, что отношение $\sim$ рефлексивно, симметрично и транзитивно, а потому является отношением эквивалентности. Поэтому множество дробей M распадается на классы эквивалентных дробей. Обозначим через P_1 множество классов эквивалентных дробей (таким образом, элементами P_1 являются не отдельные дроби, а классы эквивалентных дробей).

Определим сложение классов следующим образом:

$$\left\{\frac{a}{b}\right\} + \left\{\frac{c}{d}\right\} = \left\{\frac{ad + bc}{bd}\right\}. \tag{4}$$

Иными словами, чтобы сложить классы, содержащие соответственно дроби $\frac{a}{b}$ и $\frac{c}{d}$, надо сложить эти дроби по формуле (1) и взять класс дробей, содержащий эту сумму. Аналогично определяется умножение классов дробей:

$$\left\{\frac{a}{b}\right\} \cdot \left\{\frac{c}{d}\right\} = \left\{\frac{ac}{bd}\right\}. \tag{5}$$

Надо показать, что эти определения не зависят от выбора представителей в классах. Иными словами, надо показать, что если $\frac{a}{b} \sim \frac{a_1}{b_1}$ и $\frac{c}{d} \sim \frac{c_1}{d_1}$, то

$$\frac{a}{b} + \frac{c}{d} \sim \frac{a_1}{b_1} + \frac{c_1}{d_1}, \quad \frac{a}{b} \cdot \frac{c}{d} \sim \frac{a_1}{b_1} \cdot \frac{c_1}{d_1}.$$

Но если $\frac{a}{b} \sim \frac{a_1}{b_1}$ и $\frac{c}{d} \sim \frac{c_1}{d_1}$, то $ab_1 = ba_1$ и $cd_1 = dc_1$. Умножим обе

части первого из этих равенств на dd_1, а второго на bb_1 и сложим:

$$ab_1dd_1 + cd_1bb_1 = ba_1dd_1 + c_1dbb_1,$$

т. е.

$$(ad + bc)b_1d_1 = (a_1d_1 + b_1c_1)bd.$$

Это равенство и значит, что

$$\frac{ad+bc}{bd} \sim \frac{a_1d_1 + b_1c_1}{b_1d_1}.$$

Точно так же, перемножая равенства $ab_1 = ba_1$, $cd_1 = c_1d$, получаем: $acb_1d_1 = a_1c_1bd$. Это значит, что $\frac{ac}{bd} = \frac{a_1c_1}{b_1d_1}$. Таким образом, введенные определения действий над классами дробей не зависят от выбора дробей в классах.

Из коммутативности сложения и умножения в R следует коммутативность сложения и умножения дробей:

$$\frac{a}{b} + \frac{c}{d} = \frac{c}{d} + \frac{a}{b}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{c}{d} \cdot \frac{a}{b}.$$

В самом деле,

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \quad \frac{c}{d} + \frac{a}{b} = \frac{cb+da}{db},$$

а дроби $\frac{ad+bc}{bd}$ и $\frac{cb+da}{db}$ равны, так как $ad + bc = cb + da$ и $bd = db$. Точно так же

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \quad \frac{c}{d} \cdot \frac{a}{b} = \frac{ca}{db}, \text{ а } \frac{ac}{bd} = \frac{ca}{db},$$

так как $ac = ca$, $bd = db$.

Из коммутативности сложения и умножения дробей вытекает, что сложение и умножение классов дробей обладает тем же свойством. Точно так же доказывается, что эти операции ассоциативны, а умножение дистрибутивно относительно сложения.

Из равенств

$$\frac{a}{b} + \frac{0}{d} = \frac{ad + 0 \cdot b}{b \cdot d} = \frac{ad}{bd} \sim \frac{a}{b}$$

и

$$\frac{a}{b} \cdot \frac{c}{c} = \frac{ac}{bc} \sim \frac{a}{b}$$

видно, что класс дробей вида $\frac{0}{d}$ $(d \neq 0)$ играет роль нуля в P_1, а класс дробей вида $\frac{c}{c}$ $(c \neq 0)$ — роль единицы. Далее,

$$\frac{a}{b} + \frac{-a}{b} = \frac{ab - ab}{b^2} = \frac{0}{b^2} \sim \frac{0}{d}$$

и

$$\frac{a}{b}\cdot\frac{b}{a}=\frac{ab}{ba}\sim\frac{c}{c}$$

(при $a\neq 0$). Поэтому в P_1 каждый элемент имеет противоположный, а каждый ненулевой элемент—обратный. Этим доказано, что P_1—поле.

Построим в P_1 подкольцо R_1, изоморфное кольцу R. С этой целью поставим в соответствие каждому элементу $a\in R$ класс дробей $\left\{\frac{ab}{b}\right\}$, $a\to\left\{\frac{ab}{b}\right\}$. Любые две дроби из этого класса эквивалентны: $\frac{ab}{b}\sim\frac{ac}{c}$, поскольку $(ab)c=(ac)b$. С другой стороны, любая дробь эквивалентная дроби $\frac{ab}{b}$, имеет вид $\frac{ac}{c}$ (проверьте это сами).

Покажем, что если $a\neq a_1$, то $\frac{ab}{b}\not\sim\frac{a_1c}{c}$. В самом деле, если $a\neq a_1$, то $abc\neq a_1bc$, а тогда $\frac{ab}{b}\not\sim\frac{a_1c}{c}$. Значит, отображение $a\to\left\{\frac{ab}{b}\right\}$ ставит в соответствие различным элементам кольца R различные классы. Равенства

$$\frac{ab}{b}+\frac{a_1c}{c}=\frac{abc+a_1bc}{bc}=\frac{(a+a_1)bc}{bc};\quad\frac{ab}{b}\cdot\frac{a_1c}{c}=\frac{aa_1\cdot bc}{bc}$$

показывают, что при этом соответствии сохраняются операции сложения и умножения. Иными словами, кольцо R_1, состоящее из классов дробей вида $\left\{\frac{ab}{b}\right\}$, изоморфно кольцо R.

При этом P_1 — поле отношений для R_1: любая дробь $\frac{a}{b}\in P_1$ может быть представлена в виде:

$$\frac{a}{b}=\left(\frac{ae}{e}\right)\left(\frac{be}{e}\right)^{-1}$$

$\left(\text{в самом деле, } \frac{ae}{e}\left(\frac{be}{e}\right)^{-1}=\left(\frac{a}{e}\right)\left(\frac{b}{e}\right)^{-1}=\frac{a}{e}\cdot\frac{e}{b}=\frac{ae}{eb}=\frac{a}{b}\right)$.

Мы построили поле P_1 и в нем подкольцо R_1, изоморфное R и такое, что P_1 — поле отношений для R_1. Чтобы завершить доказательство теоремы, заменим каждый класс дробей вида $\left\{\frac{ab}{b}\right\}$ элементом a и соответственно определим операции $\left(\text{например, } a+\frac{c}{d}=\frac{ae}{e}+\frac{c}{d}=\frac{ad+c}{d}\right)$. Мы получаем поле P, содержащее кольцо R.

Наименьшее подполе в P, содержащее кольцо R, совпадает с P. Поэтому P называют *полем отношений кольца* R.

Примеры.

1. Пусть $\mathbf{Z}$ — кольцо целых чисел. Полем отношений для $\mathbf{Z}$ является поле $\mathbf{Q}$ рациональных чисел. *Рациональным числом* мы называем класс эквивалентных друг другу дробей. При этом дроби $\frac{a}{b}$ и $\frac{c}{d}$ (где $b \neq 0$, $d \neq 0$) эквивалентны в том и только том случае, когда $ad = bc$.

2. Пусть $\mathbf{Z}[i]$ — кольцо целых гауссовых чисел. Полем отношений для $\mathbf{Z}[i]$ является множество классов эквивалентных дробей вида $\frac{a+bi}{c+di}$, где a, b, c, d — целые числа, $c + di \neq 0$. Но любая дробь такого вида эквивалентна дроби

$$\frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{(ac+bd)(bc-ad)i}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i.$$

Так как $\frac{ac+bd}{c^2+d^2}$ и $\frac{bc-ad}{c^2+d^2}$ — обыкновенные дроби, задающие рациональные числа r и s, то поле отношений для $\mathbf{Z}[i]$ состоит из чисел вида $r + si$, где r и s — рациональные числа. Это поле обозначают $\mathbf{Q}[i]$.

3. Пусть $\mathbf{R}[x]$ — кольцо многочленов с действительными коэффициентами. Поле отношений для $\mathbf{R}[x]$ состоит из классов эквивалентных алгебраических дробей.

Замечание. Если подкольца R и R' полей S и S' изоморфны, то и соответствующие поля отношений P и P' изоморфны. Если изоморфизм между R и R' имеет вид: $a \to a'$, то изоморфизм между P и P' задается формулой:

$$\frac{a}{b} \to \frac{a'}{b'}.$$

Вопросы для самопроверки и упражнения

1. Дайте определение гомоморфизма колец. Какие кольца называются изоморфными?

2. Обозначим через R кольцо из элементов a, b, c с правилами действий, $a + a = a$, $a + b = b$, $a + c = c$, $b + b = c$, $b + c = a$, $c + c = b$, $aa = ab = ac = a$, $bb = b$, $bc = c$, $cc = b$.

Поставим в соответствие целому числу x элемент a, если x делится на 3, элемент b, если остаток деления x на 3 равен 1, и элемент c, если этот остаток равен 2.

Покажите, что это отображение является гомоморфным отображением $\mathbf{Z}$ на R.

3. Можно ли отобразить гомоморфно поле на неизоморфное ему поле?

4. Что называется ядром гомоморфизма? Всякое ли подмножество кольца может быть ядром гомоморфизма?

5. Всякий ли идеал может быть ядром гомоморфизма?

6. Что такое поле отношений? Какие кольца обладают полем отношений?

7. Напишите таблицы сложения и умножения для фактор-колец $\mathbf{Z}/(6)$ и $\mathbf{Z}/(5)$.

8. В кольце $\mathbf{Z}[x]$ многочленов с целочисленными коэффициентами найдите идеал (x^2+1) и постройте фактор-кольцо $\mathbf{Z}[x]/(x^2+1)$. Докажите, что фактор-кольцо $\mathbf{Z}[x]/(x^2+1)$ изоморфно кольцу $\mathbf{Z}[i]$ целых гауссовых чисел.

9. В кольце $\mathbf{Z}[i]$ целых гауссовых чисел постройте идеал (i) и фактор-кольцо $\mathbf{Z}[i]/(i)$.

10. В каждом классе вычетов по идеалу (x^2) в кольце $\mathbf{Z}[x]$ есть многочлен первой степени $a+bx$. Как надо определить сложение и умножение таких многочленов, чтобы получилось кольцо, изоморфное фактор-кольцу $\mathbf{Z}[x]/x^2$?

Глава III
ТЕОРИЯ СРАВНЕНИЙ И ЕЕ АРИФМЕТИЧЕСКИЕ ПРИЛОЖЕНИЯ

§ 1. ОСНОВНЫЕ СВОЙСТВА СРАВНЕНИЙ

1. Сравнение по модулю. Целое число m порождает в кольце целых чисел $\mathbf{Z}$ идеал (m), состоящий из всех чисел, кратных m (см. п. 1 § 2 главы II). При этом идеалы, порожденные числом m и $-m$, совпадают, $(m) = (-m)$ (делимость на m равносильна делимости на $-m$). Поэтому, не теряя общности, можно считать, что $m > 0$.

Определение 1. Два числа, сравнимые по идеалу (m), называются *сравнимыми по модулю* m.

Если числа a и b сравнимы по модулю m, то пишут $a \equiv b \pmod m$.

Условие $a \equiv b \pmod m$ означает, что $a - b \in (m)$, т. е. что $a - b$ делится на m. Поэтому числа a и b сравнимы по модулю m в том и только том случае, когда $a - b$ делится на m.

$$a \equiv b \pmod m \leftrightarrow (a - b) \vdots m.$$

Примеры.

1. $m = 3$; $8 \equiv 5 \pmod 3$, так как $8 - 5 = 3$ и 3 делится на 3.
2. $m = 5$; $12 \equiv 2 \pmod 5$, так как $12 - 2 = 10$ и 10 делится на 5.
3. $m = 2$; $3 \equiv 7 \pmod 2$, так как $3 - 7 = -4$ и -4 делится на 2.
4. $m = 5$; $11 \not\equiv 3 \pmod 5$, так как $11 - 3 = 8$, а 8 не делится на 5.

Теорема 1 (признак сравнимости двух чисел по модулю m). *Два целых числа a и b сравнимы по модулю m тогда и только тогда, когда a и b имеют одинаковые остатки при делении на m.*

Доказательство. Пусть остатки при делении a и b на m равны, т. е.

$$a = mq_1 + r, \tag{1}$$

$$b = mq_2 + r, \tag{2}$$

где $0 \leqslant r < m$.

Вычтем (2) из (1); получим $a - b = m\,(q_1 - q_2)$, т. е. $a - b \vdots m$ или $a \equiv b \pmod m$.

Обратно, пусть $a \equiv b \pmod m$. Это означает, что $a - b \vdots m$ или

$$a - b = mt,\ t \in \mathbf{Z}. \tag{3}$$

Разделим b на m; получим $b = mq + r$, $0 \leqslant r < m$. Подставив $b = mq + r$ в (3), будем иметь $a = m\,(q + t) + r$, т. е. при делении a на m получается тот же остаток, что и при делении b на m.

Пример. Определим, сравнимы ли числа 13 и 49 по модулю 6.

Решение. При делении 13 и 49 на 6 получаются одинаковые остатки $r_1 = r_2 = 1$. Следовательно, $13 \equiv 49 \pmod 6$.

Определение 2. Два или несколько чисел, дающие при делении на m одинаковые остатки, называются *равноостаточными* или *сравнимыми по модулю m*.

Отметим далее несколько часто используемых фактов:

1. Если два целых числа a и b сравнимы по модулю m, то это можно записать различными способами: $a \equiv b \pmod m$ или $a = b + mt$ (где t — целое число), или $a - b = mt$, или $(a - b) \vdots m$.

2. Если $a \vdots m$, то и $a - 0 \vdots m$ или $a \equiv 0 \pmod m$, т. е. всякое число, кратное m, сравнимо с нулем по модулю m.

3. Если $a = mq + r$, т. е. a при делении на m дает остаток r, то $a - r = mq$ или $a \equiv r \pmod m$. Таким образом, всякое целое число a всегда сравнимо с остатком r, получающимся при делении его на m.

2. Свойства сравнений.

1. Свойства сравнений, не зависящие от модуля.

Поскольку отношение $a \equiv b \pmod m$ является частным случаем отношения сравнения по идеалу, все свойства таких отношений, доказанные в п. 3 § 3 главы II, сохраняют силу и для отношения $a \equiv b \pmod m$.

1) *Отношение* $a \equiv b \pmod m$ *является отношением эквивалентности*, т. е. удовлетворяет требованиям:

а) *рефлексивности*: $a \equiv a \pmod m$ (всякое целое число a сравнимо с самим собой по модулю m);

в) *симметричности*: если $a \equiv b \pmod m$, то и $b \equiv a \pmod m$;

с) *транзитивности*: если $a \equiv b \pmod m$, а $b \equiv c \pmod m$, то $a \equiv c \pmod m$.

2) *Сравнения по одному и тому же модулю можно почленно складывать.*

3) *Два сравнения по одному и тому же модулю можно почленно вычитать одно из другого.*

4) (следствие свойств 1, 2, 3). *К обеим частям сравнения можно прибавлять одно и то же целое число.*

Действительно, пусть $a \equiv b \pmod m$ и k — любое целое число. По свойству рефлексивности $k \equiv k \pmod m$, а согласно свойствам 2 и 3 имеем $a + k \equiv b + k \pmod m$.

Следствие. *Члены сравнения можно переносить из одной части сравнения в другую с противоположным знаком.*

5) *Сравнения по одному и тому же модулю можно почленно перемножать.*

Следствие. *Обе части сравнения можно возводить в одну и ту же целую неотрицательную степень: если* $a \equiv b \pmod m$ *и* s *— целое неотрицательное число, то* $a^s \equiv b^s \pmod m$.

6) *Обе части сравнения можно умножать на одно и то же целое число.*

2. Свойства сравнений, зависящие от модуля.

7) *Если* $a \equiv b \pmod m$ *и* $m \vdots n$, *то* $a \equiv b \pmod n$.

Доказательство. Так как $a \equiv b \pmod m$, то $(a - b) \vdots m$. А так как $m \vdots n$, то в силу транзитивности отношения делимости $(a - b) \vdots n$, т. е. $a \equiv b \pmod n$.

8) *Обе части сравнения и модуль можно умножить на одно и то же целое положительное число.*

Действительно, пусть $a \equiv b \pmod m$ и c — целое положительное число. Тогда

$$a - b = mt \text{ и } ac - bc = mtc, \text{ или } ac \equiv bc \pmod{mc}.$$

9) *Если* $ak \equiv bk \pmod m$ и $(k, m) = d$, *то* $a \equiv b \left(\mathrm{mod}\,\frac{m}{d}\right)$.

Доказательство. Пусть $k = k_1 d$, $m = m_1 d$.

Из $ak \equiv bk \pmod m$ следует $(ak - bk) \vdots m$, или $(a - b) \cdot k_1 d \vdots m_1 d$, откуда $(a - b) k_1 \vdots m_1$. Так как $(k_1, m_1) = 1$, то $(a - b) \vdots m_1$, или $a - b \vdots \frac{m}{d}$, т. е. $a \equiv b \left(\mathrm{mod}\,\frac{m}{d}\right)$.

Следствие 1. *Если* $d = k$, т. е. если $m \vdots k$, *то из* $ak \equiv bk \pmod m$ *следует* $a \equiv b \left(\mathrm{mod}\,\frac{m}{k}\right)$, а это означает, что *обе части сравнения и модуль можно разделить на любой их общий делитель.*

Большое значение имеет

Следствие 2. *Если* $d = 1$, т. е. если $(k, m) = 1$, *то из* $ak \equiv bk \pmod m$ *следует* $a \equiv b \pmod m$, а это означает, что *обе части сравнения можно разделить на их общий делитель, если он взаимно прост с модулем.*

Пример. $60 \equiv 9 \pmod{17}$. После деления обеих частей сравнения на 3 получим $20 \equiv 3 \pmod{17}$.

Делить обе части сравнения на число, не взаимно простое с модулем, вообще говоря, нельзя, так как после деления могут получиться числа, несравнимые по данному модулю.

Пример. $8 \equiv 4 \pmod 4$, но $2 \not\equiv 1 \pmod 4$.

Из рассмотренных свойств сравнений вытекает следующее общее свойство.

10) *Пусть $P(x)$ — многочлен с целыми коэффициентами, а и b — переменные, принимающие целые значения. Тогда если $a \equiv b \pmod m$, то $P(a) \equiv P(b) \pmod m$.*

Доказательство. Пусть $P(x) = c_0x^n + c_1x^{n-1} + \ldots + c_{n-1}x + c_n$. По условию $a \equiv b \pmod m$, тогда $a^k \equiv b^k \pmod m$ при $k = 0, 1, 2, \ldots, n$.

Умножая обе части каждого из полученных $n + 1$ сравнений на c_{n-k}, получим:

$$c_{n-k}a^k \equiv c_{n-k}b^k \pmod m,$$

где $k = 0, 1, 2, \ldots, n$.

Складывая последние сравнения, получим:

$$P(a) \equiv P(b) \pmod m.$$

Если $a \equiv b \pmod m$ и $c_i \equiv d_i \pmod m$, $0 \leqslant i \leqslant n$, то

$$c_0a^n + c_1a^{n-1} + \ldots + c_{n-1}a + c_n \equiv d_0b^n + d_1b^{n-1} + \ldots + d_{n-1}b + d_n \pmod m.$$

Таким образом, в сравнении по модулю m отдельные слагаемые и множители можно заменять числами, сравнимыми по тому же модулю m. В частности, все числа, кратные модулю, можно заменять нулями (так как если $a \vdots m$, то $a \equiv 0 \pmod m$).

Вместе с тем следует обратить внимание на то, что встречающиеся в сравнениях показатели степеней заменять таким образом нельзя: из $a^n \equiv c \pmod m$ и $n \equiv k \pmod m$ не следует, что $a^k \equiv c \pmod m$.

Свойство 10 имеет ряд важных применений. В частности, с его помощью можно дать теоретическое обоснование признаков делимости. Для иллюстрации в качестве примера дадим вывод признака делимости на 3.

Всякое натуральное число N можно представить в виде систематического числа: $N = a_0 10^n + a_1 \cdot 10^{n-1} + \ldots + a_{n-1}10 + a_n$.

Рассмотрим многочлен $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$. Так как $10 \equiv 1 \pmod 3$, то по свойству 9 $f(10) \equiv f(1) \pmod 3$ или

$$N = a_0 10^n + a_1 10^{n-1} + \ldots + a_{n-1} \cdot 10 + a_n \equiv a_1 + a_2 + \ldots + a_{n-1} + a_n \pmod 3,$$

т. е. для делимости N на 3 необходимо и достаточно, чтобы сумма цифр этого числа делилась на 3.

Вопросы для самопроверки и упражнения

1. Что означает запись $a \equiv b \pmod m$?
2. Какое условие является необходимым и достаточным для того, чтобы два числа были сравнимы по модулю m?
3. Установите, сравнимы ли числа 726 и 162 по модулю 5, пользуясь: а) определением; б) признаком сравнимости чисел по модулю.
4. Сформулируйте свойства сравнений, аналогичные свойствам равенств.
5. Сформулируйте свойства сравнений, отличные от свойств равенств.

6. В каком случае можно разделить на одно и то же число: а) обе части сравнения и модуль; б) обе части сравнения, не изменяя модуля?

7. Докажите свойства сравнений 1, 2, 3, 4, 5, 6 непосредственно, не опираясь на сведения из теории колец и идеалов.

8. Запишите в виде сравнений условия:

а) числа 219 и 128 дают одинаковые остатки при делении на 7 (проверить!);

б) число — 352 при делении на 31 дает остаток, равный 20;

в) число 487 — 7 делится на 12;

г) 20 — остаток от деления числа 389 на 41.

9. Запишите в виде сравнений следующие утверждения:

а) число N четно; б) число N нечетно; в) число N имеет вид $4k + 1$; г) число N имеет вид $8k - 3$; д) число N имеет вид $10k + 3$.

§ 2. КЛАССЫ ВЫЧЕТОВ ПО ДАННОМУ МОДУЛЮ

1. Кольцо вычетов по модулю m. Так как (m) — идеал в кольце целых чисел $\mathbf{Z}$, то $\mathbf{Z}$ разбивается на классы вычетов по идеалу (m), или, как говорят, по модулю m. Два числа a и b принадлежат одному и тому же классу вычетов по модулю m в том и только том случае, когда $a - b \in (m)$, т. е. когда $(a - b) \vdots m$.

Все числа, принадлежащие одному и тому же классу вычетов по модулю m, имеют одинаковые остатки при делении на m. Поэтому можно обозначать классы вычетов с помощью этих остатков. Чтобы отличать классы вычетов от остатков, будем писать над классами вычетов черточку. Так как при делении на m получаются остатки $0, 1, \ldots, m - 1$, то соответствующие классы вычетов обозначают $\overline{0}, \overline{1}, \ldots, \overline{m-1}$. Класс вычетов $\overline{0}$ состоит из чисел, кратных m, т. е. совпадает с идеалом (m), класс вычетов $\overline{1}$ состоит из чисел, дающих при делении на m остаток 1, и т. д.

Множество классов вычетов по модулю m обозначим $\mathbf{Z}_m$. Ясно, что $\mathbf{Z}_m$ — это фактор-кольцо $\mathbf{Z}$ по идеалу (m), $\mathbf{Z}_m = \mathbf{Z}/(m)$. Его называют *кольцом вычетов по модулю m*.

Из определения сравнения по модулю m получаем: целое число x принадлежит классу вычетов $\overline{a}$ по модулю m в том и только том случае, когда x имеет вид $x = a + mt$, где $t \in \mathbf{Z}$, т. е. когда $x \equiv a \pmod m$.

Примеры.

1. Пусть $m = 2$. При делении целых чисел на 2 будем получать лишь два различных остатка: 0 и 1. Множество всех целых чисел разобьется на два класса: $\overline{0}$ и $\overline{1}$. Класс $\overline{0}$ содержит все четные числа, а класс $\overline{1}$ — нечетные.

2. Пусть $m = 5$. При делении различных целых чисел на 5 будем получать 5 различных остатков: 0, 1, 2, 3, 4. Множество всех целых чисел разобьется на 5 классов: $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}$ или $x \equiv 0, 1, 2, 3, 4 \pmod 5$.

Отображение, ставящее каждому целому числу x содержащий его класс вычетов, является гомоморфным отображением $\mathbf{Z}$ на $\mathbf{Z}_m$ (см. п. 4 § 3 главы II).

При этом операции сложения и умножения в кольцах $\mathbf{Z}_m$ определяются как в любых кольцах вычетов: чтобы сложить классы вычетов $\overline{a}$ и $\overline{b}$ по модулю m, надо выбрать в $\overline{a}$ число a, в $\overline{b}$ число b, сложить эти числа и взять класс вычетов, содержащий $a+b$; этот класс вычетов и является суммой $\overline{a}$ и $\overline{b}$. Точно так же определяется умножение классов вычетов.

Иными словами,

$$\overline{a}+\overline{b}=\overline{a+b},\ \overline{a}\cdot\overline{b}=\overline{ab}.$$

Так как $\mathbf{Z}$ — коммутативное ассоциативное кольцо с единицей, то и все кольца $\mathbf{Z}_m$ коммутативны, ассоциативны и имеют единицу.

Класс вычетов $\overline{0}$ играет роль нуля в кольце $\mathbf{Z}_m$: для любого $\overline{a}\in\mathbf{Z}_m$ имеем: $\overline{a}+\overline{0}=\overline{a}$. Класс вычетов $\overline{1}$ играет роль единицы в $\mathbf{Z}_m$: для любого $a\in\mathbf{Z}_m$ имеем: $\overline{a}\cdot\overline{1}=\overline{a}$.

Аддитивная группа кольца вычетов состоит из m элементов: $\overline{0}$, $\overline{1}$, ..., $\overline{m-1}$, кратных классу вычетов $\overline{1}$. Она является, таким образом, циклической группой порядка m, порожденной $\overline{1}$.

Так как кольца $\mathbf{Z}_m$ конечны, операции в них можно задавать конечными таблицами сложения и умножения.

Примеры.

1. Напишем таблицы сложения и умножения для кольца $\mathbf{Z}_5$. Мы имеем 5 классов вычетов по модулю 5: $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$.
Таблица сложения и умножения имеет вид:

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

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

2. Напишем таблицы сложения и умножения для кольца $\mathbf{Z}_6$. Здесь мы имеем 6 классов вычетов: $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$.

Таблицы сложения и умножения имеют вид:

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

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

2. Полные системы вычетов и их основные свойства. Выберем из каждого класса вычетов по модулю m по одному числу. Получим m целых чисел: $x_1, \ldots, x_m$. Множество $\{x_1, \ldots, x_m\}$ называют *полной системой вычетов по модулю* m.

Так как каждый класс содержит бесчисленное множество вычетов, то можно составить бесчисленное множество различных полных систем вычетов по данному модулю m, каждая из которых содержит m вычетов.

Пример. Составить несколько полных систем вычетов по модулю $m = 5$. Имеем классы: $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$.

$$\begin{aligned}
\overline{0} &= \{\ldots\ -10,\ -5,\ \ 0,\ \ 5,\ 10,\ \ldots\} \\
\overline{1} &= \{\ldots\ \ -9,\ \ -4,\ \ 1,\ \ 6,\ 11,\ \ldots\} \\
\overline{2} &= \{\ldots\ \ -8,\ \ -3,\ \ 2,\ \ 7,\ 12,\ \ldots\} \\
\overline{3} &= \{\ldots\ \ -7,\ \ -2,\ \ 3,\ \ 8,\ 13,\ \ldots\} \\
\overline{4} &= \{\ldots\ \ -6,\ \ -1,\ \ 4,\ \ 9,\ 14,\ \ldots\}
\end{aligned}$$

Составим несколько полных систем вычетов, взяв по одному вычету из каждого класса:

$$\begin{array}{rrrrr}
0, & 1, & 2, & 3, & 4 \\
5, & 6, & 2, & 8, & 9 \\
-10, & -9, & -8, & -7, & -6 \\
-\ 5, & -4, & -3, & -2, & -1
\end{array}$$

и т. д. (Мы будем писать системы вычетов без фигурных скобок.)

Наиболее употребительны:

а) *Полная система наименьших неотрицательных вычетов*: $0, 1, \ldots, m-1$. В приведенном выше примере: 0, 1, 2, 3, 4.

Такая система вычетов составляется просто: надо выписать все неотрицательные остатки, получающиеся при делении на m.

б) *Полная система наименьших положительных вычетов*: 1, 2, ..., m. В нашем примере: 1, 2, 3, 4, 5.

в) *Полная система абсолютно наименьших вычетов* (из каждого класса берется наименьший по абсолютной величине вычет). В приведенном примере: 0, 1, 2, —2, —1.

Если в классе содержится два вычета, a и $-a$, имеющие одинаковую абсолютную величину, то можно взять любой из них. Так, если $m = 8$, то из класса $\overline{4}$ можно взять вычет 4 или —4.

Рассмотрим теперь основные свойства полной системы вычетов.

Теорема 1. *Любая совокупность m целых чисел*:

$$x_1, x_2, \ldots, x_m, \tag{1}$$

попарно не сравнимых по модулю m, образует полную систему вычетов по модулю m.

Доказательство. а) Каждое из чисел совокупности (1) принадлежит некоторому классу.

б) Любые два числа x_i и x_j из (1) несравнимы между собой, т. е. принадлежат различным классам.

в) Всего в (1) m чисел, т. е. столько же, сколько имеется классов по модулю m.

Следовательно, совокупность чисел x_1, x_2, ..., x_m — полная система вычетов по модулю m.

Теорема 2. *Пусть* $(a, m) = 1$, b *— произвольное целое число; тогда если* $x_1, x_2, \ldots, x_m$*—полная система вычетов по модулю m, то и совокупность чисел* $ax_1 + b$, $ax_2 + b$, ..., $ax_m + b$ *тоже полная система вычетов по модулю m.*

Доказательство. Рассмотрим

$$ax_1 + b,\ ax_2 + b,\ \ldots,\ ax_m + b. \tag{2}$$

а) Каждое из чисел совокупности (2) принадлежит некоторому классу.

б) Любые два числа $ax_i + b$ и $ax_j + b$ из (2) несравнимы между собой, т. е. принадлежат различным классам.

Действительно, если бы в (2) имелись такие два числа, что $ax_i + b \equiv ax_j + b \pmod m$, $(i \neq j)$, то получили бы $ax_i \equiv ax_j \pmod m$. Так как $(a, m) = 1$, то по следствию 2 к свойству 9 сравнений можно сократить обе части сравнения на a. Получаем $x_i \equiv x_j \pmod m$.

По условию же $x_i \not\equiv x_j \pmod m$ при $i \neq j$, так как x_1, x_2, ..., x_m — полная система вычетов.

в) Совокупность чисел (2) содержит m чисел, т. е. столько, сколько имеется классов по модулю m.

Итак, $ax_1 + b$, $ax_2 + b$, ..., $ax_m + b$ — полная система вычетов по модулю m.

Пример. Пусть $m = 10$, $a = 3$, $b = 4$.

Возьмем какую-нибудь полную систему вычетов по модулю 10, например: 0, 1, 2, ..., 9. Составим числа вида $ax + b$. Получим: 4, 7, 10, 13, 16, 19, 22, 25, 28, 31. Полученная совокупность чисел — полная система вычетов по модулю 10, в чем легко убедиться, найдя остатки от деления их на 10.

3. Теорема об остатках. *Пусть m и n — целые числа*; так как $mn \vdots m$ и $mn \vdots n$, то из сравнения $x \equiv y \pmod{mn}$ вытекает, что $x \equiv y \pmod{m}$ и $x \equiv y \pmod{n}$. Таким образом, *каждый класс вычетов $\overline{c}$ по модулю mn содержится как в некотором классе вычетов $\overline{a}$ по модулю m, так и в некотором классе вычетов $\overline{b}$ по модулю n.* Этим определяется отображение $\overline{c} \to (\overline{a}, \overline{b})$, где $\overline{c}$ — класс вычетов по модулю mn, $\overline{a}$ — класс вычетов по модулю m и $\overline{b}$ — класс вычетов по модулю n. Если $\overline{c} \to (\overline{a}, \overline{b})$ и $x \in \overline{c}$, то $x \in \overline{a}$ и $x \in \overline{b}$.

Пример. Пусть $m = 5$, $n = 4$. Тогда $mn = 20$. Выберем класс вычетов по модулю 20, содержащий число 17. Так как $17 \equiv 2 \pmod 5$ и $17 \equiv 1 \pmod 4$, то классу вычетов $\overline{17}$ по модулю 20 соответствует пара $(\overline{2}, \overline{1})$, где $\overline{2}$ — класс вычетов по модулю 5, а $\overline{1}$ — класс вычетов по модулю 4. Если $x \equiv 17 \pmod{20}$, то $x \equiv 2 \pmod 5$ и $x \equiv 1 \pmod 4$.

Выясним, является ли построенное выше соответствие $\overline{c} \to (\overline{a}, \overline{b})$ между классами вычетов по модулю mn и парами классов вычетов по модулям m и n взаимно-однозначным. Вообще говоря, это не так. Но если числа m и n взаимно просты, то указанное соответствие является взаимно-однозначным. Чтобы доказать это утверждение, нам понадобится следующая лемма:

Лемма. *Пусть числа m и n взаимно просты. Расположим полную систему наименьших положительных вычетов по модулю mn в виде прямоугольной $m \times n$-матрицы.*

$$\begin{array}{llll} 1, & 2, & \ldots, & m, \\ m+1, & m+2, & \ldots, & 2m, \\ 2m+1, & 2m+2, & \ldots, & 3m, \\ \cdots & \cdots & \cdots & \cdots \\ (n-1)\,m+1, & (n-1)\,m+2, & \ldots, & nm. \end{array} \qquad (1)$$

Тогда каждая строка этой матрицы является полной системой вычетов по m, а каждый столбец — полной системой вычетов по n.

Доказательство. k-я строка матрицы (1) состоит из чисел $(k-1)\,m + 1, \ldots, km$.

Остатки от деления этих чисел на m равны соответственно $1, 2, \ldots, m-1, 0$. Поскольку числа $1, 2, \ldots, m-1, 0$ образуют полную систему вычетов по модулю m, то и числа $(k-1)\,m + 1, \ldots, km$ образуют полную систему вычетов по m. s-й столбец матрицы (1) состоит из чисел вида $jm + s$, где j пробегает полную систему вычетов по n, $j = 0, 1, \ldots, n-1$. Так как 0 и n по условию взаимно просты, то в силу свойства 2 полной системы вычетов

числа $jm + s$, $0 \leqslant j \leqslant n - 1$, тоже образуют полную систему вычетов по n. Лемма доказана.

Теорема 3. *Пусть m и n — взаимно простые числа. Тогда для любых классов вычетов $\bar{a}$ по модулю m и $\bar{b}$ по модулю n найдется класс вычетов $\bar{c}$ по модулю mn, такой, что $x \in \bar{c}$ тогда и только тогда, когда $x \in \bar{a}$ и $x \in \bar{b}$.*

Доказательство. Выберем в $\bar{a}$ наименьший положительный вычет a. Расположим наименьшие положительные вычеты по модулю mn в виде прямоугольной таблицы, как в лемме 1. Числа столбца $jm + a$, $0 \leqslant j \leqslant n - 1$, и только они сравнимы с a по модулю m. Но эти числа образуют по лемме полную систему вычетов по модулю n. Поэтому среди них найдется одно число $c = jm + a$, принадлежащее классу вычетов $\bar{b}$.

Итак, $c \in \bar{a}$ и $c \in \bar{b}$. Обозначим через $\bar{c}$ класс вычетов по модулю mn, содержащий число c. Если $y \in \bar{c}$, то $y \equiv c \pmod{mn}$, а тогда $y \equiv c \pmod{m}$, и поскольку $c \equiv a \pmod{m}$, то $y \equiv a \pmod{m}$ и $y \in \bar{a}$. Точно так же доказывается, что $y \in \bar{b}$.

Итак, мы нашли класс вычетов $\bar{c}$ по модулю mn, такой, что из $y \in \bar{c}$ вытекает $y \in \bar{a}$ и $y \in \bar{b}$. Если $\bar{d}$ — другой класс вычетов по модулю mn и d — наименьший положительный вычет в $\bar{d}$, то d либо стоит в другом столбце, чем c, либо в том же столбце, но в другой строке. Если d и c стоят в разных столбцах, то у них разные вычеты по модулю m. Если же d и c стоят в одном столбце, но в разных строках, то у них разные вычеты по модулю n — ведь числа этого столбца образуют полную систему вычетов по модулю n и потому принадлежат разным классам вычетов. Итак, $\bar{c}$ — единственный класс вычетов по модулю mn, такой, что из $y \in \bar{c}$ следует $y \in \bar{a}$ и $y \in \bar{b}$.

С помощью математической индукции доказывается следующее обобщение теоремы 3:

Теорема 3′. *Пусть числа $m_1, \ldots, m_k$ попарно взаимно просты. Для любых классов вычетов $\bar{a}_1, \ldots, \bar{a}_k$ по модулям $m_1, \ldots, m_k$ соответственно найдется класс вычетов $\bar{b}$ по модулю $m = m_1, \ldots, m_k$, такой, что из $y \in \bar{b}$ вытекает $y \in \bar{a}_1$, $y \in \bar{a}_2$, ... и $y \in \bar{a}_k$.*

Иными словами, если числа $m_1, \ldots, m_k$ попарно взаимно просты, то для любых чисел $a_1, \ldots, a_k$, таких, что $0 \leqslant a_j < m_j$, можно найти такое число b, что остаток от деления b на m_1 равен a_1, остаток от деления b на m_2 равен a_2 и т. д. При этом число b определено однозначно с точностью до кратного $m_1 \ldots m_n$.

Теорему 3 называют *теоремой об остатках*.

Пример.

Пусть $m = 5$, $m = 4$. Расположим вычеты по модулю 20 в виде прямоугольной матрицы:

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20

А теперь заменим каждое число в таблице парой чисел, первое из которых равно его вычету по модулю 5, а второе — по модулю 4:

(1, 1)	(2, 2)	(3, 3)	(4, 4)	(5, 1)
(1, 2)	(2, 3)	(3, 4)	(4, 1)	(5, 2)
(1, 3)	(2, 4)	(3, 1)	(4, 2)	(5, 3)
(1, 4)	(2, 1)	(3, 2)	(4, 3)	(5, 4)

Мы видим, что в каждой строке первые числа пробегают множество $\{1, 2, 3, 4, 5\}$, т. е. полную систему вычетов по модулю 5, а в каждом столбце вторые числа пробегают полную систему вычетов по модулю 4, т. е. множество $\{1, 2, 3, 4\}$.

Вопросы для самопроверки и упражнения

1. Какое условие является необходимым и достаточным для того, чтобы два числа принадлежали одному и тому же классу по модулю m?

2. Напишите 4 числа из класса вычетов $\overline{3}$ по модулю 6.

3. При каком условии числа a и $-a$ принадлежат одному классу вычетов по модулю m?

4. Как определяются операции сложения и умножения классов? Найдите $\overline{5} + \overline{7}$ и $\overline{5} \cdot \overline{8}$, если $m = 9$.

5. Приведите пример кольца классов вычетов с делителями нуля и пример кольца классов вычетов без делителей нуля.

6. Содержат ли делители нуля кольца классов вычетов по модулю m, если: а) $m = 17$, б) $m = 45$, в) $m = 100$, г) $m = 101$?

7. Как получить полную систему вычетов по модулю m?

8. Напишите полную систему абсолютно наименьших неотрицательных вычетов и произвольных вычетов по модулю 8.

9. Где при доказательстве свойства 2 полной системы вычетов использовалось условие $(a, m) = 1$?

10. Проверьте справедливость свойства 2 на числовом примере.

11. Каким классам вычетов по модулю 8 принадлежат все простые числа $p > 3$? Запишите общий вид этих чисел в виде равенств и сравнений.

12. Скольким классам вычетов по модулю 21 принадлежат вычеты из одного класса по модулю 7?

13. Пусть модуль $m = 20$; найдите: а) $\overline{7} \cdot \overline{19}$; б) $\overline{8} \cdot \overline{9}$; в) класс, противоположный классу $\overline{13}$; г) классы, которые являются делителями нуля.

14. Решите уравнение $\overline{3} - \overline{x} = \overline{7}$, где $\overline{3}$ и $\overline{7}$ — классы вычетов по модулю 11.

15. Найдите наименьшие неотрицательные и абсолютно наименьшие вычеты по модулю 13 для чисел 3, 8, 16, —43, 132, 278, —423, 1327. Какие из этих чисел принадлежат одному и тому же классу по модулю 13?

16. Образуют ли степени 2^0, 2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10} вместе с числом 0 полную систему вычетов по модулю 11?

17. Пусть x пробегает полную систему наименьших неотрицательных вычетов по модулю 8; найдите соответственные наименьшие неотрицательные вычеты для выражения $7x + 4$.

18. В линейной форме $y = ax$ число x пробегает полную систему вычетов по модулю m, причем $(a, m) = d > 1$. Сколько чисел полученной системы делится на m?

§ 3. ОБРАТИМЫЕ ЭЛЕМЕНТЫ В КОЛЬЦЕ ВЫЧЕТОВ

1. Приведенная система вычетов. Докажем следующую теорему:

Теорема 1. *Числа одного и того же класса вычетов по модулю m имеют с m один и тот же наибольший общий делитель: если $a \equiv b \pmod m$, то $(a, m) = (b, m)$.*

Доказательство. Пусть $a \equiv b \pmod m$. Тогда $a = b + mt$, где $t \in \mathbf{Z}$. Из этого равенства следует, что $(a, m) = (b, m)$ (см. п. 2 § 2 главы I). Теорема доказана.

Определение 1. Наибольший общий делитель модуля m и любого числа a из данного класса вычетов по m называется *наибольшим общим делителем* m и этого класса вычетов.

Определение 2. Класс вычетов $\bar{a}$ по модулю m называется *взаимно простым с модулем* m, если наибольший общий делитель $\bar{a}$ и m равен 1 (т. е. если m и любое число из $\bar{a}$ взаимно просты).

Пример. Пусть $m = 6$. Класс вычетов $\bar{2}$ состоит из чисел $\{..., -10, -4, 2, 8, 14, ...\}$. Наибольший общий делитель любого из этих чисел и модуля 6 равен 2. Значит, $(\bar{2}, 6) = 2$. Наибольший общий делитель любого числа из класса $\bar{5}$ и модуля 6 равен 1. Значит, класс $\bar{5}$ взаимно прост с модулем 6.

Выберем из каждого класса вычетов, взаимно простого с модулем m, по одному числу. Получим систему вычетов, составляющую часть полной системы вычетов. Ее называют приведенной системой вычетов по модулю m.

Определение 3. Совокупность вычетов по модулю m, взятых по одному из каждого взаимно простого с m класса вычетов по этому модулю, называется *приведенной системой вычетов*.

Из определения 3 следует способ получения приведенной системы вычетов по модулю m: надо выписать какую-либо полную систему вычетов и удалить из нее все вычеты, не взаимно простые с m. Оставшаяся совокупность вычетов — приведенная система вычетов. Приведенных систем вычетов по модулю m, очевидно, можно составить бесчисленное множество.

Если в качестве исходной взять полную систему наименьших неотрицательных или абсолютно наименьших вычетов, то указанным способом получим соответственно приведенную систему наименьших неотрицательных или абсолютно наименьших вычетов по модулю m.

Так, если $m = 8$, то 1, 3, 5, 7 — приведенная система наименьших неотрицательных вычетов, 1, 3, —3, —1 — приведенная система абсолютно наименьших вычетов. Отметим следующее утверждение:

Теорема 2. *Пусть число классов, взаимно простых с m, равно k. Тогда любая совокупность k целых чисел*

$$x_1, x_2, \ldots, x_k, \tag{1}$$

попарно несравнимых по модулю m и взаимно простых с m, представляет собой приведенную систему вычетов по модулю m.

Доказательство. а) Каждое число совокупности (1) принадлежит некоторому классу.

б) Все числа из (1) попарно несравнимы по модулю m, т. е. принадлежат различным классам по модулю m.

в) Каждое число из (1) взаимно просто с m, т. е. все эти числа принадлежат различным классам, взаимно простым с модулем m.

г) Всего в (1) имеется k чисел, т. е. столько, сколько должна содержать приведенная система вычетов по модулю m.

Следовательно, совокупность чисел (1) — приведенная система вычетов по модулю m.

2. Мультипликативная группа обратимых элементов в кольце вычетов. Напомним, что элемент a коммутативного кольца R с единицей e называется обратимым, если существует такой элемент $b \in R$, что $ab = e$. В п. 2 § 1 главы II было показано, что обратимые элементы образуют группу относительно умножения, причем единицей этой группы является e. Иными словами, произведение двух обратимых элементов обратимо, равно как и элемент, обратный обратимому.

Описание обратимых элементов в кольце вычетов $\mathbf{Z}_m$ дается следующей теоремой:

Теорема 3. *Для того чтобы класс вычетов $\bar{a}$ по модулю m был обратимым, необходимо и достаточно, чтобы $\bar{a}$ и m были взаимно просты.*

Доказательство. Пусть класс вычетов $\bar{a}$ взаимно прост с m. Выберем в $\bar{a}$ число a. Так как по условию числа a и m взаимно просты, $(a, m) = 1$, то найдутся такие числа x и y, что $ax + my = 1$ (см. п. 3 § 2 главы I). Но тогда $ax - 1 = -my$ делится на m, и потому $ax \equiv 1 \pmod{m}$. Из этого равенства следует, что $\bar{a}\bar{x} = \bar{1}$, где $\bar{x}$ — класс вычетов, содержащий x. Это и значит, что $\bar{a}$ — обратимый элемент в $\mathbf{Z}_m$.

Обратно, пусть $\bar{a}$ — класс вычетов по m, являющийся обратимым в $\mathbf{Z}_m$. Тогда существует такой класс вычетов $\bar{x}$ по m, что $\bar{a}\bar{x} =$

$= 1$. Выберем в $\bar{a}$ элемент a, а в $\bar{x}$ элемент x. Тогда $ax \equiv 1 \pmod{m}$, т. е. $(ax - 1) \vdots m$, или $ax - 1 = my$, $y \in \mathbf{Z}$. Из этого равенства следует, что наибольший общий делитель a и m равен 1, т. е. что $(a, m) = 1$. А тогда a и m взаимно просты. Теорема доказана.

Обозначим через Γ_m множество классов вычетов по m, взаимно простых с m. Из теоремы 1 вытекает, что это множество совпадает с множеством обратимых элементов в $\mathbf{Z}_m$, а потому образует группу относительно умножения. Ее называют *мультипликативной группой обратимых элементов в* $\mathbf{Z}_m$.

Из того, что множество Γ_m образует группу, вытекают следующие утверждения:

1) *Если* $\bar{a}$ *и* $\bar{b}$ *— классы вычетов по модулю* m, *взаимно простые с* m, *то* $\bar{a}\bar{b}$ *тоже класс вычетов, взаимно простой с* m (*если* $\bar{a} \in \Gamma_m$, $\bar{b} \in \Gamma_m$, *то* $\bar{a}\bar{b} \in \Gamma_m$).

2) *Если* $\bar{a}$ *— класс вычетов по модулю* m, *взаимно простой с* m, *то существует единственный класс вычетов* $\bar{b}$ *по модулю* m, *такой, что* $\bar{a}\bar{b} = \bar{1}$. *Этот класс вычетов тоже взаимно прост с* m. Мы будем называть его *обратным к* $\bar{a}$ и обозначать $\bar{a}^{-1}$.

3) *Если* $\bar{a}$ *— любой класс вычетов по модулю* m, *взаимно простой с* m, *и* $\bar{x} \neq \bar{y}$ *— классы вычетов по модулю* m, *взаимно простые с* m, *то* $\bar{a}\bar{x} \neq \bar{a}\bar{y}$. В самом деле, если $\bar{a}\bar{x} = \bar{a}\bar{y}$, то $\bar{a}^{-1}\bar{a}\bar{x} = \bar{a}^{-1}\bar{a}\bar{y}$, т. е. $\bar{x} = \bar{y}$, вопреки предположению.

Из 3) вытекает следующее утверждение:

4) *Пусть группа* Γ_m *состоит из классов вычетов* $\bar{x}_1, \ldots, \bar{x}_k$ *и пусть* $\bar{a} \in \Gamma_m$. *Тогда классы вычетов* $\bar{a}\bar{x}_1, \ldots, \bar{a}\bar{x}_k$ *— это те же классы вычетов* $\bar{x}_1, \ldots, \bar{x}_k$, *но взятые, быть может, в ином порядке.*

В самом деле, по свойству 1 все классы вычетов $\bar{a}\bar{x}_1, \ldots, \bar{a}\bar{x}_k$ являются некоторыми из классов вычетов $\bar{x}_1, \ldots, \bar{x}_k$, т. е. принадлежат Γ_m. При этом если $\bar{x}_i \neq \bar{x}_j$, то по свойству 3 имеем: $\bar{a}\bar{x}_i \neq \bar{a}\bar{x}_j$. Так как количество классов вычетов $\bar{a}\bar{x}_1, \ldots, \bar{a}\bar{x}_k$ тоже равно k, то множества $\{\bar{a}\bar{x}_1, \ldots, \bar{a}\bar{x}_k\}$ и $\{\bar{x}_1, \ldots, \bar{x}_k\}$ совпадают.

Утверждения 2 и 4 могут быть сформулированы на языке приведенной системы вычетов:

2′) Для каждого числа a из приведенной системы вычетов по модулю m найдется такое число b из такой же системы вычетов, что $ab \equiv 1 \pmod{m}$.

4′) Если $x_1, \ldots, x_k$ — приведенная система вычетов по модулю m и a взаимно просто с m, то числа $ax_1, \ldots, ax_k$ тоже образуют приведенную систему вычетов по модулю m.

Пример.

Рассмотрим приведенную систему вычетов по модулю 12. Она состоит из чисел 1, 5, 7 и 11. Составим таблицу умножения для

этих вычетов, выполняя каждый раз приведение произведения по модулю 12. Получаем:

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Мы видим, что в каждой строке этой таблицы стоят те же числа 1, 5, 7 и 11, взятые в ином порядке. Но строки эти и состоят из произведений вида ax_l, где x_l пробегает приведенную систему вычетов $\{1, 5, 7, 11\}$ по модулю 12.

Теорема 4. *Для того чтобы кольцо вычетов* $\mathbf{Z}_m$ *было полем, необходимо и достаточно, чтобы модуль* m *был простым числом. Если* m *— составное число, то в* $\mathbf{Z}_m$ *есть делители нуля.*

Доказательство. Пусть модуль m — простое число. Тогда все классы вычетов $\overline{1}, \overline{2}, \ldots, \overline{m-1}$ взаимно просты с m и потому обратимы. Это означает, что для любого из этих классов вычетов $\overline{a}$ есть обратный ему класс вычетов $\overline{b}$, такой, что $\overline{ab} = \overline{1}$. Но кольцо, в котором любой, отличный от нуля элемент имеет обратный, называется полем. Значит, $\mathbf{Z}_m$ — поле.

Покажем теперь, что если $m > 0$ — составное число, то $\mathbf{Z}_m$ не является полем. В самом деле, если m — составное число, то оно имеет делители k и l, каждый из которых по модулю меньше, чем m, $m = kl$, $|k| < m$, $|l| < m$. Но тогда классы вычетов $\overline{k}$ и $\overline{l}$ не являются нулевыми, в то время как $\overline{k}\,\overline{l} = \overline{kl} = \overline{m} = \overline{0}$. Значит, в $\mathbf{Z}_m$ есть делители нуля, а потому $\mathbf{Z}_m$ не является полем. Теорема доказана.

Теорема 5. *Если наибольший общий делитель модуля* m *и класса вычетов* $\overline{a} \neq \overline{0}$ *по* m *отличен от* 1, *то* $\overline{a}$ *является делителем нуля в кольце вычетов* $\mathbf{Z}_m$.

Доказательство. Выберем в $\overline{a}$ число a. По условию $(a, m) = d \neq 1$. Поэтому $a = dl$, $m = dn$. При этом $0 < d < m$, и потому $\overline{d}$ не является нулевым классом вычетов, $\overline{d} \neq \overline{0}$. Из равенства $an = dln = ldn = lm$ следует, что an делится на m, а потому $\overline{ad} = \overline{0}$, в то время как $\overline{d} \neq \overline{0}$. Это и показывает, что $\overline{a}$ — делитель нуля в $\mathbf{Z}_m$.

Следствие. *Любой класс вычетов* $\overline{a}$ *в* $\mathbf{Z}_m$ *является либо нулевым, либо делителем нуля, либо обратим в* $\mathbf{Z}_m$.

Доказательство. Класс вычетов $\overline{a} \neq \overline{0}$ либо взаимно прост с m, либо не является взаимно простым с m. В первом случае $\overline{a}$ обратим, а во втором — делитель нуля в $\mathbf{Z}_m$.

Вопросы для самопроверки и упражнения

1. Сформулируйте основные свойства приведенной системы вычетов по модулю m.

2. Найдите приведенную систему наименьших неотрицательных вычетов по модулю 40.

3. Какими элементами отличается приведенная система вычетов по простому модулю p от полной системы вычетов по этому модулю?

4. Напишите приведенную систему наименьших неотрицательных вычетов и произвольную систему вычетов по модулю 12.

5. Составьте таблицу умножения для группы Γ_{24} обратимых элементов по модулю 24. Пользуясь этой таблицей, найдите обратный класс для $\overline{7}$.

6. Составьте таблицу значений функции $y = 2x$, если x пробегает множество обратимых классов вычетов по модулю 9.

7. Является ли класс вычетов $\overline{6}$ по модулю 15 обратимым? а класс вычетов $\overline{8}$? Найдите класс, обратный классу $\overline{8}$ по модулю 15.

8. Какие классы вычетов обратимы по модулю 19? Какие классы вычетов обратимы по модулю 14?

9. Может ли произведение двух необратимых классов вычетов оказаться обратимым? а произведение обратимого класса вычетов на необратимый класс вычетов?

10. Какие из колец $\mathbf{Z}_5$, $\mathbf{Z}_8$, $\mathbf{Z}_{11}$, $\mathbf{Z}_{20}$ являются полями?

§ 4. ФУНКЦИЯ ЭЙЛЕРА. ТЕОРЕМЫ ЭЙЛЕРА И ФЕРМА

1. Функция Эйлера. Обозначим через $\varphi(m)$ число классов вычетов по модулю m, взаимно простых с m, т. е. число элементов приведенной системы вычетов по модулю m. Функция $\varphi(m)$ является числовой. Ее называют *функцией Эйлера*.

Выберем в качестве представителей классов вычетов по модулю m числа $1, \ldots, m-1, m$. Тогда $\varphi(m)$ — количество таких чисел, взаимно простых с m. Иными словами, $\varphi(m)$ — *количество положительных чисел, не превосходящих m и взаимно простых с m.*

Примеры.

1. Пусть $m = 9$. Полная система вычетов по модулю 9 состоит из чисел 1, 2, 3, 4, 5, 6, 7, 8, 9. Из них взаимно просты с 9 числа 1, 2, 4, 5, 7, 8. Так как количество этих чисел равно 6, то $\varphi(9) = 6$.

2. Пусть $m = 12$. Полная система вычетов состоит из чисел 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12. Из них взаимно просты с 12 числа 1, 5, 7, 11. Значит, $\varphi(12) = 4$.

При $m = 1$ полная система вычетов состоит из одного класса $\overline{1}$. Общим натуральным делителем чисел 1 и 1 является 1, $(1, 1) = 1$. На этом основании полагают $\varphi(1) = 1$.

Перейдем к вычислению функции Эйлера.

1) Если $m = p$ — простое число, то $\varphi(p) = p - 1$.

Доказательство. Вычеты $1, 2, \ldots, p-1$ и только они взаимно просты с простым числом p. Поэтому $\varphi(p) = p - 1$.

2) Если $m = p^k$ — степень простого числа p, то

$$\varphi(m) = p^{k-1}(p-1). \tag{1}$$

Доказательство. Полная система вычетов по модулю $m = p^k$ состоит из p^k чисел $1, \ldots, p^k - 1, p^k$. Натуральные делители m являются степенями p. Поэтому число a может иметь общий делитель с m, отличный от 1, лишь в случае, когда a делится на p. Но среди чисел $1, \ldots, p^k - 1$ на p делятся лишь числа $p, 2p, \ldots, p^2, \ldots p^k$, количество которых равно $p^k : p = p^{k-1}$. Значит, взаимно просты с $m = p^k$ остальные $p^k - p^{k-1} = p^{k-1}(p-1)$ чисел. Тем самым доказано, что $\varphi(p^k) = p^{k-1}(p-1)$.

Теорема 1. *Функция Эйлера мультипликативна, т. е. для взаимно простых чисел m и n* имеем $\varphi(mn) = \varphi(m)\varphi(n)$.

Доказательство. Первое требование в определении мультипликативной функции выполняется тривиальным образом: функция Эйлера определена для всех натуральных чисел, причем $\varphi(1) = 1$. Нам надо лишь показать, что если m и n взаимно простые числа, то

$$\varphi(mn) = \varphi(m)\varphi(n). \tag{2}$$

Расположим полную систему вычетов по модулю mn в виде $n \times m$ — матрицы

$$\begin{array}{ccccc} 1 & 2 & & & m \\ m+1 & m+2 & & & 2m \\ \cdot\cdot\cdot & \cdot\cdot\cdot & & & \cdot\cdot\cdot \\ (n-1)m+1 & (n-1)m+2 & & & nm \end{array}$$

(см. с. 110). Поскольку m и n взаимно просты, то число взаимно просто с mn тогда и только тогда, когда x взаимно просто с m и x взаимно просто с n (см. теорему 5 § 3 главы I). Но число $km + t$ взаимно просто с m в том и только том случае, когда t взаимно просто с m. Поэтому числа, взаимно простые с m, располагаются в тех столбцах, для которых t пробегает приведенную систему вычетов по модулю m. Число таких столбцов равно $\varphi(m)$. В каждом столбце представлена полная система вычетов по модулю n (см. лемму из п. 3 § 2). Из этих вычетов $\varphi(n)$ взаимно просты с n. Значит, общее количество чисел, взаимно простых и с m и с n, равно $\varphi(m)\varphi(n)$ ($\varphi(m)$ столбцов, в каждом из которых берется $\varphi(n)$ чисел). Эти числа, и только они, взаимно просты с mn. Тем самым доказано, что $\varphi(mn) = \varphi(m)\varphi(n)$.

Теперь мы можем вычислить значение функции Эйлера $\varphi(m)$, зная каноническое представление числа m:

$$m = p_1^{\alpha_1} \ldots p_k^{\alpha_k}.$$

В силу мультипликативности $\varphi(m)$ имеем:

$$\varphi(m) = \varphi(p_1^{\alpha_1}) \ldots \varphi(p_k^{\alpha_k}).$$

Но по формуле (1) получаем, что $\varphi(p_j^{\alpha_j}) = p_j^{\alpha_j - 1}(p_j - 1)$, и потому

$$\varphi(m) = p_1^{\alpha_1 - 1} \ldots p_k^{\alpha_k - 1}(p_1 - 1) \ldots (p_k - 1). \qquad (3)$$

Равенство (3) можно переписать в виде:

$$\varphi(m) = p_1^{\alpha_1} \ldots p_k^{\alpha_k}\left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_k}\right).$$

Поскольку $p_1^{\alpha_1} \ldots p_k^{\alpha_k} = m$, то

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_k}\right). \qquad (4)$$

Формула (3) или, что то же самое, (4) и является искомой.

Примеры.

1. Так как $288 = 2^5 \cdot 3^2$, то

$$\varphi(288) = 288\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 96.$$

2. Так как $30 = 2 \cdot 3 \cdot 5$, то

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

2. Тождество Гаусса. Для функции Эйлера имеет место тождество:

$$\sum_{d/n} \varphi(d) = n, \qquad (1)$$

где суммирование в левой части равенства распространено на все делители d числа n. Его называют *тождеством Гаусса*.

Чтобы доказать это тождество, применим к $\varphi(n)$ общее тождество для мультипликативных числовых функций:

$$\sum_{d/n} \varphi(d) = (1 + \varphi(p_1) + \ldots + \varphi(p_1^{k_1})) \ldots (1 + \varphi(p_m) + \ldots + \varphi(p_m^{k_m})), \qquad (2)$$

где $n = p_1^{k_1} \ldots p_m^{k_m}$ (см. теорему 4 п. 2 § 6 главы I).

Так как $\varphi(p_1) = p_1 - 1$, $\varphi(p_1^2) = p_1^2 - p_1$, ..., $\varphi(p_1^{k_1}) = p_1^{k_1} - p_1^{k_1 - 1}$, то

$$1 + \varphi(p_1) + \ldots + \varphi(p_1^{k_1}) = 1 + p_1 - 1 + p_1^2 - p_1 + \\ + \ldots + p_1^{k_1} - p_1^{k_1 - 1}.$$

Ясно, что все слагаемые, кроме $p_1^{k_1}$, взаимно уничтожаются, и потому

$$1 + \varphi(p_1) + \ldots + \varphi(p_1^{k_1}) = p_1^{k_1}.$$

Аналогично вычисляем остальные скобки в правой части тождества (2) и получаем:

$$\sum_{d/n} \varphi(d) = p_1^{k_1} \ldots p_m^{k_m} = n.$$

Тождество Гаусса доказано.

3. Теоремы Эйлера и Ферма. Вернемся к изучению группы Γ_m делителей единицы в кольце вычетов $\mathbf{Z}_m$. Эта группа коммутативна и содержит $\varphi(m)$ элементов. Любой элемент $\bar{a}$ группы Γ_m порождает циклическую подгруппу, порядок s которой по теореме Лагранжа («Алгебра», с. 43) является делителем числа $\varphi(m)$, $\varphi(m) = st$ (число s называют *порядком* класса $\bar{a}$). Так как $\bar{a}^s = \bar{1}$, то $\bar{a}^{\varphi(m)} = \bar{a}^{st} = (\bar{a}^s)^t = \bar{1}^t = \bar{1}$. Для любого класса вычетов $\bar{a} \in \Gamma_m$ выполняется равенство $\bar{a}^{\varphi(m)} = \bar{1}$.

Обычно это утверждение формулируется на языке сравнений: вместо равенства $\bar{a}^{\varphi(m)} = \bar{1}$ пишут сравнение $a^{\varphi(m)} \equiv 1 \pmod m$. Итак, мы доказали следующую теорему:

Теорема 2 (Эйлера). *Если a — такое число, что $(a, m) = 1$, то*

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

Пример.

Пусть $a = 2$, $m = 9$. Тогда $\varphi(m) = 6$, и по теореме Эйлера получаем: $2^6 \equiv 1 \pmod 9$. В справедливости этого равенства легко убедиться, если учесть, что $2^6 = 64$.

Особенно простой вид теорема Эйлера принимает, если $m = p$ — простое число. В этом случае $\varphi(p) = p - 1$, а потому получаем следующее утверждение:

Теорема 3 (малая теорема Ферма). *Если p — простое число и a — целое число, такое, что $(a, p) = 1$, то*

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

Часто используется следствие малой теоремы Ферма. Если p — простое число, то для любого целого числа a имеет место сравнение:

$$a^p \equiv a \pmod p.$$

Доказательство. а) Если $(a, p) = 1$, то согласно теореме Ферма $a^{p-1} \equiv 1 \pmod p$. После умножения обеих частей этого равенства на a, получим: $a^p \equiv a \pmod p$.

б) Если $(a, p) \neq 1$, то a делится на p. Но тогда и произведение $a(a^{p-1} - 1) = a^p - a$ тоже делится на p, т. е. $a^p - a \equiv 0 \pmod p$, или $a^p \equiv a \pmod p$.

Итак, для любого целого числа a имеем:

$$a^p \equiv a \pmod p.$$

Рассмотрим примеры на применение теорем Эйлера и Ферма.

1. Найдем остаток от деления 3^{28} на 7.

Согласно теореме Ферма $3^6 \equiv 1 \pmod 7$, тогда $3^2 \equiv 1 \pmod 7$.

Кроме того, $3^4 \equiv 81 \equiv 4 \pmod 7$.

Тогда $3^{28} \equiv 4 \pmod 7$. Следовательно, искомый остаток $r = 4$.

2. Найдем остаток от деления 243^{13} на 34.

Имеем: $243 \equiv 5 \pmod{34}$. Тогда $243^{132} \equiv 5^{132} \pmod{34}$. Согласно теореме Эйлера $5^{\varphi(34)} \equiv 1 \pmod{34}$, или $5^{16} \equiv 1 \pmod{34}$. Далее делим 132 на 16: $132 = 16 \cdot 8 + 4$. Тогда $243^{132} \equiv 5^{132} \equiv 5^{16 \cdot 8 + 4} \equiv (5^{16})^8 \cdot 5^4 \equiv 625 \equiv 13 \pmod{34}$. Таким образом, $243^{132} \equiv 13 \pmod{34}$.

Следовательно, $r = 13$.

Вопросы для самопроверки и упражнения

1. Дайте определение функции Эйлера. Что означает символ $\varphi(m)$?

2. Какими основными свойствами обладает функция Эйлера?

3. Напишите выражение для $\varphi(m)$ по каноническому разложению числа m. Вычислите, пользуясь этим выражением, $\varphi(144)$, $\varphi(2000)$, $\varphi(168)$.

4. Выпишите все классы вычетов по модулю 20 и найдите число классов вычетов, взаимно простых с 20. Сравните ответ с полученным по формуле Эйлера.

5. Напишите тождество Гаусса.

6. Чему равна сумма:

$$\varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) + \varphi(9) + \varphi(18)?$$

7. Сформулируйте теоремы Эйлера и Ферма. На основании какой теоремы о конечных группах доказывается теорема Эйлера?

8. Найдите количество натуральных чисел, не превосходящих x и взаимно простых с n, если: а) $x = 1000$; $n = 363$; б) $x = 2429$; $n = 568$; в) $x = 12\,317$; $n = 1575$.

9. Сколько натуральных чисел, не превосходящих 120 и взаимно простых с 30?

10. Сколько существует положительных правильных несократимых дробей вида $\frac{a}{b}$ при заданном b?

11. Найдите число всех положительных правильных несократимых дробей $\frac{a}{b}$ со знаменателями $b = 2, 3, 4, 5, 6, 7, 8, 9, 10$.

12. Докажите, что если d делитель n, то число натуральных чисел, не превосходящих n и имеющих с n наибольшим общим делителем число d, равно $\varphi\left(\frac{n}{d}\right)$. Пользуясь этим утверждением, найдите количество натуральных чисел, меньших числа n и имеющих с ним наибольшим общим делителем число d, если: а) $n = 300$, $d = 20$; б) $n = 450$, $d = 15$; в) $n = 1665$, $d = 37$; г) $n = 1476$, $d = 41$.

13. Докажите, что если:

а) $n = mp$, где $(m, p) = p$ и p — простое число, то $\varphi(n) = \varphi(mp) = \varphi(m) \cdot p$;

б) $n = mq$, где $(m, q) = 1$ и q — простое число, то $\varphi(n) = \varphi(mq) = \varphi(m)(q - 1)$.

14. Докажите, что $\varphi(4n) = 2 \cdot \varphi(2n)$ и $\varphi(4n + 2) = \varphi(2n+1)$.

15. Дано: а) $\varphi(11^n) = 13\,310$; б) $\varphi(7^n) = 705\,894$. Найдите n.

16. Дано, что $\varphi(n) = 1792$ и $n = 2^\alpha \cdot 5^\beta \cdot 13^\gamma$. Найдите n.

17. Найдите натуральное число x из условия: а) $\varphi(2x) = \varphi(3x)$; б) $\varphi(5x) = \varphi(7x)$.

18. При каком натуральном n имеют место равенства: а) $\varphi(n) = \frac{1}{2} n$; б) $\varphi(n) = \frac{1}{3} n$?

19. Докажите, что для натурального числа n равенство $\varphi(n) = \frac{1}{4} n$ невозможно.

20. Тождество $\sum_{d/n} \varphi(d) = n$ проверьте на примерах: $n = 40$, 100, 320, 1240.

21. Составьте таблицу значений функции $\varphi(n)$ для всех $n = 1, 2, \ldots, 50$, пользуясь только формулой $\varphi(p^\alpha) = p^{\alpha-1}(p - 1)$ и тем, что $\varphi(n)$ — мультипликативная функция.

22. Покажите, что сумма (S) чисел, взаимно простых с числом n и меньших n, вычисляется по формуле:

$$S = \frac{1}{2} m \cdot \varphi(m).$$

23. Проверьте формулы: $5^{\varphi(26)} \equiv 1 \pmod{26}$; $2^{\varphi(45)} \equiv 1 \pmod{45}$; $3^{\varphi(40)} \equiv 1 \pmod{40}$.

24. Пользуясь теоремами Эйлера и Ферма, найдите остаток от деления: а) 3^{78} на 11; б) 4^{93} на 13; в) 46^{921} на 21; г) 327^{8493} на 29; д) 473^{569} на 45.

25. Пользуясь теоремой Эйлера, найдите последнюю цифру в десятичном представлении чисел:

а) 3^{100}; б) 13^{219}; в) 17^{500}; г) 243^{402}; д) 473^{1971}.

26. Найдите последние две цифры в десятичном представлении чисел предыдущей задачи.

27. Докажите, что квадрат всякого нечетного числа сравним с единицей по модулю 8.

28. Докажите, что нечетное число вида $4k + 3$ нельзя представить как сумму двух квадратов целых чисел.

29. Покажите, что если $(n, 6) = 1$, то $n^2 \equiv 1 \pmod{24}$.

30. Пользуясь малой теоремой Ферма, докажите, что p и $8p^2 - 1$ могут быть одновременно простыми только при $p = 3$.

31. Докажите, что при любом целом x имеет место сравнение: $x^7 \equiv x \pmod{42}$.

32. Докажите, что при любом целом x имеют место сравнения:

а) $x^{561} \equiv x \pmod{11}$; б) $x^{13} \equiv x \pmod{2730}$.

33. Исходя из разложения по биному Ньютона для $(a + b)^p$,

докажите, что $(a+b)^p \equiv a^p + b^p \pmod{p}$. Обобщая этот результат для случая трех и т. д. чисел, выведите малую теорему Ферма.

34. Докажите, что натуральное число p тогда и только тогда является простым, когда

$$C_{p-1}^k \equiv (-1)^k \pmod{p},$$

где C_{p-1}^k — всевозможные биномиальные коэффициенты в разложении $(a+b)^{p-1}$ $(k = 0, 1, 2, \ldots, p-1)$.

§ 5. РЕШЕНИЕ СРАВНЕНИЙ

1. Корни сравнений. Пусть m — целое число и

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n —$$

многочлен с целыми коэффициентами $a_0, a_1, \ldots, a_n$. Если подставить вместо x целые числа, значения многочлена $f(x)$ тоже будут целыми числами.

Определение 1. Пусть $f(x) = a_0x^n + \ldots + a_n$, $\varphi(x) = b_0x^k + \ldots + b_k$ — многочлены с целыми коэффициентами $a_0, \ldots, a_n, b_0, \ldots, b_k$. *Решить сравнение* $f(x) \equiv \varphi(x) \pmod{m}$ — значит найти все целые числа x, при подстановке которых в многочлены $f(x)$ и $\varphi(x)$ получаются целые числа, разность которых делится на m. Если $f(c) \equiv \varphi(c) \pmod{m}$, то говорят, что целое число c удовлетворяет сравнению $f(x) \equiv \varphi(x) \pmod{m}$, или, иначе, является *корнем* этого сравнения.

Теорема 1. *Если число c удовлетворяет сравнению*

$$f(x) \equiv \varphi(x) \pmod{m}, \qquad (1)$$

то и любое число c_1, такое, что $c \equiv c_1 \pmod{m}$, удовлетворяет тому же сравнению.

Доказательство. Так как c удовлетворяет сравнению (1), то $f(c) \equiv \varphi(c) \pmod{m}$, т. е. $f(c) - \varphi(c) \equiv 0 \pmod{m}$. Но так как $c \equiv c_1 \pmod{m}$, то по свойству 10 сравнений (см. п. 2 § 1) и $f(c_1) \equiv \varphi(c_1) \pmod{m}$. Теорема доказана.

Из доказанной теоремы вытекает, что если целое число c удовлетворяет сравнению $f(x) \equiv 0 \pmod{m}$, то и все числа из содержащего c класса вычетов c по модулю m удовлетворяют тому же сравнению. Поэтому задача о решении сравнений может быть поставлена иначе:

Определение 1′. *Решить сравнение*:

$$f(x) \equiv \varphi(x) \pmod{m},$$

где $f(x)$ и $\varphi(x)$ — многочлены с целыми коэффициентами — значит найти все классы вычетов по модулю m, любое число из которых удовлетворяет сравнению (1) (т. е. при подстановке в (1) любого числа из этих классов вычетов получаются числа, сравнимые по модулю m).

Из определения 1′ вытекает, что любое сравнение вида (1) можно решить, сделав m проб, а именно, подставив в $f(x)$ и $\varphi(x)$ вместо x по очереди все числа из полной системы вычетов по модулю m

(например, числа 0, 1, ..., $m-1$). После этого надо вычислить значения $f(c)$ и $\varphi(c)$ и отобрать те, для которых $f(c) - \varphi(c)$ делится на m.

Примеры.

1. Решим сравнение:

$$f(x) = x^3 - 3 \equiv 0 \pmod 6. \qquad (2)$$

Надо подставить вместо x числа 0, 1, 2, 3, 4, 5. Так как $f(0) = -3$, а -3 не делится на 6, то 0 не удовлетворяет сравнению (2). Далее находим:

$$f(1) = -2,\ f(2) = 5,\ f(3) = 24,\ f(4) = 61,\ f(5) = 122.$$

Только $f(3) = 24$ делится на 6. Значит, решением сравнения (2) является класс вычетов $\overline{3} = \{\ldots -9, -3, 3, 9 \ldots\}$.

Разумеется, вместо чисел 0, 1, 2, 3, 4, 5 можно было подставить числа, образующие иную полную систему вычетов по модулю 6, например числа $-2, -1, 0, 1, 2, 3$.

Существуют сравнения, совсем не имеющие решений.

2. Решим сравнение:

$$x^4 + 2x - 1 \equiv 0 \pmod 7.$$

Ни один из вычетов полной системы абсолютно наименьших вычетов 0, 1, 2, 3, -3, -2, -1 по модулю 7 не удовлетворяет данному сравнению (читателю предлагается убедиться в этом самостоятельно). Следовательно, сравнение решений не имеет.

С теоретической точки зрения задача решения сравнений вида $f(x) \equiv 0 \pmod m$ очень проста: мы просто ищем решения в конечном множестве классов (m классов) по модулю m, что достигается, как мы уже установили, путем конечного числа испытаний вычетов некоторой полной системы вычетов по модулю m. Однако на практике указанный прием испытания вычетов при больших модулях оказывается затруднительным, так как приводит к большому количеству испытаний. Например, для решения сравнения $19x^3 + 13x^2 - 2x + 17 \equiv 0 \pmod{625}$, следуя указанному приему решения сравнений, надо проверить 625 вычетов.

Естественно возникает вопрос: нельзя ли упростить работу и свести ее к выполнению меньшего числа операций? Оказывается, можно. Существуют способы, позволяющие найти число решений сравнения, а в ряде случаев и найти все решения значительно быстрее.

2. Равносильность сравнений с одним неизвестным.

Определение 2. Два сравнения:

$$f_1(x) \equiv \varphi_1(x) \pmod m \text{ и } f_2(x) \equiv \varphi_2(x) \pmod m$$

называются *равносильными*, если множество чисел, удовлетворяющих одному из них, совпадает с множеством чисел, удовлетворяющих другому сравнению.

Очевидно, что сравнение $f(x) \equiv \varphi(x) \pmod m$ равносильно сравнению $f(x) - \varphi(x) \equiv 0 \pmod m$. Поэтому в дальнейшем мы ограничимся сравнениями вида $f(x) \equiv 0 \pmod m$.

Теорема 2. *Если в сравнении* $f(x) = a_0x^n + a_1x^{n-1} \ldots + a_{n-1}x + a_n \equiv 0 \pmod m$ *коэффициенты* $a_0, a_1, \ldots a_n$ *заменить числами, сравнимыми с ними по модулю* m, *то полученное сравнение*

$$f_1(x) = b_0x^n + b_1x^{n-1} + \ldots + b_n \equiv 0 \pmod m$$

будет равносильно данному.

Доказательство. Пусть $a_0 \equiv b_0 \pmod m$, $a_1 \equiv b_1 \pmod m$, ..., $a_n \equiv b_n \pmod m$. Умножим эти сравнения соответственно на α^n, α^{n-1}, ..., $\alpha^0 = 1$, где α — какое-нибудь целое число; получим:

$$a_0\alpha^n \equiv b_0\alpha^n \pmod m,\ a_1\alpha^{n-1} \equiv b_1\alpha^{n-1} \pmod m, \ldots,$$
$$a_n \equiv b_n \pmod m.$$

Складывая последние сравнения почленно, получим:

$$a_0\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha + a_n \equiv b_0\alpha^n + b_1\alpha^{n-1} + \ldots + b_{n-1}\alpha + b_n \pmod m,$$

или, кратко, $f(\alpha) \equiv f_1(\alpha) \pmod m$.

Обе части полученного сравнения могут быть сравнимы с нулем по модулю m лишь одновременно, а это означает, что сравнения $f(x) \equiv 0 \pmod m$ и $f_1(x) \equiv 0 \pmod m$ равносильны.

Из теоремы 2 вытекает, что все коэффициенты сравнения

$$a_0x^n + \ldots + a_n \equiv 0 \pmod m,$$

делящиеся на m, можно заменить нулями и опустить соответствующие члены сравнения.

Определение 3. *Степенью сравнения*

$$a_0x^n + \ldots + a_n \equiv 0 \pmod m$$

называют наивысший показатель степени, коэффициент при котором не делится на m.

Примеры. Найдем степени сравнений:

1) Сравнение $2x^3 - 3x + 4 \equiv 0 \pmod 5$ имеет степень $n = 3$, так как 2 не делится на 5, т. е. $2 \not\equiv 0 \pmod 5$.

2) Сравнение $9x^3 + 2x^2 - x + 1 \equiv 0 \pmod 3$ имеет степень $n = 2$, так как $9 \equiv 0 \pmod 3$, а $2 \not\equiv 0 \pmod 3$.

3) Сравнение $16x^5 + 12x^4 - 3x^3 - x + 3 \equiv 0 \pmod 4$ имеет степень $n = 3$, так как $16 \equiv 0 \pmod 4$, $12 \equiv 0 \pmod 4$, а $-3 \not\equiv 0 \pmod 4$.

Сравнение, у которого все коэффициенты делятся на модуль m, рассматривается как не имеющее степени. Такому сравнению удовлетворяет любое целое число.

Пример. Сравнение $28x^2 + 7x + 14 \equiv 0 \pmod 7$ степени не имеет (все его коэффициенты кратны модулю 7). Ему удовлетворяет любое целое число, так как при любом целом x левая часть делится на 7.

Теорема 2 позволяет производить упрощение сравнений: все коэффициенты сравнения $f(x) \equiv 0 \pmod m$ можно заменить соответствующими вычетами, обычно наименьшими неотрицательными или абсолютно наименьшими вычетами по модулю m.

Пример. Решим сравнение

$$21x^3 + 17x^2 + 9x + 30 \equiv 0 \pmod 7,$$

$21 \equiv 0$; $17 \equiv 3$; $9 \equiv 2$; $30 \equiv 2$ по модулю 7

Данное сравнение можно заменить более простым равносильным ему сравнением

$$3x^2 + 2x + 2 \equiv 0 \pmod 7.$$

Проверяя теперь вычеты полной системы абсолютно наименьших вычетов 0, 1, 2, 3, —3, —2, —1, находим решения данного сравнения: классы $x \equiv 1 \pmod 7$ и $x \equiv 3 \pmod 7$.

При решении сравнений, содержащих неизвестную величину, иногда приходится умножать обе части сравнения на одно и то же число. Однако такое преобразование не всегда приводит к равносильному сравнению.

Пример. Сравнение $2x^3 - x + 1 \equiv 0 \pmod 3$ имеет единственное решение: $x \equiv 2 \pmod 3$.

Умножив обе части данного сравнения, например, на 6, получим сравнение: $12x^3 - 6x + 6 \equiv 0 \pmod 3$, которому удовлетворяет любое число. Таким образом, полученное при умножении на 6 сравнение оказалось не равносильно данному.

Выясним, в каких случаях умножение обеих частей сравнения, содержащего неизвестное, на одно и то же число приводит к равносильному сравнению.

Теорема 3. *Если обе части сравнения*

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \equiv 0 \pmod m \qquad (1)$$

умножить на целое число l, взаимно простое с модулем m, то полученное сравнение будет равносильно данному.

Доказательство. По условию $(l, m) = 1$.

Пусть $\bar{a}$ — какое-нибудь решение сравнения (1) и $\alpha \in \bar{a}$, тогда

$$f(\alpha) = a_0\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha + a_n \equiv 0 \pmod m. \qquad (2)$$

Умножим обе части сравнения (2) на l, получим:

$$lf(\alpha) = la_0\alpha^n + la_1\alpha^{n-1} + \ldots + la_{n-1}\alpha + la_n. \qquad (3)$$

Из (3) следует, что $\bar{a}$ является решением сравнения:

$$lf(x) = la_0x^n + la_1x^{n-1} + \ldots + la_{n-1}x + la_n \equiv 0 \pmod m. \qquad (4)$$

Обратно, пусть $\bar{a}$ — какое-нибудь решение сравнения (4) и $\alpha \in \bar{a}$, тогда будет иметь место сравнение (3). Но так как $(l, m) = 1$, то обе части сравнения (3) можно разделить на l; получим сравнение (2). Следовательно, $\bar{a}$ — решение сравнения (1). Теорема доказана.

Отметим также, что равносильные сравнения не обязательно должны иметь одну и ту же степень. Например, сравнения $3x - 1 \equiv 0 \pmod 5$ и $3x^3 + 4x^2 + x - 2 \equiv 0 \pmod 5$ равносильны, хотя и имеют разные степени.

Если модуль $m = p$ — простое число, то для понижения степени сравнения можно воспользоваться теоремой Ферма:

$$x^p \equiv x \pmod{p}.$$

Пример. Заменить сравнение:

$$2x^8 + 6x^7 - x^6 + 2x^5 + 3x^4 - x^3 + 4x^2 + 8x - 1 \equiv 0 \pmod 5$$

равносильным сравнением более низкой степени.

Так как $x^5 \equiv x \pmod 5$, то $x^6 \equiv x^2 \pmod 5$, $x^7 \equiv x^3 \pmod 5$, $x^8 \equiv x^4 \pmod 5$, и потому данное сравнение равносильно сравнению:

$$2x^4 + 6x^3 - x^2 + 2x + 3x^4 - x^3 + 4x^2 + 8x - 1 \equiv 0 \pmod 5,$$

т. е. сравнению:

$$5x^4 + 5x^3 + 3x^3 + 10x - 1 \equiv 0 \pmod 5,$$

или, что то же самое,

$$3x^2 - 1 \equiv 0 \pmod 5.$$

Некоторые свойства сравнений похожи на свойства уравнений. Но если, например, квадратное уравнение может иметь лишь два корня, сравнение второй степени может иметь и более двух решений. Например, сравнение:

$$x^2 \equiv 1 \pmod 8$$

имеет 4 решения: 1, 3, 5, 7.

Однако если модуль p — простое число, то имеет место следующее утверждение:

Теорема 4. *Пусть p — простое число. Тогда сравнение $a_0x^n + \ldots + a_n \equiv 0 \pmod p$ имеет не более n различных решений.*

Мы отложим доказательство этой теоремы до изучения в последней части курса «Алгебра и теория чисел» общей теории уравнений. Отметим лишь, что справедливость этой теоремы связана с тем, что кольцо вычетов $\mathbf{Z}_p$ по простому модулю является полем.

Следствие. *Если $p > 2$ — простое число, то единственными решениями сравнения*:

$$x^2 \equiv 1 \pmod p \qquad (5)$$

являются $x = 1$ и $x = p - 1$.

В самом деле, сравнение (5) может иметь лишь два решения, а $1^2 \equiv 1 \pmod p$ и $(p-1)^2 \equiv (-1)^2 \equiv 1 \pmod p$.

Доказанное утверждение означает, что среди классов вычетов $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ по простому модулю $p > 2$ лишь $\overline{1}$ и $\overline{p-1}$ удовлетворяют уравнению $\overline{x}^2 = \overline{1}$.

3. Теорема Вильсона. При решении многих вопросов теории чисел оказывается полезной следующая теорема, доказанная английским математиком Вильсоном.

Т е о р е м а (Вильсона). *Если p — простое число, то справедливо сравнение:*

$$(p-1)! \equiv -1 \pmod{p}. \tag{1}$$

Д о к а з а т е л ь с т в о. При $p = 2$ сравнение (1) справедливо, так как $(2-1)! = 1 \equiv -1 \pmod 2$. Пусть теперь $p > 2$. Так как p — простое число, то группа обратимых элементов Γ_p состоит из классов вычетов $\overline{1}, \overline{2}, \ldots, \overline{p-1}$. Каждый из этих классов вычетов имеет обратный. При этом лишь классы вычетов $\overline{1}$ и $\overline{p-1}$ обратны сами себе. В самом деле, если класс вычетов $\overline{x}$ обратен сам себе, то $\overline{x}^2 = \overline{1}$, а лишь классы $\overline{1}$ и $\overline{p-1}$ удовлетворяют этому уравнению.

Таким образом, в произведении $\overline{1} \cdot \overline{2} \cdot \ldots \cdot \overline{p-1}$ все множители, за исключением $\overline{1}$ и $\overline{p-1}$, разбиваются на пары взаимно обратных элементов, дающих в произведении $\overline{1}$. Значит, $\overline{1} \cdot \overline{2} \cdot \ldots \cdot \overline{(p-1)} = \overline{1} \cdot \overline{(p-1)} = \overline{p-1}$.

Иными словами,

$$1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv p-1 \equiv -1 \pmod{p}.$$

Теорема доказана.

С л е д с т в и е. *Если p — простое число, то*

$$(p-2)! \equiv 1 \pmod{p}. \tag{2}$$

В самом деле, сравнение (1) можно переписать так:

$$(p-1)! \equiv -1 \equiv p-1 \pmod{p}.$$

Поскольку $(p-1, p) = 1$, то обе части этого сравнения можно сократить на $p-1$. Получаем сравнение (2).

П р и м е р. При $p = 7$ получаем:

$$(7-1)! = 720 \equiv -1 \pmod 7.$$

Заметим, что справедлива и теорема, обратная теореме Вильсона:

Т е о р е м а. *Если $(n-1)! \equiv -1 \pmod{n}$, то n — простое число.*

Доказательство этой теоремы мы опускаем.

Вопросы для самопроверки и упражнения

1. Что называется сравнением n-й степени с неизвестной величиной?
2. Почему сравнение $f(x) \equiv 0 \pmod{m}$ имеет не более чем m решений? Почему при решении этого сравнения достаточно ограничиться испытанием чисел $0, 1, 2, \ldots, (m-1)$?
3. Какие сравнения называются равносильными?

4. Всегда ли при умножении обеих частей сравнения с неизвестной величиной на целое число получается равносильное сравнение?

5. Получим ли равносильное сравнение при умножении обеих частей сравнения и модуля на целое число?

6. Чему равна степень сравнения:

$$7x^6 + 14x^5 + 3x^2 - 6x + 1 \equiv 0 \pmod 7?$$

7. Может ли сравнение:

$$4x^5 + 2x^3 - 3x^2 + 1 \equiv 0 \pmod{41}$$

иметь 7 корней?

8. Упростите сравнение:

$$6x^9 - 5x^8 + 4x^7 + x^3 - 2x^2 + x - 3 \equiv 0 \pmod 7.$$

9. При помощи испытаний решите сравнения: а) $x^2 \equiv 3 \pmod{37}$; б) $x^5 - 5 \equiv 0 \pmod 7$; в) $x^5 - 7x^4 + 11x^3 - 5x + 1 \equiv 0 \pmod{12}$; г) $2^x \equiv x^2 \pmod 5$; д) $x^3 \equiv 31 \pmod{37}$; е) $x^7 + x^6 + 2x + 5 \equiv 0 \pmod{11}$.

10. Докажите, что если сравнение n-й степени $f(x) \equiv 0 \pmod p$ имеет n различных решений и $f(x)$ по модулю p раскладывается на два множителя $f_1(x)$ и $f_2(x)$ k-й и l-й степеней ($k + l = n$), т. е. тождественно

$$f(x) \equiv f_1(x) \cdot f_2(x) \pmod p,$$

то сравнение $f_1(x) \equiv 0 \pmod p$ имеет k различных решений, а сравнение $f_2(x) \equiv 0 \pmod p$ имеет l различных решений (p — простое число).

11. Докажите, что каждое из сравнений:

$$x^{\frac{p-1}{2}} \equiv 1 \pmod p \text{ и } x^{\frac{p-1}{2}} \equiv -1 \pmod p,$$

где p — простое число, $p > 2$, имеет ровно $\frac{p-1}{2}$ решений.

12. Выясните, имеют ли максимальное число различных решений сравнения:

а) $3x^3 - x^2 + 4x + 1 \equiv 0 \pmod 7$; б) $x^4 + x + 4 \equiv 0 \pmod{11}$; в) $x^3 - x^2 + 3x - 3 \equiv 0 \pmod{37}$.

13. Какому сравнению степени ниже 11 равносильно сравнение:

$$6x^{18} + 18x^{15} + 3x^4 - 8x^3 + x^2 + 3 \equiv 0 \pmod{11}.$$

14. Сведите сравнение:

$$5x^{24} + 4x^{23} + 2x^{21} + x^{20} + 6x^{19} + 4x^{18} + 3x^{17} + 4x^{16} + 6x^{15} + 5x^{14} + 2x^{13} + x^{12} + 2x^{11} + x^{10} + 3x^9 + 4x^8 + 2x^7 + 5x^6 + x + 6x^5 + 5x^4 + 3x^3 + 4x^2 + 4x + 2 \equiv 0 \pmod 7$$

к равносильному сравнению степени ниже 7 и затем решите его.

15. Сформулируйте теорему Вильсона.

16. Проверьте теорему Вильсона для $p = 11$ и $p = 17$.

17. Разбейте классы вычетов $\overline{2}, \ldots, \overline{p-2}$ на пары взаимно обратных при $p = 5, 7, 11$.

18. Пользуясь теоремой Вильсона, докажите, что сравнению:

$$x^2 \equiv -1 \pmod{p},\ p = 4n + 1$$

удовлетворяет число $(2n)!$ Например:

$$(6!)^2 \equiv -1 \pmod{13}.$$

19. Докажите, что для простого p и любого целого a имеет место сравнение:

$$a^p + (p-1)!\, a \equiv 0 \pmod{p}.$$

20. Докажите критерий (Лейбница) простоты данного числа: для того чтобы натуральное число $p > 2$ было простым, необходимо и достаточно, чтобы $(p-2)! - 1 \equiv 0 \pmod{p}$.

§ 6. СРАВНЕНИЯ ПЕРВОЙ СТЕПЕНИ С ОДНИМ НЕИЗВЕСТНЫМ

1. Решение сравнений первой степени. Любое сравнение первой степени с неизвестным x можно привести к виду:

$$ax \equiv b \pmod{m}, \quad \text{где } a \not\equiv 0 \pmod{m}. \tag{1}$$

Выясним условия, при которых сравнение (1) имеет единственное решение, несколько решений или не имеет ни одного решения.

Теорема 1. *Если* $(a, m) = 1$, *то сравнение* (1) *имеет решение и притом единственное.*

Доказательство. Рассмотрим какую-нибудь полную систему вычетов по модулю m:

$$x_1, x_2, \ldots, x_m. \tag{2}$$

По условию $(a, m) = 1$. Тогда согласно теореме 2 из п. 2 § 2 совокупность чисел:

$$ax_1 + 0,\ ax_2 + 0,\ \ldots,\ ax_m + 0 \text{ или } ax_1, ax_2, \ldots, ax_m$$

тоже полная система вычетов по модулю m. Таким образом, если в (1) вместо x подставлять последовательно все вычеты полной системы вычетов (2), то левая часть этого сравнения пробегает все значения полной системы вычетов. Но это означает, что для одного и только для одного x_i $(1 \leqslant i \leqslant m)$ число ax_i окажется в том же самом классе, к которому принадлежит число b; при этом

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

Итак, если $(a, m) = 1$, то сравнение (1) имеет и притом единственное решение

$$x \equiv x_i \pmod{m}, \text{ или } x \equiv x_i + mt,\ t \in \mathbf{Z}.$$

Решение сравнения (1) можно найти путем испытания полной системы абсолютно наименьших вычетов. Для нахождения решения сравнения (1) можно также воспользоваться следующей теоремой.

Теорема 2. *Если* $(a, m) = 1$, *то решением сравнения* $ax \equiv b \pmod m$ *является класс* $x \equiv ba^{\varphi(m)-1} \pmod m$.

Доказательство. По условию $(a, m) = 1$, тогда согласно теореме Эйлера $a^{\varphi(m)} \equiv 1 \pmod m$, откуда $a^{\varphi(m)}b \equiv b \pmod m$, или $a \cdot a^{\varphi(m)-1}b \equiv b \pmod m$. Сравнивая последнее сравнение с $ax \equiv b \pmod m$, находим, что класс $x \equiv ba^{\varphi(m)-1} \pmod m$ является решением сравнения $ax \equiv b \pmod m$, а согласно теореме 1 это решение единственно.

Пример. Решить сравнение $5x \equiv 3 \pmod 6$.

Так как $(5, 6) = 1$, то сравнение имеет единственное решение: $x \equiv 3 \cdot 5^{\varphi(6)-1} = 3 \cdot 5 = 15 \equiv 3 \pmod 6$; $x \equiv 3 \pmod 6$, так как $\varphi(6) = \varphi(3) \cdot \varphi(2) = 2 \cdot 1 = 2$.

Теперь рассмотрим случай, когда a и m не взаимно просты.

Теорема 3. *Если* $(a, m) = d > 1$ *и* b *не делится на* d, *то сравнение* $ax \equiv b \pmod m$ *решений не имеет.*

Доказательство. Допустим, что сравнение $ax \equiv b \pmod m$ имеет решение — класс $\overline{x_1}$ по модулю m и $x_1 \in \overline{x_1}$, тогда $ax_1 \equiv b \pmod m$, или $ax_1 - b = m \cdot t$.

В силу того что a делится на d и m делится на d, из последнего равенства следует, что и b делится на d. По условию же b не делится на d. Полученное противоречие доказывает теорему.

Пример. Решим сравнение $45x \equiv 31 \pmod{100}$. Так как $(45, 100) = 5$, 31 не делится на 5, то сравнение решений не имеет.

Теорема 4. *Если* $(a, m) = d > 1$ *и* b *делится на* d, *то сравнение*

$$ax \equiv b \pmod m \tag{3}$$

имеет d *различных решений. Все эти решения образуют один класс по модулю* $\frac{m}{d}$.

Доказательство. По условию каждое из чисел a, b и m делится на d. Положим, $a = a_1d$, $b = b_1d$, $m = m_1d$. Разделив обе части сравнения (3) и модуль на d, получим равносильное ему сравнение:

$$a_1x \equiv b_1 \pmod{m_1}. \tag{4}$$

Действительно, пусть $x = \alpha$ — целое число, удовлетворяющее сравнению (3); тогда $a\alpha \equiv b \pmod m$, а после деления обеих частей сравнения и модуля на α получим: $a_1\alpha \equiv b_1 \pmod{m_1}$. Следовательно, α удовлетворяет сравнению (4).

Обратно, пусть $x = \beta$ удовлетворяет сравнению (4), тогда $a_1\beta \equiv b_1 \pmod{m_1}$. Умножив обе части и модуль этого сравнения на d, получим $a\beta \equiv b \pmod m$. Значит, β удовлетворяет сравнению (3).

Таким образом, сравнения (3) и (4) равносильны.

В сравнении (4) $(a_1, m_1) = 1$, поэтому оно имеет единственное решение $x \equiv x_0 \pmod{m_1}$ или $x = x_0 + m_1 t$ (где x_0 — наименьший неотрицательный вычет по модулю m_1, а t — любое целое число), или

$$\ldots\ x_0 - 2m_1,\ x_0 - m_1,\ x_0,\ x_0 + m_1,\ x_0 + 2m_1,\ \ldots,\ x_0 + (d-1)\,m_1,\ x_0 + dm_1,\ \ldots \qquad (5)$$

Все вычеты из (5) и только они удовлетворяют сравнению (4) и равносильному ему сравнению (3).

По модулю $m_1 = \frac{m}{d}$ все числа из (5) принадлежат одному классу. По модулю же $m = m_1 d$ они будут принадлежать различным классам, вычетами которых являются:

$$x_0,\ x_0 + m_1,\ x_0 + 2m_1,\ \ldots,\ x_0 + (d-1)\,m_1. \qquad (6)$$

Следовательно, сравнение (3) имеет d различных решений по модулю m:

$$x \equiv x_0 \pmod{m},\ x \equiv x_0 + m_1 \pmod{m},\ x \equiv x_0 + 2m_1 \pmod{m},\ \ldots,$$
$$x \equiv x_0 + (d-1)\,m_1 \pmod{m},$$

где x_0 — наименьший неотрицательный вычет из класса — решения сравнения (4).

Примеры.

1. Решим сравнение: $3x \equiv 6 \pmod 9$. Так как $(3, 9) = 3$ и 6 делится на 3, то данное сравнение имеет три решения. Делим обе части и модуль данного сравнения на 3, получим: $x \equiv 2 \pmod 3$. Тогда решениями данного сравнения будут: $x \equiv 2 \pmod 9$, $x \equiv 2 + 3 = 5 \pmod 9$, $x \equiv 2 + 2 \cdot 3 = 8 \pmod 9$, т. е.

$$x \equiv 2,\ 5,\ 8 \pmod 9.$$

2. Решим сравнение: $51x \equiv 141 \pmod{234}$. Здесь $(51, 234) = 3$ и 141 делится на 3; следовательно, сравнение имеет три решения.

После деления обеих частей сравнения и модуля на 3 получим сравнение: $17x \equiv 47 \pmod{78}$.

Полученное сравнение имеет единственное решение, так как $(17, 78) = 1$. Его решением является: $x \equiv 67 \pmod{78}$.

Теперь легко найти решения заданного сравнения:

$$x \equiv 67 \pmod{234},\ x \equiv 67 + 78 = 145 \pmod{234},$$
$$x \equiv 67 + 2 \cdot 78 \equiv 223 \pmod{234},\ \text{т. е. } x \equiv 67,\ 145,\ 223 \pmod{234}.$$

2. Сравнения первой степени и неопределенные уравнения. Одно уравнение с несколькими неизвестными имеет, как правило, бесконечное множество решений. Поэтому такие уравнения называют *неопределенными*. В теории чисел рассматривают задачу об отыскании целочисленных решений неопределенных уравнений (такие уравнения решал древнегреческий математик Диофант и потому их называют еще *диофантовыми* уравнениями). Мы покажем сейчас, что отыскание целочисленных решений неопределенного уравнения первой степени

$$ax + by = c, \qquad (1)$$

где a, b, c — целые числа, тесно связано с решением сравнений.

Мы можем ограничиться рассмотрением случая, когда числа a и b отличны от нуля (если, например, $b = 0$, то уравнение (1) принимает вид $ax = c$).

Итак, пусть $a \neq 0$, $b \neq 0$ и (x_0, y_0) — одно из целочисленных решений уравнения $ax + by = c$. Тогда $ax_0 + by_0 = c$, и потому разность $ax_0 - c = -by_0$ делится на b, т. е. $ax_0 \equiv c \pmod{b}$.

Обратно, пусть x_0 — решение сравнения $ax \equiv c \pmod{b}$. Тогда $ax_0 \equiv c \pmod{b}$, т. е. $(ax_0 - c) \vdots b$. Это значит, что $ax_0 - c = -by_0$, где y_0 — целое число, т. е. что $ax_0 + by_0 = c$.

Иными словами, (x_0, y_0) — целочисленное решение уравнения $ax + by = c$.

Мы доказали следующее утверждение:

Теорема 5. *Если (x_0, y_0) — целочисленное решение неопределенного уравнения*

$$ax + by = c,$$

где a, b, c — целые числа и $a \neq 0$, $b \neq 0$, то x_0 — решение сравнения $ax_0 \equiv c \pmod{b}$.

Обратно, если x_0 — решение сравнения $ax_0 \equiv c \pmod{b}$, то существует такое целое число y_0, что (x_0, y_0) — решение неопределенного уравнения $ax + by = c$.

Теорема 5 позволяет свести решение неопределенных уравнений вида $ax + by = c$ к решению сравнений первой степени, и обратно. В частности, из полученных выше утверждений о сравнениях первой степени получаем следующую теорему:

Теорема 6. *Если $(a, b) = d$, то неопределенное уравнение $ax + by = c$ имеет целочисленное решение в том и только том случае, когда c делится на d.*

В частности, если $(a, b) = 1$, то уравнение $ax + by = c$ при любом целом c имеет целочисленное решение (см. теорему 4 п. 1).

Процесс нахождения целочисленных решений уравнений вида $ax + by = c$ распадается на два этапа: нахождение хотя бы одного такого решения и нахождение общего вида решений. Рассмотрим сначала второй этап.

Теорема 7. *Если известно частное целочисленное решение (x_0, y_0) неопределенного уравнения*

$$ax + by = c \tag{1}$$

и $(a, b) = d$, то общее решение этого уравнения имеет вид:

$$\begin{aligned} x &= x_0 - \frac{b}{d}t, \\ y &= y_0 + \frac{a}{d}t, \end{aligned} \tag{2}$$

где t пробегает множество $\mathbf{Z}$ целых чисел.

Доказательство. Покажем сначала, что при любом целом t числа $x = x_0 - \frac{b}{d}t$ и $y = y_0 + \frac{a}{d}t$ удовлетворяют уравнению (1) (заметим, что $d = (a, b)$, и потому $\frac{a}{d}$ и $\frac{b}{d}$, а значит, и $x_0 - \frac{b}{d}t$, $y_0 + \frac{a}{d}t$ — целые числа). В самом деле, так как (x_0, y_0) — одно из решений уравнения (1), то $ax_0 + by_0 = c$, и потому

$$a\left(x_0 - \frac{b}{d}t\right) + b\left(y_0 + \frac{a}{d}t\right) = ax_0 + by_0 = c.$$

Значит, при любом целом t выражения (2) дают решение уравнения (1).

Покажем теперь, что этим исчерпываются все целочисленные решения уравнения (1). В самом деле, пусть (x_1, y_1) — такое решение. Тогда $ax_1 + by_1 = c$ и $ax_0 + by_0 = c$. Вычитая почленно эти равенства, получаем:

$$a(x_1 - x_0) + b(y_1 - y_0) = 0. \tag{3}$$

Так как $(a, b) = d$, то числа $\frac{a}{d}$ и $\frac{b}{d}$ взаимно просты. Деля обе части равенства на d и перенося второе слагаемое в правую часть, получаем:

$$\frac{a}{d}(x_1 - x_0) = -\frac{b}{d}(y_1 - y_0).$$

Но $\frac{a}{d}$ и $\frac{b}{d}$ взаимно просты, а левая часть равенства делится на $\frac{a}{d}$. Поэтому $y_1 - y_0$ делится на $\frac{a}{d}$, $y_1 - y_0 = \frac{a}{d}t_1$, т. е. $y_1 = y_0 + \frac{a}{d}t_1$. Подставляя значение $y_1 - y_0 = \frac{a}{d}t_1$ в (3), получаем:

$$\frac{a}{d}(x_1 - x_0) = -\frac{b}{d} \cdot \frac{a}{d} \cdot t_1, \tag{4}$$

и потому

$$x_1 - x_0 = -\frac{b}{d}t_1, \quad x_1 = x_0 - \frac{b}{d}t.$$

Мы нашли такое целое t, что

$$x_1 = x_0 - \frac{b}{d}t_1, \quad y_1 = y_0 + \frac{a}{d}t_1.$$

Теорема 7 доказана.

В частном случае, когда a и b взаимно просты, формулы общего решения (2) принимают вид:

$$x = x_0 - bt, \; y = y_0 + at. \tag{5}$$

Для нахождения частных решений применяют те же способы, что и для решения сравнений (например, можно использовать теорему Эйлера). Покажем, как искать частные решения неопределенных уравнений (а тем самым и сравнений) с помощью цепных дробей.

Пусть a и b — взаимно простые натуральные числа. Для отыскания частного решения уравнения $ax + by = c$ разложим $\frac{a}{b}$ в цепную дробь: $\frac{a}{b} = [q_0; q_1, \ldots, q_n]$ и найдем подходящие дроби. Последняя подходящая дробь $\frac{P_n}{Q_n} = \frac{a}{b}$.

Так как по условию $(a, b) = 1$ и $(P_n, Q_n) = 1$ (по свойству 3 подходящих дробей), то $P_n = a$, $Q_n = b$.

Согласно свойству 2 подходящих дробей имеем:

$P_{n-1}Q_n - P_nQ_{n-1} = (-1)^n$, или $P_nQ_{n-1} - P_{n-1}Q_n = (-1)^{n-1}$, или

$$aQ_{n-1} - bP_{n-1} = (-1)^{n-1}. \tag{6}$$

Умножая обе части (6) на $(-1)^{n-1}c$, получим:

$$a(-1)^{n-1}cQ_{n-1} + b(-1)^n c P_{n-1} = c. \tag{7}$$

Сравнивая (7) с (2), находим частное решение уравнения (2):

$$x_0 = (-1)^{n-1}c\, Q_{n-1},\ y_0 = (-1)^n cP_{n-1}. \tag{8}$$

Из (5) и (8) следует, что общее решение уравнения имеет вид:

$$x = (-1)^{n-1}c\, Q_{n-1} - bt,\ y = (-1)^n c\, P_{n-1} + at, \tag{9}$$

где P_{n-1} и Q_{n-1} — числитель и знаменатель предпоследней подходящей дроби разложения $\frac{a}{b}$ в цепную дробь, а t — любое целое число.

Примеры.

1. Решим в целых числах уравнение:

$$-117x + 343y = 119,\ (117, 119) = 1.$$

Представим его в виде: $117(-x) + 343y = 119$. Будем искать неизвестные $(-x)$ и y. Здесь $a = 117$, $b = 343$, $c = 119$.

Разлагая $\frac{117}{343}$ в цепную дробь, получим:

$\frac{117}{343} = [0;\ 2,\ 1,\ 13,\ 1,\ 1,\ 1,\ 2]$. Здесь $n = 7$, $P_{n-1} = P_6 = 44$, $Q_{n-1} = Q_6 = 129$; одним из частных решений будет:
$(-x)_0 = (-1)^6 119 \cdot 129 = 15\,351$; $y_0 = (-1)^7\ 119 \cdot 44 = -5236$.

Общее решение согласно (9) будет:

$$-x = 15\,351 + 343t,\ y = -5236 + 117t,$$

или

$$x = -15\,351 + 343t,\ y = -5236 + 117t.$$

Здесь частные значения x_0 и y_0 получились сравнительно большими по абсолютному значению; из общего решения легко получить другие частные значения для x и y (даже наименьшие по абсолютной величине). Так, например, полагая $t = 45$, получим: $x = 84$, $y = 29$, и общее решение данного уравнения можно будет записать в другом виде: $x = 84 + 343t$, $y = 29 + 117t$.

Заметим, что можно было бы в этой задаче находить сразу x и y. В самом деле, разлагая $-\frac{117}{343}$ в цепную дробь, получим:

$$-\frac{117}{343} = [-1,\ 1,\ 1,\ 1,\ 13,\ 1,\ 1,\ 1,\ 2].$$

Здесь $n = 8$, $a = -117$, $b = 343$, $c = 119$, $P_{n-1} = P_7 = -44$, $Q_{n-1} = Q_7 = 129$; поэтому $x_0 = (-1)^7 119 \cdot 129 = -15\,351$, $y_0 = (-1)^8 119 \cdot (-44) = -44 \cdot 119 = -5236$, следовательно, $x = -15\,351 + 343t$, $y = -5236 + 117t$. Это тот же самый результат, что и полученный выше.

2. Требуется проложить трассу газопровода на участке длиной в 450 м. В распоряжении строителей имеются трубы двух размеров: длиной 9 и 13 м.

Сколько труб того и другого размера надо взять, чтобы проложить трассу? Трубы резать не следует, число сварных швов должно быть минимальным.

Р е ш е н и е. Пусть x и y — число труб длиной 9 м и 13 м соответственно. Получим уравнение: $9x + 13y = 450$.
Поскольку $(9, 13) = 1$, это уравнение имеет решения. Чтобы найти их, заменим уравнение сравнением $9x \equiv 450 \pmod{13}$. Из этого сравнения находим $x \equiv 11 \pmod{13}$. Если взять $x_0 = 11$, то для нахождения y_0 имеем уравнение

$$9 \cdot 11 + 13y_0 = 450,$$

откуда $y_0 = 27$.

Получили частное решение: $x_0 = 11$, $y_0 = 27$. Находим все решения уравнения в целых числах

$$x = 11 + 13t,\ y = 27 - 9t, \text{ где } t = 0, \pm 1, \pm 2, \ldots$$

Найдем далее те целые t, при которых $x \geqslant 0$, $y \geqslant 0$:

$$\begin{cases} 11 + 13t \geqslant 0 \\ 27 - 9t \geqslant 0 \end{cases} \Bigg| \quad -\frac{11}{13} \leqslant t \leqslant 3, \text{ а целые } t = 0, 1, 2, 3.$$

Составим таблицу:

t	0	1	2	3
x	11	24	37	50
y	27	18	9	0
$x + y$	38	42	46	50

Из таблицы видно, что задача имеет четыре решения. Минимальное количество швов будет, если взять 11 девятиметровых труб и 27 тринадцатиметровых труб.

3. **Решение систем сравнений первой степени.** Рассмотрим систему сравнений:

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ a_2 x \equiv b_2 \pmod{m_2} \\ \ldots\ldots\ldots\ldots \\ a_k x \equiv b_k \pmod{m_k}. \end{cases} \tag{1}$$

Если b_1 не делится на $d_1 = (a_1, m_1)$, то первое сравнение системы не имеет ре-

шений, а тогда их не имеет и вся система. Если же $b_1 \vdots d_1$, то, решая указанное сравнение, найдем для x выражение вида:

$$x = x_1 + \frac{m_1}{d_1} y, \tag{2}$$

где $y \in \mathbf{Z}$. Подставим это выражение во второе сравнение системы.

После упрощения получим сравнение для отыскания y выражение вида:

$$a_2' y \equiv b_2' \pmod{m_2},$$

где для краткости положено $a_2' = \frac{a_2 m_1}{d_1}$ и $b_2' = b_2 - a_2 x_1$.

Это сравнение тоже либо не имеет решений, либо имеет решение вида:

$$y = y_0 + \frac{m_2}{d_2} z,$$

где $d_2 = (a_2', m_2)$. Подставляя это выражение в (2), получаем для x выражение вида:

$$x = x_2 + \frac{m_1 m_2}{d_1 d_2} z,$$

где для краткости положено $x_2 = x_1 + \frac{m_1}{d_1} y_0$.

Продолжая описанный процесс, мы либо на каком-то шагу придем к неразрешимому сравнению, а тогда не имеет решения и вся система сравнений, либо получим решение вида:

$$x = x_k + \frac{m_1 \dots m_k}{d_1 \dots d_k} y, \text{ где } y \in \mathbf{Z}.$$

Особенно простым является случай, когда $(a_j, m_j) = 1$, $j = 1, \dots, k$ и числа $m_1, \dots, m_k$ попарно взаимно просты. В этом случае система разрешима, причем ее решение имеет вид: $x = x_k + m_1 \dots m_k t$ (поскольку все d_j равны 1).

Примеры.

1) Решим систему сравнений:

$$\begin{cases} 3x \equiv 1 \pmod 5 \\ 5x \equiv 4 \pmod 7). \end{cases} \tag{3}$$

Решая сравнение $3x \equiv 1 \pmod 5$, получаем, что $x \equiv 2 \pmod 5$, т. е. $x = 2 + 5y$. Подставим это выражение в сравнение $5x \equiv 4 \pmod 7$, получаем сравнение: $10 + 25y \equiv 4 \pmod 7$, или $4y \equiv 1 \pmod 7$. Отсюда находим, что $y \equiv 2 \pmod 7$, т. е. $y = 2 + 7t$. Значит, $x = 2 + 5(2 + 7t) = 12 + 35t$, $t \in \mathbf{Z}$.

2. Решим систему сравнений:

$$\begin{cases} 3x \equiv 1 \pmod{20} \\ 2x \equiv 3 \pmod{15}. \end{cases} \tag{4}$$

Из сравнения $3x \equiv 1 \pmod{20}$ получаем, что $x = 7 + 20y$. Подставляя это выражение во второе сравнение, получаем для y сравнение $40y \equiv 4 \pmod{15}$. Это сравнение неразрешимо, так как $(40, 15) = 5$, а 4 не делится на 5. Значит, и вся система сравнений (4) неразрешима.

Вопросы для самопроверки и упражнения

1. Каково условие разрешимости сравнения первой степени с одним неизвестным?

2. Сколько решений имеет сравнение $ax \equiv b \pmod m$ в случае его разрешимости?

3. Как найти все решения сравнения $ax \equiv b \pmod{m}$ при условии $(a, m) = d > 1$, если известно одно решение этого сравнения?

4. Каковы условия разрешимости неопределенного уравнения с двумя неизвестными?

Имеют ли решения уравнения: а) $32x - 86y = 7$; б) $12x + 86y = 16$?

5. Как найти общее решение неопределенного уравнения в целых числах, зная какое-либо его частное решение?

6. Запишите частное решение уравнения $ax + by = c$, где $(a, b) = 1$ (с помощью цепных дробей).

7. Как найти решения уравнения $ax + by = c$ в целых положительных числах? Проиллюстрируйте это на примере $3x + 5y = 2$.

8. Решите сравнения первой степени: а) $7x \equiv 13 \pmod{29}$; б) $8x \equiv 15 \pmod{29}$; в) $9x \equiv 17 \pmod{31}$; г) $17x \equiv 13 \pmod{123}$; д) $243x \equiv 271 \pmod{317}$; е) $221x \equiv 111 \pmod{360}$; ж) $141x \equiv 73 \pmod{320}$; з) $139x \equiv 118 \pmod{239}$.

9. Решите сравнения первой степени: а) $327x \equiv 78 \pmod{379}$; б) $239x \equiv 302 \pmod{471}$; в) $23x \equiv 667 \pmod{693}$.

10. Решите сравнения первой степени: а) $9x \equiv 15 \pmod{48}$; б) $21x \equiv 15 \pmod{111}$; в) $15x \equiv 120 \pmod{85}$; г) $75x \equiv 62 \pmod{111}$; д) $2560x \equiv 45 \pmod{3605}$; е) $36x \equiv 64 \pmod{18}$.

11. Составьте сравнение первой степени по модулю 21: а) имеющее одно решение; б) имеющее 3 или 7 решений; в) имеющее 2, 10, 15 решений.

12. С помощью сравнений решите в целых числах следующие неопределенные уравнения: а) $53x + 17y = 25$; б) $47x - 105y = 4$; в) $18x - 33y = 112$; г) $11x + 16y = 156$.

13. Определите день и месяц рождения, зная, что сумма произведений числа месяца на 12 и номера месяца на 31 равна 436.

14. Припишите справа к числу 32 такое двузначное число, чтобы полученное четырехзначное число делилось на 3 и 7.

15. Припишите справа к числу 629 такое трехзначное число, чтобы полученное шестизначное число делилось на 5, 8 и 11.

16. Припишите справа к числу 723 такое двузначное число, чтобы полученное пятизначное число при делении на 31 давало в остатке число 7.

17. С помощью решения сравнений первой степени выясните, при каких наименьших натуральных значениях a и b уравнение $ax - by = 31$ имеет решение (5; 9).

18. На прямой $ax + by = c$ найдите количество целых точек, лежащих между точками с абсциссами a_1 и a_2: а) $10x - 11y = 15$, $a_1 = -30$, $a_2 = 50$; б) $31x - 47y = 23$, $a_1 = -50$, $a_2 = 60$; в) $101x - 39y = 89$, $a_1 = 0$, $a_2 = 100$.

19. Докажите, что число внутренних целых точек отрезка с целыми концами $A(x_1, y_1)$, $B(x_2, y_2)$ равно $d - 1$, где $d = (y_1 - y_2, x_1 - x_2)$.

20. Через сколько целых точек проходят стороны треугольника с вершинами: A (2, 3), B (7, 8), C (13, 5)?

21. Решите следующие системы сравнений: а) $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$, $x \equiv 4 \pmod 9$; б) $x \equiv 1 \pmod 3$, $x \equiv 5 \pmod 7$, $x \equiv 9 \pmod{11}$; в) $x \equiv 14 \pmod{19}$, $x \equiv 5 \pmod 7$, $x \equiv 9 \pmod{10}$, $x \equiv 1 \pmod 3$.

22. Найдите расстояние между соседними целыми точками прямой

$$ax + by = c,\ (a, b) = 1.$$

23. Решите следующие системы сравнений: а) $37x \equiv 73 \pmod{91}$, $x \equiv 9 \pmod{16}$, $x \equiv 5 \pmod 7$; б) $24x \equiv 20 \pmod{22}$, $13x \equiv 19 \pmod{27}$; в) $75x \equiv 35 \pmod{40}$, $8x \equiv 12 \pmod{44}$, $51x \equiv 50 \pmod{63}$; г) $5x \equiv 200 \pmod{251}$, $11x \equiv 192 \pmod{401}$, $3x \equiv -151 \pmod{907}$.

24. Найдите числа, которые: а) при делении на 4, 5, 7 дают соответственно остатки 2, 3, 4; б) при делении на 3, 7, 8 дают соответственно остатки 2, 4, 5; в) при делении на 7, 13, 17 дают соответственно остатки 4, 9, 1; г) при делении на 13, 21, 23 дают соответственно остатки 9, 1, 13; д) при делении на 3, 5, 7, 11 дают соответственно остатки 1, 2, 3, 9.

25. Найдите наименьшее натуральное число, кратное семи и дающее остаток 1 при делении его на 2, 3, 4, 5 и 6.

26. Между 100 и 500 найдите все натуральные числа, которые при делении на 3, 5, 8 дают соответственно остатки 2, 3, 4.

27. Припишите справа к числу 79 такое двузначное число, чтобы полученное четырехзначное число при делении на 11 и 13 дало бы соответственно остатки 3 и 5.

§ 7. ПОРЯДОК КЛАССА ВЫЧЕТОВ, ПЕРВООБРАЗНЫЕ КОРНИ, ИНДЕКСЫ

1. Порядок класса вычетов. В этом параграфе мы изучим подробнее строение группы Γ_m, состоящей из обратимых элементов в кольце вычетов $\mathbf{Z}_m$. Напомним, что эта группа состоит из классов вычетов, взаимно простых с модулем m (см. п. 2 § 3). Она содержит $\varphi(m)$ классов вычетов (см. п. 1 § 4). Так как умножение в кольце $\mathbf{Z}_m$ коммутативно, то Γ_m — коммутативная группа, состоящая из $\varphi(m)$ элементов. Как отмечалось на с. 120, отсюда следует, что все элементы $\bar{a}$ группы Γ_m (т. е. все классы вычетов по m, взаимно простые с m) имеют конечный порядок и этот порядок является делителем $\varphi(m)$ (числа элементов группы Γ_m).

Мы назвали порядком класса $\bar{a}$ порядок порожденной им циклической подгруппы в Γ_m. Как отмечалось в «Алгебре» на с. 29, этот порядок является наименьшим показателем степени, при котором выполняется равенство $\bar{a}^k = \bar{1}$. Значит, получаем следующее определение:

Определение 1. *Порядком класса вычетов* a, взаимно простого с модулем m, называют наименьшее натуральное число δ, такое, что $\overline{a}^{\delta} = \overline{1}$.

Число δ называют также порядком всех чисел a, входящих в класс вычетов $\overline{a}$. Если $a \in \overline{a}$, то из равенства $\overline{a}^k = \overline{1}$ следует, что $a^k \equiv 1 \pmod{m}$.

Таким образом, получаем следующее определение:

Определение 2. Пусть число a взаимно просто с m, $(a, m) = 1$. *Порядком числа* a *по модулю* m называют наименьшее натуральное число δ, такое, что $\alpha^{\delta} \equiv 1 \pmod{m}$.

Если порядок класса вычетов $\overline{a}$ (соответственно числа a) по модулю m равен δ, то говорят, что δ является *показателем* $\overline{a}$ (соответственно числа a) по модулю m, или что $\overline{a}$ (соответственно a) принадлежит показателю δ по модулю m.

Если порядок класса вычетов $\overline{a}$ по модулю m равен δ, то циклическая подгруппа, порожденная классом вычетов $\overline{a}$ в группе Γ_m, состоит из δ элементов. Мы можем применить к этой подгруппе все результаты о циклических подгруппах, полученные в п. 4 § 3 главы I книги «Алгебра».

Теорема 1. *Если порядок класса вычетов* $\overline{a}$ *по модулю* m *равен* δ*, то* $\overline{a}^{\gamma} = 1$ *в том и только том случае, когда* γ *делится на* δ.

Следствие 1. *Если порядок класса вычетов* $\overline{a}$ *по модулю* m *равен* δ, *то* $\overline{a}^s = \overline{a}^t$ *в том и только том случае, когда* $s - t$ *делится на* δ (т. е. *когда* $s \equiv t \pmod{\delta}$).

Следствие 2. *Если порядок класса вычетов* $\overline{a}$ *по модулю* m *равен* δ, *то все классы вычетов*

$$\overline{1}, \overline{a}, \ldots, \overline{a}^{\delta-1}$$

попарно различны.

Теорема 2. *Если порядок класса вычетов* $\overline{a}$ *по модулю* m *равен* δ, *то порядок класса вычетов* $\overline{a}^k$ *равен* $\delta / (k, \delta)$.

Следствие 1. *Если порядок класса вычетов* $\overline{a}$ *по модулю* m *равен* δ *и* $(k, \delta) = 1$, *то порядок класса вычетов* $\overline{a}^k$ *тоже равен* δ.

Следствие 2. *Если порядок класса вычетов* $\overline{a}$ *по модулю* m *равен* δ, *то среди классов вычетов* $\overline{1}, \overline{a}, \ldots, \overline{a}^{\delta-1}$ *порядок* δ *имеют* $\varphi(\delta)$ *классов.*

Доказательство. По следствию 2 из теоремы 1 все классы вычетов $\overline{1}, \overline{a}, \ldots, \overline{a}^k, \ldots, \overline{a}^{\delta-1}$ различны. Порядок δ имеют те из этих классов, для которых $(k, \delta) = 1$. Число таких классов равно $\varphi(\delta)$.

---

* Здесь, разумеется, мы считаем, что класс $\overline{a}$ взаимно прост с модулем m.

Все сформулированные сейчас утверждения можно сформулировать и как утверждения о сравнениях по модулю m. В нижеследующих формулировках через a обозначено число, взаимно простое с модулем m, а через δ — порядок этого числа по модулю m.

Теорема 1′. *Сравнение* $a^\gamma \equiv 1 \pmod m$ *выполняется в том и только том случае, когда* γ *делится на* δ.

Следствие 1. *Сравнение* $a^s \equiv a^t \pmod m$ *выполняется в том и только том случае, когда* $s - t$ *делится на* δ.

Следствие 2. *Числа*

$$1, a, \ldots, a^{\delta-1}$$

попарно несравнимы друг с другом по модулю m.

Теорема 2′. *Порядок числа* a^k *по модулю* δ *равен* $\delta/(k, \delta)$.

Следствие 1. *Если* $(k, \delta) = 1$, *то порядок числа* a^k *по модулю* m *равен* δ.

Следствие 2. *Среди чисел вида* $1, a, \ldots, a^{\delta-1}$ *есть* $\varphi(\delta)$ *попарно несравнимых по модулю* m *чисел, имеющих порядок* δ.

Пример. Найдем порядок класса вычетов $\overline{7}$ по модулю 43, а также все классы вычетов по этому модулю, порядок которых равен порядку класса вычетов $\overline{7}$.

Мы знаем, что порядок любого класса вычетов является делителем числа $\varphi(m) = \varphi(43) = 42$. Натуральными делителями этого числа являются 1, 2, 3, 6, 7, 14, 21, 42. Будем возводить число 7 в степени с показателями 1, 2, 3, 6, 7, 14, 21 и 42 до тех пор, пока не получим число, сравнимое с 1 по модулю 43. Мы имеем: $7^1 \equiv 7^2 \pmod{43}$, $7^2 = 49 \equiv 6 \pmod{43}$, $7^3 = 7^2 \cdot 7 \equiv 6 \cdot 7 = 42 \equiv -1 \pmod{43}$, $7^6 = 7^3 \cdot 7^3 \equiv (-1)(-1) = 1 \pmod{43}$. Значит, порядок числа 7 по модулю 43 равен 6.

Чтобы найти остальные классы вычетов по модулю 43, имеющие порядок 6, берем числа 0, 1, 2, 3, 4, 5 и отбираем из них числа, взаимно простые с $\delta = 6$, т. е. числа 1 и 5. Значит, искомыми классами вычетов являются $\overline{7}^1$ и $\overline{7}^5$. Но

$$7^5 \equiv 7^2 \cdot 7^2 \cdot 7 \equiv 6 \cdot 6 \cdot 7 \equiv 252 \equiv 13 \pmod{43},$$

и потому получаем классы вычетов $\overline{7}$ и $\overline{13}$.

2. Первообразные корни по простому модулю. Пусть p — простое число. Группа Γ_p обратимых элементов кольца $\mathbb{Z}_p$ состоит из классов вычетов $\overline{1}, \overline{2}, \ldots, \overline{p-1}$. По теореме 1 п. 1 порядок каждого из этих классов вычетов является делителем числа $\varphi(p) = p - 1$.

Определение 3. *Первообразным корнем по простому модулю* p называют класс вычетов $\overline{g}$ по этому модулю, порядок которого равен $p - 1$.

Из следствия 1 к теореме 1 п. 1 получаем:

Если $\overline{g}$ *— первообразный корень по простому модулю* p, *то* $\overline{g}^s = \overline{g}^t$ *в том и только том случае, когда* $s - t$ *делится на* $p - 1$.

Из следствия 2 к той же теореме получаем:

Если $\overline{g}$ *— первообразный корень по простому модулю* p, *то в ряду степеней*

$$\overline{1},\ \overline{g},\ \ldots,\ \overline{g}^{p-2}$$

все члены различны (в этом случае $\delta = p - 1$).

Но этот ряд степеней содержит $p - 1$ элемент, т. е. столько же элементов, сколько их в приведенной системе вычетов по модулю p (или, что то же самое, в группе Γ_p обратимых элементов кольца $\mathbf{Z}_p$). Так как все степени $\overline{g}$ взаимно просты с $\overline{p}$ (т. е. обратимы), то получаем следующий важный результат:

Если $\overline{g}$ — первообразный корень по простому модулю p, то множество классов вычетов $\overline{1},\ \overline{g},\ \ldots,\ \overline{g}^{p-2}$ совпадает с множеством классов вычетов, взаимно простых с p:

$$\{\overline{1},\ \overline{g},\ \ldots,\ \overline{g}^{p-2}\} = \{\overline{1},\ \overline{2},\ \ldots,\ \overline{p-1}\}.$$

Полученный результат можно сформулировать следующим образом:

Т е о р е м а 3. *Если* $\overline{g}$ *— первообразный корень по простому модулю* p, *то для любого ненулевого класса вычетов* $\overline{x}$ *по модулю* p *найдется одно и только одно число* γ, *такое, что* $\overline{x} = \overline{g}^{\gamma}$ *и* $0 \leqslant \gamma \leqslant p - 2$.

Из следствия 2 к теореме 2 п. 1 вытекает, что если существует хотя бы один первообразный корень $\overline{g}$ по простому модулю p, то общее число таких корней равно $\varphi(p-1)$. Это будут классы вычетов вида $\overline{g}^k$, где k взаимно просто с $p - 1$ и $0 \leqslant k \leqslant p - 2$.

Мы покажем теперь, что условие существования хотя бы одного первообразного корня излишне: такой корень существует для любого простого модуля $p > 2$. Это утверждение вытекает из следующей теоремы:

Т е о р е м а 4. *Пусть* $p > 2$ *— простое число и* $\delta \mid p - 1$. *Тогда количество классов вычетов по модулю* p, *имеющих порядок* δ, *равно* $\varphi(\delta)$.

Д о к а з а т е л ь с т в о. По следствию 1 к теореме 1 п. 1 порядок любого из классов вычетов $\overline{1},\ \overline{2},\ \ldots,\ \overline{p-1}$ является делителем $\varphi(p)$, т. е. числа $p - 1$. Обозначим через $\psi(\delta)$ число классов вычетов по модулю p, имеющих порядок δ. По следствию 2 к теореме 2 из п. 1 получаем, что если есть хотя бы один класс вычетов порядка δ, то их число равно $\varphi(\delta)$. Таким образом,

$$\psi(\delta) = \begin{cases} \varphi(\delta), & \text{если есть хотя бы один класс вычетов по модулю } p \text{ порядка } \delta; \\ 0, & \text{если нет ни одного класса вычетов по модулю } p \text{ порядка } \delta. \end{cases}$$

Поэтому для любого делителя δ числа $p - 1$ выполняется неравенство $\psi(\delta) \leqslant \varphi(\delta)$.

Обозначим делители числа $p-1$ через $\delta_1, \ldots, \delta_k$. Так как порядок любого из классов вычетов $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ является одним из делителей числа $p-1$, т. е. одним из чисел δ_j, $1 \leqslant j \leqslant k$, то $\psi(\delta_1) + \ldots + \psi(\delta_k)$ равно общему числу этих классов вычетов, т. е. $p-1$,

$$\psi(\delta_1) + \ldots + \psi(\delta_k) = p - 1. \qquad (1)$$

С другой стороны, по тождеству Гаусса (см. п. 2 § 4) имеем:

$$\varphi(\delta_1) + \ldots + \varphi(\delta_k) = p - 1. \qquad (2)$$

Из равенств (1) и (2) вытекает, что

$$\psi(\delta_1) + \ldots + \psi(\delta_k) = \varphi(\delta_1) + \ldots + \varphi(\delta_k). \qquad (3)$$

Но для любого j, $1 \leqslant j \leqslant k$, выполняется неравенство $\psi(\delta_j) \leqslant \varphi(\delta_j)$. Поэтому равенство (3) может иметь место лишь при условии, что для всех j имеем: $\psi(\delta_j) = \varphi(\delta_j)$. А это и означает, что количество классов по модулю p, имеющих порядок δ_j, равно $\varphi(\delta_j)$. Теорема доказана.

Следствие. *Если $p > 2$ — простое число, то существует $\varphi(p-1)$ первообразных корней по модулю p.*

Для доказательства достаточно применить теорему к случаю $\delta = p - 1$.

Пример. Пусть $p = 11$, тогда $\varphi(p) = \varphi(11) = 10$, $p - 1 = 10$. Делители числа $p - 1 = 10$: $\delta = 1, 2, 5, 10$. Тогда числа приведенной системы вычетов по модулю 11 (1, 2, 3, 4, 5, 6, 7, 8, 9, 10) и классы, которым они принадлежат, распределятся по их порядкам 1, 2, 5, 10 следующим образом (вычисления предлагается сделать читателю самостоятельно):

Делители δ числа $p-1=10$	Числа порядка δ	$\psi(\delta)$	$\varphi(\delta)$
1	1	1	1
2	10	1	1
5	3, 4, 5, 9	4	4
10	2, 6, 7, 8	4	4
	Всего распределенных чисел $p-1=10$	$\Sigma\psi(\delta)=10$	$\Sigma\varphi(\delta)=10$

Заметим, что до сих пор еще не найден эффективный способ нахождения хотя бы одного первообразного корня по данному модулю. На практике пользуются обычно методом испытаний.

Если найден один первообразный корень $\overline{g}$, то, как мы уже установили выше, остальные находятся легко.

Первообразные корни по модулю p можно искать также с помощью следующей теоремы:

Теорема 5. *Пусть* $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ *— каноническое разложение числа* $\varphi(p) = p - 1$. *Для того чтобы класс* $\overline{g}$, *взаимно простой с* p, *был первообразным корнем, необходимо и достаточно, чтобы* $\overline{g}$ *не удовлетворял ни одному из равенств:*

$$\overline{g}^{\frac{p-1}{p_1}} = \overline{1}, \overline{g}^{\frac{p-1}{p_2}} = \overline{1}, \ldots, \overline{g}^{\frac{p-1}{p_k}} = \overline{1}. \tag{4}$$

Необходимость. Пусть g — первообразный корень по модулю p, тогда порядок g равен $\varphi(p) = p - 1$, т. е. $\overline{g}^{p-1} = \overline{1}$ и $p - 1$ — наименьший натуральный показатель, при котором имеет место это равенство. Это означает, что $\overline{g}$ не удовлетворяет ни одному из равенств (4).

Достаточность. Пусть $\overline{g}$ не удовлетворяет ни одному из равенств (4). Допустим, что порядок δ класса $\overline{g}$ по модулю p меньше $\varphi(p) = p - 1$ ($\delta < p - 1$). Но тогда $\varphi(p) \vdots \delta$ или $p - 1 \vdots \delta$, т. е. $p - 1 = \delta q$, или $\frac{p-1}{q} = \delta$, где q — натуральное. Тогда из $\overline{g}^{\delta} \equiv \overline{1}$ следует, что $\overline{g}^{\frac{p-1}{q}} \equiv \overline{1}$, что противоречит условиям (4). Значит, $\delta = p - 1 = \varphi(p)$, т. е. $\overline{g}$ — первообразный корень. Теорема доказана.

Пример. Найти все первообразные корни по модулю 17. Число первообразных корней по модулю p равно $\varphi(p - 1)$. В данном случае $\varphi(17 - 1) = 16\left(1 - \frac{1}{2}\right) = 8$. Чтобы найти все 8 корней, достаточно найти хотя бы один первообразный корень. Условия (4) предыдущей теоремы: $\overline{g}^{\frac{p-1}{p_i}} \neq \overline{1}$ перейдут в единственное условие: $\overline{g}^8 \neq \overline{1}$. Испытываем классы $\overline{2}$, $\overline{3}$, ..., $\overline{16}$ по порядку, начиная с $\overline{2}$ (для простоты вычислений вместо классов вычетов мы берем вычеты и заменяем равенства сравнениями по модулю 17). $2^4 = 16$, $2^8 \equiv 256 \equiv 1 \pmod{17}$, т. е. 2 не первообразный корень. $3^4 \equiv 81 \equiv 13 \pmod{17}$, $3^8 = 169 = -1 \pmod{17}$. Следовательно, $g = \overline{3}$ — первообразный корень. Далее выписываем все числа, взаимно простые с 16: 3, 5, 7, 9, 11, 13, 15. Первообразными корнями будут классы: $\overline{3}$, $\overline{3^3} = \overline{10}$; $\overline{3^5} = \overline{5}$; $\overline{3^7} = \overline{11}$; $\overline{3^9} = \overline{14}$; $\overline{3^{11}} = \overline{7}$; $\overline{3^{13}}$; $= \overline{12}$; $\overline{3^{15}} = \overline{6}$.

Итак, первообразными корнями по модулю 17 являются классы вычетов $\overline{3}$, $\overline{5}$, $\overline{6}$, $\overline{7}$, $\overline{10}$, $\overline{11}$, $\overline{12}$, $\overline{14}$.

3. Индексы. Мы доказали в п. 2, что если $\overline{g}$ — первообразный корень по простому модулю p, то для любого отличного от нуля класса вычетов $\overline{x}$ по модулю p найдется такое число γ, что $\overline{g}^{\gamma} = \overline{x}$. Такое число γ называют индексом x по модулю p при основании $\overline{g}$. Иными словами,

Определение 4. Пусть p — простое число и $\overline{g}$ — первообразный корень по модулю p. Число γ называется *индексом класса вычетов* $\overline{x}$ *по модулю* p *при основании* $\overline{g}$, если $\overline{g}^{\gamma} = \overline{x}$.

Из определения индексов видна аналогия между индексами и логарифмами. Индексы обозначаются так:

$$\gamma = \operatorname{ind}_{\overline{g}} \overline{x}, \text{ сравним с } x = \log_a N.$$

Разумеется, формулируя определение 4, можно говорить не о классах вычетов, а о самих вычетах. Число g называют первообразным корнем по простому модулю p, если его порядок по этому модулю равен $p-1$. Индексом числа x по модулю p при основании g называют такое число γ, что

$$g^{\gamma} \equiv x \pmod{p}.$$

Из свойств первообразных корней следует, что $\overline{g}^{\gamma_1} = \overline{g}^{\gamma_2}$ в том и только том случае, когда $\gamma_1 \equiv \gamma_2 \pmod{p-1}$. Поэтому, если γ — индекс числа x по простому модулю p при основании g, то и все числа γ', сравнимые с γ по модулю $p-1$, являются индексами x по модулю p при основании g.

Основные свойства индексов таковы:

Свойство 1. *Индекс произведения сравним по модулю $p-1$ с суммой индексов сомножителей.*

$$\operatorname{ind}_{\overline{g}} \overline{a} + \operatorname{ind}_{\overline{g}} \overline{b} \equiv \operatorname{ind}_{\overline{g}} \overline{ab} \pmod{p-1}. \tag{1}$$

В самом деле, по определению индексов имеем:

$$\overline{g}^{\operatorname{ind}_{\overline{g}} \overline{a}} = \overline{a},\ \overline{g}^{\operatorname{ind}_{\overline{g}} \overline{b}} = \overline{b}.$$

Перемножая эти равенства, получаем:

$$\overline{g}^{\operatorname{ind}_{\overline{g}} \overline{a} + \operatorname{ind}_{\overline{g}} \overline{b}} = \overline{ab} = \overline{g}^{\operatorname{ind}_{\overline{g}} \overline{ab}}.$$

Отсюда и следует сравнение (1).

Следствие. $\operatorname{ind}_{\overline{g}} \overline{a}^n = n \operatorname{ind}_{\overline{g}} \overline{a}$.

Обозначим через $\frac{\overline{a}}{\overline{b}}$ класс вычетов $\overline{a}\overline{b}^{-1}$ (где $\overline{b} \cdot \overline{b}^{-1} = 1$).

Свойство. 2. *Индекс дроби $\frac{\overline{a}}{\overline{b}}$ сравним по модулю $p-1$ с разностью индексов числителя и знаменателя:*

$$\operatorname{ind}_g \frac{\overline{a}}{\overline{b}} \equiv \operatorname{ind}_g \overline{a} - \operatorname{ind}_g \overline{b} \pmod{p-1}. \tag{2}$$

Доказательство. Класс вычетов $\overline{x} = \frac{\overline{a}}{\overline{b}}$ является решением уравнения $\overline{b}\overline{x} = \overline{a}$. По свойству 1 $\operatorname{ind}_{\overline{g}} \overline{a} \equiv \operatorname{ind}_{\overline{g}} \overline{b} + \operatorname{ind}_{\overline{g}} \overline{x} \pmod{p-1}$, откуда и вытекает сравнение (2).

Свойство 3. *Индекс единицы сравним с нулем по модулю $\varphi(p) = p-1$, т. е.*

$$\operatorname{ind}_{\overline{g}} 1 \equiv 0 \pmod{p-1},$$

так как $g^0 = \overline{1}$.

Свойство 4. *Индекс основания индексов $\overline{g}$ сравним с единицей по модулю $p-1$, т. е.*

$$\operatorname{ind}_{\overline{g}} \overline{g} \equiv 1 \pmod{p-1},$$

так как

$$\overline{g}^1 = \overline{g}.$$

Мы видим, что многие свойства индексов аналогичны свойствам логарифмов. Индексы имеют такие же приложения, как и логарифмы. Для практических целей составлены таблицы индексов, по которым для данного первообразного корня g можно находить либо индекс по числу, либо число по индексу.

4. Таблицы индексов. Для каждого простого модуля до 2000 построено по две таблицы. Одна — для нахождения индекса по числу, другая — для нахождения числа по индексу. Таблицы обычно содержат наименьшие неотрицательные вычеты по модулю $\varphi(p) = p - 1$ (первая таблица) и наименьшие неотрицательные приведенные вычеты чисел (вторая таблица). Эти таблицы помещаются в качестве приложения в конце каждого учебника по теории чисел. Покажем на примере составление таблиц по одному из модулей.

Пример. Построим таблицы для определения индексов по числам и чисел по индексам по модулю $p = 23$.

В качестве основания g удобно взять наименьший первообразный корень по модулю 23. Либо по таблице первообразных корней, либо путем непосредственного вычисления находим, что $g = 5$.

Последовательно приводим по модулю 23 все степени 5 до $p - 2 = 23 - 2 = 21$ включительно:

$$\begin{array}{llll} 5^0 \equiv 1 & 5^5 \equiv 20 & 5^{10} \equiv 9 & 5^{16} \equiv 3 \\ 5^1 \equiv 5 & 5^6 \equiv 8 & 5^{11} \equiv 22 & 5^{17} \equiv 15 \\ 5^2 \equiv 2 & 5^7 \equiv 17 & 5^{12} \equiv 18 & 5^{18} \equiv 6 \\ 5^3 \equiv 10 & 5^8 \equiv 16 & 5^{13} \equiv 21 & 5^{19} \equiv 7 \\ 5^4 \equiv 4 & 5^9 \equiv 11 & 5^{14} \equiv 13 & 5^{20} \equiv 12 \\ & & 5^{15} \equiv 19 & 5^{21} \equiv 14 \end{array} \pmod{23}$$

Получим таблицы:

а) для нахождения индексов по числам

N	0	1	2	3	4	5	6	7	8	9
0		0	2	16	4	1	18	19	6	10
1	3	9	20	14	21	17	8	7	12	15
2	5	13	11							

б) для нахождения чисел по индексам

I	0	1	2	3	4	5	6	7	8	9
0	1	5	2	10	4	20	8	17	16	11
1	9	22	18	21	13	9	13	15	6	7
2	12	14								

Примеры.

1. Найдем индексы чисел 6, 15, 22 и 243 по модулю 23.

На пересечении строки с номером 0 (десятки) и столбца с номером 6 (единицы) находим, что $\operatorname{ind} 6 = 18$, аналогично находим:

$$\operatorname{ind} 15 = 17, \operatorname{ind} 22 = 11.$$

Для нахождения индекса числа 243 заменяем его сравнимым с ним наименьшим неотрицательным вычетом по модулю 23. Имеем: $243 \equiv 13 \pmod{23}$; тогда $\operatorname{ind} 243 = \operatorname{ind} 13 = 14$.

2. Найти числа N_1 и N_2, если известно, что $\operatorname{ind} N_1 = 8$, $\operatorname{ind} N_2 = 17$.

По второй таблице находим, что $N_1 = 16$, $N_2 = 15$.

В большинстве задач с применением индексов, так же как и в большинстве задач с применением логарифмов, не имеет значения основание g, по которому определяются индексы, но если возникает потребность перевода индексов по одному основанию в систему индексов по другому основанию, то применяется формула перевода аналогично формуле перевода логарифмов по одному основанию в логарифмы по другому основанию:

$$\gamma_1 \equiv \gamma \operatorname{ind}_{g_1} g \pmod{\varphi(p)}.$$

5. Применения индексов. а) Решение сравнений первой степени.

Покажем на примере, как с помощью таблиц индексов решаются сравнения первой степени.

Пример. Решим с помощью таблиц индексов сравнение:

$$8x \equiv -11 \pmod{37}.$$

Правую часть сравнения заменяем положительным вычетом:

$$8x \equiv 26 \pmod{37}.$$

«Индексируем» левую и правую части сравнения:

$$\operatorname{ind} 8 + \operatorname{ind} x \equiv \operatorname{ind} 26 \pmod{36}.$$

Находим в первой таблице для простого числа 37 значения ind 8 и ind 26 и подставляем в сравнение. Получим:

$$3 + \operatorname{ind} x \equiv 12 \pmod{36},$$

откуда

$$\operatorname{ind} x \equiv 9 \pmod{36}.$$

По второй таблице находим число, соответствующее индексу 9, получим: $x \equiv 31 \pmod{37}$.

б) Решение двучленных сравнений n-й степени.

Сравнение вида $ax^n \equiv b \pmod{m}$, где $a \not\equiv 0 \pmod{m}$ и n — натуральное число, называется *двучленным сравнением с одним неизвестным*. Мы ограничимся рассмотрением двучленного сравнения по простому модулю p:

$$ax^n \equiv b \pmod{p}, \quad (a, p) = 1. \tag{1}$$

«Индексируя» обе части сравнения (1), получим равносильное ему сравнение:

$$\operatorname{ind} a + n \operatorname{ind} x \equiv \operatorname{ind} b \pmod{p-1} \text{ или } nz \equiv c \pmod{p-1}, \tag{2}$$

где $z = \operatorname{ind} x$, $c = \operatorname{ind} b - \operatorname{ind} a$. Таким образом, решение сравнения (1) сводится к решению сравнения (2) первой степени. Если $(n, p-1) = d$ и c делится на d, то сравнение (2), а следовательно, и сравнение (1), имеет d решений; если же c не делится на d, сравнение (2), а потому и сравнение (1), решений не имеет.

Пример. Решим сравнение $15x^4 \equiv 17 \pmod{23}$.
«Индексируем» обе части сравнения:

$$\operatorname{ind} 15 + 4 \operatorname{ind} x \equiv \operatorname{ind} 17 \pmod{22}.$$

Из первой таблицы для простого числа 23 находим, что $\operatorname{ind} 15 = 17$, $\operatorname{ind} 17 = 7$. Тогда получим сравнение первой степени относительно $\operatorname{ind} x$: $4 \operatorname{ind} x \equiv 12 \pmod{22}$.

Последнее сравнение имеет два решения: $\operatorname{ind} x \equiv 3; 14 \pmod{22}$. Теперь из второй таблицы для простого числа 23 находим, что

$$x \equiv 10; 13 \pmod{23}.$$

Умножим обе части сравнения (1) на такое число α, что $a\alpha = 1 \pmod{p}$; получим: $a\alpha x^n \equiv b\alpha \pmod{p}$, или

$$x^n \equiv c \pmod{p}, \tag{3}$$

где $b\alpha = c$.

Если сравнение (3) имеет решения, то c называется *вычетом степени n по модулю p*, в противном случае — *невычетом степени n*. Вычет (невычет) называется: при $n = 2$ — *квадратичным*, при $n = 3$ — *кубическим*, при $n = 4$ — *биквадратичным*.

Теорема 6. *Сравнение* (3) *имеет решение тогда и только тогда, когда* $\operatorname{ind} a$ *делится на* d, *где* $d = (n, \varphi(p)) = (n, p - 1)$. *В случае разрешимости сравнение* (3) *имеет* d *решений.*

Доказательство. Сравнение (3) равносильно такому:

$$\operatorname{ind} x \equiv \operatorname{ind} a \pmod{\varphi(p)} \text{ или } n \operatorname{ind} x \equiv \operatorname{ind} a \pmod{p - 1}. \tag{4}$$

Сравнение (4) есть сравнение первой степени относительно $\operatorname{ind} x$, которое по ранее доказанной теореме имеет решение тогда и только тогда, когда $\operatorname{ind} a$ кратен d, при этом решений сравнения (4), не сравнимых по модулю $\varphi(p) = p - 1$, будет d.

Пример 1. Решим сравнение $x^8 \equiv 23 \pmod{41}$.
Имеем:

$$8 \operatorname{ind} x \equiv \operatorname{ind} 23 \pmod{40}.$$

В данном случае $(n, \varphi(p)) = (8, 40) = 8$, $\operatorname{ind} a = \operatorname{ind} 23 = 36$. Но 36 не делится на 8, следовательно, данное сравнение не имеет решений.

Пример 2. Решим сравнение $x^{12} \equiv 37 \pmod{41}$.
Имеем:

$$12 \operatorname{ind} x \equiv \operatorname{ind} 37 \pmod{40}.$$

Здесь $d = (12, 40) = 4$, $\operatorname{ind} 37 = 32$; 32 делится на 4, следовательно, сравнение имеет четыре решения. Деля обе части последнего сравнения и модуль на 4, получим:

$$3 \operatorname{ind} x \equiv 8 \pmod{10}, \quad \text{или} \quad \operatorname{ind} x \equiv 6 \pmod{10}.$$

Отсюда для $\operatorname{ind} x$ найдем четыре значения, не сравнимых по модулю 40:

$$\operatorname{ind} x \equiv 6, 16, 26, 36 \pmod{40}.$$

По второй таблице индексов для модуля 41 найдем соответствующие этим индексам значения:

$$x \equiv 39, 18, 2, 23 \pmod{41}.$$

Теорема 7 (обобщенный критерий Эйлера).
Число a есть вычет степени n по простому модулю p тогда и только тогда, когда выполняется условие:

$$a^{\frac{\varphi(p)}{d}} \equiv 1 \pmod{p}, \text{ или } a^{\frac{p-1}{d}} \equiv 1 \pmod{p}, \tag{5}$$

где $d = (n, \varphi(p)) = (n, p - 1)$.

Доказательство. По предыдущей теореме число a есть вычет степени n по модулю m тогда и только тогда, когда $\operatorname{ind} a \vdots d$, т. е. $\operatorname{ind} a \equiv 0 \pmod{d}$, что равносильно условию:

$$\frac{\varphi(p)}{d} \operatorname{ind} a \equiv 0 \pmod{\varphi(p)} \text{ или } \frac{p-1}{d} \operatorname{ind} a \equiv 0 \pmod{p-1}. \tag{6}$$

Но условие (6) есть «индексированная» запись условия (5). Теорема доказана.

Следствие 1. *При $n = 2$ всегда и $d = 2$, так как при нечетном p число $p - 1$ — четное; поэтому сравнение* (5) *переходит в критерий Эйлера*:

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

в) Решение двучленных показательных сравнений.

Ограничимся рассмотрением показательного сравнения вида:

$$a \cdot c^x \equiv b \pmod{p}, \tag{7}$$

где p — простое число, $(a, p) = 1$ и $(c, p) = 1$.

«Индексируя» обе части сравнения (7), получим равносильное ему сравнение:

$$\operatorname{ind} a + x \operatorname{ind} c \equiv \operatorname{ind} b \pmod{p-1},$$

или

$$x \operatorname{ind} c \equiv \operatorname{ind} b - \operatorname{ind} a \pmod{p-1}. \tag{8}$$

Сравнение (8) является сравнением первой степени по модулю $p - 1$. Если $(\operatorname{ind} c, p - 1) = d$ и $\operatorname{ind} b - \operatorname{ind} a$ делится на d, то сравнение (8), а следовательно и сравнение (7), имеет d решений; если же $\operatorname{ind} b - \operatorname{ind} a$ не делится на d, то сравнение (8), а следовательно и сравнение (7), решений не имеет.

Замечание. Если $a \vdots p$ или $c \vdots p$, а b не $\vdots p$, то сравнение (7) невозможно и, следовательно, решений иметь не будет; если при этом и $b \vdots p$, то сравнение (7) будет сводиться к тождественному сравнению вида $0^x \equiv 0 \pmod{p}$, которое будет удовлетворяться любым значением x.

Пример. Решить сравнение $15 \cdot 7^{2x} \equiv 8 \cdot 3^{3x} \pmod{31}$.

Имеем:

$$\operatorname{ind} 15 + 2x \operatorname{ind} 7 \equiv \operatorname{ind} 8 + 3x \operatorname{ind} 3 \pmod{30},$$

или

$$23x \equiv 21 \pmod{30}.$$

Решая последнее сравнение, получим: $x \equiv 27 \pmod{30}$. Это решение и будет единственным решением данного сравнения.

1) В приведенной системе вычетов по модулю 41 найдем числа, принадлежащие показателю 10.

Здесь $p = 41$, $\delta = 10$, $\varphi(p) = 40$, $\frac{\varphi(p)}{\delta} = \frac{40}{10} = 4$. Числа a, определяющие δ, определяются из условия: $(\operatorname{ind} a, 40) = 4$. Отсюда: $\operatorname{ind} a \equiv 4, 12, 28, 36 \pmod{40}$. Теперь по второй таблице индексов для модуля 41 находим соответствующие значения для a: $a \equiv 25, 4, 31, 23 \pmod{41}$.

2) Найдем первообразные корни в приведенной системе вычетов по модулю 41.

Первообразные корни a определяются из условия: $(\operatorname{ind} a, 40) = 1$, откуда: $\operatorname{ind} a \equiv 1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39 \pmod{40}$.

И для a получим значения:

$a \equiv 6, 11, 29, 19, 28, 24, 26, 34, 35, 30, 12, 22, 13, 17, 15, 7 \pmod{41}$.) Всего первообразных корней 16, т. е. $\varphi(40)$.

Вопросы для самопроверки и упражнения

1. Дайте определение порядка класса вычетов по модулю m.

2. Какие значения могут принимать порядки классов вычетов по модулю 13? а по модулю 24?

3. Пусть известно, что $\overline{a^{24}}=\overline{1}$. Какие значения может иметь порядок класса вычетов $\overline{a}$?

4. Класс вычетов $\overline{4}$ имеет порядок 5 по модулю 11. Найдите четыре класса вычетов по модулю 11, имеющих порядок 5.

5. Могут ли существовать классы вычетов порядка 7 по модулю 26?

6. Сколько может быть классов вычетов порядка 9 по модулю 37?

7. Сколько существует классов вычетов порядка δ по простому модулю p?

8. Какое число называется первообразным корнем по модулю p?

9. Достаточно ли выполнимости сравнения $a^{\varphi(p)} \equiv 1 \pmod{p}$ для того, чтобы утверждать, что a — первообразный корень по модулю p?

10. Почему числа ряда $a^0 = 1, a^1, a^2, \ldots, a^{\varphi(p)-1}$ несравнимы между собой по модулю p, если a — первообразный корень? Справедливо ли это утверждение в случае произвольного модуля m?

11. Какие числа принадлежат показателю δ по модулю p, если известно, что a принадлежит показателю δ по этому модулю? Справедливо ли это утверждение для произвольного модуля m?

12. Чему равно число первообразных корней по простому модулю p? Сколько их в случае $p = 17$?

13. Какому показателю принадлежит первообразный корень по простому модулю p? $p = 43$?

14. Что называется индексом числа a по простому модулю p при основании g?

15. На основании чего можно утверждать, что всякое число a, взаимно простое с p, имеет единственный индекс γ, меньший p?

16. Зная индекс γ числа a по простому модулю p, укажите все индексы данного числа a. По какому модулю они образуют класс чисел?

17. Перечислите основные свойства индексов.

18. К решению какого сравнения первой степени сводится решение сравнения: $ax^n \equiv b \pmod{p}$, $(a, p) = 1$?

19. При каком условии сравнение $ax^n \equiv b \pmod{p}$ не имеет решений, при каком условии имеет и сколько?

20. Как можно найти в приведенной системе вычетов по модулю p все числа, принадлежащие данному показателю $\delta < \varphi(p)$? Найдите в приведенной системе вычетов по модулю $p = 17$ все числа, принадлежащие показателю $\delta = 4$.

21. Как можно найти все первообразные корни в приведенной системе вычетов по модулю p? Найдите все первообразные корни в приведенной системе вычетов по модулю 19.

22. Найдите показатель, которому принадлежит: а) 25 по модулю 31; б) 18 по модулю 29; в) 5 по модулю 61.

23. Зная, что 2 является первообразным корнем по модулю 19, составьте приведенную систему вычетов по модулю 19 при помощи степеней числа 2; б) то же для первообразного корня 2 по модулю 27.

24. Докажите, что если a принадлежит четному показателю δ по нечетному простому модулю p, то $a^{\frac{\delta}{2}} \equiv -1 \pmod{p}$.

25. Найдите наименьшие первообразные корни для чисел: а) 23; б) 41; в) 71.

26. Докажите, что если a и b — два целых числа, не делящихся на простое число p, и a принадлежит показателю α, b — показателю β по модулю p, причем $(\alpha, \beta) = 1$, то ab будет принадлежать показателю $\alpha\beta$ по модулю p.

27. Воспользовавшись предыдущим утверждением, найдите показатель, которому принадлежит число 15 по модулю 29, если известно, что числа 12 и 23 принадлежат соответственно показателям 4 и 7 по модулю 29.

28. Зная, что a принадлежит показателю δ по модулю p, найдите в приведенной системе наименьших положительных вычетов по модулю p все вычеты, принадлежащие показателю δ; значения a, δ и p даются соответственно: а) 4,14, 29; б) 25, 3, 31.

29. Найдите число классов первообразных корней по модулям: а) 19; б) 23; в) 37; г) 83.

30. Воспользовавшись утверждением задачи 26, докажите существование первообразных корней по простому модулю p.

31. Зная, что 3 является одним из первообразных корней по модулю 29, найдите остальные первообразные корни по этому модулю.

32. Докажите, что если g и g_1 — два первообразных корня простого числа p, то имеют место сравнения:

$$\operatorname{ind}_g a \equiv \operatorname{ind}_{g_1} a \cdot \operatorname{ind}_g g_1 \pmod{p-1},$$
$$\operatorname{ind}_{g_1} a \equiv \operatorname{ind}_g a \cdot \operatorname{ind}_{g_1} g \pmod{p-1}.$$

В частности,

$$\operatorname{ind}_{g_1} g \cdot \operatorname{ind}_g g_1 \equiv 1 \pmod{p-1}.$$

Эти формулы аналогичны формулам для перехода от одной системы логарифмов к другой; выражение $\operatorname{ind}_{g_1} g$ или $\operatorname{ind}_g g_1$ аналогично тому, которое в теории логарифмов называют «модуль».

33. Зная, что по модулю 47 $\operatorname{ind}_5 34 \equiv 34 \pmod{46}$, найдите по этому же модулю $\operatorname{ind}_{10} 34$ (10 — первообразный корень по модулю 47).

34. Зная, что по модулю 71 $\operatorname{ind}_7 56 \equiv 19 \pmod{70}$, найдите по этому же модулю $\operatorname{ind}_{11} 56$ (11 — первообразный корень по модулю 71).

35. Составьте таблицы индексов по модулям 29, 31, 59.

36. Определите число решений сравнений: а) $x^{16} \equiv 10 \pmod{37}$; б) $x^5 \equiv 3 \pmod{71}$; в) $x^{21} \equiv 5 \pmod{71}$.

37. Пользуясь таблицами индексов, решите сравнения:
а) $15x^4 \equiv 26 \pmod{29}$; б) $25x^5 \equiv 15 \pmod{73}$;
в) $x^{48} \equiv 2 \pmod{97}$; г) $15x \equiv 19 \pmod{59}$.

38. При помощи таблиц индексов решите показательные сравнения: а) $17 \equiv 7^x \pmod{53}$; б) $6 \cdot 11^x \equiv 56 \pmod{61}$; в) $18^x \equiv 53 \pmod{79}$.

39. Зная, что 2 является первообразным корнем по модулям 101 и 163, решите показательные сравнения: а) $3 \cdot 5^x \equiv 4 \cdot 3^{2x+1} \pmod{101}$; б) $2^x \equiv 3 \cdot 5^{3x} \pmod{163}$.

40. Найдите индекс числа -1 по простому модулю $p > 2$ при произвольном основании g.

41. Докажите, что произведение двух первообразных корней по простому модулю $p > 2$ не может быть первообразным корнем по тому же модулю.

42. Пользуясь теорией индексов, докажите теорему Вильсона для простого $p > 2$.

43. Пользуясь таблицей индексов, среди приведенной системы вычетов по модулю 19 укажите: а) квадратичные вычеты; б) кубичные вычеты.

44. Среди приведенной системы вычетов по модулю 43 укажите: а) числа, принадлежащие показателю 6; б) первообразные корни.

45. Пользуясь таблицами индексов, найдите остатки от деления: а) 342^{256} на 29; б) 581^{3792} на 37; в) $378^{561} \cdot 427^{921}$ на 41.

46. Составьте таблицу индексов для модуля 27, взяв за основание первообразный корень 2; с помощью этой таблицы решите сравнения: а) $5x \equiv 13 \pmod{27}$; б) $x^2 \equiv 10 \pmod{27}$.

47. Составьте таблицу индексов для модуля 50, взяв за основание первообразный корень 3; с помощью этой таблицы решите сравнения: а) $17x \equiv 39 \pmod{50}$; б) $x^2 \equiv 29 \pmod{50}$.

§ 8. АРИФМЕТИЧЕСКИЕ ПРИЛОЖЕНИЯ ТЕОРИИ СРАВНЕНИЙ

1. Конечные систематические дроби. В п. 2 § 8 главы I было показано, что любое натуральное число может быть представлено в виде:

$$a = a_n g^n + a_{n-1} g^{n-1} + \ldots + a_0, \tag{1}$$

где g — натуральное число, называемое основанием системы счисления, и все коэффициенты a_k, $0 \leqslant k \leqslant n$ — целые числа, такие, что $0 \leqslant a_k < g$. При этом было доказано, что

$$a_k = \mathrm{E}\left(\frac{a}{g^k}\right) - g\mathrm{E}\left(\frac{a}{g^{k+1}}\right). \tag{2}$$

Запись натурального числа в виде (1) мы назвали g-ичной или *записью в g-ичной системе счисления*.

В этом пункте мы рассмотрим аналогичное представление любых рациональных чисел. При этом, поскольку любое рациональное число может быть представлено в виде $a = n + r$, где n — целое число, а $0 \leqslant r < 1$, мы ограничимся изучением таких рациональных чисел, что $0 \leqslant r < 1$. Эти числа могут быть записаны в виде правильных положительных дробей: $r = \frac{p}{q}$, $0 \leqslant p < q$.

Самым простым является случай, когда знаменатель дроби является степенью основания системы счисления, т. е. когда $r = \frac{a}{g^n}$, где $0 \leqslant a < g^n$. В этом случае представим числитель дроби в виде g-ичного числа:

$$a = b_m g^m + \ldots + b_0,\ 0 \leqslant m < n \tag{3}$$

и разделим обе части равенства на g^n. Так как $m < n$, то получим следующее представление дроби $\frac{a}{g^n}$:

$$\frac{a}{g^n} = \frac{b_m}{g^{n-m}} + \ldots + \frac{b_0}{g^n},\ 0 \leqslant b_k < g. \tag{4}$$

Добавляя в случае необходимости нулевые слагаемые, можно представить (4) в виде:

$$\frac{a}{g^n} = \frac{b_{n-1}}{g} + \ldots + \frac{b_{n-k}}{g^k} + \ldots + \frac{b_0}{g^n}. \tag{4'}$$

Чтобы сделать запись (4′) похожей на (1), положим $b_{n-k} = a_k$. Тогда

$$\frac{a}{g^n} = \frac{a_1}{g} + \ldots + \frac{a_k}{g^k} + \ldots + \frac{a_n}{g^n}. \tag{5}$$

Мы доказали следующее утверждение:

Т е о р е м а 1. *Любую положительную правильную дробь вида* $r = \frac{a}{g^n}$ *можно представить в виде конечной суммы* (5), *где при всех* k *имеем* $0 \leqslant a_k < g$.

Вместо записи (5) обычно пишут так:

$$\frac{a}{g^n} = 0,\ a_1 \ldots a_n. \tag{5'}$$

Дробь (5′) называют *конечной g-ичной систематической дробью*. При $g = 10$ получаем известные из школы конечные десятичные дроби.

Запись дроби $\frac{a}{g^n}$ в виде (5) однозначно определена, поскольку однозначно определена запись (3) ее числителя (см. п. 2 § 8 главы I).

Запись вида (5) допускают не только дроби $\frac{a}{g^n}$, но и любые дроби $\frac{a}{b}$, обладающие следующим свойством: в разложение знаме-

нателя дроби b на простые множители входят лишь простые числа, участвующие в разложении на простые множители основания системы счисления g. Иными словами, если

$$g = p_1^{\alpha_1} \dots p_k^{\alpha_k}, \text{ то } b = p_1^{\beta_1} \dots p_k^{\beta_k} *.$$

В самом деле, пусть $b = p_1^{\beta_1} \dots p_k^{\beta_k}$ и $g = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Обозначим через β наибольший из показателей $\beta_1, \dots, \beta_k$. Тогда имеем:

$$\frac{a}{b} = \frac{a}{p_1^{\beta_1} \dots p_k^{\beta_k}} = \frac{a p_1^{\alpha_1\beta-\beta_1} \dots p_k^{\alpha_k\beta-\beta_k}}{(p_1^{\alpha_1} \dots p_k^{\alpha_k})^{\beta}} = \frac{a p_1^{\beta\alpha_1-\beta_1} \dots p_k^{\beta\alpha_k-\beta_k}}{g^{\beta}},$$

причем $\beta\alpha_j - \beta_j \geqslant 0$, так как $\alpha_j \geqslant 1$ и $\beta \geqslant \beta_j$.

Отсюда ясно, что дробь $\frac{a}{b}$ в указанном случае можно представить в виде (5).

Справедливо и обратное утверждение: *если дробь* $\frac{a}{b}$ *несократима и ее можно представить в виде (5), то в разложение* b *на простые множители входят лишь простые числа, участвующие в разложении на простые множители основания* g. В самом деле, пусть

$$\frac{a}{b} = \frac{a_1}{g} + \dots + \frac{a_n}{g^n}.$$

Приведем сумму в правой части к одному знаменателю g^n. Получаем, что $\frac{a}{b} = \frac{c}{g^n}$. Значит, $ag^n = bc$. Так как a и b взаимно просты, то по теореме 3 § 3 главы I g^n делится на b. А это может быть лишь при условии, что в разложение b на простые множители входят лишь множители, участвующие и в разложении числа g.

Итак, мы доказали следующую теорему:

Теорема 2. *Правильная несократимая дробь* $\frac{a}{b}$ *может быть представлена в виде*:

$$\frac{a}{b} = \frac{a_1}{g} + \dots + \frac{a_n}{g^n}$$

в том и только том случае, когда в разложение знаменателя b *на простые множители входят только те простые числа, которые участвуют и в разложении на простые множители основания* g.

Следствие. *Несократимая дробь* $\frac{a}{b}$ *может быть представлена в виде десятичной дроби в том и только том случае, когда в разложение ее знаменателя на простые множители входят лишь простые числа* 2 *и* 5, т. е. *когда* $b = 2^{\alpha}5^{\beta}$.

---

* Некоторые из показателей $\beta_1 \dots \beta_k$ могут равняться нулю.

Примеры.

1. Дробь $\frac{7}{96}$ можно записать в виде конечной двенадцатеричной дроби, так как $96 = 3 \cdot 2^5$, а в разложение 12 на простые множители входят лишь 2 и 3. Чтобы получить это разложение, запишем:

$$\frac{7}{96} = \frac{7}{3 \cdot 2^5} = \frac{7 \cdot 3^2 \cdot 2}{(3 \cdot 2^2)^3} = \frac{126}{12^3}.$$

Но $126 = 12 \cdot 10 + 6$, и потому

$$\frac{7}{96} = \frac{12 \cdot 10 + 6}{12^3} = \frac{10}{12^2} + \frac{6}{12^3} = 0{,}0(10)6_{12}.$$

2. Дробь $\frac{9}{160}$ можно записать в виде конечной десятичной дроби, так как $160 = 2^5 \cdot 5$.

3. Дробь $\frac{7}{96}$ нельзя представить в виде конечной десятичной дроби, так как $96 = 2^5 \cdot 3$.

2. Бесконечные систематические дроби. В п. 1 было показано, что лишь узкий класс рациональных чисел может быть представлен в виде конечных g-ичных дробей. Введем теперь бесконечные g-ичные дроби и покажем, что любое рациональное число может быть выражено периодической g-ичной бесконечной дробью. Как и выше, будем рассматривать лишь числа на промежутке $0 \leqslant r < 1$.

Определение 1. *Правильной бесконечной g-ичной дробью* называется ряд

$$\frac{a_1}{g} + \ldots + \frac{a_n}{g^n} + \ldots , \tag{1}$$

где для всех n имеем $0 \leqslant a_n < g$.

Так как для любого n имеем $\frac{a_n}{g^n} \leqslant \frac{1}{g^{n-1}}$, а ряд

$$\sum_{n=1}^{\infty} \frac{1}{g^{n-1}}$$

сходится, поскольку является геометрической прогрессией со знаменателем $g^{-1} < 1$, то и ряд (1) сходится при любых значениях коэффициентов a_n, таких, что $0 \leqslant a_n < g$. Иными словами, всегда существует действительное число a, такое, что

$$a = \frac{a_1}{g} + \ldots + \frac{a_n}{g^n} + \ldots . \tag{2}$$

Это число записывается так:

$$a = 0, a_1 \ldots a_n \ldots . \tag{2'}$$

Запись

$$x = \pm N, a_1 \ldots a \ldots \tag{3}$$

означает, что $x = \pm (N + a)$, где N — натуральное число или нуль, а $a = 0, a_1 \ldots a_n \ldots$

Таким образом, каждой бесконечной g-ичной дроби соответствует некоторое число x. В курсе «Числовые системы» доказывают, что любое действительное число можно представить в виде (3), причем такая запись однозначно определена, за исключением случая, когда x можно записать в виде конечной g-ичной дроби.

Мы разберем здесь лишь вопрос о записи в виде бесконечной g-ичной дроби рациональных чисел. При этом ограничимся случаем, когда $0 \leqslant r < 1$. В этом случае r можно записать в виде $r = \frac{a}{b}$, где $\frac{a}{b}$ — несократимая правильная дробь.

Итак, докажем следующую теорему:

Теорема 3. *Пусть* $\frac{a}{b}$ *— правильная несократимая дробь. Тогда* $\frac{a}{b}$ *можно представить в виде конечной или бесконечной* g*-ичной дроби:*

$$\frac{a}{b} = \frac{a_1}{g} + \ldots + \frac{a_n}{g^n} + \ldots , \tag{4}$$

где при всех n *имеем* $0 \leqslant a_n < g$.

Доказательство. Разделим ga на b с остатком: $ga = ba_1 + r_1$, где $0 \leqslant r_1 < b$. Далее разделим на b с остатком число gr_1: $gr_1 = ba_2 + r_2$, потом число gr_2 и т. д. В результате получим цепочку равенств:

$$\begin{aligned} ga &= ba_1 + r_1, \quad && 0 \leqslant a_1, 0 \leqslant r_1 < b, \\ gr_1 &= ba_2 + r_2, \quad && 0 \leqslant a_2, 0 \leqslant r_2 < b, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ gr_{n-1} &= ba_n + r_n, \quad && 0 \leqslant a_n, 0 \leqslant r_n < b \end{aligned}$$

(если один из остатков, скажем r_n, равен нулю, то все a_k и r_k при $k > n$ равны нулю).

Деля первое равенство на bg, получаем, что

$$\frac{a}{b} = \frac{a_1}{g} + \frac{r_1}{bg}. \tag{5}$$

Далее из второго равенства выводим, что

$$\frac{r_1}{b} = \frac{a_2}{g} + \frac{r_2}{bg}.$$

Подставляя это выражение в (5), находим, что

$$\frac{a}{b} = \frac{a_1}{g} + \frac{a_2}{g^2} + \frac{r_2}{bg^2}.$$

Проводя аналогичные рассуждения, получим, что при любом значении n выполняется равенство:

$$\frac{a}{b} = \frac{a_1}{g} + \frac{a_2}{g^2} + \ldots + \frac{a_n}{g^n} + \frac{r_n}{bg^n}, \tag{6}$$

где $0 \leqslant r_n < b$.

Так как $r_n < b$, то $0 \leqslant \frac{r_n}{bg^n} \leqslant \frac{1}{g^n}$. Значит, $\lim\limits_{n\to\infty} \frac{r_n}{bg^n} = 0$, и поэтому

$$\lim_{n\to\infty}\left(\frac{a}{b} - \frac{a_1}{g} - \ldots - \frac{a_n}{g^n}\right) = \lim_{n\to\infty} \frac{r_n}{bg^n} = 0.$$

Это означает, что $\frac{a}{b}$ является суммой ряда $\sum\limits_{n=1}^{\infty} \frac{a_n}{g^n}$, т. е. что

$$\frac{a}{b} = \frac{a_1}{g} + \ldots + \frac{a_n}{g^n} + \ldots = 0,\ a_1 \ldots a_n \ldots . \tag{7}$$

Чтобы доказать, что (7) дает разложение дроби $\frac{a}{b}$ в бесконечную g-ичную дробь, осталось убедиться в том, что для всех n выполняются неравенства $0 \leqslant a_n < g$. Но из равенства $gr_{n-1} = ba_n + r_n$, где $0 \leqslant r_n < b$, следует, что $a_n = \frac{gr_{n-1}}{b} - \frac{r_n}{b}$. Поскольку по условию $r_{n-1} < b$, то получаем, что $0 \leqslant a_n < g$. Теорема доказана.

Выясним теперь, является ли разложение (4) однозначно определенным т. е. можно ли представить $\frac{a}{b}$ в виде двух различных g-ичных дробей.

Сначала рассмотрим случай, когда $\frac{a}{b}$ — конечная g-ичная дробь:

$$\frac{a}{b} = \frac{a_1}{g} + \ldots + \frac{a_n}{g^n}. \tag{8}$$

По формуле суммы бесконечной геометрической прогрессии имеем:

$$\frac{g-1}{g^{n+1}} + \frac{g-1}{g^{n+2}} + \ldots = \frac{g-1}{g^{n+1}\left(1 - \frac{1}{g}\right)} = \frac{1}{g^n}. \tag{9}$$

Поэтому если $a_n > 0$, то

$$\frac{a_1}{g} + \ldots + \frac{a_n}{g^n} = \frac{a_1}{g} + \ldots + \frac{a_n - 1}{g^n} + \frac{g-1}{g^{n+1}} + \frac{g-1}{g^{n+2}} + \ldots .$$

Это равенство показывает, что если число $\frac{a}{b}$ может быть представлено в виде конечной суммы вида (8), то его можно представить и в виде суммы бесконечного ряда, получаемого уменьшением на 1 последнего отличного от нуля коэффициента a_n и прибавлением суммы вида (9).

Докажем, что для всех остальных рациональных чисел (т. е. для всех чисел, которые нельзя записать в виде конечной суммы (8) представление в виде ряда (4) единственно.

Теорема 4. *Если рациональное число* $r = \frac{a}{b}$, $0 \leqslant r < 1$, *нельзя представить в виде конечной суммы* (8), *то существует единственный ряд вида* (4), *суммой которого является число* r.

Доказательство. Проведем доказательство от противного. Предположим, что r допускает два представления в виде рядов:

$$r = \frac{a_1}{g} + \ldots + \frac{a_n}{g^n} + \ldots \tag{10}$$

и

$$r = \frac{b_1}{g} + \ldots + \frac{b_n}{g^n} + \ldots . \tag{11}$$

Предположим далее, что первые k коэффициентов этих рядов совпадают, $a_1 = b_1, \ldots, a_k = b_k$, но $a_{k+1} > b_{k+1}$. Так как по предположению число r нельзя представить в виде конечной суммы вида (8), то в разложении (10) найдется отличный от нуля коэффициент a_n, где $n > k + 1$. Поэтому имеем неравенство:

$$r > \frac{a_1}{g} + \ldots + \frac{a_{k+1}}{g^{k+1}}. \tag{12}$$

С другой стороны, наибольшее значение для суммы ряда (11) при заданных значениях $b_1 = a_1$, $b_k = a_k$ и b_{k+1} достигается, если

$$b_{k+2} = b_{k+3} = \ldots = g - 1.$$

Значит,

$$\frac{a}{b} \leqslant \frac{a_1}{g} + \ldots + \frac{a_k}{g^k} + \frac{b_{k+1}}{g^{k+1}} + \frac{g-1}{g^{k+2}} + \frac{g-1}{g^{k+3}} + \ldots =$$

$$= \frac{a_0}{g} + \ldots + \frac{a_k}{g^k} + \frac{b_{k+1} + 1}{g^{k+1}}. \tag{13}$$

Так как $a_{k+1} > b_{k+1}$, то $a_{k+1} \geqslant b_{k+1} + 1$, и поэтому

$$\frac{a}{b} \leqslant \frac{a_0}{g} + \ldots + \frac{a_k}{g^k} + \frac{a_{k+1}}{g^{k+1}}. \tag{14}$$

Неравенства (12) и (14) противоречат друг другу. Следовательно, предположение о существовании двух разложений (10) и (11) числа r неверно. Теорема доказана.

Если

$$\frac{a}{b} = \frac{a_1}{g} + \frac{a_2}{g^2} + \ldots + \frac{a_n}{g^n} + \ldots,$$

то

$$\mathrm{E}\left(\frac{g^n a}{b}\right) = a_1 g^{n-1} + \ldots + a_{n-1} g + a_n$$

и

$$\mathrm{E}\left(\frac{g^{n-1}a}{b}\right) = a_1 g^{n-2} + \ldots + a_{n-1}.$$

Значит,

$$a_n = \mathrm{E}\left(\frac{g^n a}{b}\right) - g\mathrm{E}\left(\frac{g^{n-1}a}{b}\right). \tag{15}$$

3. Периодические систематические дроби. Введем следующие определения:

Определение 2. Систематическая дробь по основанию g

$$0, a_1 \ldots a_n \ldots$$

называется *чисто периодической с периодом длины* s, если для всех k выполняется $a_k = a_{k+s}$, причем s — наименьшее натуральное число с этим свойством (иными словами, если $0 < q < s$, то найдется такое k, что $a_k \neq a_{k+q}$).

Определение 3. Систематическая дробь

$$0, a_1 \ldots a_n \ldots$$

называется *смешанной периодической с периодом длины* s, если найдется такое $m > 0$, что для всех $k > m$ имеем: $a_k = a_{k+s}$, причем s — наименьшее натуральное число с этим свойством.

Чисто периодическую дробь с периодом *длины* s записывают:

$$0, (a_1 \ldots a_s),$$

а смешанную периодическую дробь:

$$0, a_1 \ldots a_m(a_{m+1} \ldots a_{m+s}).$$

Примеры.

1. Дробь

$$0{,}142142142 \ldots = 0, (142) —$$

чисто периодическая с периодом 3.

2. Дробь

$$0{,}178212121 \ldots = 0{,}178\,(21) —$$

смешанная периодическая с периодом 2.

Важность понятия периодической систематической дроби становится ясной из следующей теоремы:

Теорема 5. *Пусть знаменатель несократимой правильной дроби* $\frac{a}{b}$ *взаимно прост с основанием системы счисления,* $(b, g) = 1$. *Тогда дробь* $\frac{a}{b}$ *представима в виде чисто периодической* g*-ичной дроби, период* s *которой равен порядку числа* g *по модулю* b (см. п. 1 § 7):

$$\frac{a}{b} = 0, (a_1 a_2 \ldots a_s).$$

Доказательство. Пусть порядок числа g по модулю b равен s. Это значит, что s — наименьшее натуральное число, такое, что

$$g^s \equiv 1 \pmod{b}.$$

Отсюда следует, что $c = \frac{g^s - 1}{b}$ — целое число. Но тогда для любого k имеем:

$$\frac{g^{k+s}a}{b} = \frac{g^k a}{b} + \frac{g^k a\,(g^s - 1)}{b} = \frac{g^k a}{b} + g^k ac,$$

и потому

$$\mathrm{E}\left(\frac{g^{k+s}a}{b}\right) = \mathrm{E}\left(\frac{g^k a}{b}\right) + g^k ac.$$

Значит, по формуле (15) п. 2 для любого k выполняется равенство:

$$a_{k+s} = \mathrm{E}\left(\frac{g^{k+s}a}{b}\right) - g\mathrm{E}\left(\frac{g^{k+s-1}a}{b}\right) = \mathrm{E}\left(\frac{g^k a}{b}\right) + g^k ac - g\left[\mathrm{E}\left(\frac{g^{k-1}a}{b}\right) + g^{k-1}ac\right] = \mathrm{E}\left(\frac{g^k a}{b}\right) - g\mathrm{E}\left(\frac{g^{k-1}a}{b}\right) = a_k.$$

Итак, мы доказали, что для всех k выполняется равенство $a_{k+s} = a_k$.

Чтобы доказать, что s — период, осталось показать, что s — наименьшее натуральное число, такое, что $a_{k+s} = a_k$ для всех k. Предположим, что существует такое число t, что $0 < t < s$, но для всех k выполняется равенство $a_{k+t} = a_k$. Тогда имеем:

$$a_{t+1} = a_1,\ a_{t+2} = a_2,\ \ldots,\ a_{2t} = a_t,\ a_{2t+1} = a_{t+1} = a_1 \text{ и т. д.}$$

Поэтому

$$\frac{a}{b} = \frac{a_1}{g} + \ldots + \frac{a_t}{g^t} + \frac{a_1}{g^{t+1}} + \ldots + \frac{a_t}{g^{2t}} + \ldots.$$

Следовательно,

$$\frac{ag^t}{b} = a_1 g^{t-1} + \ldots + a_t + \frac{a_1}{g} + \ldots + \frac{a_t}{g^t} + \ldots = N + \frac{a}{b},$$

где $N = a_1 g^{t-1} + \ldots + a_t$. Значит,

$$ag^t = Nb + a,\ a\,(g^t - 1) = N^b,$$

и потому

$$a\,(g^t - 1) \equiv 0 \pmod{b}.$$

Так как по условию $(a, b) = 1$, то это сравнение можно сократить на a. Мы получаем, что $g^t \equiv 1 \pmod{b}$, а этого не может быть, поскольку $0 < t < s$, а s — наименьшее натуральное число, для которого $g^s \equiv 1 \pmod{b}$. Теорема доказана.

Мы разобрали полностью два крайних случая: когда b — делитель одного из чисел g^n (см. теорему 2 п. 1) и когда b и g взаимно просты. Рассмотрим теперь общий случай, когда в каноническое разложение числа b входят как простые множители, входящие в

разложение числа g, так и простые множители, не входящие в разложение g.

Теорема 6. *Пусть разложение числа b на простые множители имеет вид:*

$$b = p_1^{\alpha_1} \dots p_k^{\alpha_k} \cdot q_1^{\beta_1} \dots q_l^{\beta_l},$$

причем g делится на $p_1, \dots, p_k$ и не делится на $q_1, \dots, q_s$. Тогда правильная несократимая дробь $\frac{a}{b}$ может быть представлена в виде:

$$\frac{a}{b} = 0, a_1 \dots a_m (a_{m+1} \dots a_{m+s}),$$

где справа стоит смешанная периодическая g-ичная дробь. Период этой дроби равен порядку s числа g по модулю $c = q_1^{\beta_1} \dots q_l^{\beta_l}$, а число цифр между запятой и началом первого периода равно наибольшему из показателей $\alpha_1, \dots, \alpha_k$, т. е. показателей при тех простых числах, на которые делится и основание g, $m = \max(\alpha_1, \dots, \alpha_k)$.

Доказательство. По условию число b можно представить в виде: $b = p_1^{\alpha_1} \dots p_k^{\alpha_k} c$, где $c = q_1^{\beta_1} \dots q_l^{\beta_l}$, а потому $(q, c) = 1$, а $p_1, \dots, p_k$ — простые множители, входящие и в разложение числа g. Пусть $m = \max(\alpha_1, \dots, \alpha_k)$. Тогда g^m делится без остатка на $p_1^{\alpha_1} \dots p_k^{\alpha_k}$, и потому дробь $\frac{ag^m}{b}$ равна несократимой дроби со знаменателем c, взаимно простым с g:

$$\frac{ag^m}{b} = \frac{A}{c}, \quad (g, c) = 1.$$

По теореме 5 дробь $\frac{A}{c}$ можно представить в виде суммы натурального числа N и чисто периодической g-ичной дроби с периодом s, равным порядку g по модулю c. Записывая N в g-ичной системе счисления, получаем, что

$$\frac{A}{c} = a_1 \ g^{m-1} + \dots + a_m + \frac{a_{m+1}}{g} + \dots + \frac{a_{m+s}}{g^s} + \\ + \frac{a_{m+1}}{g^{s+1}} + \dots + \frac{a_{m+s}}{g^{s+m}} + \dots . \qquad (1)$$

Но $\frac{A}{c} = \frac{ag^m}{b}$, и потому $\frac{a}{b} = \frac{A}{cg^m}$. Поэтому, чтобы получить разложение дроби $\frac{a}{b}$, надо обе части равенства (1) разделить на g^m. Мы получим:

$$\frac{a}{b} = \frac{a_1}{g} + \dots + \frac{a_m}{g^m} + \frac{a_{m+1}}{g^{m+1}} + \dots + \frac{a_{m+s}}{g^{m+s}} + \frac{a_{m+1}}{g^{m+s+1}} + \dots + \frac{a_{m+s}}{g^{m+2s}} + \dots,$$

т. е. $\frac{a}{b} = 0, a_1 \dots a_m (a_{m+1} \dots a_{m+s})$. Теорема доказана.

Примеры.

1. Пусть $g = 10$.

а) $\frac{3}{20}$ можно представить в виде конечной десятичной дроби, так как $20 = 2^2 \cdot 5$ (2 и 5 — делители основания $g = 10$).

б) $\frac{7}{13}$ можно представить в виде чистой периодической десятичной дроби, так как $(13, 10) = 1$.

в) $\frac{17}{60}$ можно представить в виде смешанной периодической десятичной дроби. Действительно, $30 = 2^2 \cdot 5 \cdot 3$; 2 и 5 входят в каноническое разложение основания $g = 10$, а 3 не входит.

2. Определим число цифр в периоде десятичной дроби, получающейся при обращении обыкновенной дроби со знаменателем 450.

Имеем: $450 = 5^2 \cdot 2 \cdot 3^2 = 5^2 \cdot 2 \cdot 9$; $10 \equiv 1 \pmod 9$, т. е. 10 принадлежит показателю $s = 1$. Число цифр между запятой и первым периодом равно 2, число цифр в периоде равно 1.

3. Определим число знаков в периоде десятичной дроби, получающейся при обращении обыкновенной дроби $\frac{149}{665}$.

Имеем: $665 = 5 \cdot 7 \cdot 19$.

Множитель 5 основания 10 входит в разложение с показателем 1, следовательно, между запятой и периодом 1 цифра.

Найдем число s цифр в периоде:
$10^s \equiv 1 \pmod{7 \cdot 19}$; $7 \cdot 19 = 133$, $\varphi(133) = \varphi(7) \cdot \varphi(19) = 6 \cdot 18 = 108$. Испытываем последовательно делители числа 108, т. е. 1, 2, 3, 4, 6, 12, 18, 36, 54; находим:

$$10^1 \equiv 10 \pmod{133}$$
$$10^2 \equiv 100 \equiv -33 \pmod{133}$$
$$10^3 \equiv -330 \equiv 39 \pmod{133}$$
$$10^4 \equiv 390 \equiv -9 \pmod{133}$$
$$10^6 \equiv -33 \cdot 9 \equiv -31 \pmod{133}$$
$$10^{12} \equiv 961 \equiv 30 \pmod{133}$$
$$10^{18} \equiv -31 \cdot 30 \equiv 1 \pmod{133}, \text{ т. е. } s = 18.$$

Таким образом, число цифр в периоде $s = 18$.

Ответ. Между запятой и первым периодом 1 цифра, в периоде 18 цифр.

Замечание. Число s цифр в периоде можно находить и другим способом. Из сравнения $10^s \equiv 1 \pmod b$ следует $999 \ldots 9 \equiv 0 \pmod b$; поэтому s можно найти и так: делим 9 на b, затем 99 на b, потом 999 на b и т. д., пока не получим 0 в остатке. Число девяток в этом делимом, а следовательно и число цифр частного, будет равно искомому показателю s.

4. Найдем длину периода, получающегося при обращении дробей $\frac{a_l}{21}$ (где a_l — любое целое, взаимно простое с 21) в десятичные. Здесь $b = 21$.

Делим:

```
99999999... | 21
-99         |---
 84         | 047619
-84
 159
-147
  129
 -126
   39
  -21
   189
  -189
    0
```

В частном получили 6 цифр (считая 0, который соответствует первой девятке); следовательно, $s = 6$, так что искомый период состоит из шести цифр.

4. Нахождение остатков при делении на данное число. Остаток и частное при делении на данное число можно получать с помощью алгоритма деления. Однако при больших числах применение алгоритма деления приводит к длинным вычислениям. Во многих случаях можно значительно проще получить результат, используя свойства сравнений.

Так как каждое целое число может быть представлено в виде суммы или разности целых чисел, в виде степени или суммы степеней, то достаточно научиться быстро находить остаток от деления суммы, разности, степени, суммы степеней на некоторое число m.

Из теории сравнений известно, что целое число a и остаток r от деления a на число m принадлежит одному и тому же классу по модулю m, т. е. $a \equiv r \pmod m$. Остаток r является наименьшим неотрицательным вычетом числа a по модулю m.

Пусть r_1, r_2, ..., r_n — остатки от деления чисел a_1, a_2, ..., a_n на m. Тогда:

$$\begin{aligned} a_1 &\equiv r_1 \pmod m \\ a_2 &\equiv r_2 \pmod m \\ &\cdots\cdots\cdots \\ a_n &\equiv r_n \pmod m \end{aligned} \qquad (1)$$

а) Складывая почленно сравнения (1), получим:

$$a_1 + a_2 + \ldots + a_n \equiv r_1 + r_2 + \ldots + r_n \pmod m. \qquad (2)$$

Из (2) следует, что остатки от деления чисел

$$a_1 + a_2 + \ldots + a_n \text{ и } r_1 + r_2 + \ldots + r_n \text{ на } m$$

равны. Следовательно, нахождение остатка от деления числа $a_1 + a_2 + \ldots + a_n$ на m можно заменить более легкой задачей — нахождением остатка от деления числа $r_1 + r_2 + \ldots + r_n$ на m.

Если $r_1 + r_2 + \ldots + r_n < m$, то $r_1 + r_2 + \ldots + r_n$ и будет искомым остатком.

Вычитая, например, второе сравнение (1) из первого почленно, получим: $a_1 - a_2 \equiv (r_1 - r_2) \pmod m$ (можно и наоборот, тогда $a_2 - a_1 \equiv (r_2 - r_1) \pmod m$). Вывод аналогичен предыдущему.

б) Умножая почленно сравнения (1), получим сравнение $a_1 a_2 \ldots a_n \equiv r_1 r_2 \ldots r_n \pmod m$. Отсюда вытекает утверждение, аналогичное утверждению пункта а).

в) Если $a_1 = a_2 = \ldots = a_n = a$, то получим:

$$a^n \equiv r^n \pmod m.$$

Следовательно, нахождение остатка от деления a^n на m сводится к нахождению остатка от деления r^n на m. Задача упрощается, но при больших n и m может оказаться все же трудоемкой. Остановимся на наиболее употребительных приемах, применяющихся в этом случае.

1) Последовательное возведение в степень сравнения $r \equiv r \pmod m$ с последовательной заменой правой части получающегося сравнения абсолютно наименьшими вычетами по модулю m. Перемножение соответствующих сравнений (см. пример 2).

2) Если r и m взаимно просты, т. е. $(r, m) = 1$, то можно воспользоваться теоремой Эйлера (в случае $m = p$ — теоремой Ферма).

По теореме Эйлера: $r^{\varphi(m)} \equiv 1 \pmod m$. Разделим далее n на $\varphi(m)$ с остатком: $n = \varphi(m)\, q + k$. Тогда получим:

$$r^n = r^{\varphi(m)q+k} = r^{\varphi(m)q} \cdot r^k \equiv r^k \pmod m,$$

и задача отыскания остатка от деления r^n на m, таким образом, сводится к нахождению остатка от деления r^k на m (где $k < \varphi(m)$), что практически часто уже не вызывает затруднений.

3) Если $m = p$ — число простое, то можно воспользоваться свойствами (и таблицами) индексов.

Имеем: $r^n \equiv x \pmod p$. Решая это сравнение, находим последовательно $n \operatorname{ind} r \equiv \operatorname{ind} x \pmod{p-1}$, $x \equiv l \pmod p$. Наименьший неотрицательный вычет из этого класса чисел по модулю p — искомый остаток, он равен l.

Рассмотрим примеры.

Примеры.

1. Найдем наименьший неотрицательный остаток от деления числа $n = (5622 + 179 - 346) \cdot 923$ на 23.

Находим остатки от деления на 23 чисел: $5622+179-346=5455$ и 923; получим соответственно 4 и 3. Далее, так как $4 \cdot 3 = 12$, то $n \equiv 12 \pmod{23}$. Искомый остаток $r = 12$.

2. Найдем наименьший неотрицательный остаток от деления числа $n = (631^{57} + 250^{28}) \cdot 926$ на 12.

1) Находим остаток r_1 от деления числа 631^{57}. Так как $631 \equiv 7 \pmod{12}$, то $631^{57} \equiv 7^{57} \pmod{12}$. Но $\varphi(12) = 4$ и потому $7^4 \equiv 1 \pmod{12}$. Значит, $7^{57} = 7^{4 \cdot 14} \cdot 7 \equiv 7 \pmod{12}$.
Следовательно, $r_1 = 7$.

2) Находим остаток r_2 от деления 250^{28} на 12.
Так как $250 \equiv 10 \pmod{12}$, то $250^{28} \equiv 10^{28} \equiv 2^{28} \cdot 5^{28} \pmod{12}$.

Но по теореме Эйлера $5^4 \equiv 1 \pmod{12}$ и потому $5^{28} \equiv 1 \pmod{12}$. Теорема Эйлера непосредственно к 2^{28} не применима, так как числа 2 и 12 не являются взаимно простыми. Но $2^2 \equiv 1 \pmod{3}$, а потому $2^{26} = (2^2)^{13} \equiv 1 \pmod{3}$. Значит, $2^{28} = 2^{26} \cdot 2^2 \equiv 2^2 \pmod{12}$. Итак, $10^{28} \equiv 1 \cdot 4 \pmod{12}$.

Следовательно, $r_2 = 4$.

3) Находим остаток r_3 от деления числа 926 на 12; $r_3 = 2$. Таким образом, $n \equiv (7 + 4) \cdot 2 = 22 \equiv 10 \pmod{12}$, а искомый остаток $r = 10$.

3. Вычислим остаток от деления числа $7^{161} - 3^{80}$ на 100.

Здесь $(7, 100) = 1$, $(3, 100) = 1$, $\varphi(100) = 100\left(1 - \frac{1}{5}\right) = 40$, а потому $7^{161} - 3^{80} = (7^{40})^4 \cdot 7 - (3^{40})^2 \equiv 1^4 \cdot 7 - 1^2 \equiv 6 \pmod{100}$, т. е. остаток равен 6.

4. Вычислим остаток от деления 272^{1141} на 135.
Имеем: $(272, 135) = 1$, $\varphi(135) = 135\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 72$.
Так как $272 \equiv 2 \pmod{135}$ и $1141 = 15 \cdot 72 + 61$, то

$$272^{1141} \equiv 2^{1141} \equiv (2^{72})^{15} \cdot 2^{61} \equiv 2^{61} \pmod{135}$$

(так как $2^{72} \equiv 1 \pmod{135}$ согласно теореме Эйлера).

Далее, $61 = 1 + 32 + 16 + 8 + 4$:

$$\begin{aligned}
2 &\equiv 2 \pmod{135} \ (*)\\
2^2 &\equiv 4 \pmod{135}\\
2^4 &\equiv 16 \pmod{135} \ (*)\\
2^8 &\equiv 256 \equiv 121 \equiv -14 \pmod{135} \ (*)\\
2^{16} &\equiv 196 \equiv -39 \pmod{135} \ (*)\\
2^{32} &\equiv 1521 \equiv 34 \pmod{135} \ (*)
\end{aligned}$$

Умножая сравнения (*), получим: $2^{61} \equiv 2 \cdot 16 \cdot (-14) \cdot (-39) \times 34 = (2 \cdot 16 \cdot 14) \cdot (39 \cdot 34) = 448 \cdot 1326 \equiv 43 \cdot 111 \equiv 48 \pmod{135}$.
Окончательно имеем: $272^{1141} \equiv 2^{61} \equiv 48 \pmod{135}$, т. е. искомый остаток равен 48.

5. Найдем остаток от деления числа 763^{17} на 29.

Так как $763 \equiv 9 \pmod{129}$, то $763^{17} \equiv 9^{17} \pmod{29}$. Число 29 простое, и можно поэтому воспользоваться свойствами индексов. Имеем: $9^{17} \equiv x \pmod{29}$; тогда

$$17 \operatorname{ind} 9 \equiv \operatorname{ind} x \pmod{28},\ 17 \cdot 10 \equiv x \pmod{28},$$
$$\operatorname{ind} x \equiv 170 \equiv 2 \pmod{28},\ x \equiv 4 \pmod{29},$$

следовательно, искомый остаток $r = 4$.

5. Признаки делимости. Очень часто возникает потребность, не производя самого деления, ответить на вопрос о делимости одного числа на другое. Критерий, устанавливающий необходимое и достаточное условие делимости произвольного натурального числа N на данное натуральное число m, называется *признаком делимости на* m.

Различают общие признаки, имеющие силу для любого m, и частные — для отдельных значений m.

Общий признак делимости выражает правило, посредством которого по цифрам числа N, записанного в системе счисления с основанием g, можно судить о делимости его на другое число m.

Французский математик Блез Паскаль (1623—1662) нашел общий признак делимости, который в терминах сравнений может быть сформулирован следующим образом:

Теорема 7 (общий признак делимости Паскаля). *Для того чтобы число* N, *записанное в произвольной* g*-ичной системе счисления в виде*:

$$N = a_n g^n + a_{n-1} g^{n-1} + \ldots + a_1 g + a_0,$$

делилось на число m, *необходимо и достаточно, чтобы число* $Q = a_n r_n + a_{n-1} r_{n-1} + \ldots + a_1 r_1 + a_0$ *делилось на* m (здесь a_i — цифры числа N, а r_i — абсолютно наименьшие вычеты соответствующих степеней g^i по модулю m, $i = 1, 2, \ldots, n$).

Доказательство. Пусть $g^i \equiv r_i \pmod{m}$, где r_i — абсолютно наименьший вычет числа g^i по модулю m ($i = 1, 2, \ldots, n$). Тогда

$$N = a_n g^n + a_{n-1} g^{n-1} + \ldots + a_1 g + a_0 \equiv a_n r_n + a_{n-1} r_{n-1} + \ldots + a_1 r_1 + a_0 \pmod{m}. \quad (1)$$

Число N делится на m тогда и только тогда, когда

$$N = a_n g^n + a_{n-1} g^{n-1} + \ldots + a_1 g + a_0 \equiv 0 \pmod{m}. \quad (2)$$

Из сравнений (1) и (2) и транзитивности отношения сравнимости получаем условие, равносильное условию (2):

$$Q = a_n r_n + a_{n-1} r_{n-1} + \ldots + a_1 r_1 + a_0 \equiv 0 \pmod{m}. \quad (3)$$

Из доказанного следует вывод: для того чтобы N делилось на m, необходимо и достаточно, чтобы Q делилось на m.

Теорема доказана.

В качестве следствий из общего признака Паскаля вытекают различные частные признаки делимости. Рассмотрим некоторые из них (наиболее часто используемые на практике).

Следствие 1. *Пусть m — делитель числа $g-1$. Для того чтобы число, записанное в g-ичной системе счисления, делилось на m, необходимо и достаточно, чтобы сумма его цифр делилась на m.*

Доказательство. В данном случае $g^i \equiv 1 (\mathrm{mod}\ (g-1))$, а $g-1 \vdots m$; тогда $g^i \equiv 1 \pmod m$, т. е. $r_i = 1$, а потому:

$$Q = a_n + a_{n-1} + \ldots + a_1 + a_0.$$

Таким образом, для того чтобы N делилось на m, необходимо и достаточно, чтобы сумма цифр этого числа делилась на m.

Для чисел, записанных в десятичной системе, из сформулированного признака вытекают известные признаки делимости на 9 и 3.

Следствие 2. *Пусть m — делитель числа $g+1$. Для того чтобы число, записанное в g-ичной системе счисления, делилось на m, необходимо и достаточно, чтобы разность между суммами цифр на четных и нечетных местах делилась на m.*

Доказательство. В данном случае $g^i \equiv (-1)^i \pmod{(g+1)}$, а $g+1 \vdots m$; тогда $g^i \equiv (-1)^i \pmod m$, т. е. $r_i = (-1)^i$, а потому $Q = a_n(-1)^n + a_{n-1}(-1)^{n-1} + \ldots + a_2(-1)^2 + a_1(-1) + a_0$. Отсюда вытекает утверждение следствия.

Для чисел, записанных в десятичной системе, получаем известный признак делимости на 11: для того чтобы число делилось на 11, необходимо и достаточно, чтобы разность между суммами цифр на четных и нечетных местах делилась на 11.

Например, число 25 697 058 не делится на 11, так как разность $(2+6+7+5)-(5+9+0+8) = 20-22 = -2$ не делится на 11.

Число 905 784 делится на 11.

Следствие 3. *Пусть m — делитель числа g^k. Для того чтобы число, записанное в g-ичной системе счисления, делилось на m, необходимо и достаточно, чтобы число, записанное последними k цифрами данного числа, делилось на m.*

Доказательство. В данном случае $g^i \equiv 0 \pmod{g^k}$ для $i \geqslant k$, а потому

$$N = a_n g^n + \ldots + a_k g^k + a_{k-1}g^{k-1} + \ldots + a_1 g + a_0 \equiv a_{k-1}g^{k-1} + \ldots + a_1 g + a_0 \pmod{g^k}.$$

Но так как $g^k \vdots m$, то

$$N \equiv a_{k-1}g^{k-1} + \ldots + a_1 g + a_0 \pmod m$$

или

$$\overline{a_{k-1} \dots a_1 a_{0_g}} \equiv 0 \pmod{m}. \qquad (*)$$

Из (*) вытекает утверждение следствия.

Для чисел, записанных в десятичной системе, из следствия 3 вытекает целый ряд частных признаков делимости.

1) Основание 10^1 (здесь $k = 1$) делится на 2, 5, 10.

В этом случае получим признаки делимости на 2, 5, 10.

а) Для делимости числа на 2 необходимо и достаточно, чтобы последняя цифра была четной.

б) Для делимости числа на 5 необходимо и достаточно, чтобы последняя цифра делилась на 5 (последняя цифра 0 или 5).

в) Для делимости числа на 10 необходимо и достаточно, чтобы оно оканчивалось нулем.

2) Делителем числа 10^2 (здесь $k = 2$) являются числа 4, 25, 50, 100.

Применяя следствие 3, получаем известные признаки делимости на 4, 25, 50, 100.

В частности, для того чтобы число делилось на 4, необходимо и достаточно, чтобы число, записанное последними двумя ($k = 2$) цифрами, делилось на 4.

3) Аналогично можно вывести признаки делимости на делители числа 10^3 ($k = 3$), т. е. на числа 8, 125, ... Здесь надо рассматривать число, записанное последними тремя цифрами данного числа.

В заключение выведем общий признак делимости на 7, 11, 13. Признак делимости на 7 и на 13 можно получить и непосредственно из общего признака Паскаля, но он получается неудобным для практического использования. Мы воспользуемся другим приемом и сразу для десятичной системы.

Т е о р е м а 8. *Для того чтобы число 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 (или наоборот), делилась на 7, или на 11, или на 13.*

Д о к а з а т е л ь с т в о. Любое число N можно представить в виде $N = n \cdot 1000 + Q$, где Q — число, записанное последними тремя цифрами числа N, а n — всеми остальными цифрами (пример: $829\,296 = 829 \cdot 1000 + 296$).

Заметим также, что $7 \cdot 11 \cdot 13 = 1001$.

Запишем далее N так:

$$N = n \cdot 1001 - n + Q = n \cdot 1001 + (n - Q);$$

отсюда получим:

$$N \equiv n - Q \pmod{1001}, \qquad (4)$$

или

$$N = n - Q \pmod{7 \cdot 11 \cdot 13}.$$

Из (4) следует вывод: для того чтобы число N делилось на 7, или на 11, или на 13, необходимо и достаточно, чтобы число $n - Q$ (или $Q - n$) делилось на 7, или на 11, или на 13.

Примеры.

1. Делится ли число 56 704 на одно из чисел: 7, 11, 13?

Находим: $Q - n = 704 - 56 = 648$. Но число 648 не делится ни на 7, ни на 11, ни на 13; следовательно, и данное число не делится ни на одно из чисел: 7, 11, 13.

2. Делится ли число 454 111 на 7?

$454 - 111 = 343$, $343 \vdots 7$; следовательно, $454\,111 \vdots 7$.

6. Проверка результатов арифметических действий. С помощью сравнений легко указать необходимые признаки правильности и достаточные признаки неправильности результатов выполнения арифметических действий сложения, вычитания и умножения целых чисел.

Результат действия сложения, вычитания и умножения есть целая рациональная функция компонент, а потому если вместо данных чисел взять наименьшие положительные или наименьшие по абсолютной величине вычеты этих чисел по какому-либо модулю, то результат действий над этими вычетами должен быть сравним по тому же модулю с наименьшим вычетом проверяемого результата. Если сравнение не имеет места, то результат получен неверно. В качестве модуля удобнее брать число, наименьшие вычеты по которому легко вычисляются (например, для десятичной системы счисления — 9 или 11). В случае 9 можно брать вместо наименьших вычетов просто сумму цифр, в случае 11 — разность между суммами цифр, стоящих на четных и нечетных местах (считая справа налево).

Следует отметить, что неправильность соответствующего сравнения гарантирует неправильность выполнения действий. Правильность соответствующего сравнения лишь подтверждает, но не гарантирует правильность результата. Дело в том, что проверкой с помощью 9 или 11 не может быть обнаружена ошибка на число, кратное 9 или 11 соответственно. Поэтому чаще всего проверяют одновременно числами 9 и 11. В этом случае возможна ошибка на число, кратное 99, но вероятность такой ошибки очень мала.

Примеры.

1. Проверим правильность выполнения действий (с помощью 9 и 11):

$$8\,740\,297 - 561\,245 = 8\,179\,052.$$

а) Проверка девяткой. Заменяем числа суммами их цифр:

$$37 - 23 \equiv 32 \pmod 9, \quad 14 \equiv 32 \pmod 9.$$

Сравнение подтверждает, но не гарантирует правильности выполнения действий.

б) Проверка числом 11.

$$8\,740\,297 \equiv (7 + 2 + 4 + 8) - (9 + 0 + 7) \equiv 5 \pmod{11},$$
$$561\,245 \equiv (5 + 2 + 6) - (4 + 1 + 5) \equiv 3 \pmod{11},$$
$$8\,179\,052 \equiv (2 + 0 + 7 + 8) - (5 + 9 + 1) \equiv 2 \pmod{11}.$$

Получим: $5 - 3 \equiv 2 \pmod{11}$, $2 \equiv 2 \pmod{11}$).

Проверка одиннадцатью подтверждает правильность получения результата (хотя абсолютной гарантии нет, так как возможна ошибка на число, кратное 99).

2. Проверим правильность выполнения действий (с помощью 9):

$$375\,426 \cdot 3846 = 1\,443\,888\,276.$$

Заменяем числа суммами их цифр:

$$27 \cdot 21 \not\equiv 51 \pmod 9, \text{ так как } 0 \cdot 3 \not\equiv 6 \pmod 9.$$

Следовательно, действие выполнено неправильно.

Результат деления проверяется с помощью контроля умножения (делимое равно делителю, умноженному на частное, плюс остаток). Вообще следует иметь в виду, что соблюдение контроля при неверных вычислениях связано, по меньшей мере, с двукратной ошибкой в вычислениях, поэтому следует признать контроль (даже одним числом) действенным.

Вопросы для самопроверки и упражнения

1. От чего зависит характер разложения обыкновенной дроби $\frac{a}{b}$ в систематическую с основанием g?

2. В чем заключается необходимое условие возможности представления обыкновенной дроби $\frac{a}{b}$ в виде конечной систематической дроби с основанием g? Как это условие формулируется, если $g=10$?

3. В чем заключается достаточное условие возможности представления обыкновенной дроби $\frac{a}{b}$ в виде конечной g-ичной дроби? Как это условие формулируется, если $g = 10$?

4. Какая из следующих обыкновенных дробей представима в виде конечной десятичной дроби? Объясните почему.

а) $\frac{27}{40}$; б) $\frac{35}{61}$; в) $\frac{41}{140}$.

5. В чем заключается достаточное условие возможности представления обыкновенной дроби $\frac{a}{b}$:

а) в виде чисто периодической g-ичной дроби;

б) в виде смешанной периодической g-ичной дроби?

6. Основание системы счисления $g = 10$. Установите вид десятичной дроби, которая получится при обращении обыкновенной дроби:

а) $\frac{37}{41}$; б) $\frac{73}{85}$; в) $\frac{49}{60}$.

7. Как находится длина периода и длина предпериода при обращении обыкновенной дроби в g-ичную? Сформулируйте правило; найдите длину периода и длину предпериода при обращении дроби $\left(\frac{7}{12}\right)_{10}$ в десятичную (не производя самого обращения).

8. Существует ли рациональное число, обращающееся в бесконечную непериодическую дробь?

9. Основание системы счисления $g = 12$. Установите вид двенадцатеричной дроби, в которую обратится обыкновенная дробь:

а) $\left(\frac{1}{6}\right)_{12}$; б) $\left(\frac{1}{29}\right)_{12}$; в) $\left(\frac{2}{5}\right)_{12}$.

10. Какие из следующих обыкновенных дробей могут быть представлены в виде конечных десятичных дробей? Объясните почему.

а) $\frac{12}{43}$; б) $\frac{16}{155}$; в) $\frac{37}{80}$; г) $\frac{361}{480}$; д) $4\frac{500}{503}$; е) $\frac{517}{500}$; ж) $\frac{59}{600}$.

11. Какие из следующих обыкновенных дробей могут быть представлены в виде смешанных периодических дробей:

а) $\frac{13}{71}$; б) $8\frac{89}{310}$; в) $\frac{89}{160}$; г) $\frac{101}{242}$?

12. Какие из следующих дробей могут быть представлены в виде чисто периодических десятичных дробей:

а) $\frac{49}{741}$; б) $\frac{30}{83}$; в) $\frac{109}{80}$; г) $\frac{113}{227}$; д) $\frac{100}{349}$?

13. Представьте в виде систематических следующие обыкновенные дроби:

а) $\left(\frac{1}{2}\right)_3$; б) $\left(\frac{1}{20}\right)_5$; в) $\left(\frac{17}{40}\right)_8$; г) $\left(\frac{11}{23}\right)_6$; д) $\left(\frac{11}{12}\right)_4$; е) $\left(\frac{1}{5}\right)_7$; ж) $\left(\frac{25}{5}\right)_{11}$; з) $\left(\frac{10}{8}\right)_{12}$; и) $\left(\frac{3}{13}\right)_9$.

14. Основание системы счисления $g = 12$. Какие обыкновенные дроби обратятся в конечные, в чисто периодические, в смешанные периодические двенадцатеричные дроби?

15. Найдите число цифр в периоде чистых десятичных дробей, в которые обращаются несократимые обыкновенные дроби со знаменателями: 3, 7, 9, 11, 13, 19, 21, 23, 27, 37.

16. Найдите длину предпериода и длину периода, получающихся при обращении следующих обыкновенных дробей в десятич-

ные: а) $\frac{13}{45}$; б) $\frac{13}{110}$; в) $\frac{35}{11}$; г) $\frac{17}{24}$; д) $\frac{12}{35}$; е) $\frac{43}{280}$; ж) $\frac{599}{280}$; з) $\frac{43}{17200}$; и) $\frac{109}{97000}$.

17. Найдите длину периода и число цифр между запятой и периодом десятичных дробей, в которые обращаются обыкновенные несократимые дроби со знаменателями: а) 6; б) 12; в) 14; г) 18; д) 44; е) 220; ж) 432; з) 888.

18. Докажите, что сумма, разность, произведение и частное двух периодических дробей — периодическая дробь.

19. Докажите, что сумма трех чисел, обратных трем последовательным натуральным числам, обращается в смешанную бесконечную периодическую десятичную дробь.

20. Докажите, что бесконечная десятичная дробь 0,12345678910111213141516..., полученная записью после запятой всех натуральных чисел, не является периодической десятичной дробью.

21. Найдите длину периода δ, число цифр γ между запятой и периодом десятичных дробей, в которые обращаются обыкновенные несократимые дроби со знаменателями: а) $3 \cdot 11$; б) $11 \cdot 17$; в) $19 \cdot 27$; г) $2^3 5^2 \cdot 19 \cdot 37$; д) $2^4 \cdot 5^3 \cdot 13 \cdot 17 \cdot 19 \cdot 37$.

22. Докажите, что если 10 есть первообразный корень по модулю m, то периоды всех несократимых дробей со знаменателем m будут состоять из круговых перестановок одной и той же системы $k = \varphi(m)$ цифр.

23. Найдите знаменатель дроби, обращающейся в чистую периодическую дробь с тремя цифрами в периоде.

24. При помощи таблиц индексов определите количество цифр в периоде разложения дробей $\frac{1}{43}$, $\frac{1}{89}$, $\frac{1}{9797}$ в бесконечную десятичную дробь.

25. Обратите следующие периодические десятичные дроби в обыкновенные: а) 0,35 (62); б) 5,1 (538); в) 3, (27); г) 11, 12 (31).

26. К какой задаче сводится нахождение неотрицательного остатка от деления целого числа m на натуральное число n?

27. К какой задаче сводится нахождение неотрицательного остатка от деления на натуральное число m:

а) суммы целых чисел $a_1 + a_2 + \ldots + a_n$,

б) произведения целых чисел $a_1 \cdot a_2 \ldots a_n$,

в) степени a^n?

28. Какие приемы используются для нахождения неотрицательного остатка от деления r^n на m? В каком случае возможно использовать: а) теорему Эйлера; б) свойства (и таблицы) индексов?

29. Можно ли для нахождения остатка от деления $2^{27} + 3^{150}$ на 3 применить теорему Эйлера? теорему Ферма? Почему?

30. Как применить свойства и таблицы индексов для вычисления остатков от деления на простое число p?

31. Что называется признаком делимости числа N на натуральное число m?

32. Сформулируйте общий признак делимости Паскаля. Что означают a_i и r_i в выражении $Q = a_n r_n + a_{n-1} r_{n-1} + a_1 r_1 + a_0$?

33. Сформулируйте следствия признака делимости Паскаля для случая, когда g равно десяти.

34. Сформулируйте признак делимости на 4, 25, 50, 100.

35. Сформулируйте признаки делимости на 2 и 5, на 3 и 9, на 7, 11, 13. Делится ли 29 617 на 7, 2596 на 11, 28 793 на 13?

36. На каком утверждении основана проверка арифметических действий с помощью сравнений?

37. Какое условие является необходимым для того, чтобы результат арифметических действий $N = f(N_1, N_2, \ldots, N_k)$, где f — многочлен от целых чисел $N_1, N_2, \ldots, N_k$, был правильным? Является ли это условие достаточным? Почему?

38. Сформулируйте необходимое условие проверки результатов действий сложения, вычитания и умножения числами 9 и 11.

39. Как проверить правильность результата деления?

40. Найдите остаток от деления: а) $7^{100} + 11^{100}$ на 13; б) $8^{80} + 13^{90}$ на 17; в) $(85^{70} + 19^{32})^{17}$ на 21; г) $(84^{80} + 23^{40})^{15}$ на 25; д) $(15728 + 19^{30})^7$ на 57; е) $(12371^{56} + 34^{28})$ на 243.

41. Докажите, что: а) число $1^{18} + 2^{18} + 3^{18} + 4^{18} + 5^{18} + 6^{18} + 1$ делится на 7; б) число $7^{40} - 5^{30}$ делится на 11; в) число $8^{80} + 13^{90}$ делится на 17; г) число $13^{176} - 1$ делится на 89.

42. Покажите, что остаток от деления числа $3^{19} \cdot 37 - 1$ на $19 \cdot 37$ равен 1.

43. Какие остатки может иметь сотая степень целого числа N при делении на 125?

44. Найдите последнюю цифру числа: а) 9^{9^9}; б) 2^{3^4}.

45. Найдите две последние цифры числа: а) 2^{999}; б) 3^{999}.

46. Найдите последние три цифры числа 243^{402}.

47. Руководствуясь таблицей индексов, найдите остаток от деления: а) 10^{10} на 67; б) 12^{12} на 73; в) $85 \cdot 79$ на 97.

48. Методом сравнений докажите такие утверждения:

1) при любом натуральном n: а) $n^7 + 6n$ делится на 7; б) $10^n (9n - 1) + 1$ делится на 9; в) $3 \cdot 5^{2n+1} + 2^{3n+1}$ делится на 17;

2) $2^{5n} - 1$ делится на 31;

3) а) $2222^{5555} + 5555^{2222}$ делится на 7; б) $43^{23} + 24^{43}$ делится на 66.

49. 13-я степень некоторого однозначного числа имеет цифрой единиц 7. Пользуясь таблицами индексов, найдите число.

50. Выведите признаки делимости чисел в десятичной системе счисления на 13.

51. Для каких чисел m признаки делимости на m в системах счисления с основаниями: а) 13 и б) 25 аналогичны признакам делимости на 3 в десятичной системе счисления?

52. В какой системе счисления признаки делимости на числа 2, 3, 4, ... , n аналогичны признакам делимости на 3 в десятичной системе?

53. Укажите системы счисления, для которых признаки делимости на 13 и 11 те же, что для десятичной системы счисления.

54. Принимая за основание системы счисления $g = 1000$, выведите признаки делимости на $\alpha = 3, 9, 27, 111, 333, 999$.

Замечание. При $\alpha = 3; 9$ к числу μ снова можно применить известный для них признак делимости: $\mu \equiv \mu_1 = a_0 + a_1 + a_2 \pmod{3; 9}$.

55. Найдите признаки делимости на 2, 3, 4, 5, 7, 9 для восьмеричной системы счисления.

56. Найдите признаки делимости на 2, 3, 4, 5, 6, 7, 8, 9, 11, 13 для двенадцатеричной системы счисления.

57. Пусть $p \neq 2; 5$ — простое число. Разбивая число на грани, по $\frac{p-1}{2}$ цифр в каждой грани, т. е. переходя к системе счисления с основанием $g = 10^{\frac{p-1}{2}}$, мы получим признак делимости на p, аналогичный признаку делимости на 9 или на 11, в зависимости от того, будет ли 10 являться соответственно квадратным вычетом или невычетом по модулю p. Докажите это утверждение.

58. Проверьте правильность результата вычислений числом 9:

а) $12\,376 \cdot (809\,376 - 745\,934) + 43^2 \cdot 97\,215 = 964\,907\,727$;

б) $(378^3 - 7\,298\,348) \cdot 10 + (427\,019 - 451^2) \cdot 50 = 578\,298\,940$.

59. Проверьте правильность результата вычислений числом 11:

а) $437 \cdot 86 + 16\,384 = 54\,866$; б) $8264 \cdot 5201 = 42\,981\,064$;

в) $(2708^2 - 8\,513\,874) \cdot 18 - 37^3 \cdot 179 = 276\,181\,597$.

60. Проверьте правильность выполнения арифметических действий числами 9 и 11:

а) $3125 \cdot 256 = 800\,000$; б) $4325 \cdot 897 = 454\,125$;

в) $6735 \cdot 324 = 2\,178\,900$; г) $3745 \cdot 8067 = 30\,210\,915$.

КРАТКИЕ ИСТОРИЧЕСКИЕ СВЕДЕНИЯ О РАЗВИТИИ ТЕОРИИ ЧИСЕЛ

Возникновение первых представлений о натуральных числах относится к доисторическому периоду. Археологи, изучив графику палеолита (древнекаменного века), нашли предметы, покрытые черточками и точками, которые были сгруппированы по 3, по 4 или по 5. Некоторые знаки были сгруппированы по 7 и, по-видимому, отражали наблюдения за фазами Луны. Следующим этапом в развитии понятия о числе было выделение множеств-посредников, позволявших сравнивать друг с другом численность иных множеств. В качестве элементов таких множеств-посредников использовались камешки, раковины, пальцы. В дальнейшем были выделены множества-эталоны, что привело в конце концов к созданию общего представления о натуральном числе. Впоследствии люди пришли к идее о бесконечности множества натуральных чисел («Псаммит» Архимеда, III в. до н. э.).

В древнейших дошедших до нас письменных памятниках (древнеегипетские папирусы, ассиро-вавилонская клинопись) уже имеются обозначения для чисел и содержатся математические задачи, решение которых сводится к арифметическим операциям над натуральными числами. Математики Древнего Вавилона имели представление о квадратах и кубах чисел, знали теорему Пифагора и умели решать несложные квадратные уравнения.

В эту эпоху натуральные числа выступали как орудие познания, но не являлись предметом изучения. Исследование свойств натуральных чисел начинается в Древней Греции в школе знаменитого математика и философа Пифагора (VI в. до н. э.). Изучение музыкальной гармонии привело пифагорейцев к рассмотрению отношений между длинами струн. В результате этого они пришли к выводу, что «элементы чисел являются элементами всех вещей и что весь мир в целом является гармонией и числом».

Изучая свойства натуральных чисел, пифагорейцы выделили разные виды таких чисел: четные и нечетные, простые и составные. Значительное внимание они уделяли числам, представимым в виде суммы членов арифметических прогрессий, начинающихся с числа 1. Эти числа изображались как количества точек в некоторых геометрических фигурах (треугольниках, квадратах и т. д.). Поэтому их называли *фигурными числами*. Например, складывая члены натурального ряда чисел 1, 2, 3, ..., получали *треугольные*

числа 1, $1+2=3$, $1+2+3=6$ и т. д. А складывая нечетные числа, получали *квадратные числа*, т. е. квадраты натуральных чисел (1, $1+3=4$, $1+3+5=9$, $1+3+5+7=16$ и т. д.). Наряду с этими *многоугольными числами* рассматривали *пирамидальные числа*, являвшиеся суммами многоугольных чисел, например 1, $1+3=4$, $1+3+6=10$, $1+3+6+10=20$ и т. д. или $1,1+4=5,1+4+9=14,1+4+9+16=30$ и т. д.

Пифагорейцы пытались выразить с помощью натуральных чисел такие абстрактные понятия, как совершенство, дружба и т. д. Например, они считали *совершенными* числа, равные сумме своих делителей, отличных от самого числа ($6=1+2+3$, $28=1+2+4+7+14$), а *дружественными* они называли два числа, каждое из которых равнялось сумме делителей другого числа, отличных от самого числа (например, дружественными являются числа 284 и 220, так как $1+2+4+71+142=220$, а $1+2+4+5+10+11+20+22+44+55+110=284$). В настоящее время с помощью ЭВМ найдено несколько десятков дружественных пар чисел.

В школе Пифагора были доказаны первые теоретические утверждения о натуральных числах, в частности построена теория делимости на 2. Возможно, что интерес к этой проблематике был вызван полученным пифагорейцами доказательством важного утверждения: *диагональ квадрата несоизмерима с его стороной*. Это доказательство опирается как раз на свойства делимости на 2. По-видимому, в эту же эпоху были исследованы и «пифагорейские тройки чисел», т. е. такие тройки натуральных чисел x, y, z, что $x^2+y^2=z^2$.

О дальнейших успехах в области изучения натуральных чисел мы можем судить по арифметическим главам знаменитой книги александрийского математика Евклида «Начала» (III в. до н. э.), где, кроме пифагорейской теории делимости на 2, содержится общая теория делимости натуральных чисел, в том числе алгоритм Евклида для отыскания наибольшего общего делителя, доказательство бесконечности множества простых чисел, свойства прогрессий и т. д. Завершаются арифметические книги «Начал» доказательством теоремы, что числа вида $2^n(2^{n+1}-1)$ совершенны, если $2^{n+1}-1$ — простое число. Впоследствии многие математики изучали простые числа вида 2^n-1.

Вопросам арифметики целых чисел посвящена и книга Никомаха Геразского (I—II в. н. э.), в которой содержатся любопытные утверждения, восходящие, по-видимому, к пифагорейской традиции. Например, он доказывает, что если разбить последовательности нечетных чисел на части, содержащие по одному, двум, трем и т. д. числам, то суммы чисел каждой части дают по порядку все кубы натуральных чисел ($1, 3+5=8, 7+9+11=27$ и т. д.). Эти утверждения относятся к так называемой *аддитивной теории чисел*.

Теория чисел как самостоятельная наука выделяется в трудах

греческого математика Диофанта (середина III в. н. э.). В своей книге «Арифметика» Диофант рассматривает степени натуральных чисел до шестой включительно и вводит для них особые обозначения. Он рассмотрел методы решений уравнений первой и второй степеней, используя особую символику, являвшуюся зародышем алгебраической. Основное же содержание его книги, от которой до нас дошло менее половины, заключается в решении неопределенных уравнений и систем уравнений первой и второй степеней (т. е. систем уравнений, в которых число неизвестных превышает число уравнений). Для таких уравнений Диофант искал лишь рациональные решения. Вот несколько примеров:

а) Найти два числа так, чтобы их произведение находилось в данном отношении к их сумме (уравнение $xy = a(x + y)$, где a — данное число).

б) Разложить данное квадратное число на сумму двух квадратов (уравнение $x^2 + y^2 = a^2$, где a — данное число).

в) Найти три числа так, чтобы произведение любых двух из них, увеличенное на квадрат третьего, было бы полным квадратом (система трех уравнений $xy + z^2 = u^2$, $yz + x^2 = v^2$, $xz + y^2 = w^2$ с шестью неизвестными).

г) К кубу и квадрату прибавить один и тот же квадрат так, чтобы куб остался кубом, а квадрат — квадратом (система двух уравнений $x^3 + z^2 = u^3$, $y^2 + z^2 = v^3$ с пятью неизвестными).

д) Найти три квадрата так, чтобы сумма их квадратов тоже была квадратом (уравнение $x^2 + y^2 + z^2 = u^2$).

Методы, применявшиеся Диофантом для решения этих задач, близки, по мнению некоторых специалистов, к методам, которые через полторы тысячи лет использовались в алгебраической геометрии.

Неопределенными уравнениями занимались также китайский математик Сунь Цзы (III в. н. э.) и индийские математики Ариабхата (V—VI вв. н. э.), Брахмагупта (VII в. н. э.) и Бхаскара (XII в. н. э.). Они дали общий метод решения в целых числах уравнения вида $ax + by = c$, близкий к методу непрерывных дробей, а Брахмагупта изучал решение в целых числах уравнения $x^2 - Dy^2 = a$ и его важного частного случая $x^2 - Dy^2 = 1$ (это уравнение исторически необоснованно называется *уравнением Пелля*, хотя английский математик Пелль им не занимался). Метод решения этих уравнений, открытый Бхаскарой, был через много столетий переоткрыт в XVIII веке французским математиком Лагранжем (1736—1813). Сунь Цзы дал также метод отыскания числа по его остаткам при делении на заданные числа («китайская теорема об остатках»).

После упадка античной цивилизации в Европе на протяжении многих столетий не велись исследования по теории чисел. Лишь в начале XIII века в Италии была опубликована книга Леонардо Пизанского (1180—1240), в которой содержалось решение некоторых теоретико-числовых задач, восходящих к классической древ-

ности. После отыскания рукописи книги Диофанта и ее публикации интерес к теории чисел возрастает. Наиболее крупные результаты в этой области, далеко превзошедшие все, что было до того создано, получил французский математик Пьер Ферма (1601—1665). Он был по основной специальности юристом и занимался математикой лишь в часы досуга. Основные его результаты изложены в письмах другим математикам и в заметках на полях принадлежащего ему экземпляра сочинений Диофанта. Так как они записывались почти без доказательств, их пришлось потом доказывать математикам последующих веков. В настоящее время установлено, что все результаты Ферма были верны, за исключением двух (один из них, верность которого Ферма лишь предполагал, оказался неверным, а второй, так называемая великая теорема Ферма, до сих пор не доказан и не опровергнут).

Неверное предположение Ферма состояло в том, что числа вида $2^{2^n}+1$ простые. Это верно при $n=0, 1, 2, 3, 4$, но, как показал Эйлер, ложно при $n=5$. До сих пор не найдено ни одного значения n, большего четырех, для которого $2^{2^n}+1$ просто. При исследовании чисел на простоту Ферма пользовался своей теоремой о делимости $a^{p-1}-1$ на простое число p.

Ферма изучал, каким арифметическим прогрессиям принадлежат простые числа, представимые в виде $p=ax^2+2bxy+cy^2$, где a, b, c, x, y — целые числа. Он решил этот вопрос для форм

$$x^2+y^2,\quad x^2+2y^2,\quad x^2+3y^2,\quad x^2+xy+y^2,\quad x^2-2y^2.$$

Например, оказалось, что вид x^2+y^2 могут иметь лишь простые числа, принадлежащие арифметической прогрессии $4k+1$, причем каждое простое число этой прогрессии представимо в виде суммы квадратов единственным образом. Например, $29=4\cdot 7+1=5^2+2^2$.

Далее, Ферма нашел, что формой x^2+2y^2 представимы все простые числа вида $8n+1$ и $8n+3$ и только они, а формами x^2+3y^2 и x^2+xy+y^2 — простые числа вида $6n+1$. Эти исследования Ферма были обобщены математиками XVIII века и легли в основу теории *квадратичных форм с целыми коэффициентами*, построенной Гауссом (1777—1855). Ферма утверждал, что он доказал предположение о представимости любого натурального числа в виде суммы четырех квадратов и более общее утверждение, что *любое натуральное число является суммой n n-угольных чисел.* Полное доказательство этой теоремы опубликовано в начале XIX века Коши (1789—1857).

Важные результаты были получены Ферма в области неопределенных уравнений. Он занимался уравнением $x^2-Dy^2=1$, а также утверждал, что владеет доказательством следующей теоремы: уравнение $x^n+y^n=z^n$ при $n>2$ не имеет решений в натуральных числах. Эту теорему и называют *великой теоремой Ферма.* Как указывалось выше, она до сих пор не доказана и не опровергнута, хотя с помощью самых современных математических методов удалось доказать ее справедливость для показателей n до 100 000

включительно. Позднее исследования, связанные с великой теоремой Ферма, привели к созданию арифметики числовых колец и теории идеалов.

В XVIII веке основные результаты в области теории чисел были получены членом Петербургской Академии наук уроженцем Швейцарии Леонардом Эйлером (1707—1783). Он написал более ста работ по теории чисел. В этих работах были доказаны многие теоремы, высказанные без доказательства Ферма, в частности Эйлер доказал справедливость великой теоремы Ферма при $n = 3$ и при $n = 4$. Далее, он обобщил малую теорему Ферма на случай составного модуля (см. теорему 2 § 4 главы III). Изучая остатки при делении квадратов натуральных чисел на простые числа, Эйлер пришел к замечательному закону взаимности. Этот закон имеет вид

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}},$$

где p и q — нечетные простые числа, а $\left(\frac{p}{q}\right)$ — введенный позднее Лежандром символ, который равен 1, если существует решение сравнения $x^2 \equiv q \pmod{p}$, и равен — 1 в противном случае. Эйлер не дал доказательства этому закону — оно было получено позднее Лежандром (1752—1833). Несколько доказательств квадратичного закона взаимности нашел в XIX веке один из самых выдающихся математиков Гаусс (1777—1855). Позднее были получены обобщения закона взаимности на степенные вычеты при иных значениях показателя.

Эйлер был основоположником применения к проблемам теории чисел методов математического анализа. В частности, он предложил связывать с каждой последовательностью натуральных чисел $a_0, a_1, \ldots, a_n$ ее *производящую функцию*, т. е. функцию $f(x)$, разложение которой в степенной ряд имеет вид

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n.$$

Применяя эту идею, он вывел ряд важных тождеств для функции, выражающей, сколькими способами можно разбить на слагаемые данное натуральное число n.

В своих исследованиях по теории чисел Эйлер часто прибегал к неполной индукции и математическому эксперименту. Он писал, что «свойства чисел, известные сегодня, по большей части были открыты путем наблюдения и открыты задолго до того, как их истинность была подтверждена строгими доказательствами. Имеется даже много свойств чисел, с которыми мы хорошо знакомы, но которые мы все еще не можем доказать; только наблюдения привели нас к их познанию. Отсюда мы видим, что в теории чисел, которая все еще очень несовершенна, наши самые большие надежды мы можем возлагать на наблюдения; они непрерывно будут вести нас к новым свойствам, которые мы позже будем пытаться доказать».

Одним из таких свойств, замеченных Эйлером и сформулирован-

ных в его переписке с немецким математиком Хр. Гольдбахом (1690—1764), было утверждение, что *каждое четное число является суммой двух простых чисел* (Гольдбах ранее заметил, что *каждое нечетное число является суммой трех простых чисел* — в то время 1 считали простым числом). Это утверждение не поддавалось доказательству в течение двух столетий и лишь в 30-е годы XX века советский математик академик И. М. Виноградов (1891—1983) доказал, что любое четное число, начиная с некоторого, является суммой четырех простых чисел.

Ряд других утверждений, также относящихся к аддитивной теории чисел, содержится в вышедшей в 1770 г. книге английского математика Варинга (1734—1798). В частности, в этой книге без доказательства сформулировано следующее утверждение: для любого натурального числа n существует такое число $N(n)$, что любое натуральное число x представимо в виде суммы не более чем $N(n)$ слагаемых, являющихся точными n-ми степенями. Первое доказательство этого утверждения было получено в 1909 году знаменитым немецким математиком Д. Гильбертом (1862—1943), однако у него значение $N(n)$ оказалось очень большим. Позднее И. М. Виноградов доказал, что это число имеет порядок $n \ln n$. Заметим, что в той же книге впервые была опубликована гипотеза Гольдбаха, о которой шла речь выше.

Широко использовался в XVIII веке для решения проблем теории чисел аппарат непрерывных дробей. Эти дроби были введены в 1572 году итальянским математиком Бомбелли. Современное обозначение непрерывных дробей встречается у итальянского математика Катальди в 1613 г. Теорию непрерывных дробей построил Х. Гюйгенс (1629—1695), встретившийся с ними при конструировании планетария. С помощью непрерывных дробей швейцарский математик Ламберт (1728—1777) доказал иррациональность чисел e и π. Этот результат был значительно усилен в XIX веке французским математиком Ш. Эрмитом (1822—1901), который доказал, что число e не только иррационально, но даже трансцендентно, т. е. не может быть корнем какого-либо алгебраического уравнения $a_0x^n + \ldots + a_n = 0$ с целыми коэффициентами. Основываясь на результатах Эрмита, немецкий ученый Линдеман (1852—1939) доказал трансцендентность числа π. Отсюда вытекала, в частности, невозможность квадратуры круга. В другом направлении изучал непрерывные дроби Лагранж, который доказал, что только для квадратических иррациональностей разложение в непрерывную дробь периодично.

Новую эпоху в теории чисел открыли исследования Гаусса, начатые им на студенческой скамье. Опубликованные в 1801 году «Арифметические исследования» послужили источником новых идей и одновременно моделью для арифметических теорий XIX века. В этой книге была исследована арифметика квадратичных полей (т. е. полей чисел вида $a + b\sqrt{D}$, где a и b—рациональные числа и $D > 0$) и построена алгебра над конечным полем. По сути дела

в этой книге содержалась и теория конечных коммутативных групп (хотя общее понятие группы было определено через несколько десятилетий). Гаусс привел в систему разбросанные в работах Эйлера, Лагранжа и Лежандра сведения о сравнениях и развил общую теорию сравнений, аналогичную теории алгебраических уравнений. В книге Гаусса доказано существование первообразного корня (см. п. 2, § 7 главы III) по любому простому модулю и введено понятие индекса, аналогичное понятию логарифма (см. п. 3 § 7 главы III).

Позднее Гаусс расширил область своих исследований, изучив арифметику *целых комплексных чисел* (т. е. чисел вида $a + bi$, где a и b — целые числа). Он определил для таких чисел понятия простого и составного числа, ввел алгоритм Евклида, доказал единственность разложения на простые множители, построил теорию степенных вычетов, доказал аналог малой теоремы Ферма, ввел понятие первообразного корня и развил теорию индексов.

Попытки ряда ученых доказать великую теорему Ферма привели к изучению арифметики других квадратичных расширений поля рациональных чисел. Оказалось, что для некоторых из таких расширений неверна теорема о единственности разложения на простые множители. Как отмечалось в главе II, это привело к построению теории идеалов в кольцах. Важные исследования по арифметике числовых колец провел безвременно погибший русский математик Е. И. Золотарев (1847—1878).

Значительный вклад в развитие алгебраической теории чисел внесли в XIX веке французский математик Ш. Эрмит и немецкие ученые Ф. Эйзенштейн (1823—1852), Л. Кронекер (1823—1891), Р. Дедекинд (1831—1916) и Г. Вебер (1842—1913). Созданную ими теорию значительно развил и обобщил Д. Гильберт, который в своем «Отчете о теории алгебраических чисел» подвел итоги значительному этапу развития этой теории и наметил пути ее дальнейшего прогресса. В ходе дальнейшего развития выяснились глубокие связи между теориями алгебраических чисел, алгебраических функций и некоторыми разделами теории аналитических функций. Геометрические аспекты теории чисел были вскрыты в работах Г. Минковского (1864—1909), Г. Ф. Вороного (1868—1908) и других ученых. В частности, Минковский установил связи между некоторыми вопросами теории чисел и теорией выпуклых тел, а также пространственных решеток.

С работ Эйлера началось широкое использование в теории чисел методов математического анализа. В частности, с их помощью удалось решить проблему о распределении простых чисел (см. с. 34—37).

Таким образом, теория чисел превратилась в ветвь математики, в которой применяются методы самых разнообразных разделов этой науки. В то же время методы и идеи, возникавшие первоначально в связи с решением проблем теории чисел, приводили к созданию новых весьма общих теорий в других областях математики. В частности, развитие современной алгебры в

значительной мере стимулировалось запросами теории чисел, равно как и развитие некоторых разделов математического анализа (например, теории целых функций).

Начиная с середины XIX века, все большее влияние на развитие теории чисел оказывает деятельность русских ученых. Как пишет в своей книге «Петербургская школа теории чисел» Б. Н. Делоне, «русские математики дали ряд работ по теории чисел, создавших славу русской науке. Замечательные исследования по теории чисел принадлежат члену нашей академии Леонарду Эйлеру. Однако русская школа теории чисел в собственном смысле слова начинается с Чебышева». На с. 34—37 уже говорилось о роли работ П. Л. Чебышева в решении проблемы о распределении простых чисел. Значительный вклад в теорию чисел внесли ученики Чебышева, выдающиеся русские математики Е. И. Золотарев, А. Н. Коркин (1837—1908), А. А. Марков (1856—1922), а также такие видные ученые, как Г. Ф. Вороной, И. М. Виноградов, Б. Н. Делоне (1890—1981), А. О. Гельфонд (1906—1968), Л. Г. Шнирельман (1905—1938), Ю. В. Линник (1915—1972) и многие другие.

В частности, в работах Е. И. Золотарева, А. Н. Коркина, А. А. Маркова и Г. Ф. Вороного детально изучена теория квадратичных форм. И. М. Виноградов с помощью разработанного им метода тригонометрических сумм решил целый ряд труднейших проблем аддитивной теории чисел, Б. Н. Делоне доказал ряд утверждений о кубических иррациональностях, используя геометрические методы, А. О. Гельфонд исследовал ряд проблем, связанных с трансцендентностью чисел вида α^{β}, решив при этом одну из проблем, которые в начале XX века поставил Д. Гильберт в качестве труднейших проблем математики, Л. Г. Шнирельман исследовал аддитивные проблемы теории чисел с помощью введенного им понятия плотности подмножества натурального ряда чисел (в частности, он еще до работ И. М. Виноградова доказал, что любое число можно представить в виде суммы ограниченного количества простых слагаемых). Ю. В. Линник использовал в теории чисел теоретико-вероятностные методы.

В настоящее время теория чисел представляет собой важную ветвь математической науки, методы которой применяются не только в теоретических, но и в прикладных вопросах (теории кодирования, передаче информации, приближенном вычислении многомерных интегралов и т. д.).

ТАБЛИЦЫ ИНДЕКСОВ

Простое число 3

N	0	1	2	3	4	5	6	7	8	9
0		0	1							

I	0	1	2	3	4	5	6	7	8	9
0	1	2								

Простое число 5

N	0	1	2	3	4	5	6	7	8	9
0		0	1	3	2					

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	3						

Простое число 7

N	0	1	2	3	4	5	6	7	8	9
0		0	2	1	4	5	3			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	2	6	4	5				

Простое число 11

N	0	1	2	3	4	5	6	7	8	9
0		0	1	8	2	4	9	7	3	6
1	5									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	5	10	9	7	3	6
1										

Простое число 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							

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

Простое число 17

N	0	1	2	3	4	5	6	7	8	9
0		0	14	1	12	5	15	11	10	2
1	3	7	13	4	9	6	8			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	10	13	5	15	11	16	14
1	8	7	4	12	2	6				

Простое число 19

N	0	1	2	3	4	5	6	7	8	9
0		0	1	13	2	16	14	6	3	8
1	17	12	15	5	7	11	4	10	9	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	13	7	14	9	18
1	17	15	11	3	6	12	5	10		

Простое число 23

N	0	1	2	3	4	5	6	7	8	9
0		0	2	16	4	1	18	19	6	10
1	3	9	20	14	21	17	8	7	12	15
2	5	13	11							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	2	10	4	20	8	17	16	11
1	9	22	18	21	13	19	3	15	6	7
2	12	14								

Простое число 29

N	0	1	2	3	4	5	6	7	8	9
0		0	1	5	2	22	6	12	3	10
1	23	25	7	18	13	27	4	21	11	9
2	24	17	26	20	8	16	19	15	14	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	3	6	12	24	19
1	9	18	7	14	28	27	25	21	13	26
2	23	17	5	10	20	11	22	15		

Простое число 31

N	0	1	2	3	4	5	6	7	8	9
0		0	24	1	18	20	25	28	12	2
1	14	23	19	11	22	21	6	7	26	4
2	8	29	17	27	13	10	5	3	16	9
3	15									

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	19	26	16	17	20	29
1	25	13	8	24	10	30	28	22	4	12
2	5	15	14	11	2	6	18	23	7	21

Простое число 37

N	0	1	2	3	4	5	6	7	8	9
0		0	1	26	2	23	27	32	3	16
1	24	30	28	11	33	13	4	7	17	35
2	25	22	31	15	29	10	12	6	34	21
3	14	9	5	20	8	19	18			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	27	17	34	31
1	25	13	26	15	30	23	9	18	36	35
2	33	29	21	5	10	20	3	6	12	24
3	11	22	7	14	28	19				

Простое число 41

N	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

I	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7

Простое число 43

N	0	1	2	3	4	5	6	7	8	9
0		0	27	1	12	25	28	35	39	2
1	10	30	13	32	20	26	24	38	29	19
2	37	36	15	16	40	8	17	3	5	41
3	11	34	9	31	23	18	14	7	4	33
4	22	6	21							

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	38	28	41	37	25	32
1	10	30	4	12	36	22	23	26	35	19
2	14	42	40	34	16	5	15	2	6	18
3	11	33	13	39	31	7	21	20	17	8
4	24	29								

Простое число 47

N	0	1	2	3	4	5	6	7	8	9
0		0	18	20	36	1	38	32	8	40
1	19	7	10	11	4	21	26	16	12	45
2	37	6	25	5	28	2	29	14	22	35
3	39	3	44	27	34	33	30	42	17	31
4	9	15	24	13	43	41	23			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	31	14	23	21	11	8	40
1	12	13	18	43	27	41	17	38	2	10
2	3	15	28	46	42	22	16	33	24	26
3	36	39	7	35	34	29	4	20	6	30
4	9	45	37	44	32	19				

Простое число 53

N	0	1	2	3	4	5	6	7	8	9
0		0	1	17	2	47	18	14	3	34
1	48	6	19	24	15	12	4	10	35	37
2	49	31	7	39	20	42	25	51	16	46
3	13	33	5	23	11	9	36	30	38	41
4	50	45	32	22	8	29	40	44	21	28
5	43	27	26							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	11	22	44	35
1	17	34	15	30	7	14	28	3	6	12
2	24	48	43	33	13	26	52	51	49	45
3	37	21	42	31	9	18	36	19	38	23
4	46	39	25	50	47	41	29	5	10	20
5	40	27								

Простое число 59

N	0	1	2	3	4	5	6	7	8	9
0		0	1	50	2	6	51	18	3	42
1	7	25	52	45	19	56	4	40	43	38
2	8	10	26	15	53	12	46	34	20	28
3	57	49	5	17	41	24	44	55	39	37
4	9	14	11	33	27	48	16	23	54	36
5	13	32	47	22	35	31	21	30	29	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	5	10	20	40
1	21	42	25	50	41	23	46	33	7	14
2	28	56	53	47	35	11	22	44	29	58
3	57	55	51	43	27	54	49	39	19	38
4	17	34	9	18	36	13	26	52	45	31
5	3	6	12	24	48	37	15	30		

Простое число 61

N	0	1	2	3	4	5	6	7	8	9
0		0	1	6	2	22	7	49	3	12
1	23	15	8	40	50	28	4	47	13	26
2	24	55	16	57	9	44	41	18	51	35
3	29	59	5	21	48	11	14	39	27	46
4	25	54	56	43	17	34	58	20	10	38
5	45	53	42	33	19	37	52	32	36	31
6	30									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	3	6	12	24
1	48	35	9	18	36	11	22	44	27	54
2	47	33	5	10	20	40	19	38	15	30
3	60	59	57	53	45	29	58	55	49	37
4	13	26	52	43	25	50	39	17	34	7
5	14	28	56	51	41	21	42	23	46	31

Простое число 67

N	0	1	2	3	4	5	6	7	8	9
0		0	1	39	2	15	40	23	3	12
1	16	59	41	19	24	54	4	64	13	10
2	17	62	60	28	42	30	20	51	25	44
3	55	47	5	32	65	38	14	22	11	58
4	18	53	63	9	61	27	29	50	43	46
5	31	37	21	57	52	8	26	49	45	36
6	56	7	48	35	6	34	33			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	61	55	43
1	19	38	9	18	36	5	10	20	40	13
2	26	52	37	7	14	28	56	45	23	46
3	25	50	33	66	65	63	59	51	35	3
4	6	12	24	48	29	58	49	31	62	57
5	47	27	54	41	15	30	60	53	39	11
6	22	44	21	42	17	34				

Простое число 71

N	0	1	2	3	4	5	6	7	8	9
0		0	6	26	12	28	32	1	18	52
1	34	31	38	39	7	54	24	49	58	16
2	40	27	37	15	44	56	45	8	13	68
3	60	11	30	57	55	29	64	20	22	65
4	46	25	33	48	43	10	21	9	50	2
5	62	5	51	23	14	59	19	43	4	3
6	66	69	17	53	36	67	63	47	61	41
7	35									

I	0	1	2	3	4	5	6	7	8	9
0	1	7	49	59	58	51	2	14	27	47
1	45	31	4	28	54	23	19	62	8	56
2	37	46	38	53	16	41	3	21	5	35
3	32	11	6	42	10	70	64	22	12	13
4	20	69	57	44	24	26	40	67	43	17
5	48	52	9	63	15	34	25	33	18	55
6	30	68	50	66	36	39	60	65	29	61

Простое число 73

N	0	1	2	3	4	5	6	7	8	9
0		0	8	6	16	1	14	33	24	12
1	9	55	22	59	41	7	32	21	20	62
2	17	39	63	46	30	2	67	18	49	35
3	15	11	40	61	29	34	28	64	70	65
4	25	4	47	51	71	13	54	31	38	66
5	10	27	3	53	26	56	57	68	43	5
6	23	58	19	45	48	60	69	50	37	52
7	42	44	36							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	52	41	59	3	15	2	10
1	50	31	9	45	6	30	4	20	27	62
2	18	17	12	60	8	40	54	51	36	34
3	24	47	16	7	35	29	72	68	48	21
4	32	14	70	58	71	63	23	42	64	28
5	67	43	69	53	46	11	55	56	61	13
6	65	33	19	22	37	39	49	26	57	66
7	38	44								

Простое число 79

N	0	1	2	3	4	5	6	7	8	9
0		0	4	1	8	62	5	53	12	2
1	66	68	9	34	57	63	16	21	6	32
2	70	54	72	26	13	46	38	3	61	11
3	67	56	20	69	25	37	10	19	36	35
4	74	75	58	49	76	64	30	59	17	28
5	50	22	42	77	7	52	65	33	15	31
6	71	45	60	55	24	18	73	48	29	27
7	41	51	14	44	23	47	40	43	39	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	2	6	18	54	4	12
1	36	29	8	24	72	58	16	48	65	37
2	32	17	51	74	64	34	23	69	49	68
3	46	59	19	57	13	39	38	35	26	78
4	76	70	52	77	73	61	25	75	67	43
5	50	71	55	7	21	63	31	14	42	47
6	62	28	5	15	45	56	10	30	11	33
7	20	60	22	66	40	41	44	53		

Простое число 83

N	0	1	2	3	4	5	6	7	8	9
0		0	1	72	2	27	73	8	3	62
1	28	24	74	77	9	17	4	56	63	47
2	29	80	25	60	75	54	78	52	10	12
3	18	38	5	14	57	35	64	20	48	67
4	30	40	81	71	26	7	61	23	76	16
5	55	46	79	59	53	51	11	37	13	34
6	19	66	39	70	6	22	15	45	58	50
7	36	33	65	69	21	44	49	32	68	43
8	31	42	41							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	45	7	14
1	28	56	29	58	33	66	49	15	30	60
2	37	74	65	47	11	22	44	5	10	20
3	40	80	77	71	59	35	70	57	31	62
4	41	82	81	79	75	67	51	19	38	76
5	69	55	27	54	25	50	17	34	68	53
6	23	46	9	18	36	72	61	39	78	73
7	63	43	3	6	12	24	48	13	26	52
8	21	42								

Простое число 89

N	0	1	2	3	4	5	6	7	8	9
0		0	16	1	32	70	17	81	48	2
1	86	84	33	23	9	71	64	6	18	35
2	14	82	12	57	49	52	39	3	25	59
3	87	31	80	85	22	63	34	11	51	24
4	30	21	10	29	28	72	73	54	65	74
5	68	7	55	78	19	66	41	36	75	43
6	15	69	47	83	8	5	13	56	38	58
7	79	62	50	20	27	53	67	77	40	42
8	46	4	37	61	26	76	45	60	44	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	81	65	17	51	64	14
1	42	37	22	66	20	60	2	6	18	54
2	73	41	34	13	39	28	84	74	44	43
3	40	31	4	12	36	19	57	82	68	26
4	78	56	79	59	88	86	80	62	8	24
5	72	38	25	75	47	52	67	23	69	29
6	87	83	71	35	16	48	55	76	50	61
7	5	15	45	46	49	58	85	77	53	70
8	32	7	21	63	11	33	10	30		

Простое число 97

N	0	1	2	3	4	5	6	7	8	9
0		0	34	70	68	1	8	31	6	44
1	35	186	42	25	65	71	40	89	78	81
2	69	5	24	77	76	2	59	18	3	13
3	9	46	74	60	27	32	16	91	19	95
4	7	85	39	4	58	45	15	84	14	62
5	36	63	93	10	52	87	37	55	47	67
6	43	64	80	75	12	26	94	57	61	51
7	66	11	50	28	29	72	53	21	33	30
8	41	88	23	17	73	90	38	83	92	54
9	79	56	49	20	22	82	48			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	28	43	21	8	40	6	30
1	53	71	64	29	48	46	36	83	27	38
2	93	77	94	82	22	13	65	34	73	74
3	79	7	35	78	2	10	50	56	86	42
4	16	80	12	60	9	45	31	58	96	92
5	72	69	54	76	89	57	91	67	44	26
6	33	68	49	51	61	14	70	59	4	20
7	3	15	75	84	32	63	24	23	18	90
8	62	19	95	87	47	41	11	55	81	17
9	85	37	88	52	66	39				

ГЛАВА I.

§ 6.

9. 67. 15. а) 24; б) 80; в) 115.

§ 8.

9. 45_8, 60_9, 55_{12}. 13. а) да; б) нет, правильно 51435_8.
27. а) нет, правильно $44\,673_9$; б) да; в) нет, правильно 7237_{15}.
28. а) нет, правильно $21\,022_5$; б) да.
29. а) $g = 6$; б) $g = 11$; в) $g = 8$.
31. а) $10\,110\,011_2$; б) 2025_6; в) $156\,003_8$; г) $7\,(10)331_{13}$; д) $90\,162_{12}$; е) $49\,204_{12}$.
32. а) $1\,110\,100_2$; б) 1435_6; в) $754\,335_9$; г) $3\,(11)768_{12}$; д) $11\,(11)3_{12}$.
33. а) $100\,010\,111_2$; б) $314\,012_5$; в) $1\,531\,315_7$; г) $535\,(11)_{12}$.
34. а) $11\,011_2$; б) $23\,041_5$; в) $15\,476_8$; г) $(10)\,539_{11}$.
35. Получим $21\,400_5$; $214\,000_5$.
43. Получим 2340. 44. 7; 7^2; 7^3; ...

§ 9.

15. а) 6 231 000; б) 22 673 000; в) 20 985 073.
16. а) [0; 2,5, 3,2]; б) [2; 1, 1, 1, 1,1, 3, 7, 1,2]; в) [1; 5, 4, 8, 2, 1, 2]; г) [2; 2, 16, 39]; д) [0; 4, 14, 1, 8, 2, 7, 2]; е) [2; 1, 96, 1, 1, 1, 10]; ж) [2; 1,2, 1, 1,4, 1,1, 6, 10, 1, 1,2]; з) [3; 7, 15, 1,25, 1, 7, 4].

17. а) $\dfrac{343}{226} = [1;\ 1,\ 1,\ 13,\ 1,\ 1,\ 1,\ 2]$,

$\dfrac{226}{343} = [0;\ 1,\ 1,\ 1,\ 13,\ 1,\ 1,\ 1,\ 2]$.

Подходящие дроби будут соответственно равны:

$$\frac{1}{1},\ \frac{2}{1},\ \frac{3}{2},\ \frac{41}{27},\ \frac{44}{29},\ \frac{85}{56},\ \frac{129}{85},\ \frac{343}{226}.$$
$$\frac{0}{1},\ \frac{1}{1},\ \frac{1}{2},\ \frac{2}{3},\ \frac{27}{41},\ \frac{29}{44},\ \frac{56}{85},\ \frac{86}{129},\ \frac{226}{343}.$$

б) $-\dfrac{117}{343} = [-1;\ 1,\ 1,\ 1,\ 13,\ 1,\ 1,\ 1,\ 2]$,

$-\dfrac{343}{117} = [-3;\ 14,\ 1,\ 1,\ 1,\ 2]$.

в) Подходящие дроби будут соответственно равны:

$$-1;\ 0;\ -\frac{1}{3};\ -\frac{14}{41};\ -\frac{15}{44};\ -\frac{29}{85};\ -\frac{44}{129};\ -\frac{117}{343};\ -\frac{3}{1};\ -\frac{41}{14};$$
$$-\frac{44}{15};\ -\frac{85}{29};\ -\frac{129}{44};\ -\frac{343}{117}.$$

18. а) $\dfrac{43}{19}$; б) $\dfrac{1421}{552}$; в) $\dfrac{157}{225}$; г) $-1\dfrac{159}{215}$; д) $\dfrac{893}{11\,953}$.

19. [0; 2, 3, 47, 3]; $\frac{P_2}{Q_2} = \frac{3}{7}$.

20. а) $\frac{7}{23}$; б) $\frac{17}{13}$; в) $\frac{97}{113}$; г) $\frac{173}{1201}$; д) $\frac{101}{1013}$; е) $\frac{53}{57}$.

21. а) $x = 2$.

22. а) $t \approx \frac{85}{31}$ с избытком; б) $t \approx \frac{277}{101}$ с недостатком.

ГЛАВА III.

§ 1.

8. а) $219 \equiv 128 \pmod 7$; б) $-352 \equiv 20 \pmod{31}$; в) $487 \equiv 7 \pmod{12}$; г) $20 \equiv 389 \pmod{41}$.

9. а) $N \equiv 0 \pmod 2$; б) $N \equiv 1$ или $-1 \pmod 2$; в) $N \equiv 1 \pmod 4$; г) $N \equiv -3 \equiv 5 \pmod 8$; д) $N \equiv 3 \pmod{10}$.

§ 2.

11. $\overline{1}$, $\overline{3}$, $\overline{5}$, $\overline{7}$; простые числа p имеют вид: $8k + 1$, $8k + 3$, $8k + 5$ или $8k \pm 1$, $8k \pm 3$; $p \equiv \pm 1 \pmod 8$, $p \equiv \pm 3 \pmod 8$.

12. 3 (d). **13.** а) $\overline{6}$; б) $\overline{12}$; в) $\overline{7}$; г) $\overline{2}$, $\overline{4}$, $\overline{5}$, $\overline{10}$.

14. $\overline{x} = 6$.

15. Наименьшими неотрицательными вычетами будут соответственно числа 3, 8, 3, 9, 2, 5, 6, 1; абсолютно наименьшими вычетами будут соответственно 3, -5, 3, -4, 2, 5, 6, 1; числа 3 и 16 принадлежат к одному и тому же классу по модулю 13, т. е. $3 \equiv 16 \pmod{13}$.

16. Образуют. **17.** Если $x = 0, 1, 2, 3, 4, 5, 6, 7$, то соответственно $7x + 4 \equiv 4, 3, 2, 1, 0, 7, 6, 5 \pmod 8$.

18. d.

§ 4.

8. а) 607; б) 1198; в) 5631; **9.** 32. **10.** $\varphi(b)$. **11.** 31.

12. а) 8; б) 8; в) 24; г) 12. **15.** а) $n = 4$; б) $n = 7$.

16. $n = 2^3 \cdot 5 \cdot 113 = 4520$. **17.** а) $x = 2^\alpha \cdot y$, где $\alpha > 0$ и y — натуральное число, не делящееся на 2 и 3; б) такого x не существует.

18. а) $n = 2^\alpha$, где $\alpha > 0$; б) $n = 2^\alpha \cdot 3^\beta$, где $\alpha > 0$, $\beta > 0$.

24. а) 5; б) 12; в) 1; г) 15; д) 23.

25. а) 1; б) 7; в) 1; г) 9; д) 7.

26. а) 01; б) 97; в) 01; г) 49; д) 97.

§ 5.

9. а) $x \equiv 15{,}22 \pmod{37}$; б) $x \equiv 3 \pmod 7$; в) решений не имеет; г) $x \equiv 2{,}4 \pmod 5$; д) $x \equiv 6, 8, 23 \pmod{37}$; е) решений не имеет.

12. а) да; б) нет; в) да. **13.** $6x^8 + 7x^5 + 3x^4 + x^2 + 3 \equiv 0 \pmod{11}$.

14. $x \equiv 2 \pmod 7$.

§ 6.

8. а) $x \equiv 6 \pmod{29}$; б) $x \equiv 20 \pmod{29}$;
в) $x \equiv 26 \pmod{31}$; г) $x \equiv 8 \pmod{123}$;
д) $x \equiv 112 \pmod{317}$; е) $x \equiv 51 \pmod{360}$;
ж) $x \equiv 173 \pmod{320}$; з) $x \equiv 147 \pmod{239}$.

9. а) $x \equiv 188 \pmod{379}$; б) $x \equiv 19 \pmod{471}$; в) $x \equiv 29 \pmod{693}$.

10. а) $x \equiv 7, 23, 39 \pmod{48}$; б) $x \equiv 6, 43, 80 \pmod{111}$; в) $x \equiv 8, 25, 42, 59, 76 \pmod{85}$; г) сравнение решений не имеет; д) $x \equiv 100, 821, 1542, 2263, 2984 \pmod{3605}$; е) сравнение тождественное.

11. а) $ax \equiv b \pmod{21}$, где $(a, 21) = 1$ и b — целое; б) для того чтобы сравнение $ax \equiv b \pmod{21}$ имело, например, 3 решения, необходимо и достаточно, чтобы $(a, 21) = 3$ и b делилось бы на 3; в) такого сравнения составить нельзя.

12. а) $x = 4 + 17t$, $y = -11 - 53t$; б) $x = 47 + 105t$, $y = 21 + 47t$; в) неразрешимо; г) $x = 4 + 16t$, $y = 7 - 11t$. **13.** 26 апреля. **14.** $x \equiv 13 \pmod{21}$, т. е. $x = 13, 34, 55, 76$.

15. $x \equiv 200 \pmod{440}$, т. е. $x = 200, 640$.

16. $x \equiv 30 \pmod{31}$, т. е. $x = 30, 61, 92$.

17. $a = 8$, $b = 1$. **18.** а) 7 точек; б) 2 точки; в) 2 точки.

20. 12 точек. **21.** а) $x \equiv 58 \pmod{315}$; б) $x \equiv -2 \pmod{231}$; в) $x \equiv 2959 \pmod{3990}$.

23. а) $x \equiv 425 \pmod{1456}$; б) $x \equiv 43, 340 \pmod{594}$; в) решений не имеет; г) $x \equiv 7\,777\,777 \pmod{91\,290\,457}$. **24.** а) $x \equiv 18 \pmod{140}$; б) $x \equiv 53 \pmod{168}$; в) $x \equiv 256 \pmod{1547}$; г) $x \equiv 841 \pmod{6279}$; д) $x \equiv 262 \pmod{1155}$.

25. 301. **26.** 188, 308, 428. **27.** $x = 45$.

§ 7.

21. $g = 2, 3, 10, 13, 15$. **22.** а) 3; б) 28; в) 30.

23. а) $2^0, 2^1, 2^2, \ldots, 2^{17}$; б) $2^0, 2, 2^2, \ldots, 2^{17}$.

25. а) 5; б) 6; в) 7. **27.** 28. **28.** а) 4 5, 6, 9, 13, 22; б) 5, 25. **29.** а) 6; б) 10; в) 12; г) 40.

31. 2, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27.

33. $\mathrm{ind}_{10} 34 \equiv 26 \pmod{46}$. **34.** $\mathrm{ind}_{11} 56 \equiv 16 \pmod{70}$.

36. а) 4; б) решений не имеет; в) 7.

37. а) $x \equiv 3, 7, 22, 26 \pmod{29}$; б) $x \equiv 5 \pmod{73}$; в) решений не имеет; г) $x \equiv 17 \pmod{59}$.

38. а) $x \equiv 17, 43 \pmod{52}$; б) $x \equiv 3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59 \pmod{60}$; в) неразрешимо.

39. а) $x \equiv 7,57 \pmod{100}$; б) решений не имеет.

40. $\frac{1}{2}(p-1)$. **43.** а) 1, 4, 5, 6, 7, 11, 16, 17; б) 1, 7, 8, 11, 12, 18.

44. а) 7,37; б) 3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34.

45. а) 24; б) 1; в) 30. **46.** $x \equiv 8 \pmod{27}$, $x \equiv \pm 8 \pmod{27}$.

47. а) $x \equiv 17 \pmod{50}$; б) $x \equiv \pm 23 \pmod{50}$.

СОДЕРЖАНИЕ

Николай Алексеевич Казачек, Георгий Николаевич Перлатов, Наум Яковлевич Виленкин, Алексей Иванович Бородин

АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ

Часть III

Н/К

Заведующий редакцией Р. А. Хабиб. Редакторы Л. В. Антонова, Л. В. Туркестанская. Младший редактор Н. Т. Протасова. Технический редактор В. В. Новоселова. Корректор Н. В. Бурдина.

Сдано в набор 25.11.83. Подписано к печати 28.04.84. Формат 60×90¹/₁₆. Бумага кн.-журн. Гарн. лит. Печать высокая. Усл. печ. л. 12,0. Усл. кр. отт. 12,25. Уч.-изд. л. 11,50. Тираж 27000 экз. Зак. 738. Цена 40 коп. Заказное.

Издательство «Просвещение» Государственного комитета РСФСР по делам издательств, полиграфии и книжной торговли. 129846, Москва, 3-й проезд Марьиной рощи, 41.

Саратовский ордена Трудового Красного Знамени полиграфический комбинат Росглавполиграфпрома Государственного комитета РСФСР по делам издательств, полиграфии и книжной торговли. Саратов, ул. Чернышевского, 59.

40 коп.