О. В. МАТЫСИК
А. А. ТРОФИМУК

ТЕОРИЯ ЧИСЕЛ

КУРС ЛЕКЦИЙ

Брест, 2013

УДК 512 (075.8)
ББК 22.15я73
М33

Рекомендовано редакционно-издательским советом учреждения образования «Брестский государственный университет имени А.С. Пушкина»

Рецензенты:
директор Брестского филиала
ГУО «Институт непрерывного образования» БГУ,
кандидат физико-математических наук, доцент
В.Ф. Савчук

заведующий кафедрой методики преподавания
математики и информатики
Брестского государственного университета имени А.С. Пушкина,
кандидат педагогических наук, доцент
Е.П. Гринько

Матысик, О.В.
М33 Теория чисел : курс лекций для студ. отд-ний 1-02 05 03-02 «Математика и информатика» и 1-02 05 01 «Математика» (заоч. форма обучения) физ.-мат. фак. / О.В. Матысик, А.А. Трофимук ; Брест. гос. университет им. А.С. Пушкина, каф. алгебры и геометрии. – Брест : Изд-во БрГУ, 2013. – 105 с.
ISBN

Курс лекций написан в соответствии с действующей типовой программой по курсу «Теория чисел» и ставит своей целью облегчить самостоятельную работу студентов с теоретическим материалом при подготовке к лекциям, практическим занятиям и к экзамену.

Предназначено для студентов отделений 1-02 05 03-02 «Математика и информатика» и 1-02 05 01 «Математика» (заочная форма обучения) физико-математического факультета.

УДК 512 (075.8)
ББК 22.15я73

ISBN

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ

Настоящий курс лекций предназначен для студентов специальности «Математика. Информатика» и студентов заочной формы обучения физико-математического факультета. Он написан в соответствии с действующей типовой программой по курсу «Теория чисел», утверждённой первым заместителем Министра образования Республики Беларусь.

В издании излагается теоретический материал, содержащий вопросы: отношение и свойства делимости в кольце $\mathbb{Z}$; НОД и НОК; алгоритм Евклида; решето Эратосфена: системы счисления; простые и составные числа; гауссовы числа; линейные диофантовы уравнения; числовые функции и их основные свойства; сравнения в кольце $\mathbb{Z}$ и их свойства; теоремы Эйлера, Ферма и Вильсона; сравнения 1-ой степени с одним неизвестным, по простому модулю и высших степеней; первообразные корни; индексы по простому модулю; периодические дроби; арифметические приложения теории сравнений. Теоретический материал иллюстрируется многочисленными примерами решения задач.

Курс лекций ставит своей целью облегчить самостоятельную работу студентов с теоретическим материалом при подготовке к лекциям, практическим занятиям и к экзамену.

Авторы.

ОБОЗНАЧЕНИЯ

$a \equiv b (\mathrm{mod}\ p)$ — число a сравнимо с числом b по модулю p;
$m \vdots n$, $n \mid m$ — число n делит число m;
$p^a \top n$ — p^a делит n, но p^{a+1} не делит n.
$\theta(a \mod m)$ — порядок (показатель) числа a по модулю m;
$n!$ — факториал числа n;
НОД(a, b) — наибольший общий делитель чисел a и b;
НОК(a, b) — наименьшее общее кратное чисел a и b;
Множества
$\mathbb{P}$ — множество всех простых чисел;
$\mathbb{N}$ — множество всех натуральных чисел;
$\mathbb{Z}$ — множество всех целых чисел;
$\mathbb{Q}$ — множество всех рациональных чисел;
$\mathbb{R}$ — множество всех действительных чисел;
$\mathbb{Z}_m$ — множество вычетов по модулю m;
$\mathbb{U}_m$ — мультипликативная группа кольца $\mathbb{Z}_m$;
Функции
$[x]$ — целая часть числа x;
$\{x\}$ — дробная часть числа x;
$\varphi(n)$ — функция Эйлера числа n.
$\tau(n)$ — число натуральных делителей числа n;
$\sigma(n)$ — сумма натуральных делителей числа n;
$\pi(n)$ — число простых чисел от 1 до n.

1. ОТНОШЕНИЕ ДЕЛИМОСТИ В КОЛЬЦЕ $\mathbb{Z}$

1.1. Делимость целых чисел. Свойства делимости в кольце $\mathbb{Z}$. Теорема о делении с остатком

Определение 1.1.1. Целое число a делится на целое число b, отличное от нуля, если существует целое число q, такое, что верно равенство $a = bq$.

Введём символы, обозначающие «a делится на b»: $a \vdots b$. Вместо выражения «a делится на b» говорят также «a кратно b», «b делитель a». Также, как и в школьном курсе алгебры, числа a, b, q называем: делимое, делитель, частное.

Лемма 1.1.1. (Простейшие свойства делимости).

1. Нуль делится на любое отличное от нуля целое число a.

2. Любое целое число делится на 1, -1.

3. Любое целое число $a \neq 0$ делится само на себя.

4. Знак числа не влияет на делимость, т.е. если $a \vdots b$, то $a \vdots (-b)$, $(-a) \vdots b$, $(-a) \vdots (-b)$.

5. Если $a \vdots b$ и $b \vdots c$, то $a \vdots c$ (транзитивность делимости).

6. Если каждое слагаемое суммы делится на некоторое целое число, то и сумма делится на это число. (Обратное утверждение неверно. Приведите контрпример).

7. Если одно из двух целых чисел делится на какое-либо целое число b, то сумма делится на b тогда и только тогда, когда и второе число делится на b.

8. Если уменьшаемое и вычитаемое делятся на целое число b, то и их разность делится на это число, т.е. из $a \vdots b$ и $c \vdots b$ вытекает, что $(a - c) \vdots b$. (Обратное утверждение неверно. Приведите контрпример).

9. Если хотя бы один из сомножителей делится на какое-либо целое число, то и произведение этих сомножителей делится на это число. (Обратное утверждение неверно. Приведите контрпример).

10. Если $a \vdots b$ и $a \neq 0$, то $|a| \geq |b|$.

$\square$. Доказательство утверждений (1)–(4), (7)–(9) проведите самостоятельно.

5) Так как $a \vdots b$, то существует $q_1 \in \mathbb{Z}$ такое, что

$$a = bq_1. \tag{1.1}$$

Так как $b \vdots c$, то существует $q_2 \in \mathbb{Z}$ такое, что

$$b = cq_2. \tag{1.2}$$

Подставим (1.2) в (1.1). Получим $a = bq_1 = (cq_2)q_1 = c(q_2q_1) = cq_3$, значит, $a \vdots c$. Здесь $q_3 = q_2q_1 \in \mathbb{Z}$.

6) Из $a \vdots b$ и $c \vdots b$ следует $(a + c) \vdots b$, поэтому из $a_i \vdots b$, $i = \overline{1, k}$ следует $\left(\sum\limits_{i=1}^{k} a_i\right) \vdots b$.

10) Поскольку $a \vdots b$, то существует $q \in \mathbb{Z},\ q \neq 0$ такое, что $a = bq$. Очевидно, что $|a| = |bq| = |b| \cdot |q|$. Так как $|q| \geq 1$, то $|b| \cdot |q| \geq |b|$. Отсюда $|a| \geq |b|$. ⊠

Следствие 1.1.1. Если $a \vdots b$, то либо $a = 0$, либо $|a| \geq |b|$.

Следствие 1.1.2. Если $a \vdots b$ и $b \vdots a$, то $|a| = |b|$.

Следствие 1.1.3. Если $1 \vdots a$, то $a = 1$ или $a = -1$.

Определение 1.1.2. Целое число a делится с остатком на целое число b, $b \neq 0$, если существуют целые числа $q,\ r$ такие, что $a = bq + r$, причем $0 \leq r < |b|$.

Теорема 1.1.1. (о делении с остатком). Для любых целых чисел a и b $(b \neq 0)$ существует единственная пара целых чисел $q,\ r$, удовлетворяющих условию $a = bq + r$, где $0 \leq r < |b|$.

□. Пусть a и b любые целые числа, причем $b \neq 0$. Доказательство теоремы разобьем на два этапа. Сначала докажем, что такое деление возможно, а затем его единственность.

I этап: 1) Рассмотрим любые целые a, b такие, что $b > 0$. Пусть $b(-2),\ b(-1), b \cdot 0, b \cdot 1, b \cdot 2, \ldots$ — кратные числу b, расположенные в порядке возрастания, и пусть bq — наибольшее кратное числа b и не превосходящее a, $q \in \mathbb{Z}$. Имеем $b(q + 1) > bq$. Отсюда $bq + b > bq$, $b(q + + 1) > a$ (в силу выбора bq). Следовательно, $bq \leq a < b(q + 1)$, $bq \leq a < < bq + b$. Из последнего неравенства вычтем bq, получим $0 \leq a - bq < b$. Таким образом, существует $q \in \mathbb{Z}$ такое, что a, b и q связаны условием

$0 \leq a - bq < b$. Так как $b > 0$, то $|b| = b$. Пусть $a - bq = r$ или $a = bq + r$, где $0 \leq r < |b|$. Мы получили, что для любых двух данных целых чисел a и b, существуют $q,\ r \in \mathbb{Z}$ такие, что $a = bq + r$, где $0 \leq r < |b|$.

2) Рассмотрим теорему для случая произвольных целых a и b таких, что $b < 0$.

Заметим, что $-b$ является положительным числом. Тогда, используя случай 1, существуют $q_1, r \in \mathbb{Z}$ такие, что

$$a = -bq_1 + r, 0 \leq r < |-b|. \tag{1.3}$$

Из равенства (1.3) получаем

$$a = b(-q_1) + r = bq + r, \tag{1.4}$$

где $q = -q_1$, т.е. для чисел $a, b \in \mathbb{Z}$, $b < 0$ существуют $q,\ r \in \mathbb{Z}$ такие, что справедливо равенство (1.4), причем $0 \leq r < |b|$.

Таким образом, доказано, что существуют $q, r \in \mathbb{Z}$ такие, что выполняется условие $a = bq + r$, $0 \leq r < |b|$, для любых $a, b \in \mathbb{Z}$, $b \neq 0$.

II этап: Докажем единственность чисел q и r, удовлетворяющих условию

$$a = bq + r, 0 \leq r < |b|, \forall a, b \in \mathbb{Z}, b \neq 0. \tag{1.5}$$

Воспользуемся методом доказательства от противного. Пусть существует вторая пара целых чисел $q_1, r_1 \in \mathbb{Z}$ таких, что

$$a = bq_1 + r_1, 0 \leq r_1 < |b|. \tag{1.6}$$

Из равенства (1.4) и (1.6) имеем $bq_1 + r_1 = bq + r$,

$$b(q_1 - q) = r - r_1, b \neq 0. \tag{1.7}$$

Пусть $q_1 - q_2 \neq 0$, тогда $r - r_1 \neq 0$. Из равенства (1.7) следует, что $(r - r_1) \vdots b$, поэтому $|r - r_1| \geq |b|$, см. свойство 10 леммы 1.1.1. Числа r_1 и r удовлетворяют условиям $0 \leq r_1 < |b|$ и $0 \leq r < |b|$. Следовательно, $-|b| < r - r_1 < |b|$ и $|r - r_1| < |b|$. Получили противоречие.

Значит, предположение неверно. Таким образом, существуют единственные $q, r \in \mathbb{Z}$, удовлетворяющие условию (1.5). $\boxtimes$

Пример 1.1.1. Разделите ± 257 на ± 23.

$\square$. Так как $253 = 23 \cdot 11 < 257 < 23 \cdot 12 = 276$, то $257 = 23 \cdot 11 + 4$. Здесь 11 — неполное частное, 4 — остаток.

Разделим -257 на 23. Для этого найдем целое q, такое, что $23q \leq -257 < 23(q+1)$. Так как $23(-12) = -276 < -257 < 23(-11)$, то $-257 = 23(-12) + 19$.

Делим на -23. Берем $257 = 23 \cdot 11 + 4$ и записываем в виде $257 = (-23)(-11) + 4$. Для деления -257 на -23 берем $-257 = 23(-12) + 19$ и записываем в виде $-257 = (-23)12 + 19$.

Ответ: $257 = 23 \cdot 11 + 4$, $257 = (-23)(-11) + 4$,
$-257 = 23(-12) + 19$, $-257 = (-23)12 + 19$. $\boxtimes$

Пример 1.1.2. Докажите, что для любого натурального числа n целое число $a = -n^3 - 17n + 12$ делится на 6.

$\square$. Воспользуемся методом математической индукции. При $n = 1$ число $a = -6$ делится на 6 и утверждение верно. Предположим, что утверждение верно для любого натурального числа $n \leq k$. Докажем справедливость утверждения при $n = k+1$. Число $a = -(k+1)^3 - 17(k+1) + 12 = -(k^3+3k^2+3k+1) - 17k - 17 + 12 = (-k^3 - 17k + 12) - 3k^2 - 3k - 1 - 17 = (-k^3 - 17k + 12) - 3k(k+1) - 18$. По предположению индукции $(-k^3 - 17k + 12)$ делится на 6. Одно из двух последовательных натуральных чисел $k, k+1$ четно, и поэтому слагаемое $3k(k+1)$ делится на 6. Так как каждое слагаемое в выражении $(-k^3 - 17k + 12) - 3k(k+1) - 18$ делится на 6, то и вся сумма, которая является числом a, делится на 6. Согласно принципу математической индукции, число $a = -n^3 - 17n + 12$ делится на 6 для любого натурального числа n. $\boxtimes$

1.2. Общие делители целых чисел. НОД целых чисел

Теорема 1.2.1. Любое целое число a, неравное нулю, имеет конечное число целых делителей.

$\square$. Пусть b — любой целый делитель числа a. Тогда $|a| \geq |b|$. Следовательно, $-|a| \leq b \leq |a|$. Так как на отрезке $[-|a|, |a|]$ находится конечное число целых чисел, то число a имеет конечное число целых делителей. $\boxtimes$

Определение 1.2.1. *Общим делителем* целых чисел $a_1, a_2, \ldots, a_k$, $k \geq 2$ называется целое число, которое делит каждое из чисел a_i, $i = \overline{1,k}$.

Пусть среди чисел a_i хотя бы одно отлично от нуля. Тогда в силу теоремы 1.2.1 существует конечное число общих делителей, среди которых можно выбрать наибольший делитель (НОД). Заметим, что общим делителем любой совокупности целых чисел является число 1. Поэтому наибольший общий делитель этих чисел будет равен либо 1, либо больше 1, т.е. НОД — число натуральное. Будем обозначать наибольший общий делитель целых чисел $a_1, a_2, \ldots, a_k$

$$\text{НОД}(a_1, a_2, \ldots, a_k).$$

Определение 1.2.2. Целые числа $a_1, a_2, \ldots, a_k$, $k \geq 2$ называются *взаимно простыми*, если их наибольший общий делитель равен 1.

Определение 1.2.3. Целые числа $a_1, a_2, \ldots, a_k$, $k \geq 2$ называются *попарно взаимно простыми*, если наибольший общий делитель любых двух чисел этой совокупности равен 1, т.е. $\text{НОД}(a_i, a_j) = 1$, где $i, j = \overline{1,k}$, $i \neq j$.

Теорема 1.2.2. $\text{НОД}(a_1, a_2, \ldots, a_k) = \text{НОД}(|a_1|, |a_2|, \ldots, |a_k|)$.

□. *Доказать самостоятельно.* ⊠

Теорема 1.2.3. Если $a \in \mathbb{Z}$, $b \in \mathbb{N}$ и $a \vdots b$, то $\text{НОД}(a, b) = b$.

□. *Доказать самостоятельно.* ⊠

Теорема 1.2.4. Если целые числа a, b, c, m связаны равенством $a = bc + m$, то $\text{НОД}(a, b) = \text{НОД}(b, m)$, где a, b, m одновременно не равны нулю.

□. Пусть $\text{НОД}(a, b) = d$, $d \in \mathbb{N}$. По определению наибольшего общего делителя двух целых чисел $a \vdots d$ и $b \vdots d$. Так как $a = bc + m$ и $a \vdots d$ и $b \vdots d$, то по критерию делимости суммы получим $m \vdots d$, следовательно, $\text{ОД}(b, m) = d$.

Докажем, что d является НОДом чисел b и m.

Пусть $\text{НОД}(b, m) = d_1$, $d_1 \in \mathbb{N}$, $d_1 > d$.

По определению НОДа двух целых чисел $b \vdots d_1$ и $m \vdots d_1$. Тогда по свойству делимости суммы двух целых чисел из равенства $a = bc + m$ следует, что $a \vdots d_1$. Так как $\text{НОД}(a, b) = d$, то $d \vdots d_1$, что невозможно, так как $d_1 > d$. Следовательно, предположение было сделано неверно. ⊠

1.3. Алгоритм Евклида. Свойства НОДа. Теорема о линейной форме НОДа

Теорема 1.3.1. (о линейном представлении наибольшего общего делителя целых чисел). Наибольший общий делитель d целых чисел $a_1, a_2, \ldots, a_k$, $k \geq 2$ представим в виде целочисленной линейной комбинации этих чисел, т.е. в форме $d = x_1a_1 + x_2a_2 + \ldots + x_ka_k$, где $x_i \in \mathbb{Z}$, $i = \overline{1,k}$.

□. *Доказательство теоремы см.* [11, с. 373-374]. ⊠

Теорема 1.3.2. (критерий наибольшего общего делителя целых чисел). Натуральный общий делитель целых чисел $a_1, a_2, \ldots, a_k$, $k \geq 2$ является их наибольшим общим делителем тогда и только тогда, когда частные от деления чисел a_i, $i = \overline{1,k}$ на этот общий делитель являются взаимно простыми числами.

□. **Необходимость.** Докажем, что если натуральный общий делитель целых чисел $a_1, a_2, \ldots, a_k$, $k \geq 2$, является их наибольшим общим делителем, то частные от деления этих чисел на наибольший общий делитель являются взаимно простыми числами.

Пусть НОД$(a_1, a_2, \ldots, a_k) = d$. Тогда по определению наибольшего общего делителя верно:

$$a_1 = dq_1, a_2 = dq_2, \ldots, a_k = dq_k, \tag{1.8}$$

т.е. $a_i = dq_i$, где $q_i \in \mathbb{Z}$, $i = \overline{1,k}$.

Докажем, что НОД$(q_1, q_2, \ldots q_k) = 1$. По теореме 1.3.1 существуют $x_i \in \mathbb{Z}$, $i = \overline{1,k}$ такие, что $d = x_1a_1 + x_2a_2 + \ldots + x_ka_k$. Подставим (1.8) в данное равенство

$$d = x_1(dq_1) + x_2(dq_2) + \ldots + x_k(dq_k).$$

Так как умножение целых чисел ассоциативно и коммутативно, то получим

$$d = d(x_1q_1) + d(x_2q_2) + \ldots + d(x_kq_k).$$

Разделим обе части последнего равенства на d, получим

$$1 = x_1q_1 + x_2q_2 + \ldots + x_kq_k.$$

Получили, что натуральный общий делитель 1 целых чисел $q_1, q_2, \ldots, q_k$ представим в виде целочисленной линейной комбинации этих чисел. Следовательно, 1 является наибольшим общим делителем этих чисел.

Достаточность. Покажем, что если частные от деления целых чисел на их общий делитель взаимно простые числа, то этот общий делитель является наибольшим общим делителем этих чисел этих чисел.

Пусть $d = \text{ОД}(a_1, a_2, \ldots, a_k)$, $d \in \mathbb{N}$. Тогда

$$a_i = dq_i, \tag{1.9}$$

где $\text{НОД}(q_1, q_2, \ldots, q_k) = 1$. Докажем, что $d = \text{НОД}(a_1, a_2, \ldots, a_k)$. Действительно, так как $\text{НОД}(q_1, q_2, \ldots, q_k) = 1$, то $1 = x_1q_1 + x_2q_2 + \ldots + x_kq_k$, $x_i \in \mathbb{Z}$, $i = \overline{1, k}$.

Умножив обе части этого равенства на d получим

$$d = d(x_1q_1) + d(x_2q_2) + \ldots + d(x_kq_k).$$

Применив ассоциативный и коммутативный законы умножения целых чисел, получим

$$d = x_1(dq_1) + x_2(dq_2) + \ldots + x_k(dq_k).$$

Учитывая (1.9), имеем $d = x_1a_1 + x_2a_2 + \ldots + x_ka_k$. Следовательно, $d = \text{НОД}(a_1, a_2, \ldots, a_k)$. ⊠

Определение 1.3.1. *Алгоритмом Евклида* для двух целых чисел a и b, $b \neq 0$ называется процесс последовательного деления, который можно описать следующими равенствами с соответствующими условиями, выполняемыми для этих равенств:

$$a = bq_1 + r_1,\ 0 < r_1 < |b|,$$
$$b = r_1q_2 + r_2,\ 0 < r_2 < r_1,$$
$$r_1 = r_2q_3 + r_3,\ 0 < r_3 < r_2$$

и т.д.

Вопрос о конечности данного процесса решается следующим образом: заметим, что остатки удовлетворяют условию $|b| > r_1 > r_2 > r_3 > \ldots$, т.е. образуют убывающий натуральный ряд, который убывать бесконечно не может, так как числа этого ряда натуральные. Следовательно, в этом процессе число остатков конечно, а, значит, и сам процесс конечен. Этот процесс остановит нулевой остаток,

так как следующий шаг алгоритма будет состоять в делении на нуль, что невозможно.

Пусть $r_{k+1} = 0$. Тогда предпоследний и последний шаги в алгоритме Евклида запишутся следующим образом

$$r_{k-2} = r_{k-1}q_k + r_k,\ 0 < r_k < r_{k-1},$$
$$r_{k-1} = r_k q_{k+1}.$$

Теорема 1.3.3. Наибольший общий делитель двух целых чисел равен последнему ненулевому остатку в алгоритме Евклида для этих чисел.

□. Пусть a и b целые числа, $b \neq 0$. Запишем для этих чисел алгоритм Евклида:

$$a = bq_1 + r_1,\ 0 < r_1 < |b|,$$
$$b = r_1q_2 + r_2,\ 0 < r_2 < r_1,$$
$$r_1 = r_2q_3 + r_3,\ 0 < r_3 < r_2,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$r_{k-2} = r_{k-1}q_k + r_k,\ 0 < r_k < r_{k-1},$$
$$r_{k-1} = r_k q_{k+1} + 0,$$
$$r_{k+1} = 0.$$

В силу теоремы 1.2.4 из первого равенства получим НОД$(a, b) =$ $=$ НОД(b, r_1), из второго и последующих равенств, используя свойство наибольшего общего делителя, получим

$$\text{НОД}(a, b) = \text{НОД}(b, r_1) = \text{НОД}(r_1, r_2) = \text{НОД}(r_2, r_3) = \ldots =$$
$$= \text{НОД}(r_{k-1}, r_k) = \text{НОД}(r_k, 0) = r_k.$$

⊠

Теорема 1.3.4. Любой общий делитель целых чисел $a_1, a_2, \ldots, a_k$, $k \geq 2$ является делителем наибольшего общего делителя этих чисел.

□. Пусть $D = \text{НОД}(a_1, a_2, \ldots, a_k)$, $d = \text{ОД}(a_1, a_2, \ldots, a_k)$, $k \geq 2$. Докажем, что $D \vdots d$. Так как $d = \text{ОД}(a_1, a_2, \ldots, a_k)$, то

$$a_1 \vdots d, a_2 \vdots d, \ldots, a_k \vdots d. \tag{1.10}$$

По теореме 1.3.1

$$D = x_1a_1 + x_2a_2 + \ldots + x_ka_k, \tag{1.11}$$

где $x_i \in \mathbb{Z}$, $i = \overline{1,k}$. Тогда по свойству делимости суммы из (1.10) и (1.11) следует, что $D \vdots d$. ⊠

Теорема 1.3.5. Каждый делитель наибольшего общего делителя целых чисел $a_1, a_2, \ldots, a_k$, $k \geq 2$ является общим делителем этих чисел.

□. Пусть $d = \text{НОД}(a_1, a_2, \ldots, a_k)$ и c — произвольный делитель наибольшего общего делителя d, т.е. $d \vdots c$. Докажем, что $c = \text{ОД}(a_1, a_2, \ldots, a_k)$. Так как $d \vdots c$, то $d = cq$, $q \in \mathbb{N}$, т.е. $\text{НОД}(a_1, a_2, \ldots, a_k) = cq$, следовательно, $a_i \vdots cq$, $i = \overline{1,k}$. Тогда $a_i \vdots c$, значит, $c = \text{ОД}(a_1, a_2, \ldots, a_k)$ ⊠

Теорема 1.3.6. $\text{НОД}(ba_1, ba_2, \ldots, ba_k) = b\text{НОД}(a_1, a_2, \ldots, a_k)$.

Теорема 1.3.7. $\text{НОД}\left(\frac{a_1}{b}, \frac{a_2}{b}, \ldots, \frac{a_k}{b}\right) = \frac{\text{НОД}(a_1, a_2, \ldots, a_k)}{b}$.

Теорема 1.3.8.

$$\text{НОД}(a_1, a_2, \ldots, a_{k-1}, a_k) = \text{НОД}(\text{НОД}(a_1, a_2, \ldots, a_{k-1}), a_k).$$

Пример 1.3.1. Вычислите $\text{НОД}(96, 165)$ и $\text{НОД}(2585, 7975)$. Выразите НОД через исходные числа.

□. Составим алгоритм Евклида для чисел 165 и 96, последовательно выполняя деление с остатком: $165 = 96 \cdot 1 + 69$, $96 = 69 \cdot 1 + 27$, $69 = 27 \cdot 2 + 15$, $27 = 15 \cdot 1 + 12$, $15 = 12 \cdot 1 + 3$, $12 = 3 \cdot 4$. Последний отличный от нуля остаток в алгоритме Евклида является наибольшим общим делителем чисел 165 и 96, то есть $\text{НОД}(96, 165) = 3$.

Чтобы выразить $\text{НОД}(96, 165)$ через исходные числа 96 и 165, будем двигаться в алгоритме Евклида снизу вверх, последовательно выражая остатки: $\text{НОД}(96, 165) = 3 = 15 - 12 = 15 - (27 - 15) = 2 \cdot 15 - 27 = 2(69 - 27 \cdot 2) - 27 = 2 \cdot 69 - 5 \cdot 27 = 2 \cdot 69 - 5(96 - 69) = 7 \cdot 69 - 5 \cdot 96 = 7(165 - 96) - 5 \cdot 96 = 7 \cdot 165 - 12 \cdot 96$. Поэтому $3 = 96(-12) + 7 \cdot 165$.

Производя деление для чисел 2585 и 7975, получаем равенства: $7975 = 2585 \cdot 3 + 220$, $2585 = 220 \cdot 11 + 165$, $220 = 165 \cdot 1 + 55$, $165 = 55 \cdot 3$. Последний отличный от нуля остаток равен 55, это и есть наибольший общий делитель чисел 2585 и 7975. Так как $55 = 220 - 165 = 220 - (2585 - 220 \cdot 11) = 220 \cdot 12 - 2585 = (7975 - 2585 \cdot 3)12 - 2585 = 2585(-37) + 7975 \cdot 12$, то $55 = 2585(-37) + 7975 \cdot 12$.

Ответ: $\text{НОД}(96, 165) = 3 = 96(-12) + 7 \cdot 165$.

$\text{НОД}(2585, 7975) = 55 = 2585(-37) + 7975 \cdot 12$. ⊠

Кроме алгоритма Евклида, для нахождения НОД используется также *бинарный алгоритм*. Он основан на следующих трех очевидных свойствах НОД.

Лемма 1.3.1. Для любых целых чисел a и b, отличных от нуля, справедливы следующие утверждения:

1) $\text{НОД}(2a, 2b) = 2\text{НОД}(a, b)$;

2) $\text{НОД}(2a, 2b+1) = \text{НОД}(a, 2b+1)$;

3) $\text{НОД}(a, b) = \text{НОД}(a-b, b)$.

В соответствии с этими свойствами для нахождения $d = \text{НОД}(a, b)$ осуществляются следующие действия.

Шаг 1. Выделяют наибольшую степень 2^k двойки, на которую делятся числа a и b. Уменьшают числа a и b в 2^k раз: $a = 2^k a_1$, $b = 2^k b_1$. Одно из чисел a_1 или b_1 нечетно, пусть нечетно b_1. Теперь $d = 2^k d_1$, где $d_1 = \text{НОД}(a_1, b_1)$.

Шаг 2. Если a_1 четно, то делят его на максимально возможную степень 2, оставив b_1 без изменения. Получают $a_1 = 2^t a_2$, a_2 и b_1 нечетны и $d_1 = \text{НОД}(a_1, b_1) = \text{НОД}(a_2, b_1)$. Теперь надо найти НОД двух нечетных чисел a_2, b_1.

Шаг 3. Вычитают из большего числа меньшее. Если $a_2 > b_1$, то $\text{НОД}(a_2, b_1) = \text{НОД}(a_2 - b_1, b_1)$. Число $a_2 - b_1$ четное как разность двух нечетных чисел.

Шаг 4. Применяют к $a_2 - b_1$ действие шага 2, затем действие шага 3 и т. д.

После выполнения действий шага 2 и шага 3 НОД не меняется, а хотя бы одно из чисел пары уменьшается. Поэтому в некоторый момент оба числа станут равными друг другу и равными d_1. Искомый $\text{НОД}(a, b)$ вычисляется после этого как произведение чисел 2^k и d_1.

В бинарном алгоритме используются лишь две операции: вычитание и деление на 2. Это позволяет при «ручном» нахождении НОД избежать вычислительных ошибок, ведь необходимо только правильно вычитать и делить на 2.

Пример 1.3.2. Найдите $\text{НОД}(29\,568, 8580)$.

□. Шаг 1. Выделяем наибольшую степень двойки, на которую делятся эти числа: $29\,568 = 2^2 \cdot 7392$, $8580 = 2^2 \cdot 2145$. Запоминаем 2^2.

Шаг 2. Число 7392 четное. Делим его на максимально возможную

степень 2, оставляя второе число 2145 без изменения. $7392 = 2^5 \cdot 231$. Теперь надо искать $d = \text{НОД}(231, 2145)$.

Шаг 3. Вычитаем из большего числа 2145 меньшее 231. Имеем: $2145 - 231 = 1914$, $d = \text{НОД}(231, 1914)$.

Шаг 4. Применяем к 1914 действие шага 2. Получаем $1914 = 2 \cdot 957$. Теперь $d = \text{НОД}(231, 957)$, и надо возвращаться к действиям шага 2 и шага 3 и т. д.

Все эти вычисления записываются следующим образом.

шаг 1	$29\,568 = 2^2 \cdot 7392$	$8580 = 2^2 \cdot 2145$
шаг 2	$7392 = 2^5 \cdot 231$	
шаг 3		$2145 - 231 = 1914$
шаг 2		$1914 = 2 \cdot 957$
шаг 3		$957 - 231 = 726$
шаг 2		$726 = 2 \cdot 363$
шаг 3		$363 - 231 = 132$
шаг 2		$132 = 2^2 \cdot 33$
шаг 3	$231 - 33 = 198$	
шаг 2	$198 = 2 \cdot 99$	
шаг 3	$99 - 33 = 66$	
шаг 2	$66 = 2 \cdot 33$	
шаг 3	$33 - 33 = 0$	

Итак, $\text{НОД}(29\,568, 8580) = 2^2 \cdot 33 = 132$.

Вычислим НОД с помощью алгоритма Евклида. $29\,568 = 8580 \cdot 3 + 3828$, $8580 = 3828 \cdot 2 + 924$, $3828 = 924 \cdot 4 + 132$, $924 = 132 \cdot 7$.

Ответ: $\text{НОД}(29\,568, 8580) = 132$. ⊠

Можно соединить алгоритм Евклида с бинарным алгоритмом следующим образом. Если $a \geq b > 0$ нечетны, то $a = bq + r$, где $0 \leq |r| < b$ и r четно. Поэтому, если $r \neq 0$, то r делим на максимальную степень 2, пока r не станет нечетным. Затем пару a, b заменяем парой $b, |r|$ и повторяем этот процесс.

Пример 1.3.3. Найдите $\text{НОД}(29\,568, 8580)$.

□. $\text{НОД}(29\,568, 8580) = 2^2\text{НОД}(7392, 2145)$, $7392 = 2145 \cdot 4 - 1188$, $1188 = 4 \cdot 297$, $2145 = 297 \cdot 7 + 66$, $66 = 2 \cdot 33$, $297 = 33 \cdot 9$. Итак, $\text{НОД}(7392, 2145) = 33$.

Ответ: $\text{НОД}(29\,568, 8580) = 4 \cdot 33 = 132$. ⊠

1.4. Теоремы о взаимно простых числах.

Теорема 1.4.1. Целые числа $a_1, a_2, \ldots, a_k$, $k \geq 2$ взаимно просты, т.е. НОД$(a_1, a_2, \ldots, a_k) = 1$, тогда и только тогда, когда 1 можно представить в виде целочисленной линейной комбинации этих чисел, т.е. существуют единственные $x_1, x_2, \ldots, x_k \in \mathbb{Z}$ такие, что $a_1x_1 + a_2x_2 + \ldots + a_kx_k = 1$.

Теорема 1.4.2. Если произведение двух целых чисел a и b делится на $c \in \mathbb{Z}$, взаимно простое с одним из сомножителей, то второй сомножитель делится на это число.

$\square$. Пусть ab делится на c и НОД$(a, c) = 1$. Докажем, что $b \vdots c$.

Так как НОД$(a, c) = 1$, то по теореме 1.4.1 существуют $x_1, x_2 \in \mathbb{Z}$ такие, что

$$ax_1 + cx_2 = 1. \tag{1.12}$$

Умножив равенство (1.12) на b, получим $b(ax_1)+b(cx_2) = b$, $(ab)x_1+ + (cb)x_2 = b$, так как операция умножения на $\mathbb{Z}$ ассоциативна и коммутативна. Так как $ab \vdots c$ и $c \vdots c$, то по свойству делимости суммы следует, что $b \vdots c$. $\boxtimes$

Теорема 1.4.3. Если каждое из двух целых чисел a и b взаимно просто с третьим числом c, то и произведение этих чисел ab взаимно просто с этим числом.

$\square$. Пусть НОД$(a, c) = 1$, НОД$(b, c) = 1$. Докажем, что НОД$(ab, c) = 1$. По теореме 1.4.1 из НОД$(a, c) = 1$ вытекает $ax_1 + cx_2 = 1$, $x_1, x_2 \in \mathbb{Z}$, и из НОД$(b, c) = 1$ следует

$$by_1 + cy_2 = 1, y_1, y_2 \in \mathbb{Z}. \tag{1.13}$$

Перемножив равенства (1.12) и (1.13), получим

$$1 = (ax_1)(by_1) + (ax_1)(cy_2) + (cx_2)(by_1) + (cx_2)(cy_2),$$
$$1 = (ab)(x_1y_1) + c(ax_1y_2 + bx_2y_1 + cx_2y_2),$$
$$x_1, y_1 \in \mathbb{Z},\ ax_1y_2 + bx_2y_1 + x_2y_2 \in \mathbb{Z}.$$

Обозначив $x_1y_1 = m$, $ax_1y_1+bx_1y_1+x_2y_2 = n$, получим $1 = (ab)m+ + cn$, $m,\ n \in \mathbb{Z}$. Тогда по теореме 1.4.1 НОД$(ab, c) = 1$ $\boxtimes$

Следствие 1.4.1. (обобщение теоремы 1.4.3). Если каждое из целых чисел $a_1, a_2, \ldots, a_k$, $k \geq 2$ взаимно просто с целым числом b, то и

$$\text{НОД}\left(\prod_{i=1}^{k} a_i, b\right) = 1.$$

Следствие 1.4.2. Если каждое из целых чисел одной совокупности $a_1, a_2, \ldots, a_k$, $k \geq 2$ взаимно просто с каждым из чисел другой совокупности $b_1, b_2, \ldots, b_n$, то произведение чисел первой совокупности взаимно просто с произведением чисел второй совокупности

$$\text{НОД}\left(\prod_{i=1}^{k} a_i, \prod_{j=1}^{n} b_j\right) = 1.$$

Следствие 1.4.3. Если $\text{НОД}(a, b) = 1$, то $\text{НОД}\left(a^k, b^n\right) = 1$, $k, n \in \mathbb{N}$.

Следствие 1.4.4. Если дробь $\dfrac{a}{b}$ несократима, т.е. $\text{НОД}(a, b) = 1$, то и $\dfrac{a^k}{b^n}$ несократима, где $k, n \in \mathbb{N}$, т.е. $\text{НОД}\left(a^k, b^n\right) = 1$.

Теорема 1.4.4. Если $a \vdots b$, $a \vdots c$ и $\text{НОД}(b, c) = 1$, то $a \vdots bc$.

$\square$. Так как $a \vdots b$, то

$$a = bq_1, q_1 \in \mathbb{Z}. \tag{1.14}$$

Так как $a \vdots c$, то

$$a = cq_2, q_2 \in \mathbb{Z}. \tag{1.15}$$

Из (1.14) и (1.15) следует, что $bq_1 = cq_2$. Так как $\text{НОД}(b, c) = 1$, то $q_1 \vdots c$, а значит,

$$q_1 = cq_3, q_3 \in \mathbb{Z}. \tag{1.16}$$

Подставив (1.16) в (1.14), получим $a = b(cq_3) = (bc)q_3$, значит, $a \vdots bc$. $\boxtimes$

Следствие 1.4.5. (обобщение теоремы 1.4.4). Если $a \vdots b_1$, $a \vdots b_2, \ldots, a \vdots b_k$, $k \geq 2$ и $\text{НОД}(b_i, b_j) = 1$, $i \neq j$, то $a \vdots b_1 \cdot b_2 \cdot \ldots \cdot b_k$.

1.5. Наименьшее общее кратное. Свойства НОКа

Определение 1.5.1. Общим кратным целых чисел $a_1, a_2, \ldots, a_k$, $k \geq 2$ отличных от нуля называется целое число, которое делится на каждое из этих чисел (ОК).

Очевидно, что для любой совокупности целых чисел $a_1, a_2, \ldots a_k$, $a_i \neq 0$, $i = \overline{1,k}$ существует бесконечно много общих кратных, например, число вида чисел $a_1 \cdot a_2 \cdot \ldots \cdot a_k \cdot n$, где $n \in \mathbb{Z}$.

Заметим, что $|a_1 \cdot a_2 \cdot \ldots \cdot a_k|$ — натуральное общее кратное совокупности целых чисел $a_1, a_2, \ldots, a_k$, $k \geq 2$, поэтому наименьшее натуральное общее кратное либо равно этому числу, либо меньше его. Если натуральное НОК меньше $|a_1 \cdot a_2 \cdot \ldots \cdot a_k|$, то оно содержится в промежутке от 1 до $|a_1 \cdot a_2 \cdot \ldots \cdot a_k|$, где находится конечное число натуральных чисел, а, значит, и конечное число натуральных общих кратных совокупности $a_1, a_2, \ldots, a_k$, среди которых найдется наименьшее.

Определение 1.5.2. Наименьшее натуральное ОК целых чисел, отличных от нуля, называется наименьшим общим кратным этих чисел и обозначается НОК$(a_1, a_2, \ldots, a_k)$ или $[a_1, a_2, \ldots, a_k]$, $k \geq 2$.

Теорема 1.5.1. НОК$(a_1, a_2, \ldots, a_k)$=НОК$(|a_1|, |a_2|, \ldots, |a_k|)$.

Теорема 1.5.2. НОК(a, b)=$\dfrac{a \cdot b}{\text{НОД}(a, b)}$, $a, b \in \mathbb{N}$.

$\square$. Пусть m любое ОК(a, b). Тогда по определению $m \vdots a$ и $m \vdots b$, следовательно,

$$m = aq_1, m = bq_2, q_1, q_2 \in \mathbb{Z}. \tag{1.17}$$

Отсюда, $aq_1 = bq_2$. Пусть НОД$(a, b) = d$. Тогда

$$a = dq_3, b = dq_4, \text{НОД}(q_3, q_4) = 1. \tag{1.18}$$

Из (1.17) и (1.18) получим $q_1 q_3 = q_2 q_4$, отсюда $q_1 q_3$ делится на q_4. Поскольку НОД$(q_3, q_4) = 1$, то $q_1 \vdots q_4$. По определению делимости целых чисел $q_1 = q_4 q = \dfrac{b}{d} q$, где $q \in \mathbb{Z}$.

Из последнего равенства и равенства (1.17) получим

$$m = a\frac{b}{d}q = \frac{ab}{d}q,\ q \in \mathbb{Z}.$$

Среди всех общих кратных выбираем наименьшее, которое получим при $q = 1$, т.е. $\text{НОК}(a, b) = \dfrac{ab}{\text{НОД}(a, b)}$. ⊠

Пример 1.5.1. Найдите $\text{НОК}(2585, 7975)$.

□. По теореме 1.5.2 имеем:

$$\text{НОК}(2585, 7975) = \frac{2585 \cdot 7975}{\text{НОД}(2585, 7975)} = \frac{2585 \cdot 7975}{55} = 374\,825.$$

Ответ: $\text{НОК}(2585, 7975) = 374\,825$. ⊠

Теорема 1.5.3. Любое общее кратное целых чисел делится на их наименьшее общее кратное.

□. *Доказать самостоятельно для двух чисел.* ⊠

Теорема 1.5.4. Частные от деления наименьшего общего кратного целых чисел на эти числа суть взаимно простые числа.

Теорема 1.5.5. $\text{НОК}(ca_1, a_2, \ldots, a_k) = c\text{НОК}(a_1, a_2, \ldots, a_k)$.

Теорема 1.5.6. $\text{НОК}\left(\dfrac{a_1}{c}, \dfrac{a_2}{c}, \ldots, \dfrac{a_k}{c}\right) = \dfrac{\text{НОК}(a_1, a_2, \ldots, a_k)}{c}$.

Теорема 1.5.7.

$$\text{НОК}(a_1, a_2, \ldots, a_{k-1}, a_k) = \text{НОК}\left(\text{НОК}(a_1, a_2, \ldots, a_{k-1}), a_k\right).$$

Пример 1.5.2. Найти $\text{НОК}(65, 210, 102)$.

□. $\text{НОК}(65, 210, 102) = \text{НОК}\left(\text{НОК}(65, 210), 102\right)$.

$$\text{НОК}(65, 210) = \frac{65 \cdot 210}{\text{НОД}(65, 210)} = \frac{65 \cdot 210}{5} = 2730,$$

$$\text{НОК}(65, 210, 102) = \text{НОК}(2730, 102) = \frac{2730 \cdot 102}{\text{НОД}(2730, 102)} =$$

$$= \frac{2730 \cdot 102}{6} = 46410.$$

Ответ: $\text{НОК}(65, 210, 102) = 46410$. ⊠

Заметим, что вообще говоря $\text{НОК}(a, b, c) \neq \dfrac{abc}{\text{НОД}(a, b, c)}$; равенство имеет место лишь тогда, когда a, b, c попарно взаимно просты.

Теорема 1.5.8. Наименьшее общее кратное попарно взаимно простых чисел равно модулю произведения этих чисел, т.е. $\text{НОК}(a_1, a_2, \ldots, a_k) = |a_1 \cdot a_2 \cdot \ldots \cdot a_k|$, где $\text{НОД}(a_i, a_j) = 1$, $i \neq j$.

Пример 1.5.3. Найдите натуральные числа a и b, если НОД$(a, b) = 24$, а НОК$(a, b) = 2496$.

$\square$. Пусть $a = 24m$, $b = 24n$. Так как НОД$(a, b) = 24$, то m и n — взаимно простые натуральные числа. Пусть для определенности $m < n$. Используя связь НОК и НОД натуральных чисел, имеем $24 \cdot 2496 = 24m \cdot 24n$, откуда $m \cdot n = 104 = 2^3 \cdot 13$. Поскольку m и n взаимно просты, то возможны два случая:

1) $m = 1$, $n = 104$. Тогда $a = 24$, $b = 2496$;

2) $m = 2^3$, $n = 13$. Тогда $a = 192$, $b = 312$.

Ответ: $a = 24$, $b = 2496$ или $a = 192$, $b = 312$. $\boxtimes$

1.6. Конечные цепные дроби. Подходящие дроби

Всякое рациональное число t можно представить в виде дроби

$$t = \frac{a}{b}, \text{ где } a \in \mathbb{Z},\ b \in \mathbb{N}.$$

Такое представление называют обыкновенной дробью. Наряду с этим t можно представить в виде так называемой конечной цепной дроби.

Применим алгоритм Евклида к числам a и b. Получим

$$\begin{gathered}
a = b \cdot q_0 + r_1 \Rightarrow \tfrac{a}{b} = q_0 + \tfrac{r_1}{b}, \\
b = r_1 \cdot q_1 + r_2 \Rightarrow \tfrac{b}{r_1} = q_1 + \tfrac{r_2}{r_1}, \\
r_1 = r_2 \cdot q_2 + r_3 \Rightarrow \tfrac{r_1}{r_2} = q_2 + \tfrac{r_3}{r_2}, \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
r_{n-2} = r_{n-1} \cdot q_{n-1} + r_n \Rightarrow \tfrac{r_{n-2}}{r_{n-1}} = q_{n-1} + \tfrac{r_n}{r_{n-1}}, \\
r_{n-1} = r_n \cdot q_n \Rightarrow \tfrac{r_{n-1}}{r_n} = q_n.
\end{gathered}$$

Из второго равенства находим

$$\frac{r_1}{b} = \frac{1}{q_1 + \dfrac{r_2}{r_1}}. \tag{1.19}$$

Выполнив подстановку в первое равенство из второго, получим:

$$\frac{a}{b} = q_0 + \frac{1}{q_1 + \dfrac{r_2}{r_1}}. \tag{1.20}$$

Из третьего равенства имеем:

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

Подставим это выражение в равенство (1.20), получим:

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

и т.д.

В конечном итоге будем иметь

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ldots + \cfrac{1}{q_n}}}, q_0 \in \mathbb{Z}, q_i \in \mathbb{N}, i = \overline{1,n}, q_n \neq 1. \qquad (1.21)$$

Определение 1.6.1. Представление (1.21) рационального числа $t = \frac{a}{b}$ называется *конечной цепной дробью.*

Определение 1.6.2. Числа $q_0, q_1, \ldots, q_n$ в цепной дроби (1.21) называют *неполными частными числа* t или *элементами цепной дроби.*

Сокращенную цепную дробь (1.21) записывают

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

Теорема 1.6.1. Всякое рациональное число $\frac{a}{b}$ однозначно представимо в виде конечной цепной дроби. Причем элементами цепной дроби будут являться неполные частные из алгоритма Евклида для чисел a и b.

Определение 1.6.3. Пусть (1.21) — представление рационального числа $\frac{a}{b}$ в виде цепной дроби. Тогда дроби

$$\delta_0 = \frac{q_0}{1},\ \delta_1 = q_0 + \frac{1}{q_1},\ \delta_2 = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2}},\ \ldots,\ \delta_n = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ldots + \cfrac{1}{q_n}}}$$

называют *подходящими дробями цепной дроби (1.21) или рационального числа* $\frac{a}{b}$.

Легко заметить, что подходящая дробь δ_i получается из дроби δ_{i-1} заменой в ней q_{i-1} на $q_{i-1} + \dfrac{1}{q_i}$, где $i = \overline{1,n}$.

Всякая подходящая дробь δ_s есть рациональное число, следовательно, представима в виде обыкновенной дроби, т.е. в виде $\dfrac{P_s}{Q_s}$, где $P_s \in$ $\in \mathbb{Z}$, $Q_s \in \mathbb{N}$, где $s = \overline{0, n}$.

Выведем рекуррентные формулы для вычисления числителя P_s и знаменателя Q_s подходящей дроби δ_s.

$$\delta_0 = \frac{q_0}{1} = \frac{P_0}{Q_0} \Rightarrow P_0 = q_0, Q_0 = 1;$$

$$\delta_1 = q_0 + \frac{1}{q_1} = \frac{q_0 \cdot q_1 + 1}{q_1} = \frac{P_1}{Q_1} \Rightarrow P_1 = q_0 \cdot q_1 + 1, Q_1 = q_1;$$

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

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

Предположим, что нами уже получено равенство

$$\delta_{s-1} = \frac{P_{s-2} \cdot q_{s-1} + P_{s-3}}{Q_{s-2} \cdot q_{s-1} + Q_{s-3}} = \frac{P_{s-1}}{Q_{s-1}}$$

для подходящей дроби δ_{s-1}. Покажем, что аналогичное равенство справедливо и для δ_s.

$$\delta_s = \frac{P_{s-2} \cdot \left(q_{s-1} + \frac{1}{q_s}\right) + P_{s-3}}{Q_{s-2} \cdot \left(q_{s-1} + \frac{1}{q_s}\right) + Q_{s-3}} = \frac{P_{s-2} \cdot q_{s-1} \cdot q_s + P_{s-2} + P_{s-3} \cdot q_s}{Q_{s-2} \cdot q_{s-1} \cdot q_s + Q_{s-2} + Q_{s-3} \cdot q_s} =$$

$$= \frac{(P_{s-2} \cdot q_s + P_{s-3})q_s + P_{s-2}}{(Q_{s-2} \cdot q_s + Q_{s-3})q_s + Q_{s-2}} = \frac{P_{s-1}q_s + P_{s-2}}{Q_{s-1}q_s + Q_{s-2}} = \frac{P_s}{Q_s}. \tag{1.22}$$

Таким образом,

$$\delta_s = \frac{P_s}{Q_s} = \frac{P_{s-1}q_s + P_{s-2}}{Q_{s-1}q_s + Q_{s-2}} \Rightarrow$$

$$\Rightarrow P_s = P_{s-1}q_s + P_{s-2}, Q_s = Q_{s-1}q_s + Q_{s-2}. \tag{1.23}$$

Эти формулы справедливы для $s = 2$, и из предположения, что они справедливы для $s - 1$, вытекает, что они верны и для s. На основании

принципа математической индукции заключаем, что они справедливы для любого $s \leq n$.

Вычисление числителей и знаменателей подходящих дробей удобно выполнять по следующей схеме:

s		0	1	2	...	s	...	n
q_s		q_0	q_1	q_2	...	q_s	...	q_n
P_s	1	q_0	$q_0 \cdot q_1 + 1$	$P_1 \cdot q_2 + P_0$	...	$P_{s-1} \cdot q_s + P_{s-2}$	...	$P_{n-1} \cdot q_n + P_{n-2}$
Q_s	0	1	q_1	$Q_1 \cdot q_2 + Q_0$	...	$Q_{s-1} \cdot q_s + Q_{s-2}$	...	$Q_{n-1} \cdot q_n + Q_{n-2}$

Для вычисления $P_s(Q_s)$ по данной схеме нужно число q_s, стоящее сверху, умножить на число $P_{s-1}(Q_{s-1})$, стоящее слева, и к произведению прибавить число $P_{s-2}(Q_{s-2})$, которое предшествует P_{s-1}.

Пример 1.6.1. Представить в виде цепной дроби число $2,718$ и найти все подходящие дроби этого числа.

$\square$. Применим алгоритм Евклида к числам $a = 2718$ и $b = 1000$.

$$\begin{array}{llll} q_0 = 2; & r_1 = 718; & q_1 = 1; & r_2 = 282; \\ q_2 = 2; & r_3 = 154; & q_3 = 1; & r_4 = 128; \\ q_4 = 1; & r_5 = 26; & q_5 = 4; & r_6 = 24; \\ q_6 = 1; & r_7 = 2; & q_7 = 12. & \end{array}$$

Таким образом,

$$2,718 = [2; 1, 2, 1, 1, 4, 1, 12] = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{12}}}}}}}.$$

Подходящие дроби находим по схеме

s		0	1	2	3	4	5	6	7
q_s		2	1	2	1	1	4	1	12
P_s	1	2	3	8	11	19	87	106	1359
Q_s	0	1	1	3	4	7	32	39	500

Выпишем все подходящие дроби

$$\delta_0 = \frac{2}{1} = 2;\ \delta_1 = \frac{3}{1} = 3;\ \delta_2 = \frac{8}{3};\ \delta_3 = \frac{11}{4};$$
$$\delta_4 = \frac{19}{7};\ \delta_5 = \frac{87}{32};\ \delta_6 = \frac{106}{39};\ \delta_7 = \frac{1359}{500}.$$

⊠

Пример 1.6.2. Разложите рациональное число $\frac{53}{21}$ в цепную дробь.

□. Применим алгоритм Евклида к числам $a = 53$ и $b = 21$.

$$\begin{array}{ll} q_0 = 2; & r_1 = 11; \qquad q_1 = 1; \quad r_2 = 10; \\ q_2 = 1; & r_3 = 1; \qquad q_3 = 10. \end{array}$$

Следовательно, $\frac{53}{21} = [2; 1, 1, 10]$ — разложение данного рационального числа в конечную цепную дробь.

Для ответа на второй вопрос составим таблицу.

s		0	1	2	3
q_s		2	1	1	10
P_s	1	2	3	5	53
Q_s	0	1	1	2	21

Выпишем все подходящие дроби

$$\delta_0 = \frac{2}{1} = 2;\ \delta_1 = \frac{3}{1} = 3;\ \delta_2 = \frac{5}{2};\ \delta_3 = \frac{53}{21}.$$

Ответ: $\frac{53}{21} = [2; 1, 1, 10]$.

⊠

Свойства подходящих дробей.

Лемма 1.6.1. Числители и знаменатели двух соседних подходящих дробей связаны соотношением

$$P_s \cdot Q_{s-1} - P_{s-1} \cdot Q_s = (-1)^{s-1}. \tag{1.24}$$

□. Доказательство проведем индукцией по s. При $s = 1$ имеем

$$P_1 \cdot Q_0 - P_0 \cdot Q_1 = (q_0 \cdot q_1 + 1) \cdot 1 - q_0 \cdot q_1 = 1 = (-1)^0.$$

Таким образом, при $s = 1$ свойство справедливо. Предположим, что свойство выполняется при $s = k$, т.е.

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

Тогда при $s = k+1$ будем иметь: $P_{k+1} \cdot Q_k - P_k \cdot Q_{k+1} = (P_k \cdot q_{k+1} + + P_{k-1}) \cdot Q_k - P_k \cdot (Q_k \cdot q_{k+1} + Q_{k-1}) = P_{k-1} \cdot Q_k - P_k \cdot Q_{k-1} = -(-1)^{k-1} = = (-1)^k$.

Итак, соотношение (1.24) верно при $s = 1$ и из предположения, что оно верно для $s = k$, вытекает справедливость и для $s = k + 1$. На основании принципа математической индукции заключаем, что соотношение (1.24) верно для любого s. ⊠

Лемма 1.6.2. Всякая подходящая дробь $\delta_s = \dfrac{P_s}{Q_s}$ несократима.

Лемма 1.6.3. Подходящие дроби $\delta_0, \delta_2, \delta_4, \ldots$ с четными номерами образуют возрастающую последовательность, а подходящие дроби $\delta_1, \delta_3, \ldots$ с нечетными номерами — убывающую последовательность чисел.

Лемма 1.6.4. Всякая подходящая дробь с четным номером меньше всякой подходящей дроби с нечетным номером.

Лемма 1.6.5. Всякая подходящая дробь числа $\dfrac{a}{b}$ с нечетным номером является приближением этого числа по недостатку, а всякая подходящая дробь числа $\dfrac{a}{b}$ с нечетным номером является его приближением по избытку.

Лемма 1.6.6. $Q_s \in \mathbb{N}$, $Q_s > Q_{s-1}$, $s = \overline{1, n}$.

1.7. Системы счисления

Определение 1.7.1. Всякий способ записи и наименования чисел называют *системой счисления или нумерацией*.

В любой системе счисления числа записывают с помощью символов, которые называют цифрами.

Различают позиционные и непозиционные системы счисления. В позиционных системах значение каждой цифры определяется не только самой цифрой, но и ее позицией в записи числа. В непозиционных системах счисления значение каждой цифры не зависит от ее места расположения в записи числа.

Примером непозиционной системы счисления может служить римская нумерация.

Под позиционной системой счисления понимают определенную конечную систему символов, понятий и правил, которая позволяет запи-

сать всякое натуральное число с помощью знаков(цифр), значения которых зависят от позиций, занимаемых ими в записи числа.

При введении позиционной системы счисления вначале берут натуральное число $g > 1$, которое называют *основанием системы счисления.* Затем вводят знаки для обозначения числа от 0 до $g - 1$ и дают наименование этим числам. Множество цифр для системы с основанием g обозначим через $Z_g = \{0,\ 1, \ldots, g-1\}$.

Определение 1.7.2. Сумму

$$a_n \cdot g^n + a_{n-1} \cdot g^{n-1} + \ldots + a_1 \cdot g + a_0 = \sum_{i=0}^{n} a_i \cdot g^i,$$

где $a_i \in Z_g$, $i = \overline{0,n}$, $a_n \neq 0$ называют *систематическим числом с основанием* g.

Теорема 1.7.1. Всякое натуральное число m можно представить и притом единственным способом в виде систематического числа с основанием g, где g — произвольное натуральное число, больше 1.

$\square$. Если $m < g$, то $m \in \mathbb{Z}_g$ и теорема верна. Пусть $m \geq g$. Разделив m на g с остатком, получим:

$$m = m_1 \cdot g + a_0.$$

Если $m_1 < g$, то, приняв $m_1 = a_1$, получим представление числа m в виде систематического числа.

$$m = a_1 \cdot g + a_0.$$

Если $m_1 \geq g$, то делим m_1 на g с остатком. Получим

$$m = m_2 \cdot g + a_1.$$

Тогда $m = m_1 \cdot g + a_0 = (m_2 \cdot g + a_1)g = m_2 \cdot g^2 + a_1 \cdot g + a_0$.

Если $m_2 < g$, то, приняв $m_2 = a_2$, получим запись числа m в виде систематического числа

$$m = a_2 \cdot g^2 + a_1 \cdot g + a_0.$$

В случае $m_2 \geq g$ процесс продолжим.

Так как $m, m_1, m_2, \ldots$ являются натуральными числами и $m > m_1 > m_2 > \ldots$, то этот процесс не может продолжаться бесконечно и на каком-то n-ом шаге получим, что $m_n < g$.

Таким образом, число m будет представлено в виде систематического числа:

$$m = a_n \cdot g^n + a_{n-1} \cdot g^{n-1} + \ldots + a_1 \cdot g + a_0. \tag{1.25}$$

Единственность такого представления следует из однозначности деления с остатком.

⊠

Вместо записи

$$m = a_n \cdot g^n + \ldots + a_1 \cdot g + a_0$$

обычно пишут $m = \overline{a_n \ldots a_1 a_0}_g$.

Черта сверху в данном случае означает, что имеется в виду упорядоченная последовательность цифр, а не произведение чисел. При записи конкретного числа черту не пишут. В десятичной системе счисления индекс $g = 10$ не ставится.

Итак, натуральное число m можно записать в любой системе счисления. В процессе решения задач часто приходится переводить числа из одной системы счисления в другую.

1. *Пусть дана g-ичная запись числа N (1.25). Надо найти десятичную запись того же числа.*

Чтобы решить поставленную задачу достаточно поставить в запись (1.25) вместо $a_n, \ldots, a_0$ и g десятичные записи этих чисел и выполнить указанные действия. Десятичная запись результата и будет искомым ответом.

Пример 1.7.1. Переведите число $35,6$ из восьмеричной системы счисления в десятичную:

□. $35,6_8 = 3 \cdot 8^1 + 5 \cdot 8^0 + 6 \cdot 8^{-1} = 29,75.$ ⊠

2. *Пусть дана десятичная запись целого числа N. Надо найти g-ичную запись того же числа*

Чтобы решить поставленную задачу нам необходимо представить число N в виде (1.25). Для этого нужно найти коэффициенты $a_0, a_1, a_2, \ldots, a_n$. Разделим число m на g с остатком в системе счисления с основанием g. Получим $m = b_0 \cdot g + a_0$. Далее делим b_0 на g с остатком,

будем иметь $b_0 = b_1 \cdot g + a_1$. Отсюда

$$m = b_0 \cdot g + a_0 = (b_1 \cdot g + a_1) \cdot g + a_0 = b_1 \cdot g^2 + a_1 \cdot g + a_0.$$

Затем делим b_1 на g и т.д. Этот процесс продолжается до тех пор, пока в частности не получится 0. В результате будем иметь представление числа m в виде (1.25).

Отметим, что остатки $a_1, a_2, \ldots, a_n$ последовательного деления будут представлены в g-ичной системе.

Пример 1.7.2. Перевести целое число 876 из десятичной системы счисления в шестнадцатеричную. Учесть, что латинские буквы от A до F служат для обозначения шестнадцатеричных цифр от 10 до 15.

□.

$$\begin{array}{r|l} 876 & 16 \\ \hline 864 & 54 \quad\Big|\; 16 \\ \hline 12 & 48 \quad\Big|\; 3 \\ \hline & 6 \end{array}$$

Ответ: 36C. ⊠

3. *Пусть дана десятичная дробь N. Надо найти g-ичную запись этой дроби.*

Чтобы решить поставленную задачу нам необходимо умножить исходное число на g, целая часть полученного произведения является первой цифрой после запятой в искомом числе. Если дробная часть произведения не равна 0, умножим ее на g, целую часть полученного числа заменим на цифру в g-ичной системе и припишем ее справа к результату. Выпоняем такие действия до тех пор, пока дробная часть произведения не станет равной нулю или не выделится период (дробная часть окажется равной уже получившейся ранее дробной части произведения).

Пример 1.7.3. Перевести дробь $0,54675$ из десятичной системы счисления в двоичную с пятью знаками.

□.

0	54675
×	2
1	09350
×	2
0	1870
×	2
0	374
×	2
0	748
×	2
1	496

Ответ: $0,10001$. ⊠

Пример 1.7.4. Выполнить указанные действия над числами в заданной системе счисления и проверить результат выполнением этих же действий над ними в десятичной системе:

a) $101001_2 + 1101_2$

b) $3CF_{16} + 378_{16}$

c) $1101_2 \times 11_2$

□. Двоичное сложение:

$$\begin{array}{r} 10\,1001 \\ +\quad 1101 \\ \hline 11\,0110 \end{array}$$

Шестнадцатеричное сложение:

$$\begin{array}{r} 3CF \\ +\ 378 \\ \hline 747 \end{array}$$

Двоичное умножение:

$$\begin{array}{rr} & 1101 \\ \times & 11 \\ \hline & 1101 \\ + & 1101 \\ \hline & 100111 \end{array}$$

Ответ: 110110_2, 747_{16}, 100111_2.

⊠

1.8. Простые и составные числа

Определение 1.8.1. Натуральное число называется *простым*, если оно имеет только два натуральных делителя (1 и само число).

Например, 2, 3, 5, 7, 11, 13, 17, ... — являются простыми числами, так как каждое из этих чисел имеет только два натуральных делителя.

Определение 1.8.2. Натуральное число называется *составным*, если оно имеет более двух натуральных делителей (хотя бы один натуральный делитель отличный от 1 и самого числа).

Утверждение 1.8.1. 1) Единица не является ни простым, ни составным числом, так как имеет только один натуральный делитель.

2) Единственным четным простым числом является число 2.

Свойства простых чисел

Лемма 1.8.1. 1. Если простое число p делится на натуральное число q и $q \neq 1$, то $p = q$.

2. Для любого целого a и простого p следует, что $a \vdots p$ или НОД$(a, p) = 1$.

3. Если произведение целых чисел делится на простое число, то хотя бы один из сомножителей делится на это число.

□. 1. Так как p — простое число, то по определению простого числа p имеет только два натуральных делителя 1 и само себя. Учитывая, что $p \vdots q$ и $q \neq 1$, получим $p = q$.

2. *Доказать самостоятельно.*

3. *Доказать самостоятельно, используя метод математической индукции.* ⊠

Следствие 1.8.1. Если произведение простых чисел делится на простое число, то хотя бы один из сомножителей равен этому простому делителю.
Лемма 1.8.2. (о наименьшем простом делителе натурального числа $a > 1$). Любое натуральное число $a > 1$ имеет хотя бы один простой делитель. Таким делителем является, например, наименьший натуральный делитель числа a отличный от 1.

$\square$. Для любого $a \in \mathbb{N}$, $a \neq 1$ существует наименьший натуральный делитель отличный от 1. Обозначим его p и докажем, что p — простое. Воспользуемся методом от противного. Предположим, что p составное. Тогда по определению составного числа p имеет хотя бы один натуральный делитель q, $q \neq 1$, $q \neq p$, т.е. $1 < q < p$.

Таким образом, $a \vdots p$ и $p \vdots q$, следовательно, $a \vdots q$, $q < p$, т.е. q — натуральный делитель числа a. Получили $q \neq 1$ и $q < p$, что противоречит выбору p. $\boxtimes$

Теорема 1.8.1. (критерий составного числа). Натуральное число $a > 1$ является составным тогда и только тогда, когда оно делится хотя бы на одно простое число, не превосходящее $\sqrt{a}$.

$\square$. Пусть a — составное натуральное число, $a > 1$. Докажем, что оно имеет хотя бы один простой делитель не превосходящий $\sqrt{a}$.

По лемме 1.8.2 a имеет хотя бы один простой делитель. Это, например, наименьший натуральный делитель p.

Покажем, что p удовлетворяет условию $p \leq \sqrt{a}$. Действительно, так как $a \vdots p$, то $a = pq$, $q \in \mathbb{N}$, $1 < q < a$. Причем, в силу выбора p

$$p \leq q. \tag{1.26}$$

Домножив (1.26) на p, получим $p^2 \leq pq = a$, $p^2 \leq a$, $p \leq \sqrt{a}$.

Обратно. Если натуральное число $a \neq 1$ делится хотя бы на одно простое число $p \leq \sqrt{a}$, то a составное.

$\boxtimes$

Теорема 1.8.2. (критерий простого числа). Натуральное число $a > 1$ является простым тогда и только тогда, когда оно не делится ни на одно простое число p, не превосходящее $\sqrt{a}$.

□. Это утверждение справедливо в силу равносильности $A \Leftrightarrow B \equiv \overline{A} \Leftrightarrow \overline{B}$. ⊠

Пример 1.8.1. Выясните простым или составным является число 101.

□. Воспользуемся критерием простого числа. Очевидно, что $\sqrt{101} \approx 10,05$. Рассмотрим $p < 10$, т.е. $2, 3, 5, 7$. Число 101 не делится ни на одно из этих чисел, значит, 101 — простое число. ⊠

Пример 1.8.2. Являются ли числа 181 и 197 простыми?

□. 181 и 197 не делятся на простые числа $2, 5, 7, 11, 13$. Так как других простых чисел не более 15 нет и $\sqrt{181} < \sqrt{197} < 15$, то числа 181 и 197 простые.
Ответ: являются. ⊠

Теорема 1.8.3. (теорема Евклида). Множество простых чисел бесконечно.

□. Применим метод от противного. Допустим, что множество простых чисел конечное множество. Тогда на этом множестве существует наибольшее простое число p. Рассмотрим число $n = 2 \cdot 3 \cdot 5 \cdot \ldots \cdot p + 1$. Очевидно, что $n \in \mathbb{N}$, $n \neq 1$ и при делении на числа $2,\ 3,\ 5, \ldots, p$ дает остаток равный 1. Т.е. n не делится ни на одно простое число, что противоречит лемме о существовании простого делителя для любого натурального числа отличного от 1. Следовательно, предположение сделано неверно, т.е. множество простых чисел бесконечно. ⊠

Пример 1.8.3. Найдите значения простого числа p, если известно, что $4p^2 + 1$ и $6p^2 + 1$ — простые числа.

□. Все натуральные числа можно представить в виде $5n$, $5n \pm 1$, $5n \pm 2$. Числа вида $5n$ являются простыми только при $n = 1$. В этом случае $p = 5$ и $4p^2 + 1 = 101$, $6p^2 + 1 = 151$, т.е. мы нашли одно значение p, удовлетворяющее условию.

Покажем, что других значений p нет. Если $p = 5n \pm 1$, то $4p^2 + \\ + 1 = 4(20n^2 \pm 8n + 1)$ — число составное; если $p = 5n \pm 2$, то $6p^2 + 1 = \\ = 5(30n^2 \pm 24n + 1)$ — число составное. ⊠

Пример 1.8.4. Методом Евклида докажите, что простых чисел вида $6n-1$ бесконечно.

$\square$. Допустим противное, что при некотором k число $p = 6k-1$ — последнее простое число. Возьмем число $N = 2 \cdot 3 \cdot 5 \cdot 7 \ldots p - 1$. Первое слагаемое в правой части имеет множитель $2 \cdot 3 = 6$, поэтому можно записать $N = 6l - 1$. Все простые делители этого числа имеют вид $6m \pm 1$. Так как произведение чисел вида $6m+1$ имеет тот же вид, в чем легко убедиться, то число N имеет еще простой делитель q вида $6t-1$. С другой стороны, число N не делится ни на одно из простых чисел $2, 3, \ldots, p$, поэтому $q > p$, что противоречит допущению. $\boxtimes$

1.9. Разложение натуральных чисел на простые множители и его единственность.

Теорема 1.9.1. (основная теорема арифметики) Любое натуральное число $a > 1$ можно разложить на простые множители и это разложение единственно с точностью до порядка следования множителей.

$\square$. Рассмотрим следующие случаи:

1). $a = p$, где p — простое число. Тогда его разложение состоит из одного множителя p, причем разложение единственно.

2). a — составное число. Докажем существование разложения числа a на простые множители.

По лемме 1.8.2 число a имеет хотя бы один простой делитель. Этим делителем является наименьший натуральный делитель p_1. Следовательно, $a \vdots p_1$, т.е. $a = p_1 \cdot q_1$.

Заметим, что $q_1 > 1$, $q_1 \in \mathbb{N}$, поэтому по лемме 1.8.2 q_1 имеет хотя бы один простой делитель, в частности наименьший p_2, т.е. $q_1 = p_2 \cdot q_2$, где $q_2 \in N$. Получим $a = p_1 \cdot p_2 \cdot q_2$. Продолжая аналогичные рассуждения, заметим, что решение задачи сводится к нахождению простых делителей числа a, количество которых конечно.

Следовательно, процесс нахождения простых делителей числа a конечен, т.е. обязательно получится частное $q_k = 1$, которое не имеет простых делителей. Число a примет вид

$$a = p_1 \cdot p_2 \cdot \ldots \cdot p_k, \tag{1.27}$$

где p_i — простые числа, $i = \overline{1,k}$. Выражение (1.27) — разложение числа a на простые множители.

Докажем единственность этого разложения. Воспользуемся методом от противного. Допустим, что существует еще одно разложение числа a на простые множители:

$$a = q_1 \cdot q_2 \cdot \ldots \cdot q_s, \tag{1.28}$$

где q_j — простые числа, $j = \overline{1,s}$, $s \neq k$.

Пусть для определенности $s > k$. Из равенств (1.27) и (1.28) получим

$$p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_s. \tag{1.29}$$

Левая часть равенства (1.29) делится на p_1 значит, и правая часть (1.29) делится на p_1, т.е. $q_1 \cdot q_2 \cdot \ldots \cdot q_s \vdots p_1$. Тогда по следствию 1.8.1 один из сомножителей q_i совпадает с p_1. Пусть для определенности это будет q_1, т.е. $p_1 = q_1$. Разделим обе части (1.29) на p_1 получим:

$$p_2 \cdot p_3 \cdot \ldots \cdot p_k = q_2 \cdot q_3 \cdot \ldots \cdot q_s. \tag{1.30}$$

Рассуждая аналогично, заметим, что в равенстве (1.30) множитель $p_2 = q_2$, поэтому $p_3 \cdot p_4 \cdot \ldots \cdot p_k = q_3 \cdot q_4 \cdot \ldots \cdot q_s$. Повторяя процесс рассуждений k раз, получим $1 = q_{k+1} \cdot q_{k+2} \cdot \ldots \cdot q_s$. Мы получим, что 1 можно представить в виде произведения простых множителей, что невозможно. Следовательно, допущение $s \neq k$ неверно, т.е. разложения числа на простые множители могут различаться лишь порядком следования множителей.

В разложении натурального числа a на простые множители могут встречаться равные множители. Пусть множитель p_1 встречается α_1 раз, p_2 — α_2 раз, ..., p_k — α_k раз. Тогда число a примет вид $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_n}$, $a_i \in \mathbb{N}$, $i = \overline{1,k}$.

Такое разложение называется *каноническим разложением* числа a. ⊠

Теорема 1.9.2. Число b является натуральным делителем числа $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, $\alpha_i \in \mathbb{N}$, $i = \overline{1,k}$ тогда и только тогда, когда $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$, где $0 \leq \beta_i \leq \alpha_i$.

Теорема 1.9.3. Наибольший общий делитель натуральных чисел равен произведению всех общих простых множителей канонических разложений этих чисел, взятых с наименьшими показателями степеней.
Теорема 1.9.4. Наименьшее общее кратное натуральных чисел равно произведению простых множителей, входящих хотя бы в одно из канонических разложений этих чисел с наибольшими показателями степеней.
Пример 1.9.1. Разложите 2353 на простые множители.

□. Так как $\sqrt{2353} < 50$, то надо испытать все простые числа не более 47. Числа 2, 3, 5, 7, 11 не делят 2353, а 13 делит $2353 = 13 \cdot 181$. В предыдущем примере установлено, что 181 — простое число.
Ответ: $2353 = 13 \cdot 181$. ⊠

При решении задач типа «Доказать, число A, заданное в общем виде, делится на фиксированное число b» мы рекомендуем следующие методы:

1) представить число A в виде суммы слагаемых, каждое из которых делится на b;

2) представить число b в виде произведения попарно взаимно простых множителей и доказать делимость числа A на каждый из них;

3) разбить кольцо $\mathbb{Z}$ на классы равноостаточных чисел при делении на b и применить метод полной индукции;

4) провести доказательство методом полной математической индукции.

Ясно, что эти методы можно комбинировать. Полезно помнить, что произведение

$$a(a-1)(a-2)\dots(a-k+1) \tag{1.31}$$

k последовательных чисел делится на $k!$
Пример 1.9.2. Докажите, что число $A = a(a+1)(2a+1) \vdots 6$ для любого $a \in \mathbb{Z}$.

□. Вариант 1. $6 = 2 \cdot 3$ и НОД$(2,3) = 1$. Так как a и $a+1$ числа разной четности, то $a(a+1) \vdots 2$. Остается доказать, что $A \vdots 3$. Имеем $a = 3q$, или $a = 3q+1$, или $a = 3q+2$. В первом случае первый множитель числа A делится на 3, во втором — 3-й множитель, так как $2a+1 = 2(3q+1) + 1 = 6q+3$, а в третьем — 2-ой множитель делится на 3.

Вариант 2. Представим число A в виде суммы слагаемых, каждое из которых делится на 6, а именно,

$$A = a(a+1)[(a+2)+(a-1)] = a(a+1)(a+2)+(a-1)a(a+1);$$

оба слагаемые делятся на 3!, как произведения трех последовательных чисел. ⊠

Пример 1.9.3. Докажите, что для любого натурального числа n произведение $(n+1)(n+2)\dots(n+n)$ делится на 2^n.

□. Действительно, при $n=1$ утверждение истинно. Предположим, что оно истинно при $n=k$, т.е. $(k+1)(k+2)\dots(k+k)\vdots 2^k$. Докажем его истинность и для $n=k+1$.

$F=[(k+1)+1][(k+1)+2]\dots[(k+1)+(k-1)][(k+1)+k][(k+1)+(k+1)] = (k+2)(k+3)\dots(k+k)(2k+1)2(k+1) = [(k+1)(k+2)\dots(k+k)]2(2k+1)$.

По предположению индукции число, стоящее в квадратной скобке, делится на 2^k, а тогда число A делится на 2^{k+1}. Следовательно, утверждение истинно для любого натурального n. ⊠

При решении задач типа: «Доказать, что n указанного вида не может быть точным квадратом» рекомендуем руководствоваться следующими соображениями:

1) равные числа имеют равные остатки при делении на данное число;

2) если число A является квадратом некоторого числа и A делится на простое число p, то A делится на p^2. Следовательно, если A, делясь на p, не делится на p^2, то A не может быть точным квадратом.

Пример 1.9.4. Докажите, что если остаток от деления натурального n на 5 равен одному из чисел 2 и 3, то число n не может быть точным квадратом.

□. Предположим, что существует $x\in\mathbb{Z}$ такое, что $n=x^2$. Разделим x на 5. Возможны следующие случаи: $x=5q$, или $x=5q+1$, или $x=5q+2$, или $x=5q+3$, или $x=5q+4$, а тогда соответственно

$$x^2 = 25q^2 = 5(5q^2)+0,$$

$$x^2 = (5q+1)^2 = 5(5q^2+2q)+1,$$

$$x^2 = (5q+2)^2 = 5(5q^2+4q)+4,$$

$$x^2 = (5q+3)^2 = 5(5q^2+6q+1)+4,$$

$$x^2 = (5q+4)^2 = 5(5q^2+8q+3)+1.$$

Отсюда видим, что при делении квадратов целых чисел на 5 возможны остатки 0, 1 и 4. Следовательно, натуральные числа вида $n = 5k+2$ и $n = 5k+3$ точными квадратами быть не могут. ⊠

Таблицу простых чисел, не превышающих заданного натурального числа n, можно составить следующим образом. Выпишем все натуральные числа от 2 до n

$$2,\ 3,\ 4,\ 5,\ 6, \ldots, n \tag{1.32}$$

Далее вычеркнем в последовательности (1.32) все числа, кратные 2. Первое, невычеркнутое число 3 является простым. Это число оставляем и затем вычеркиваем все числа, кратные 3. Первым, не вычеркнутым, числом после этого будет 5, которое является простым. Его оставляем и далее вычеркиваем все числа, кратные 5, и т.д. Наконец, вычеркнув, таким образом, все числа, кратные простым числам, не превышающим $\sqrt{n}$, выделим, тем самым, все простые числа на отрезке от 1 до n.

Данный метод выделения простых чисел называется *решетом Эратосфена* по имени древнегреческого математика, впервые использовавшего его.

Пример 1.9.5. Найдите все простые числа между 100 и 110.

□. Так как $\sqrt{109} \approx 10$, то наименьший простой делитель указанных чисел ≤ 7. Выпишем указанные числа и подчеркнем кратные 2, 3, 5 и 7: 101, <u>102</u>, 103, <u>104</u>, <u>105</u>, <u>106</u>, 107, <u>108</u>, 109. Так как $101 = 7 \cdot 14 + 3$, то наименьшее кратное семи число — четвертое от 101, т.е. 105; оно уже подчеркнуто, а следующее кратное семи число больше 109 (седьмое от 105). Следовательно, среди указанных чисел кратных 7 нет.

Ответ: 101, 103, 107 и 109. ⊠

1.10. Кольцо гауссовых чисел. Норма гауссова числа. Обратимые и союзные элементы.

Определение 1.10.1. Множество чисел вида $a+bi$, где $a, b \in \mathbb{Z}, i^2 = -1$ называется *множеством целых комплексных чисел или множеством гауссовых чисел.*

Нетрудно проверить, что для этого множества выполняются аксиомы кольца. Обозначим кольцо гауссовых чисел через $\mathbb{Z}[i]$, так как оно является расширением кольца $\mathbb{Z}$ элементом i.

Поскольку кольцо гауссовых чисел является подмножеством комплексных чисел, то для него справедливы некоторые определения и свойства комплексных чисел. Так, например, каждому гауссовому числу $a + bi$ соответствует вектор с началом в точке $(0, 0)$ и с концом в точке (a, b). Следовательно, *модуль* гауссова числа $a + bi$ есть $\sqrt{a^2 + b^2}$. Заметим, что в рассматриваемом множестве, подмодульное выражение всегда есть целое неотрицательное число. Поэтому в некоторых случаях удобнее пользоваться *нормой*, то есть квадратом модуля. Таким образом, $N(a + bi) = a^2 + b^2$.

Лемма 1.10.1. (свойства нормы гауссовых чисел). Для любых гауссовых чисел z, z_1, z_2 справедливо:

1) $N(z) \in \mathbb{N} \cup \{0\}$;
2) $N(z) = z \cdot \overline{z}$;
3) $N(z_1 \cdot z_2) = N(z_1) \cdot N(z_2)$; $\quad N\left(\dfrac{z_1}{z_2}\right) = \dfrac{N(z_1)}{N(z_2)}$, $z_2 \neq 0$;
4) $N(z) = 1 \Leftrightarrow z \in \{\pm 1, \pm i\}$;
5) $N(z) = 0 \Leftrightarrow z = 0$.

Здесь $\overline{z}$ — сопряженное число к z.

□. *Докажите самостоятельно.* ⊠

Очевидно, что $1 = 1 \cdot 1 = i \cdot (-i) = (-1)(-1) = (-i)i$. Других способов разложить 1 в произведение двух гауссовых чисел нет.

Обратимыми элементами кольца $\mathbb{Z}[i]$ (делителями единицы) являются те элементы, у которых норма равна 1, т.е. $\{\pm 1, \pm i\}$.

Определение 1.10.2. Два гауссовых числа называются *союзными*, если одно получается из другого умножением на делитель единицы.

Данное в параграфе 1.1 определение делимости целых чисел естественным образом распространяется на понятие делимости гауссовых чисел.

Лемма 1.10.2. Для любых гауссовых чисел $z \neq 0, z_1, z_2, z_3$, а также обратимых гауссовых чисел $\varepsilon_1, \varepsilon_2$ справедливы следующие свойства:

1) $N(z) \vdots z$;
2) $z_1 \vdots z_2 \Leftrightarrow \overline{z_1} \vdots \overline{z_2}$;
3) $z_1 \vdots z_2 \Leftrightarrow \varepsilon_1 z_1 \vdots \varepsilon_2 z_2$;
4) $z_1 \vdots z_2 \Leftrightarrow z_1 z \vdots z_2 z$;
5) $z_1 \vdots z_2 \wedge z_2 \vdots z_1 \Rightarrow z_1 = \varepsilon z_2$, где $\varepsilon \in \{\pm 1, \pm i\}$;
6) $z_1 \vdots z_2 \wedge z_2 \vdots z_3 \Rightarrow z_1 \vdots z_3$;
7) $z_1 \vdots z_2 \Rightarrow N(z_1) \vdots N(z_2)$;
8) $z_1 \vdots z_3 \wedge z_2 \vdots z_3 \Rightarrow (z_1 \pm z_2) \vdots z_3$.

□. *Докажите самостоятельно.* ⊠

1.11. Деление с остатком. НОД гауссовых чисел. Алгоритм Евклида.

Подобно целым числам, гауссовы числа можно делить с остатком.

Теорема 1.11.1. (о делении с остатком). Для любых гауссовых чисел α и $\beta \neq 0$ найдется гауссово число γ такое, что $N(\alpha - \beta\gamma) < N(\beta)$. В качестве γ можно взять ближайшее к комплексному числу α/β гауссово число.

□. Разделим α на β в поле комплексных чисел. Пусть $\dfrac{\alpha}{\beta} = a + bi$, $a, b \in \mathbb{R}$. Округлим действительные числа a и b до целых, получим соответственно x и y. Положим $\gamma = x + iy$. Тогда

$$N(\frac{\alpha}{\beta} - \gamma) = (a - x)^2 + (b - y)^2 \leq 0,5^2 + 0,5^2 = 0,5 < 1.$$

Умножая сейчас обе части неравенства на $N(\beta) > 0$, получим $N(\alpha - \beta\gamma) < N(\beta)$. Таким образом, в качестве неполного частного можно взять гауссово число γ, которое является ближайшим к $\dfrac{\alpha}{\beta}$. ⊠

Пример 1.11.1. Вычислите $(-2 + 3i)(2 - i) + \dfrac{3 + i}{1 - i}$.

□. Найдем сначала произведение чисел $-2+3i$ и $2-i$:

$$(-2+3i)(2-i) = -4+2i+6i-3i^2 = -1+8i.$$

Для нахождения частного $\dfrac{3+i}{1-i}$ умножим числитель и знаменатель на число $1+i$, сопряженное знаменателю:

$$\frac{3+i}{1-i} = \frac{(3+i)(1+i)}{(1-i)(1+i)} = \frac{3+3i+i+i^2}{1-i^2} = \frac{2+4i}{2} = 1+2i.$$

Наконец, найдем сумму полученных произведения и частного:

$$(-1+8i)+(1+2i) = 10i.$$

Ответ: $10i$. ⊠

Пример 1.11.2. Разделите $\alpha = 17-3i$ с остатком на $\beta = 8+5i$.

□. Прежде всего находим $\dfrac{\alpha}{\beta}$:

$$\frac{\alpha}{\beta} = \frac{17-3i}{8+5i} = \frac{(17-3i)(8-5i)}{89} = \frac{121}{89} - \frac{109}{89}i.$$

Ближайшим целым числом к числу $\dfrac{121}{89}$ будет, очевидно, 1. Ближайшим целым числом к числу $-\dfrac{109}{89}$ будет, очевидно, -1. Таким образом, $\gamma = 1-i$ и $\rho = (17-3i)-(8+5i)(1-i) = 4$. Очевидно, что $N(\rho) = 16$ и $N(\rho) < N(8+5i) = 89$. Поэтому $17-3i = (8+5i)(1-i)+4$.
Ответ: $17-3i = (8+5i)(1-i)+4$.

⊠

Определение 1.11.1. *Наибольшим общим делителем (НОД) двух гауссовых чисел α, β* называется такой их общий делитель, который делится на любой другой их общий делитель.

Как и во множестве целых чисел, во множестве гауссовых чисел для нахождения НОД используют алгоритм Евклида.

Пусть α и β данные гауссовы числа, причем $\beta \neq 0$. Разделим с остатком α на β. Если остаток будет отличен от 0, то разделим β на этот остаток, и будем продолжать последовательное деление остатков до тех пор, пока деление будет возможно. Получим цепочку равенств:

$$\alpha = \beta \cdot \gamma_1 + r_1, \text{ где } N(r_1) < N(\beta);$$
$$\beta = r_1 \cdot \gamma_2 + r_2, \text{ где } N(r_2) < N(r_1);$$
$$r_1 = r_2 \cdot \gamma_3 + r_3, \text{ где } N(r_3) < N(r_2);$$
$$\dots\dots\dots\dots\dots$$
$$r_{k-2} = r_{k-1} \cdot \gamma_k + r_k, \text{ где } N(r_k) < N(r_{k-1});$$
$$r_{k-1} = r_k \cdot \gamma_{k+1}.$$

Эта цепочка не может продолжаться бесконечно, так как имеем убывающую последовательность норм, а нормы — неотрицательные целые числа.

Теорема 1.11.2. (о существовании НОД). Наибольший общий делитель двух гауссовых чисел α и $\beta \neq 0$ равен последнему ненулевому остатку в алгоритме Евклида для этих чисел.

□. Докажем, что в алгоритме Евклида действительно получаем НОД.

Рассмотрим равенства снизу вверх. Из последнего равенства видно, что $r_{k-1} \vdots r_k$. Следовательно, $r_{k-2} \vdots r_k$ как сумма чисел делящихся на r_k. Так как $r_{k-1} \vdots r_k$ и $r_{k-2} \vdots r_k$, то $r_{k-3} \vdots r_k$. И так далее. Таким образом, $\alpha \vdots r_k$ и $\beta \vdots r_k$. Значит, r_k — общий делитель чисел α и β.

Покажем, что r_k — наибольший общий делитель, то есть r_k делится на любой другой их общий делитель.

Рассмотрим равенства сверху вниз. Пусть δ — произвольный общий делитель чисел α и β. Тогда $r_1 \vdots \delta$, как разность чисел делящихся на δ, $(r_1 = \alpha - \beta \cdot \gamma_1)$. Из второго равенства получим, что $r_2 \vdots \delta$. Таким образом, представляя в каждом равенстве остаток, как разность чисел делящихся на δ, мы из предпоследнего равенства получим, что r_k делится на δ . ⊠

Пример 1.11.3. Найдите наибольший общий делитель чисел: $\alpha = 96 - 38i$ и $\beta = 31 + 77i$.

□. $\dfrac{\alpha}{\beta} = \dfrac{96 - 38i}{31 + 77i} = \dfrac{5}{689} - \dfrac{857}{689}i$; $\gamma_1 = 0 + (-1)i = -i$;
$r_1 = \alpha - \gamma_1\beta = 96 - 38i + i(31 + 77i) = 19 - 7i$;
$\dfrac{\beta}{r_1} = \dfrac{31 + 77i}{19 - 7i} = \dfrac{5}{41} + \dfrac{166}{41}i$; $\gamma_2 = 0 + 4i = 4i$;
$r_2 = \beta - \gamma_2 r_1 = 31 + 77i - (19 - 7i)4i = 3 + i$;
$\dfrac{r_1}{r_2} = \dfrac{19 - 7i}{3 + i} = 5 - 4i$ — гауссово число.

Следовательно, $3+i$ — наибольший общий делитель чисел α и β.
Ответ: $3+i$. ⊠

Лемма 1.11.1. (о представлении НОД). Если НОД $(\alpha, \beta) = \sigma$, то существуют такие гауссовы числа φ и ψ, что $\sigma = \alpha \cdot \varphi + \beta \cdot \psi$.

□. Рассмотрим снизу вверх цепочку равенств, полученную в алгоритме Евклида. Последовательно подставляя вместо остатков их выражения через предыдущие остатки, мы выразим r_k через α и β. ⊠

1.12. Простые гауссовы числа.

Все гауссовы числа делятся на делители единицы, поэтому любое гауссово число, отличное от делителей единицы, имеет как минимум 8 делителей: 4 делителя единицы и 4 союзных с самим числом. Эти делители называются *тривиальными*.

Определение 1.12.1. *Простое гауссово число* — это гауссово число, не имеющее других делителей, кроме тривиальных.

При этом делители единицы, подобно натуральной единице, не считаются ни простыми, ни составными гауссовыми числами.

Лемма 1.12.1. (свойства простых гауссовых чисел). 1. Пусть z — простое гауссово число и ε — обратимое гауссово число, то εz — простое гауссово число.

2. Пусть p — необратимый делитель с наименьшей нормой некоторого гауссова числа. Тогда p — простое гауссово число.

3. Гауссово число, сопряженное к простому гауссовому числу, само является простым гауссовым.

4. Если произведение двух или нескольких множителей делится на простое гауссово число p, то хотя бы один из множителей делится на p.

5. Каждое простое гауссово число является делителем только одного простого числа.

□. 1. *Докажите самостоятельно.*

2. Предположим, что p является составным числом. Тогда $p = xy$, где x и y — необратимые гауссовы числа. По свойству 3 леммы 1.10.1 получим, что $N(p) = N(x)N(y)$. Так как эти нормы натуральны, то $N(x) < N(p)$, а в силу свойства 6 леммы 1.10.2, x является необратимым делителем данного гауссова числа, что противоречит выбору p.

3. Пусть $a+bi$ — простое гауссово число. Предположим, что $a-bi$ составное, т.е. $a-bi = z_1 z_2$. Тогда $\overline{a-bi} = \overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2} = a+bi$. Противоречие.

4. Для доказательства достаточно рассмотреть случай, когда произведение содержит только два множителя α и β. Покажем, что если $\alpha\beta$ делится на p, то либо α делится на p, либо β делится на p.

Пусть α не делится на p. Тогда НОД $(\alpha, p) = 1$. Следовательно, существуют такие гауссовы числа φ и ψ, что $\alpha \cdot \varphi + p \cdot \psi = 1$. Умножим обе части равенства на β, получим, что $\alpha\beta \cdot \varphi + p \cdot \psi\beta = \beta$, отсюда следует, что $\beta \vdots p$.

5. Пусть z — простое гауссово число. Тогда $N(z) \vdots z$ по свойству 1 леммы 1.10.2. По основной теореме арифметики $N(z)$ раскладывается в произведение простых чисел. По п. 4 хотя бы один из них делится на z.

Покажем сейчас, что простое гауссово число не может делить два различных простых числа. Действительно, пусть p_1 и p_2 различные простые числа, делящиеся на z. Поскольку НОД$(p_1, p_2) = 1$, то по теореме 1.3.1 существуют целые α и β такие, что $\alpha p_1 + \beta p_2 = 1$. Отсюда $1 \vdots z$, что противоречит простоте z. ⊠

Теорема 1.12.1. (аналог основной теоремы арифметики). Каждое гауссово число, не являющееся нулём или делителем единицы, можно представить в виде произведения простых гауссовых чисел, причем это представление однозначно с точностью до союзности и порядка следования множителей.

Теорема 1.12.2. 1. Простые числа вида $4k+3$, $k \in \mathbb{Z}$ являются простыми гауссовыми числами.

2) Гауссово число, норма которого есть простое число, является простым гауссовым числом.

□. 1. Предположим, что простое число p вида $4k+3$ не является простым гауссовым числом. Тогда $p = xy$, причем $N(x) > 1$ и $N(y) > 1$. Перейдем к нормам: $p^2 = N(x)N(y)$. Учитывая указанные неравенства, получим $p = N(x) = N(y)$, т.е. p — сумма квадратов двух целых чисел. Но сумма квадратов двух целых чисел не может давать остаток 3 при делении на 4. Противоречие.

2. Пусть $a+bi$ — составное гауссово число, норма которого есть простое число. Тогда $a+bi = (c+di)(x+iy)$. Рассмотрим нормы

$N(a+bi) = N((c+di)(x+iy)) = N(c+di)N(x+yi) = (c^2+d^2)(x^2+y^2)$.

Противоречие с тем, что норма $N(a+bi)$ — простое число. ⊠

Лемма 1.12.2. Для простого числа p вида $4k+1$, $k \in \mathbb{Z}$ существует целое m такое, что $(m^2+1) \vdots p$.

Теорема 1.12.3. Простые числа вида $4k+1$, $k \in \mathbb{Z}$ раскладываются в произведение двух простых сопряженных гауссовых чисел.

□. Пусть p — простое натуральное число вида $4k+1$. Тогда по лемме 1.12.2 существует целое число m такое, что $(m^2+1) \vdots p$. Пусть p — простое гауссово число. Так как $(m+i)(m-i) \vdots p$, то по свойству 4 леммы 1.12.1 на p делится хотя бы один из множителей. Пусть $(m+i) \vdots p$. Тогда существует гауссово число $x+yi$ такое, что $m+i = p(x+yi)$. Приравнивая коэффициенты мнимых частей, получим $py = 1$. Следовательно, $p = 1$. Противоречие. Значит p — составное гауссово число. Так как $N(p) = p^2$, то по теореме 1.12.1 p представимо в виде произведения двух простых сопряженных гауссовых чисел. ⊠

1.13. Диофантовы уравнения

Определение 1.13.1. *Линейным диофантовым уравнением с двумя неизвестными x, y* называется уравнение вида

$$ac + by = c, \text{ где } a, b, c \in \mathbb{Z}, \quad \text{НОД}(a, b, c) = 1, \tag{1.33}$$

т.е. уравнение (1.33) несократимо.

Определение 1.13.2. Решением уравнения (1.33) называется пара целых чисел, удовлетворяющих уравнению (1.33).

Теорема 1.13.1. (критерий разрешимости уравнения (1.33) в целых числах). Уравнение (1.33) разрешимо в целых числах тогда и только тогда, когда $\text{НОД}(a, b) = 1$, т.е. a и b взаимно просты.

□. **Необходимость.** Пусть $\text{НОД}(a, b) = d$, $d \in \mathbb{N}$. Тогда по определению НОДа двух целых чисел $a \vdots d$ и $b \vdots d$. По условию теоремы уравнение (1.33) разрешимо в целых числах, т.е. существует хотя бы одна пара целых чисел $(x_0,\ y_0)$ такая, что верно равенство $ax_0 + by_0 = c$. Так как $a \vdots d$ и $b \vdots d$, то $d = \text{ОД}(a, b, c)$. По условию $\text{НОД}(a, b, c) = 1$ и по свойству

наибольшего общего делителя НОД(a, b, c) делится на любой ОД этих чисел. Поэтому $1/d$ и $d = 1$.

Достаточность. Так как НОД$(a, b) = 1$, то по свойству линейности наибольшего общего делителя 1 представима в виде целочисленной линейной комбинации чисел a и b, т.е. существуют $x_1, y_1 \in \mathbb{Z}$ такие, что $ax_1 + by_1 = 1$.

Умножив это равенство на c, получим $(ax_1)c + (by_1)c = c$ и, так как умножение на $\mathbb{Z}$ ассоциативно, то $a(x_1c) + b(y_1c) = c$, где $x_1c \in \mathbb{Z}$, $y_1c \in \mathbb{Z}$. Обозначим $x_1c = x_0$, $y_1c = y_0$.

Отсюда $ax_0 + by_0 = c$, т.е. существует пара чисел (x_0, y_0), являющаяся решением уравнения (1.33). Мы доказали существование целочисленного решения уравнения (1.33). Возникает вопрос: сколько решений может иметь уравнение (1.33), если оно разрешимо. Рассмотрим следующие случаи:

1) При $c = 0$ уравнение (1.33) примет вид $ax + by = 0$. Учитывая, что НОД$(a, b) = 1$, то хотя бы один из коэффициентов a и b не равен нулю. Пусть для определенности $b \neq 0$, тогда $y = -\dfrac{ax}{b} \in \mathbb{Z}$. Следовательно, $ax \vdots b$. Так как НОД$(a, b) = 1$, то $x \vdots b$, поэтому $x = bt$, где $t \in \mathbb{Z}$. Тогда $y = -at$, $t \in \mathbb{Z}$. Пара $(bt, -at)$ является общим решением уравнения (1.33), где $t \in \mathbb{Z}$.

$\{(bt, -at) \mid t \in \mathbb{Z}\}$ — бесконечное множество всех решений уравнения (1.33).

2) Пусть $c \neq 0$. Обозначим через $(x_0, y_0) \in \mathbb{Z}^2$ частное решение уравнения (1.33), т.е. верно равенство

$$ax_0 + by_0 = c. \tag{1.34}$$

Пусть $(x, y) \in \mathbb{Z}^2$ — произвольное решение (общее решение) уравнения (1.33), тогда верно

$$ax + by = c. \tag{1.35}$$

Вычитая (1.34) из (1.35), получим верное равенство $a(x-x_0)+b(y-$ $- y_0) = 0$. В силу п.1 верно $x = x_0 + bt$, $y = y_0 - at$, $t \in \mathbb{Z}$.

Пара $(x_0 + bt, y_0 - at)$, $t \in \mathbb{Z}$ — общее решение уравнения (1.33) при $c = 0$.

$\{(x_0 + bt, y_0 - at) \mid t \in \mathbb{Z}\}$ — бесконечное множество всех решений уравнения (1.33) при $c \neq 0$. Заметим, что пара $(bt,\ -at)$, принадлежащая данному множеству при $x_0 = 0$, $y_0 = 0$ является частным решением уравнения (1.33) при $c = 0$.

Таким образом, $(x_0 + bt, y_0 - at)$, $t \in \mathbb{Z}$ — общее решение уравнения (1.33) для любого c. Очевидно, что для нахождения всех решений уравнения 1.33 достаточно найти частное решение $(x_0, y_0) \in \mathbb{Z}^2$. Учитывая, что $t \in \mathbb{Z}$, общее решение можно записать и так $(x_0 - bt, y_0 + at)$. ⊠

Известно несколько способов нахождения частного решения $(x_0,\ y_0)$. Рассмотрим нахождение частного решения уравнения (1.33) с помощью алгоритма Евклида. Так как НОД$(a, b) = 1$, то с помощью алгоритма Евклида выразим 1 через модули коэффициентов a и b, а затем через a и b. Имеем $ax_1 + by_1 = 1$, $x_1, y_1 \in \mathbb{Z}$. Умножив данное равенство на c, получим $a(x_1c) + b(y_1c) = c$, следовательно, частное решение (x_0, y_0) примет вид $x_0 = x_1c$, $y_0 = y_1c$, т.е. $(x_0, y_0) \in \mathbb{Z}^2$.

Пример 1.13.1. Решите уравнение

$$12x - 45y = 6, \tag{1.36}$$

□. Так как НОД$(12, -45, 6) = 3$, то уравнение (1.36) не является диофантовым. Сократив данное уравнение на 3, получим

$$4x - 15y = 2,\ \text{НОД}(4, -15, 2) = 1 \tag{1.37}$$

Поскольку НОД$(4, -15) = 1$, то уравнение (1.37) разрешимо в целых числах. С помощью алгоритма Евклида выразим 1 линейно через числа 4 и -15. $15 = 4 \cdot 3 + 3,\ 4 = 3 \cdot 1 + 1,\ 3 = 1 \cdot 3$. Отсюда $1 = 4 - 3 \cdot 1 = 4 - (15 - 4 \cdot 3) \cdot 1 = 4 - 15 \cdot 1 + 4 \cdot 3 \cdot 1 = 4 \cdot 4 - 15 \cdot 1$, т.е. $4 \cdot 4 - 15 \cdot 1 = 1$. Умножив последнее равенство на 2, получим $4 \cdot 8 - 15 \cdot 2 = 2$. Отсюда $(x_0, y_0) = (8, 2)$ — частное решение уравнения (1.37).

Таким образом, $(8 + 15t, 2 - 4t), t \in \mathbb{Z}$ — общее решение уравнения (1.37).

Ответ: $\{(8 + 15t,\ 2 - 4t) \mid t \in \mathbb{Z}\}$. ⊠

Пример 1.13.2. Решите уравнение $14x + 18y = 9$.

□. Так как НОД$(14, 18, 9) = 1$, то данное уравнение диофантово. Проверим его на разрешимость. Поскольку НОД$(14, 18) = 2$, то по критерию

уравнение не разрешимо в целых числах.
Ответ: уравнение не разрешимо в целых числах. ⊠

Методом математической индукции можно показать, что уравнение $a_1x_1 + \ldots + a_nx_n = b$, где $a_1, \ldots, a_n, b \in \mathbb{Z}$, $a_1 \neq 0, \ldots, a_n \neq 0$, разрешимо в целых числах тогда и только тогда, когда наибольший общий делитель чисел $a_1, \ldots, a_n$ делит b.

Пример 1.13.3. Решите уравнение $6x + 10y + 15z = 7$ в целых числах.

□. Имеем $(6x + 10y) + 15z = 7$, $2(3x + 5y) + 15z = 7$. Пусть $3x + 5y = w$, тогда

$$2w + 15z = 7 \tag{1.38}$$

Решим уравнение (1.38) в целых числах.

Так как НОД$(15, 2) = 1$, то согласно алгоритму Евклида $1 = 2 \cdot (-7) + 15 \cdot 1$. Следовательно, $2 \cdot (-49) + 15 \cdot 7 = 7$, т.е. $(-49, 7)$ является частным решением уравнения (1.38). Находим $w = -49 + 15u$, $z = 7 - 2u$, где $u \in \mathbb{Z}$. Имеем $3x + 5y = -49 + 15u$. Так как НОД$(5, 3) = 1$, то согласно алгоритму Евклида $1 = 2 \cdot 3 + 5(-1)$. Значит, $3(30u - 98) + 5(49 - 15u) = -49 + 15u$, т.е. для каждого $u \in \mathbb{Z}$ пара чисел $(30u - 98, 49 - 15u)$ является частным решением уравнения $3x + 5y = -49 + 15u$. Поэтому $x = (30u - 98) + 5v$, $y = (49 - 15u) - 3v$, где $v \in \mathbb{Z}$.
Ответ: $\{(30u - 98 + 5v,\ 49 - 15u - 3v,\ 7 - 2u) \mid u, v \in \mathbb{Z}\}$. ⊠

Пример 1.13.4. Решите в целых числах

$$29x + 13y + 56z = 17. \tag{1.39}$$

□. Выразим неизвестное, коэффициент при котором наименьший, через остальные неизвестные.

$$y = \frac{(17 - 29x - 56z)}{13} = (1 - 2x - 4z) + \frac{(4 - 3x - 4z)}{13}. \tag{1.40}$$

Обозначим

$$\frac{(4 - 3x - 4z)}{13} = t_1. \tag{1.41}$$

Из (1.40) следует, что t_1 может принимать только целые значения.
Из (1.41) имеем

$$13t_1 + 3x + 4z = 14. \tag{1.42}$$

Получим новое диофантово уравнение, но с меньшими, чем в (1.39) коэффициентами. Применив к (1.42) те же соображения, получим:

$$x = \frac{(4 - 13t_1 - 4z)}{13} = (1 - 4t_1 - z) + \frac{1 - t_1 - z}{3}.$$

Обозначим

$$\frac{(1 - t_1 - z)}{3} = t_2, \quad t_2 \in \mathbb{Z}. \tag{1.43}$$

Из (1.43) имеем

$$3t_2 + t_1 + z = 1. \tag{1.44}$$

В (1.44) коэффициент при z равен 1 — это конечный пункт "спуска". Теперь последовательного выражаем z, x, y через t_1 и t_2. Получим

$$z = -t_1 - 3t_2 + 1,$$

$$x = 1 - 4t_1 + t_1 + 3t_2 - 1 + t_2 = -3t_1 + 4t_2,$$

$$y = 1 + 6t_1 - 8t_2 + 4t_1 + 12t_2 - 4 + t_1 = 11t_1 + 4t_2 - 3.$$

Ответ: $\{(-3t_1 + 4t_2,\ 11t_1 + 4t_2 - 3,\ -t_1 - 3t_2 + 1) \mid t_1, t_2 \in \mathbb{Z}\}$.

⊠

Пример 1.13.5. Имеются контейнеры массой 130 и 160 кг. Нужно полностью загрузить ими грузовик грузоподъемностью 3 т. Как это можно сделать?

□. Обозначим количество контейнеров массой 130 кг и 160 кг соответственно через x и y, где $x \geq 0$, $y \geq 0$. Получим уравнение

$$130x + 160y = 3000, \tag{1.45}$$

которое не является диофантовым, так как НОД$(130, 160, 3000) = 10$. Сократим уравнение (1.45) на 10

$$13x + 16y = 300. \tag{1.46}$$

Уравнение (1.46) является диофантовым, так как НОД$(13, 16, 300) = 1$ и разрешимо в целых числах, так как НОД$(13, 16) = 1$. Составим алгоритм Евклида для чисел 13 и 16.

$16 = 13 \cdot 1 + 3, 13 = 3 \cdot 4 + 1, 3 = 1 \cdot 3$. Тогда $1 = 13 - 3 \cdot 4 = 13 - (16 - 13 \cdot 1) \cdot 4 = 13 \cdot 5 + 16 \cdot (-4)$. Умножив обе части равенства $13 \cdot 5 + 16 \cdot (-4) = 1$ на 300, получим $13 \cdot 1500 + 16 \cdot (-1200) = 300$. Отсюда $(x_0, y_0) = (1500, -1200)$ — частное решение уравнения (1.46).

Таким образом, $(x, y) = (1500 - 16t, -1200 + 13t)$, $t \in \mathbb{Z}$ — общее решение уравнения (1.46). Так как $x \geq 0$, $y \geq 0$, то $1500 - 16t \geq 0$ и $-1200 + 13t \geq 0$, $t \in \mathbb{Z}$. Решая неравенства, получим $92, 3 \leq t \leq 93, 8$, $t \in \mathbb{Z}$.

Следовательно, $t = 93$. Таким образом, имеем единственное решение $x = 1500 - 16 \cdot 93 = 12$ и $y = -1200 + 13 \cdot 93 = 9$.

Ответ: 9 контейнеров по 130 кг, 12 контейнеров по 160 кг. ⊠

1.14. Числовые функции. Мультипликативные функции. Совершенные числа. Функция Эйлера

В теории чисел рассматриваются разнообразные функции $f(n)$, значения которых при натуральных значениях n связаны с арифметической природой n. Множество рассматриваемых функций удобнее не ограничивать заранее какими-либо требованиями, кроме единственного требования: каждая функция должна быть определена для всех натуральных значений аргумента.

Определение 1.14.1. Функция $f(x)$ называется *числовой*, если она определена при всех натуральных значениях аргумента x.

Согласно этому определению значительная часть функций, рассматриваемых в математическом анализе, таких, как, например, e^x, $\sin x$, $\arctan x$, $\log_a x$, — числовые функции.

Обычно в теории чисел рассматривают числовые функции, которые либо вообще определены только при натуральных значениях аргумента, либо функции, для которых натуральные значения аргумента являются характерными точками, определяющими величину функции и в других точках. В качестве примера таких числовых функций могут служить функция Эйлера $\varphi(n)$, функция $[x]$. Функция Эйлера вообще определена только при натуральных значениях аргумента, а у функции $[x]$ все значения определяются ее значениями при целых x.

Рассмотрим сначала числовые функции $\tau(n)$ и $\sigma(n)$, зависящие от делителей аргумента. Функция $\tau(n)$ определяется как *число положи-*

тельных делителей натурального числа n, а функция $\sigma(n)$ определяется как *сумма положительных делителей натурального числа* n, т.е.

$$\tau(n) = \sum_{d|n} 1, \sigma(n) = \sum_{d|n} d. \tag{1.47}$$

Пример 1.14.1. $\tau(1) = 1$, $\tau(18) = 6$, так как у числа 18 шесть положительных делителей: 1, 2, 3, 6, 9 и 18. Если p простое, то $\tau(p) = 2$.

$$\sigma(18) = 1 + 2 = 3 + 6 + 9 + 18 = 39; \sigma(p) = 1 + p.$$

Теорема 1.14.1. Если $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$ — каноническое разложение натурального числа n, то

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_s + 1). \tag{1.48}$$

$\square$. Любой положительный делитель числа $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$ имеет вид $p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_s^{\beta_s}$, где $0 \leq \beta_1 \leq \alpha_1$, $0 \leq \beta_2 \leq \alpha_2$, ..., $0 \leq \beta_s \leq \alpha_s$, и, таким образом, число положительных делителей n равно числу кортежей $(\beta_1, \beta_2, \ldots, \beta_s)$, где β_1 принимает α_1+1 значений от 0 до α_1, β_2 принимает $\alpha_2 + 1$ значений от 0 до α_2, ..., β_s принимает $\alpha_s + 1$ значений от 0 до α_s. Согласно основному правилу произведения число таких кортежей равно

$$(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_s + 1), \text{ т.е.}$$

$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_s + 1)$. $\boxtimes$

Пример 1.14.2. $\tau(1000000) = \tau(2^6 \cdot 5^6) = 7 \cdot 7 = 49$, $\tau(48510) = \tau(2 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 11) = 2 \cdot 3 \cdot 2 \cdot 3 \cdot 2 = 72$.

Теорема 1.14.2. Если $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$ — каноническое разложение натурального числа n, то

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_s^{\alpha_s+1} - 1}{p_s - 1}. \tag{1.49}$$

$\square$.

$$\sigma(n) = \sum_{d|p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}} d = \sum_{\substack{0 \leq \beta_1 \leq \alpha_1 \\ \ldots\ldots \\ 0 \leq \beta_s \leq \alpha_s}} p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_s^{\beta_s} =$$

$$= (1 + p_1 + p_1^2 + \ldots + p_1^{\alpha_1}) \ldots (1 + p_s + p_s^2 + \ldots + p_s^{\alpha_s}). \tag{1.50}$$

Действительно, перемножая числа, стоящие в скобках, в правой части, мы получаем слагаемые вида $p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_s^{\beta_s}$, где β_1 принимает значения от 0 до α_1, β_2 — от 0 до α_2, ..., β_s — от 0 до α_s, причем каждое такое слагаемое суммы в левой части (1.50) получится один и только один раз. Чтобы получить формулу (1.49), остается только воспользоваться формулой суммы геометрической прогрессии

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

⊠

Пример 1.14.3. $\sigma(19800) = \sigma(2^3 \cdot 3^2 \cdot 5^2 \cdot 11) = \frac{2^4-1}{2-1} \cdot \frac{3^3-1}{3-1} \cdot \frac{5^3-1}{5-1} \cdot \frac{11^2-1}{11-1} =$
$= 72540.$

Определение 1.14.2. Числовая функция f называется *мультипликативной*, если $f(nm) = f(n)f(m)$ для всех взаимно простых натуральных чисел n и m.

Лемма 1.14.1. Если f — мультипликативная ненулевая функция, то $f(1) = 1$.

□. Так как f — ненулевая, то существует $n \in \mathbb{N}$ такое, что $f(n) = y \neq 0$. Теперь $y = f(n) = f(1 \cdot n) = f(1)f(n) = f(1)y$ и $f(1) = 1$. ⊠

Лемма 1.14.2. Если f — мультипликативная функция и $p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ — каноническое разложение натурального числа n, то

$$f(n) = f(p_1^{\alpha_1}) \cdot f(p_2^{\alpha_2}) \cdot \ldots \cdot f(p_k^{\alpha_k}).$$

□. Утверждение вытекает из определения мультипликативной функции. ⊠

Лемма 1.14.3. Если f — мультипликативная функция и $g(n) = \prod\limits_{d|n} f(d)$, то g — мультипликативная функция.

□. Если n и m — натуральные числа и НОД$(n, m) = 1$, то $g(mn) =$
$= \prod\limits_{d|mn} f(d) = \prod\limits_{d|m} f(d) \prod\limits_{d'|n} f(d') = g(m)g(n).$ ⊠

Теорема 1.14.3. Функции $\tau(n)$ и $\sigma(n)$ — мультипликативные функции.

$\square$. Если $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$ и $b = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_t^{\alpha_t}$ — канонические разложения взаимно простых чисел a и b (все p_i и q_j — простые числа), то $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s} \cdot q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_t^{\alpha_t}$ — каноническое разложение ab и $\tau(ab) = (\alpha_1 + 1) \cdot \ldots \cdot (\alpha_s + 1)(\beta_1 + 1) \cdot \ldots \cdot (\beta_t + 1) = \tau(a)\tau(b)$,

$$\sigma(ab) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \ldots \cdot \frac{p_s^{\alpha_s+1} - 1}{p_1 - 1} \cdot \frac{q_1^{\beta_1+1} - 1}{q_1 - 1} \cdot \ldots \cdot \frac{q_t^{\beta_t+1} - 1}{q_t - 1} = \sigma(a)\sigma(b).$$

$\boxtimes$

Пример 1.14.4. Найдите натуральное число x, если известно, что 12 делит x и $\tau(x) = 14$.

$\square$. Натуральное число x записывается в виде:

$$x = 2^\alpha 3^\beta p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k},\ \alpha \geq 2,\ \beta \geq 1,$$

$$3 < p_1 < p_2 < \ldots < p_k,\ k \geq 0.$$

По условию

$$\tau(x) = (\alpha + 1)(\beta + 1)(\alpha_1 + 1) \ldots (\alpha_k + 1) = 14 = 2 \cdot 7,$$

где $\alpha + 1 \geq 3$, $\beta + 1 \geq 2$. Это возможно лишь в случае, когда $k = 0$, $\alpha + 1 = 7$, $\beta + 1 = 2$ и $x = 2^6 \cdot 3 = 192$.
Ответ: 192. $\boxtimes$

Пример 1.14.5. Пусть $n = p^\alpha q^\beta$, где p и q — различные простые, α и β — натуральные числа. Найдите $\tau(n^3)$, если $\tau(n^2) = 81$.

$\square$. Поскольку значение $\tau(n)$ не зависит от p и q, то можно считать, что $\alpha \leq \beta$. По условию

$$\tau(n^2) = \tau(p^{2\alpha} q^{2\beta}) = (2\alpha + 1)(2\beta + 1) = 81 = 3^4.$$

Возможны только следующие случаи:

$2\alpha + 1 = 1$, $2\beta + 1 = 3^4$, откуда $\alpha = 0$, а это противоречит тому, что α — натуральное;

$2\alpha + 1 = 3$, $2\beta + 1 = 3^3$, откуда $\alpha = 1$, $\beta = 13$;

$2\alpha + 1 = 3^2$, $2\beta + 1 = 3^2$, откуда $\alpha = 4$, $\beta = 4$.

Поэтому либо

$$\tau(n^3) = \tau(p^{3\alpha}q^{3\beta}) = \tau(p^3q^{39}) = (3+1)(39+1) = 160,$$

либо

$$\tau(n^3) = \tau(p^{3\alpha}q^{3\beta}) = \tau(p^{12}q^{12}) = 13 \cdot 13 = 169.$$

Ответ: $\tau(n^3) \in \{160, 169\}$. ⊠

Сумма собственных положительных делителей натурального числа n бывает меньше, чем n ("недостаточные числа"), а бывает и больше, чем n ("избыточные числа").

Иногда встречаются числа, у которых сумма собственных положительных делителей в точности равна самому этому числу. Вместе с числом n сумма положительных делителей такого числа равна $2n$.

Определение 1.14.3. Число n называется *совершенным*, если $\sigma(n) = 2n$.

Определение 1.14.4. *Функция* $\pi(n)$ определена на множестве $\mathbb{N}$ и представляет собой количество простых чисел, не превосходящих n. Это число ещё называют *абсолютной плотностью простых чисел в интервале* $(1, n)$.

Теорема 1.14.4. (Чебышева). $a\frac{n}{\ln\ n} < \pi(n) < b\frac{n}{\ln\ n}$, где $a = 0,92129$, $b = \frac{6}{5}a$.

Для больших n справедлива интегральная формула $\pi(n) \approx \int\limits_2^n \frac{dx}{\ln\ x}$.

Определение 1.14.5. *Функция Эйлера* $\varphi(n)$ определена на множестве $\mathbb{N}$ и представляет собой число натуральных чисел, не превосходящих n и взаимно простых с ним.

Например, $\varphi(1) = \varphi(2) = 1$, $\varphi(3) = \varphi(4) = 2$ и т.д.

Теорема 1.14.5. $\varphi(p^n) = p^n(1 - \frac{1}{p}) = p^{n-1}(p-1)$

□. $1, \ldots, p, \ldots, 2p, \ldots, 3p, \ldots, pp = p^2$, $(p+1)p, \ldots, p^{n-1}p$. Ясно, что в этом ряду p^{n-1} кратных p, остальные взаимно просты с p. Поэтому $\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$. ⊠

Следствие 1.14.1. $\varphi(p) = p - 1$.

Следствие 1.14.2. Если $n = p_1^{\alpha_1} \cdot \ldots \cdot p_t^{\alpha_t}$, то

$$\varphi(n) = p_1^{\alpha_1}(1 - \frac{1}{p_1}) \cdot \ldots \cdot p_t^{\alpha_t}(1 - \frac{1}{p_t}) =$$

$$= n(1-\frac{1}{p_1})\cdot\ldots\cdot(1-\frac{1}{p_t}) = p_1^{\alpha_1-1}(p_1-1)\cdot\ldots\cdot p_t^{\alpha_t-1}(p_t-1).$$

Пример 1.14.6. $\varphi(360) = \varphi(2^3 3^2 5) = 4\cdot 3\cdot 2\cdot 4 = 96$.
Теорема 1.14.6. Функция Эйлера мультипликативна.

$\square$. Если $a = p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_s^{\alpha_s}$ и $b = q_1^{\beta_1}\cdot q_2^{\beta_2}\cdot\ldots\cdot q_t^{\alpha_t}$ — канонические разложения взаимно простых чисел a и b (все p_i и q_j — простые числа), то $p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_s^{\alpha_s}\cdot q_1^{\beta_1}\cdot q_2^{\beta_2}\cdot\ldots\cdot q_t^{\alpha_t}$ — каноническое разложение ab и $\varphi(ab) = p_1^{\alpha_1-1}(p_1-1)\cdot\ldots\cdot p_s^{\alpha_s-1}(p_s-1)\cdot q_1^{\beta_1-1}(q_1-1)\cdot\ldots\cdot q_t^{\beta_t-1}(q_t-1) =$
$= \varphi(a)\varphi(b)$ $\boxtimes$

Теорема 1.14.7.

$$\sum_{d|n}\varphi(d) = n.$$

Пример 1.14.7. Найдите все простые делители числа x из уравнения $3\varphi(x) = x$.

$\square$. По условию 3 делит x, значит $3-1=2$ делит $\varphi(x)$, а из равенства $3\varphi(x) = x$ следует, что x делится на 6. Будем считать, что

$$x = 2^\alpha 3^\beta p_1^{\alpha_1}\ldots p_k^{\alpha_k},\ 3 < p_1 < \ldots < p_k,\ k \geq 0.$$

Предположим, что $k > 0$. По условию

$$3\cdot 2^{\alpha-1}\cdot 3^{\beta-1}\cdot 2\cdot p_1^{\alpha_1-1}(p_1-1)\ldots p_k^{\alpha_k-1}(p_k-1) = 2^\alpha 3^\beta p_1^{\alpha_1}\ldots p_k^{\alpha_k},$$

поэтому $(p_1-1)\ldots(p_k-1) = p_1\ldots p_k$. Так как $p_1-1<\ldots<p_k-1<p_k$, то p_k делит $(p_1-1)\ldots(p_k-1)$, что невозможно. Поэтому допущение $k>0$ неверно. Значит, $k=0$ и $x = 2^\alpha 3^\beta$.
Ответ: 2; 3. $\boxtimes$

Пример 1.14.8. Решите уравнение $\varphi(3^x 5^y) = 40$.

$\square$. Так как $\varphi(3^x 5^y) = 3^{x-1}(3-1)5^{y-1}(5-1) = 40 = 2^3 5$, то $3^{x-1}5^{y-1} = 5$. Поэтому $x = 1$, а $y = 2$.
Ответ: $(1;2)$. $\boxtimes$

1.15. Целая и дробная часть числа

Определение 1.15.1. *Целая часть числа* $y = [x]$ — это функция с областью определения $\mathbb{R}$ и областью значения $\mathbb{Z}$, заданная следующим образом:

$$[x] = \max\{n \in \mathbb{Z} | n \leq x\}.$$

Лемма 1.15.1. Для любого $x \in \mathbb{R}$ справедливы неравенства:

$$x - 1 < [x] \leq x.$$

□. Так как $[x] = \max\{n \in \mathbb{Z} | n \leq x\}$, то $x < [x] + 1$.Поэтому $x - 1 < [x]$. Из определения ясно, что $[x] \leq x$. ⊠

Пример 1.15.1. $[\pi] = 3$. $[-\pi] = -4$. $[e] = 2$. $[-e] = -3$.

Запись $p^\alpha \top n$ означает, что p^α делит n, но $p^{\alpha+1}$ не делит n. Здесь p — простое, $\alpha \in \{0\} \cup N$, $n \in \mathbb{N}$.

Лемма 1.15.2. Пусть $x, y \in \mathbb{R}, n \in \mathbb{N}$, $a \in \mathbb{Z}$, p — простое число. Тогда справедливы следующие утверждения:

1) $[x + y] \geq [x] + [y]$;

2) $[x + n] = [x] + n$;

3) пусть x — неотрицательное число. Число натуральных чисел не превосходящих x и кратных n равно $\left[\frac{x}{n}\right]$;

4) $\left[\frac{x}{n}\right] = \left[\frac{[x]}{n}\right]$;

5) $[x] - 2\left[\frac{x}{2}\right] \in \{0, 1\}$;

6) $\left[\frac{x}{nm}\right] = \left[\frac{\left[\frac{x}{n}\right]}{m}\right] = \left[\frac{\left[\frac{x}{m}\right]}{n}\right]$.

7) если $p^\alpha \top n!$, то

$$\alpha = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots = \sum_{i=1}^{\left[\frac{\ln n}{\ln p}\right]} \left[\frac{n}{p^i}\right].$$

□. 1. Пусть

$$[x] = \max\{n \in \mathbb{Z} | n \leq x\} = n',$$

$$[y] = \max\{m \in \mathbb{Z} | m \leq x\} = m'.$$

Тогда $[x] + [y] = n' + m' \leq x + y$. Так как $[x] + [y]$ целое, то $[x + y] \geq [x] + [y]$.

2. Утверждение очевидно.

3. Пусть t — наибольшее натуральное число такое, что $tn \leq x$. Тогда

$$tn \leq x < (t+1)n,\ t \leq \frac{x}{n} < t+1.$$

Поэтому $t = \left[\frac{x}{n}\right]$. Ясно, что n, $2n$, $3n$,..., tn — все числа, кратные n и не превосходящие x. Их ровно t штук.

4. Так как $[x] \leq x$, то $\frac{[x]}{n} \leq \frac{x}{n}$ и $\left[\frac{[x]}{n}\right] \leq \left[\frac{x}{n}\right]$. С другой стороны, $[x] > x - 1$, поэтому

$$\frac{[x]}{n} > \frac{x-1}{n} = \frac{x}{n} - \frac{1}{n},$$

$$\left[\frac{[x]}{n}\right] > \left[\frac{x}{n} - \frac{1}{n}\right] \geq \left[\frac{x}{n}\right] + \left[-\frac{1}{n}\right] = \left[\frac{x}{n}\right] - 1.$$

Таким образом,

$$\left[\frac{x}{n}\right] - 1 < \left[\frac{[x]}{n}\right] \leq \left[\frac{x}{n}\right],$$

значит, $\left[\frac{[x]}{n}\right] = \left[\frac{x}{n}\right]$.

5. Так как $\frac{x}{2} - 1 < \left[\frac{x}{2}\right]$, то

$$2(\frac{x}{2} - 1) = x - 2 < 2\left[\frac{x}{2}\right],$$

поэтому $x - 2\left[\frac{x}{2}\right] < 2$. Теперь

$$[x] - 2\left[\frac{x}{2}\right] \leq x - 2\left[\frac{x}{2}\right] \leq 1.$$

С другой стороны,

$$[x] - 2\left[\frac{x}{2}\right] > x - 1 - 2\left[\frac{x}{2}\right] = -1.$$

Следовательно,

$$[x] - 2\left[\frac{x}{2}\right] \in \{0, 1\}.$$

6. Следует из свойства (4).

7. Если $p > n$, то $\alpha = 0$. Пусть $p < n$. По свойству (3) число натуральных чисел кратных p на отрезке $[1, n]$ равно $\left[\frac{n}{p}\right]$; кратных p^2 равно $\left[\frac{n}{p^2}\right]$ и т.д.

Так как $n! = 1 \cdot 2 \cdot \ldots \cdot n$, то

$$\alpha = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]. \tag{1.51}$$

Если p^t — наивысшая степень p не превосходящая n, то $p^t \leq n < p^{t+1}$. Поэтому $t \ln p \leq \ln n < (t+1) \ln p$ и $t \leq \frac{\ln n}{\ln p} < t + 1$. Значит, $t = \left[\frac{\ln n}{\ln p}\right]$.

Теперь равенство (1.51) принимает вид $\alpha = \sum\limits_{i=1}^{\left[\frac{\ln n}{\ln p}\right]} \left[\frac{n}{p^i}\right]$. ⊠

Пример 1.15.2. Найти каноническое разложение числа 100!.

□. Так как $100! = 2^{\alpha_2} 3^{\alpha_3} 5^{\alpha_5} 7^{\alpha_7} 11^{\alpha_{11}} 13^{\alpha_{13}} 17^{\alpha_{17}} \ldots 97^{\alpha_{97}}$, то

$\alpha_2 = \left[\frac{100}{2}\right] + \left[\frac{100}{2^2}\right] + \left[\frac{100}{2^3}\right] + \left[\frac{100}{2^4}\right] + \left[\frac{100}{2^5}\right] + \left[\frac{100}{2^6}\right] = 50 + 25 + 12 + 6 + 3 + 1 = 97.$

$\alpha_3 = \left[\frac{100}{3}\right] + \left[\frac{100}{9}\right] + \left[\frac{100}{27}\right] + \left[\frac{100}{81}\right] = 33 + 11 + 3 + 1 = 48,$

$\alpha_5 = \left[\frac{100}{5}\right] + \left[\frac{100}{25}\right] = 20 + 4 = 24,$

$\alpha_7 = \left[\frac{100}{7}\right] + \left[\frac{100}{49}\right] = 14 + 2 = 16,$

$\alpha_{11} = \left[\frac{100}{11}\right] = 9,\ \alpha_{13} = \left[\frac{100}{13}\right] = 7,\ \alpha_{17} = \left[\frac{100}{17}\right] = 5,$

$\alpha_{19} = \left[\frac{100}{19}\right] = 5,\ \alpha_{23} = 4,\ \alpha_{29} = \alpha_{31} = 3,$

$\alpha_{37} = \alpha_{41} = \alpha_{43} = \alpha_{47} = 2,$

$\alpha_{53} = \alpha_{59} = \alpha_{61} = \alpha_{67} = \alpha_{71} = \alpha_{73} = \alpha_{79} = \alpha_{83} = \alpha_{89} = \alpha_{97} = 1,$

Ответ: $100! = 2^{97}3^{48}5^{24}7^{16}11^{9}13^{7}17^{5}19^{5}23^{4}29^{3}31^{3}37^{2}41^{2}47^{2}53 \cdot 59 \cdot 61 \cdot 71 \cdot 73 \cdot 79 \cdot 83 \cdot 89 \cdots 97$. ⊠

Пример 1.15.3. Сколькими нулями заканчивается число 111!.

□. Нулей столько, сколько пар чисел 2 и 5 в каноническом разложении числа 111!. Так как

$$\alpha_5 = \left[\frac{111}{5}\right] + \left[\frac{100}{5^2}\right] = 22 + 4 = 26,$$

то число 111! оканчивается 26 нулями. ⊠

Пример 1.15.4. Решите уравнение $\left[\frac{x+2}{2}\right] = x - 1$.

□. Так как $\left[\frac{x+2}{2}\right]$ — целое число, то $x - 1$ — целое, а значит x — целое. Из свойств целой части следует, что

$$x - 1 \leq \frac{x+2}{2} < (x-1) + 1.$$

Решая эти неравенства, получим: $2 < x \leq 4$, $x = 3$ или $x = 4$. Теперь убеждаемся, что оба значения являются решениями.
Ответ: 3; 4. ⊠

Определение 1.15.2. *Дробной частью действительного числа* x называется число $x - [x]$. Дробная часть действительного числа x обозначается через $\{x\}$.

Таким образом, дробная часть — это функция с областью определения $\mathbb{R}$ и областью значений $[0; 1)$, которая определяется равенством: $\{x\} = x - [x]$. Например, $\{\pm 1\} = 0$, $\{-1{,}001\} = -1{,}001 - (-2) = 0{,}999$, $\{1{,}999\} = \{1{,}999\} - 1 = 0{,}999$,

$\{-\pi\} = -3{,}14\ldots - (-4) = 0{,}85\ldots$,

$\{\pi\} = 3{,}14\ldots - 3 = 0{,}14\ldots$,

$\{e\} = 0{,}71\ldots$, $\{-e\} = 0{,}28\ldots$.

Лемма 1.15.3. (свойства дробной части действительного числа.)

Пусть $x, y \in \mathbb{R}$.

1) Тогда и только тогда $\{x\} = x$, когда $0 \leq x < 1$.

2) Тогда и только тогда $\{x\} = \{y\}$, когда $x - y = k \in \mathbb{Z}$.

3) $\{x + 1\} = \{x\}$ для любого x.

Пример 1.15.5. *Решите уравнение* $\left[\frac{x-3}{4} - \left[\frac{x}{4}\right]\right] = \ln x$.
□ Поскольку $\frac{x}{4} = \left[\frac{x}{4}\right] + \left\{\frac{x}{4}\right\}$, то

$$\frac{x-3}{4} - \left[\frac{x}{4}\right] = \frac{x-3}{4} - \frac{x}{4} + \left\{\frac{x}{4}\right\} = \left\{\frac{x}{4}\right\} - \frac{3}{4}.$$

Из определения дробной части следует, что $0 \leq \left\{\frac{x}{4}\right\} < 1$. Поэтому

$$-\frac{3}{4} \leq \left\{\frac{x}{4}\right\} - \frac{3}{4} < \frac{1}{4}.$$

Так как целая часть числа, принадлежаего промежутку $[-\frac{3}{4}; \frac{1}{4})$, равна -1 или 0, то $\ln x = -1$ и $x = e^{-1}$, или $\ln x = 0$ и $x = 1$.

Сделаем проверку. Если $x = e^{-1}$, то

$$\left[\frac{e^{-1}-3}{4} - \left[\frac{e^{-1}}{4}\right]\right] = \left[\frac{1-3e}{4e} - 0\right] = -1 = \ln e^{-1} = -1,$$

т. е. $x = e^{-1}$ является решением.

Если $x = 1$, то $\left[\frac{1-3}{4} - \left[\frac{1}{4}\right]\right] = \left[-\frac{1}{2} - 0\right] = -1 \neq \ln 1 = 0$. Поэтому $x = 1$ не является решением.
Ответ: e^{-1}. ⊠

Пример 1.15.6. *Решите уравнение* $\{(x+1)^2\} = x^2$.
□ Из определения дробной части следует, что $0 \leq x^2 < 1$, т. е. $x \in (-1; 1)$. Кроме того, по свойствам дробной части равенство $\{x^2 + 2x + 1\} = x^2 = \{x^2\}$ выполняется тогда и только тогда, когда $x^2 + 2x + 1 - x^2 = 2x + 1 \in \mathbb{Z}$. Поэтому в исходном уравнении значение $2x$ должно быть целым числом. Ясно, что при $x \in (-1; 1)$ значение $2x$ целое в точности тогда, когда $x \in \{-0{,}5; 0; 0{,}5\}$. Проверка показывает, что все три значения являются решениями исходного уравнения.
Ответ: $-0{,}5$; 0; 0,5. ⊠

2. ОТНОШЕНИЕ СРАВНЕНИЯ В КОЛЬЦЕ $\mathbb{Z}$

2.1. Сравнения в кольце целых чисел. Свойства сравнений

Теорема 2.1.1. Пусть m — натуральное число, $m > 1$. Для любых целых чисел a и b следующие утверждения равносильны:

1) a и b имееют одинаковые остатки от деления на m;

2) $a - b$ делится на m, т.е. $a - b = mq$ для подходящего целого q;

3) $a = b + mq$ для некоторого целого q.

$\square$. Покажем, что из условия 1 следует условие 2. Если $a = mq_1 + r$, $b = mq_2 + r$, то $a - b = m(q_1 - q_2)$, что означает делимость $a - b$ на m. Из условия 2 очевидным образом следует условие 3. Покажем, что из условия 3 следует условие 1. Если $b = ms + r$, то из равенства $a = b + mq$ получаем: $a = b + mq = mq + ms + r = m(q + s) + r$. $\boxtimes$

Определение 2.1.1. Целые числа a и b называются *сравнимыми по модулю* m, если они удовлетворяют одному из условий теоремы 2.1.1, и пишут $a \equiv b \pmod{m}$. Данное соотношение между целыми числами называют *сравнением по модулю* m.

Например, $21 \equiv 31 \pmod{5}$.

Лемма 2.1.1. (простейшие свойства сравнений).

1. Каждое целое число сравнимо с самим собой по любому модулю (рефлексивность), т.е.

$$a \equiv a \pmod{m}.$$

2. Части сравнения можно менять местами (симметричность), т.е.

$$a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}.$$

3. Если одно целое число сравнимо с другим по модулю m, а второе сравнимо с третьим по тому же модулю, то первое сравнимо с третьим по модулю m (транзитивность), т.е.

$$a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}.$$

4. Сравнения по одному и тому же модулю можно почленно складывать, вычитать, перемножать, т.е.

$$a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \Rightarrow a \pm c \equiv b \pm d \pmod{m},$$

$$ac \equiv bd \pmod{m}.$$

5. К обеим частям сравнения можно прибавлять или вычитать из них одно и то же целое число, т.е.

$$a \equiv b \pmod{m} \Rightarrow a \pm c \equiv b \pm c \pmod{m}.$$

6. Члены сравнения можно переносить из одной части сравнения в другую с противоположным знаком, т.е.

$$a + b \equiv c \pmod{m} \Rightarrow a \equiv c - b \pmod{m}.$$

7. К любой части сравнения можно прибавлять или вычитать из неё число, кратное модулю, т.е.

$$a \equiv b \pmod{m} \Rightarrow a \pm mk \equiv b \pmod{m},$$

$$a \equiv b \pm mk \pmod{m}, k \in \mathbb{Z}.$$

8. Обе части сравнения можно умножать на одно и то же целое число, т.е.

$$a \equiv b \pmod{m} \Rightarrow ak \equiv bk \pmod{m}, k \in \mathbb{Z}.$$

9. Обе части сравнения можно возводить в одну и ту же натуральную степень, т.е.

$$a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}, n \in \mathbb{N}.$$

10. Обе части сравнения можно делить на их общий делитель, если он взаимно прост с модулем m, т.е.

$$ak \equiv bk \pmod{m} \wedge \text{НОД}(k, m) = 1 \Rightarrow a \equiv b \pmod{m}.$$

11. Обе части сравнения и модуль можно умножить на одно и то же натуральное число, т.е.

$$a \equiv b \pmod{m} \Rightarrow ak \equiv bk \pmod{mk}, k \in \mathbb{N}.$$

12. Обе части сравнения и модуль можно делить на любой их общий натуральный делитель, т.е.

$$ak \equiv bk \pmod{mk} \Rightarrow a \equiv b \pmod{m}, k \in \mathbb{N}.$$

13. Если числа сравнимы по модулю m, то они сравнимы и по

модулю k, равному любому натуральному делителю числа m, т.е.

$$a \equiv b \pmod{m} \wedge m \vdots k \Rightarrow a \equiv b \pmod{k}, k \in \mathbb{N}.$$

14. Если числа сравнимы по нескольким модулям, то они сравнимы по модулю, который является НОК данных модулей, т.е.

$$a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, ..., a \equiv b \pmod{m_k} \Rightarrow$$

$$a \equiv b \pmod{\text{НОК}(m_1, \ldots, m_k)}.$$

15. Если одна часть сравнения и модуль делятся на какое-либо число, то и другая часть сравнения делится на это число, т.е.

$$a \equiv b \pmod{m} \wedge a \vdots k \wedge m \vdots k \Rightarrow$$

$$\Rightarrow b \vdots k, k \in \mathbb{Z}.$$

16. $a \equiv b \pmod{m} \Rightarrow \text{НОД}(a, m) = \text{НОД}(b, m)$.

Обратное утверждение неверно (проверьте). Однако справедливо контрапозитивное:

$$\text{НОД}(a, m) \neq \text{НОД}(b, m) \Rightarrow a \not\equiv b \pmod{m}.$$

□. Свойства 1) — 3) докажите самостоятельно.

4. По условию, $a - b$ делится на m и $c - d$ делится на m. Следовательно, $(a - b) \pm (c - d)$ делится на m, $(a \pm c) - (b \pm d)$ делится на m и $a \pm c \equiv b \pm d \pmod{m}$.

Так как $a - b$ делится на m и $c - d$ делится на m, то $a - b = mq_1, c - d = mq_2, q_1, q_2 \in \mathbb{Z}$.

Тогда $a = b + mq_1, c = d + mq_2$ и $ac = bd + m(bq_2 + dq_1 + mq_1q_2)$. Отсюда $ac - bd = m(bq_2 + dq_1 + mq_1q_2)$ делится на m, т.е. $ac \equiv bd \pmod{m}$.

Свойства 5) — 9) докажите самостоятельно.

10. По условию, $ak - bk$ делится на m. Тогда $(a - b)k$ делится на m. Но $\text{НОД}(k, m) = 1$. Следовательно, $a - b$ делится на m, т.е. $a \equiv b \pmod{m}$.

11. Действительно, пусть

$$a \equiv b \pmod{m} \text{ и } k \in \mathbb{N}.$$

Тогда

$$a - b = mt, t \in \mathbb{Z} \text{ и } ak - bk = mtk, \text{ или } ak \equiv bk \pmod{mk}.$$

12. Если $ak \equiv bk \pmod{mk}$, то $(a-b)k$ делится на mk. Следовательно, $a-b$ делится на m, т.е. $a \equiv b \pmod{m}$.

13. Если $a \equiv b \pmod{m}$, $a-b$ делится на m. Так как m делится на k, то в силу транзитивности отношения делимости $a-b$ делится на k, $a \equiv b \pmod{k}$.

14. Если $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$, то $a-b$ делится на m_1, $a-b$ делится на m_2, ..., $a-b$ делится на m_k. Значит, $a-b = \text{ОК}(m_1, ..., m_k)$. Тогда $a-b$ делится на $\text{НОК}(m_1, ..., m_k)$.

Свойства 15) — 16) докажите самостоятельно. ⊠

Сравнения в таком виде, как их здесь рассматриваем, были введены впервые Гауссом в его знаменитой книге «Исследования по арифметике». Гаусс начал писать её в 1796 г. (с 19 лет) и значительная часть этого сочинения им была написана в студенческие годы. Печаталась эта книга крайне медленно и появилась только в 1801 г. В первом разделе книги Гаусс вводит понятие сравнения. Это понятие фактически в неявном виде употреблялось многими математиками до Гаусса, однако только Гаусс точно определил его и систематически развил соответствующую теорию. Дальнейшие фундаментальные результаты Гаусса, изложенные в этой книге, явились основой всего последующего развития теории чисел.

2.2. Кольцо классов вычетов по данному модулю

Сравнимость целых чисел по данному модулю m определяет бинарное отношение φ на множестве целых чисел: два целых числа находятся в отношении φ тогда и только тогда, когда они сравнимы друг с другом по модулю m.

Свойства 1) — 3) леммы 2.1.1 означают, что отношение сравнимости на множестве целых чисел $\mathbb{Z}$ есть отношение эквивалентности. Поэтому оно разбивает $\mathbb{Z}$ на классы эквивалентности. Всякий класс эквивалентности в данном случае состоит из всех чисел, дающих при делении на модуль m один и тот же остаток (класс равноостаточных чисел).

Определение 2.2.1. *Классом вычетов по модулю* m называется класс целых чисел, дающий один и тот же остаток при делении на m. Всякий представитель, т.е. всякое число из класса вычетов по модулю m, будем называть *вычетом* этого класса.

Как известно, всякий класс эквивалентности определяется любым своим представителем. В нашем случае всякий вычет из класса вычетов по модулю m определяет этот класс. Класс вычетов, содержащий число a, будем обозначать через $\overline{a}$. Так как при делении чисел возможны m различных остатков $0, 1, 2, \ldots, m-1$, то существуют m различных классов вычетов по модулю m, а именно: $\overline{0} = \{k \cdot m \mid k \in \mathbb{Z}\}$ — класс чисел, кратных m, $\overline{1} = \{k \cdot m + 1 \mid k \in \mathbb{Z}\}$ — класс чисел, дающих в остатке 1 при делении на m, …, $\overline{m-1} = \{k \cdot m + (m-1) \mid k \in \mathbb{Z}\}$ — класс чисел, дающих в остатке $m-1$ при делении на m.

В общем случае $\overline{a} = \{m \cdot k + a \mid k \in \mathbb{Z}\}$.

Множество всех классов вычетов по данному модулю m будем обозначать через $\mathbb{Z}_m$.

Введем на множестве $\mathbb{Z}_m$ операции сложения и умножения.

Определение 2.2.2. *Суммой классов вычетов* $\overline{a}$ и $\overline{b}$ из $\mathbb{Z}_m$ называется класс вычетов, содержащий число $a + b$, т.е. $\overline{a} + \overline{b} = \overline{a + b}$.

Пример 2.2.1. Если $m = 8$, то $\overline{5} + \overline{4} = \overline{9} = \overline{1}$.

Определение 2.2.3. *Произведением классов вычетов* $\overline{a}$ и $\overline{b}$ из $\mathbb{Z}_m$ называется класс вычетов, содержащий число $a \cdot b$, т.е. $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$.

Пример 2.2.2. Если $m = 8$, то $\overline{5} \cdot \overline{4} = \overline{20} = \overline{4}$.

Теорема 2.2.1. Множество $\mathbb{Z}_m$ классов вычетов по модулю m образует коммутативное кольцо с единицей относительно операций сложения и умножения классов вычетов.

□. Операция сложения и умножения классов вычетов на множестве $\mathbb{Z}_m$ коммутативны и ассоциативны, операция умножения дистрибутивна относительно операции сложения. Это следует из того, что указанные операции, согласно их определениям, сводятся к операциям над числами, для которых аналогичные свойства справедливы. Во множестве $\mathbb{Z}_m$ существует нулевой элемент, а именно $\overline{0}$. Противоположным для класса вычетов $\overline{a}$, очевидно, является класс вычетов $\overline{-a}$, т.е. $-\overline{a} = \overline{-a}$. Роль единичного элемента во множестве $\mathbb{Z}_m$ выполняет класс $\overline{1}$. Из всего изложенного следует, что $\mathbb{Z}_m$ образует коммутативное кольцо с 1. ⊠

Определение 2.2.4. Так как $\mathbb{Z}_m$ — кольцо, то относительно операции сложения это множество образует абелеву группу. Ее называют *аддитивной группой классов вычетов по модулю* m.

Теорема 2.2.2. 1. Если m — составное число, то кольцо $\mathbb{Z}_m$ содержит делители нуля.

2. Класс $\overline{a}$ из кольца $\mathbb{Z}_m$ обратим тогда и только тогда, когда НОД$(a, m) = 1$.

3. Если m — простое число, то $\mathbb{Z}_m$ является полем, в частности, не содержит делителей нуля.

$\square$. 1. Пусть m — составное число, тогда его можно представить в виде произведения двух натуральных чисел $m = p \cdot q$, каждое из которых меньше m. Очевидно, что $\overline{p} \neq \overline{0}$ и $\overline{q} \neq \overline{0}$. В тоже время $\overline{p} \cdot \overline{q} = \overline{p \cdot q} = \overline{0}$. Таким образом, в $\mathbb{Z}_m$ существуют элементы $\overline{p}$ и $\overline{q}$, которые отличны от нулевого, но их произведение равно $\overline{0}$, т.е. $\mathbb{Z}_m$ содержит делители нуля.

2. Если $\overline{a}$ обратим в $\mathbb{Z}_m$, то существует $\overline{x} \in \mathbb{Z}_m$ такой, что $\overline{a} \cdot \overline{x} = \overline{1}$. Это значит, $\overline{a \cdot x} = \overline{1}$ или $ax \equiv 1 \pmod{m}$. Из свойства 16 леммы 2.1.1 следует, что НОД$(a, m) = 1$.

Обратно. Если a и m взаимно просты, то согласно теореме 1.4.1 о взаимно простых числах существуют целые числа x и y такие, что $ax + my = 1$. Тогда $ax + my \equiv 1 \pmod{m}$. В таком случае ввиду свойства 7 леммы 2.1.1 верно, что $ax \equiv 1 \pmod{m}$. Это значит, $\overline{a \cdot x} = \overline{1}$ или $\overline{a} \cdot \overline{x} = \overline{1}$. Из последнего равенства следует, что $\overline{a}$ обратим в $\mathbb{Z}_m$.

3. Так как m — простое число, то по п. 2 в $\mathbb{Z}_m$ каждый ненулевой элемент обратим, а, значит, $\mathbb{Z}_m$ — поле. $\boxtimes$

Определение 2.2.5. Отметим, что множество обратимых элементов кольца $\mathbb{Z}_m$ образует абелеву группу относительно операции умножения. Ее называют *мультипликативной группой обратимых элементов кольца* $\mathbb{Z}_m$.

2.3. Полная и приведенная система вычетов

Определение 2.3.1. Совокупность любых чисел, взятых по одному из каждого класса вычетов по модулю m, называется *полной системой вычетов по данному модулю.*

Каждому модулю m соответствует бесконечное множество полных систем вычетов. Обычно в качестве полной системы вычетов употребляется *полная система наименьших неотрицательных вычетов по модулю* m, т.е. система $0, 1, \ldots, m - 1$.

Пусть m — натуральное число. Если $m = 2n$, $n \in \mathbb{N}$, то $\{0, 1, 2, \ldots, n-1, n, -(n-1), \ldots, -2, -1\}$ — полная система вычетов по модулю m. Если $m = 2n + 1$, $n \in \mathbb{N}$, то $\{0, 1, 2, \ldots, n, -n, \ldots, -2, -1\}$ — полная система вычетов по модулю m. Совокупности чисел $\{0, 1, 2, \ldots, n-1, n, -(n-1), \ldots, -2, -1\}$ при $m = 2n$ и $\{0, 1, 2, \ldots, n, -n, \ldots, -2, -1\}$ при $m = 2n + 1$ называются *полной системой наименьших по абсолютной величине вычетов по модулю* m.

Пример 2.3.1. Укажите полную систему неотрицательных вычетов и полную систему наименьших по абсолютной величине вычетов по модулю 4.

□. По модулю 4 полными системами вычетов являются следующие множества: $\{0, 1, 2, 3\}$, $\{0, 1, 2, -1\}$, $\{8, -7, 10, 7\}$, $\{0+4h_1, 1+4h_2, 2+4h_3, 3+4h_4\}$, где h_1, h_2, h_3, h_4 — произвольные целые числа. Ясно, что $\{0, 1, 2, 3\}$ — полная система наименьших неотрицательных вычетов по модулю 4. Совокупность классов $\{0, 1, 2, -1\}$ — полная система наименьших по абсолютной величине вычетов по модулю 4.

Ответ: $\{0, 1, 2, 3\}$ — полная система наименьших неотрицательных вычетов по модулю 4, $\{0, 1, 2, -1\}$ — полная система наименьших по абсолютной величине вычетов по модулю 4. ⊠

Пример 2.3.2. Составьте из чисел, кратных 2, полную систему вычетов по модулю 9.

□. Рассмотрим числа, кратные 2:

$2 \cdot 0 = 0$, $2 \cdot 1 = 2$, $2 \cdot 2 = 4$, $2 \cdot 3 = 6$, $2 \cdot 4 = 8$,

$2 \cdot 5 = 10 \equiv 1 \pmod 9$, $2 \cdot 6 = 12 \equiv 3 \pmod 9$,

$2 \cdot 7 = 14 \equiv 5 \pmod 9$, $2 \cdot 8 = 16 \equiv 7 \pmod 9$.

Так как среди приведенных кратных встречаются все числа от 0 до 8, то совокупность {0, 10, 2, 12, 4, 14, 6, 16, 8} является полной системой вычетов по модулю 9.

Ответ: {0, 10, 2, 12, 4, 14, 6, 16, 8} — полная система вычетов по модулю 9. ⊠

Теорема 2.3.1. Любая совокупность m целых чисел ($m > 1$), попарно несравнимых по модулю m, образует полную систему вычетов по этому модулю.

□. Пусть M есть совокупность m чисел, попарно несравнимых по модулю m. Тогда эти числа принадлежат различным классам вычетов по модулю m. Кроме того, M содержит столько чисел, сколько существует классов вычетов по модулю m. Следовательно, M — множество чисел, взятых по одному из каждого класса вычетов по модулю m. Поэтому M образует полную систему вычетов по модулю m. ⊠

Теорема 2.3.2. Если НОД$(a, m) = 1$ и x пробегает полную систему вычетов по модулю m, то $ax + b$, где b — любое целое число, также пробегает полную систему вычетов по модулю m.

□. Пусть M — полная система вычетов по модулю m. Тогда множество $M_1 = \{ax+b, x \in M\}$, так же как и M, содержит m элементов. Покажем, что любые два числа $ax_1 + b, ax_2 + b \in M_1$ несравнимы по модулю m. Допустим, что $ax_1+b \equiv ax_2+b \pmod m$. Тогда $ax_1 \equiv ax_2 \pmod m$. Так как НОД$(a, m) = 1$, то $x_1 \equiv x_2 \pmod m$. Учитывая, что x_1, x_2 принадлежат полной системе вычетов по модулю m, то получаем противоречие. Значит, допущение неверно. Следовательно, M_1 — полная система вычетов по модулю m. ⊠

Определение 2.3.2. Совокупность любых чисел, взятых по одному из каждого класса вычетов по модулю m и взаимно простых с m, называется *приведённой системой вычетов по модулю* m.

Обычно приведенную систему вычетов по модулю m выделяют из системы наименьших неотрицательных вычетов $0, 1, \ldots, m - 1$. Так как среди этих чисел число взаимно простых с m есть $\varphi(m)$, то число чисел приведенной системы, ровно как и число классов, содержащих числа взаимно простые с модулем, есть $\varphi(m)$.

Например, $1, 5, 7, 11$ — приведённая система наименьших положительных вычетов по модулю 12;

Теорема 2.3.3. Любая совокупность $\varphi(m)$ целых чисел $(m > 1)$ взаимно простых с m и попарно несравнимых по модулю m, образует приведённую систему вычетов по модулю m.

□. Пусть M есть совокупность $\varphi(m)$ чисел, взаимно простых с m и попарно несравнимых по модулю m. Тогда эти числа принадлежат к различным классам вычетов, взаимно простым с модулем m. Поэтому мно-

жество M содержит по одному представителю из каждого такого класса. Следовательно, M есть приведённая система вычетов по модулю m. $\boxtimes$

Теорема 2.3.4. Если НОД$(a, m) = 1$ и x пробегает приведённую систему вычетов по модулю m, то ax также пробегает приведённую систему вычетов по модулю m.

$\square$. Действительно, чисел ax будет столько же, сколько и чисел x, т.е. $\varphi(m)$. Так как произведение двух чисел, взаимно простых с третьим числом m, есть число взаимно простое с m, то числа ax взаимно просты с m. Кроме того, числа ax попарно несравнимы по модулю m. В самом деле, если $ax_1 \equiv ax_2 \ (mod\ m)$, то в силу условия НОД$(a, m) = 1$, следует, что $x_1 \equiv x_2 \pmod{m}$, что невозможно.

Таким образом, ax пробегает приведённую систему вычетов по модулю m. $\boxtimes$

2.4. Теоремы Эйлера и Ферма. Теорема Вильсона

Теорема 2.4.1. (теорема Эйлера) Если целое число a взаимно просто с натуральным m, то

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

$\square$. Пусть

$$a_1, a_2, \ldots, a_{\varphi(m)} - \tag{2.1}$$

приведённая система вычетов по модулю m. Тогда по теореме 2.3.4

$$aa_1, aa_2, ..., aa_{\varphi(m)} - \tag{2.2}$$

также приведённая система вычетов по модулю m. Следовательно, каждое число системы (2.2) сравнимо с некоторым числом системы (2.1) по модулю m, т.е.

$$aa_1 \equiv a_{i_1} \pmod{m}, \ldots, aa_{\varphi(m)} \equiv a_{i\varphi(m)} \pmod{m}. \tag{2.3}$$

Перемножая почленно сравнения (2.3) получим

$$a^{\varphi(m)} a_1 a_2 \cdot \ldots \cdot a_{\varphi(m)} \equiv a_{i_1} a_{i_2} \cdot \ldots \cdot a_{i\varphi(m)} \pmod{m}. \tag{2.4}$$

Разделив, обе части сравнения (2.4) на $a_1 a_2 \cdot \ldots \cdot a_{\varphi(m)} = a_{i_1} a_{i_2} \cdot \ldots \cdot a_{i\varphi(m)}$, получим $a^{\varphi(m)} \equiv 1 \pmod{m}$, что и требовалось доказать. ⊠

Теорема 2.4.2. (теорема Ферма) Если целое число a не делится на простое число p, то $a^{p-1} \equiv 1 \pmod{p}$.

□. Эта теорема является следствием теоремы 2.4.1. ⊠

Следствие 2.4.1. Если p — простое число и a — любое целое число, то $a^p \equiv a \pmod{p}$.

□. Возможны 2 случая.

1. Если НОД$(a, p) = 1$, то по теореме Ферма, $a^{p-1} \equiv 1 \pmod{p}$. Умножив обе части этого сравнения на a, получим: $a^p \equiv a \pmod{p}$.

2. Если a делится на p. Тогда a^p делится на p. Следовательно, $a^p - a$ делится на p. Это значит, что $a^p \equiv a \pmod{p}$. ⊠

Теорема 2.4.3. (теорема Вильсона). Для любого простого числа p выполняется сравнение $(p-1)! + 1 \equiv 0 \pmod{p}$.

□. Для $p = 2$ утверждение очевидно выполняется, поэтому далее будем считать, что p нечетно. Пусть a — некоторое целое число из промежутка $1 < a < p$. Так как НОД$(a, p) = 1$, то по теореме 2.2.2 существует целое число b, удовлетворяющее сравнению $ab \equiv 1 \pmod{\text{p}}$. При этом можно считать, что b есть наименьший неотрицательный вычет в своем классе. Ясно, что $b \neq 0$, т.е. $1 < b < p$. Кроме того, число b определяется единственным образом. Ведь если $ab_1 \equiv 1 \pmod{p}$ и $ab_2 \equiv 1 \pmod{p}$, то p делит $a(b_1 — b_2)$ и p делит $b_1 - b_2$, что при различных b_1, b_2 из промежутка $1 < b < p$ невозможно.

Если $b \equiv a \pmod{p}$, то $a^2 \equiv 1 \pmod{p}$ и p делит $(a^2 - 1) = (a-1)(a+1)$. Так как p — простое число, это возможно лишь в случае $a = 1$ или $a = p - 1$. Из доказанного следует, что множество целых чисел a из промежутка $1 < a < p - 1$ может быть разбито на пары различных целых чисел a, b, удовлетворяющих сравнению $ab \equiv 1 \pmod{p}$. Следовательно,

$$\prod_{k=2}^{p-2} k \equiv 1 \pmod{p}.$$

Умножив это сравнение на $p-1$, получим $(p-1)! \equiv p-1 \equiv$ $\equiv -1 \pmod{p}$.

Для составных чисел теорема Вильсона, конечно, нарушается. Ведь если целое число N имеет делитель d, $1 < d < N$, то $(N-1)!$ делится на d. Значит, $(N-1)!+1$ на d не делится, а потому не делится и на N. $\boxtimes$

2.5. Сравнения первой степени с одним неизвестным

Определение 2.5.1. *Сравнением первой степени с одним неизвестным* называется сравнение

$$ax \equiv b \pmod{m}, \tag{2.5}$$

где $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$, $a \not\equiv 0 \pmod{m}$.

Если в это сравнение вместо x будем подставлять различные целые числа, то будем получать верные или неверные числовые сравнения. Те значения x, которые дают верные числовые сравнения, называют *решениями сравнения* (2.5).

Легко проверить, что если x_0 — решение сравнения (2.5), то все целые числа из класса $\overline{x_0} = \{x_0 + tm \mid t \in \mathbb{Z}\}$, также будут решениями. Такие решения считаются одинаковыми. Поэтому решением сравнения (2.5) принято считать не отдельное число, а целый класс вычетов по модулю m, удовлетворяющих сравнению (2.5).

Определение 2.5.2. *Числом решений сравнения* (2.5) называют число решений сравнения в какой либо полной системе вычетов по модулю m.

Определение 2.5.3. Сравнения называются *равносильными*, если они имеют одинаковые решения.

Теорема 2.5.1. 1. Если НОД$(a, m) = 1$, то сравнение (2.5) имеет единственное решение;

2. Если НОД$(a, m) = d > 1$ и d не делит b, то сравнение (2.5) не имеет решений;

3. Если НОД$(a, m) = d > 1$ и d делит b, то сравнение (2.5) имеет d решений по модулю m: $\overline{x_0}$, $\overline{x_0 + 2m_1}$, $\ldots$, $\overline{x_0 + (d-1)m_1}$, где $m_1 = \dfrac{m}{d}$, x_0 — наименьший неотрицательный вычет из решения сравнения

$$a_1 x = b_1 \pmod{m_1}, a_1 = \frac{a}{d}, b_1 = \frac{b}{d}.$$

$\square$. Пусть НОД$(a, m) = 1$. Тогда существуют $x_0,\ y_0 \in \mathbb{Z}$ такие, что $ax_0 + my_0 = 1$.

Значит, $ax_0 + my_0 \equiv 1 \pmod{m}$. Отсюда следует, что $ax_0 \equiv 1 \pmod{m}$. Умножая обе части последнего сравнения на b, получаем $a(x_0 b) \equiv b \pmod{m}$. Следовательно, число $x_1 = x_0 b$ удовлетворяет сравнению (2.5), а класс $\overline{x_1} \in \mathbb{Z}_m$ является решением этого сравнения.

Докажем единственность решения.

Пусть $\overline{\alpha} \in \mathbb{Z}_m$ — произвольное решение сравнения (2.5), т.е. $a\alpha \equiv b \pmod{m}$. Кроме того, $ax_1 \equiv b \pmod{m}$. Тогда $a\alpha \equiv ax_1 \pmod{m}$ и так как НОД$(a, m) = 1$, то $\alpha \equiv x_1 \pmod{m}$. Поэтому $\overline{\alpha} = \overline{x_1}$. Таким образом, решение сравнения (2.5) единственное.

2. Пусть НОД$(a, m) = d > 1$ и d не делит b. Предположим, что сравнение (2.5) имеет решение $\overline{x_1} \in \mathbb{Z}_m$. Тогда $ax_1 \equiv b \pmod{m}$.

Так как a делится на d и m делится на d, то b делится на d по свойству 15 леммы 2.1.1, что противоречит условию. Следовательно, допущение неверное, т.е. сравнение (2.5) решений не имеет.

3. Пусть НОД$(a, m) = d > 1$ и d делит b. Разделим обе части сравнения (2.5) и модуль m на их общий делитель d. Получим сравнение, эквивалентное сравнению (2.5):

$$ax_1 \equiv b_1 \pmod{m_1}, a_1 = \frac{a}{d}, b_1 = \frac{b}{d}, m_1 = \frac{m}{d},\ \text{НОД}(a_1, m_1) = 1. \quad (2.6)$$

По п. 1 сравнение (2.5) имеет единственное решение $\overline{x_0} \in \mathbb{Z}_{m_1}$, x_0 — наименьший неотрицательный вычет по модулю m_1. Известно, что класс вычетов $\overline{x_0} \in \mathbb{Z}_{m_1}$ является объединением классов вычетов $\overline{x_0}, \overline{x_0 + m_1}, \cdots, \overline{x_0 + (d-1)m_1}$ кольца $\mathbb{Z}_m$ (докажите самостоятельно).

Поэтому $\overline{x_0}, \overline{x_0 + m_1}, \ldots, \overline{x_0 + (d-1)m_1}$ — все d различных решений сравнения (2.5). $\boxtimes$

Способы решения сравнения (2.5) рассматриваются только для случая, когда НОД$(a, m) = 1$, так как третий случай сводится к первому после сокращения на d.

1. Метод проб: решение находится путем непосредственного испытания наименьших неотрицательных или абсолютно наименьших вычетов по модулю m.

Пример 2.5.1. Решите сравнение

$$5x \equiv 6 \pmod 7. \tag{2.7}$$

□. Так как НОД$(5, 7) = 1$, то по теореме 2.5.1 сравнение (2.7) имеет единственное решение. Подставляя наименьшие по абсолютной величине вычеты 0, ± 1, ± 2, ± 3 по модулю 7 в сравнение (2.7), получаем, что $\overline{4} \in$ $\in \mathbb{Z}_7$ — искомое решение сравнения (2.7).
Ответ: $\overline{4}$. ⊠

2. Метод преобразования коэффициентов: используя свойства сравнений, коэффициенты сравнения (2.5) преобразуют так, чтобы коэффициент при x стал равен 1.

В сравнении (2.7) к левой части прибавим $-7x$:

$$-2x \equiv 6 \pmod 7.$$

Так как НОД$(-2, 7) = 1$, то разделим обе части последнего сравнения на (-2):

$$x \equiv -3 \equiv 4 \pmod 7.$$

3. При помощи конечных цепных дробей по формуле:

$$x \equiv (-1)^n b P_{n-1} \pmod m,$$

P_{n-1} — числитель предпоследней подходящей дроби при разложении $\dfrac{m}{a}$ в цепную дробь.

□. Можно считать, $a \in \mathbb{N}$, так как в противном случае, умножив обе части сравнения (2.5) на (–1), получим $a > 0$. Разложим $\dfrac{m}{a}$ в конечную цепную дробь.

Пусть $\dfrac{P_n}{Q_n} = \dfrac{m}{a}$. По лемме 1.6.1

$$P_n Q_{n-1} - P_{n-1} Q_n = (-1)^{n-1}$$

или

$$mQ_{n-1} - P_{n-1} a = (-1)^{n-1}.$$

Следовательно,

$$mQ_{n-1} - P_{n-1} a \equiv (-1)^{n-1} \pmod m,$$

т.е.

$$a(-P_{n-1}) \equiv (-1)^{n-1} \pmod{m}.$$

Умножая это сравнение на $(-1)^{n-1}b$, получаем: $a\left((-1)^n bP_{n-1}\right) \equiv b \pmod{m}$. Таким образом, число $(-1)^n bP_{n-1}$ удовлетворяет сравнению (2.5) и $\overline{(-1)^{n-1}bP_{n-1}} \in \mathbb{Z}_m$ — его единственное решение, что и требовалось доказать. ⊠

Решим этим способом сравнение (2.7).

Разложим $\frac{7}{5}$ в конечную цепную дробь: $\frac{7}{5} = [1; 2, 2]$. Здесь $n = 2, b = 6, p_1 = 3$. Тогда $x \equiv (-1)^2 \cdot 6 \cdot 3 \equiv 4 \pmod{7}$.

4. Метод Эйлера: Решение находится по формуле

$$x \equiv ba^{\varphi(m)-1} \pmod{m}.$$

□. Так как НОД$(a, m) = 1$, то по теореме Эйлера

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Умножим обе части последнего сравнения на b:

$$a(ba^{\varphi(m)-1}) \equiv b \pmod{m}.$$

Отсюда следует, что число $ba^{\varphi(m)-1}$ удовлетворяет сравнению (2.5) и $\overline{ba^{\varphi(m)-1}} \in \mathbb{Z}_m$ — решение данного сравнения, что и требовалось доказать.

Решим сравнение (2.7) методом Эйлера. Так как $\varphi(7) = 6$, то

$$x \equiv 6 \cdot 5^{6-1} \equiv 6 \cdot 5^3 \cdot 5^2 \equiv (-1)(-1) \cdot 4 \equiv 4 \pmod{7}.$$

⊠

Пример 2.5.2. Решите сравнение $45x \equiv 31 \pmod{100}$.

□. Так как НОД$(45, 100) = 5$ и 31 не делится на 5, то сравнение решений не имеет.

Ответ: решений нет. ⊠

Пример 2.5.3. Решите сравнение $51x \equiv 141 \pmod{234}$.

□. Здесь НОД$(51, 234) = 3$ и 141 делится на 3. Следовательно, сравнение имеет 3 решения.

После деления обеих частей сравнения и модуля на 3 получим сравнение $17x \equiv 47 \pmod{78}$. Полученное сравнение имеет единственное решение, так как НОД$(17, 78) = 1$. Его решением является $x \equiv 67 \pmod{78}$. (проверьте). Тогда $\overline{67}, \overline{145}, \overline{223}$ — решения данного сравнения.
Ответ: $\overline{67}, \overline{145}, \overline{223}$. ⊠

2.6. Сравнения первой степени и диофантовы уравнения. Сравнения высших степеней по простому модулю

Рассмотрим диофантово уравнение

$$ax + by = c, \ \text{НОД}(a, b) = 1. \tag{2.8}$$

Следовательно, уравнение (2.8) разрешимо в целых числах. Из (2.8) имеем $y = \dfrac{c - ax}{b}$. При целом x переменная y будет целой тогда и только тогда, когда $c - ax$ делится на b. А это значит, что

$$ax \equiv c \pmod{b}. \tag{2.9}$$

Пусть числа $x_0 + bt, t \in \mathbb{Z}$, удовлетворяют сравнению (2.9).

Тогда $\left(x_0 + bt, \dfrac{c - ax_0}{b} - at\right)$ — общее решение диофантова уравнения (2.8).

Пример 2.6.1. Решите уравнение

$$45x - 29y = 5. \tag{2.10}$$

□. Так как НОД$(45, -29) = 1$, то уравнение (2.10) разрешимо в целых числах. Чтобы найти решение, заменим уравнение (2.10) сравнением $45x \equiv 5 \pmod{29}$. Из этого сравнения находим $x = 13 + 29t, t \in \mathbb{Z}$. Тогда $y = 20 - 45t$. Значит, $(13 + 29t, 20 - 45t)$, $t \in \mathbb{Z}$ — общее решение уравнения (2.10).
Ответ: $\{(13 + 29t, 20 - 45t) \mid t \in \mathbb{Z}\}$. ⊠

Сравнения высших степеней по простому модулю представляют

собой наиболее простой случай сравнений. Вместе с тем это и наиболее важный случай, так как решение сравнения по составному модулю можно свести к решению сравнения по простому модулю. Пусть дано сравнение:

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 \pmod{p}, a_n \not\equiv 0 \pmod{p}. \tag{2.11}$$

Приступая к решению такого сравнения, можно, во-первых, заменить все коэффициенты соответствующими вычетами, обычно наименьшими неотрицательными или абсолютно наименьшими по модулю p, что уже даёт некоторое упрощение сравнения. Например, сравнение $21x^3+19x^2-$ $-9x+30 \equiv 0 \pmod{7}$ можно заменить более простым равносильным ему сравнением

$$-2x^2 - 2x + 2 \equiv 0 \pmod{7}. \tag{2.12}$$

Во-вторых, сравнение (2.11) можно заменить равносильным ему сравнением со старшим коэффициентом, равным 1.

Действительно, так как НОД$(a_n, p) = 1$, то существует $\alpha \in \mathbb{Z}$ такое, что $a_n\alpha \equiv 1 \pmod{p}$. Умножая обе части сравнения (2.11) на α, НОД$(\alpha, p) = 1$ получим равносильное сравнение со старшим коэффициентом $a_n\alpha$, который можно заменить сравнимым с ним вычетом 1 по модулю p.

Например, заменим сравнение (2.12) равносильным сравнением со старшим коэффициентом 1. Для этого решим сначала сравнение:

$$-2\alpha \equiv 1 \pmod{7} \Rightarrow \alpha \equiv 3 \pmod{7}.$$

Значит, умножим обе части (2.12) на 3:

$$x^2 + x - 1 \equiv 0 \pmod{7}.$$

В-третьих, более существенное упрощение сравнения достигается на основании следующей теоремы (о понижении степени сравнения).

Теорема 2.6.1. Всякое сравнение вида (2.11) при $n \geq p$ можно заменить равносильным ему сравнением $r(x) \equiv 0 \pmod{p}$ степени не выше $p-1$, где $r(x)$ — остаток от деления $f(x)$ на $x^p - x$.

□. Разделим с остатком $f(x)$ на $x^p - x$:

$$f(x) = (x^p - x)q(x) + r(x),$$

где $q(x), r(x) \in Z[x], deg(r(x)) \leq p-1$. Тогда сравнение (2.11) перепишется:

$$(x^p - x)q(x) + r(x) \equiv 0 \pmod{p}.$$

По следствию 2.4.1 $x^p - x \equiv 0 \pmod{p}$. Значит, $(x^p - x)q(x) \equiv 0 \pmod{p}$. Поэтому $r(x) \equiv 0 \pmod{p}$ — сравнение равносильное данному сравнению (2.11), что и требовалось доказать. ⊠

Пример 2.6.2. Понизьте степень

$$x^7 + 2x^3 + x^2 - x + 5 \equiv 0 \pmod{5}. \tag{2.13}$$

□. Делим $f(x) = x^7 + 2x^3 + x^2 - x + 5$ на $x^5 - x$. Получаем в остатке $r(x) = 3x^3 + x^2 - x + 5$.

Следовательно, сравнение (2.13) равносильно сравнению 3-ей степени:

$$3x^3 + x^2 - x + 5 \equiv 0 \pmod{5}.$$

Ответ: $3x^3 + x^2 - x + 5 \equiv 0 \pmod{5}$. ⊠

Утверждение 2.6.1. Для понижения степени сравнения (2.11) практически удобней воспользоваться тождеством

$$x^p \equiv x \pmod{p}.$$

Так как $x^5 \equiv x \pmod{5}$, то $x^7 \equiv x^3 \pmod{5}$ и поэтому для (2.13)

$$x^7 + 2x^3 + x^2 - x + 5 \equiv 0 \pmod{5} \Leftrightarrow 3x^3 + x^2 - x + 5 \equiv 0 \pmod{5}.$$

2.7. Системы линейных сравнений. Китайская теорема об остатках

Рассмотрим систему сравнений специального вида

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \dots\dots\dots\dots\dots \\ x \equiv a_k \pmod{m_k}. \end{cases} \tag{2.14}$$

Теорема 2.7.1. (китайская теорема об остатках). Если $m_1, \dots, m_k$ попарно взаимно просты, то система сравнений (2.14) разрешима. Определим целые числа M, M_i, b_i условиями $M = m_1 m_2 \cdot \dots \cdot m_k$, $M_i = \frac{M}{m_i}$, $M_i b_i \equiv a_i \pmod{m_i}$, $i = 1, 2, \dots, k$,

$$x_0 = M_1 b_1 + M_2 b_2 + \ldots + M_k b_k. \tag{2.15}$$

Тогда множество целых чисел, удовлетворяющих системе сравнений (2.14), составляет класс вычетов $x \equiv x_0 \pmod{M}$.

Замечание 2.7.1. Поскольку в условиях теоремы НОД$(M_i, m_i) = 1$, существование чисел b_i следует из теоремы 2.5.1. Заметим также, что числа b_i определяются не единственным способом. При использовании теоремы 2.7.1 для решения систем сравнений следует выбирать те из них, которые дают по возможности меньшие значения x_0.

$\square$. Так как m_i делит M_j при $j \neq i$, при любом i выполняются сравнения

$$x_0 \equiv M_i b_i \equiv a_i \pmod{m_i}. \tag{2.16}$$

Это значит, что множества целых чисел, удовлетворяющих системе (2.14) и системе

$$x \equiv x_0 \pmod{m_i}, \tag{2.17}$$

совпадают. По свойству 14 леммы 2.1.1 следует, что $x \equiv x_0 \pmod{\text{НОК}(m_1, \ldots, m_k)}$. Учитывая попарную взаимную простоту модулей m_i, с помощью теоремы 1.5.8 заключаем, что $x \equiv x_0 \pmod{M}$. $\boxtimes$

Пример 2.7.1. Решите систему сравнений

$$\begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 1 \pmod{12} \\ x \equiv 7 \pmod{14}. \end{cases}$$

$\square$. Из первого сравнения имеем: $x = 5t + 4$. Подставляем во второе сравнение: $5t + 4 \equiv 1 \pmod{12}$, $5t \equiv 9 \pmod{12}$, откуда $t \equiv 9 \pmod{12}$, $t = 12t_1 + 9$. Подставляя найденное значение t в равенство $x = 5t + 4$, находим: $x = 5(12t_1 + 9) + 4 = 60t_1 + 49$. Найденное значение x подставляем в третье сравнение: $60t_1 + 49 \equiv 7 \pmod{14}$, $60t_1 \equiv -42 \pmod{14}$, $4t_1 \equiv 0 \pmod{14}$. Делим обе части сравнения и модуль на 2: $2t_1 \equiv 0 \pmod{7}$, $t_1 \equiv 0 \pmod{7}$, откуда $t_1 = 7t_2$. Подставляя найденные значения t_1 в равенство $x = 60t_1 + 49$, находим: $x = 60 \cdot 7t_2 + 49 = 420t_2 + 49$.

Проверка. 49—4 делится на 5; 49—1 делится на 12; 49—7 делится на 14.
Ответ: $x \equiv 49 \pmod{2^2 \cdot 3 \cdot 5 \cdot 7}$. ⊠

Пример 2.7.2. Решите систему сравнений

$$\begin{cases} x \equiv 20 \pmod{21} \\ x \equiv 3 \pmod{5} \\ x \equiv 5 \pmod{8}, \end{cases}$$

□. Здесь $M = 21 \cdot 5 \cdot 8 = 840$, $M_1 = M/m_1 = 840/21 = 40$, $M_2 = 168$, $M_3 = 105$. Решаем сравнения:

$40x \equiv 20 \pmod{21}$, $x = 11 = b_1$,
$168x \equiv 3 \pmod{5}$, $x = 1 = b_2$,
$105x \equiv 5 \pmod{8}$, $x = 5 = b_3$.

Вычисляем значение $x_0 = M_1b_1 + M_2b_2 + M_3b_3$:

$$x_0 = 40 \cdot 11 + 168 \cdot 1 + 105 \cdot 5 = 1133.$$

Тогда $x \equiv 1133 \equiv 293 \pmod{840}$.
Ответ: $x \equiv 293 \pmod{840}$.

⊠

2.8. Порядок числа по данному модулю. Первообразные корни. Первообразные корни по простому модулю

Пусть НОД$(a, m) = 1, a \in \mathbb{Z}, m \in \mathbb{N}$.

Определение 2.8.1. *Порядком (показателем) числа a по модулю m* называется наименьшее натуральное число k такое, что $a^k \equiv 1 \pmod{m}$. Обозначается через $\theta(a \mod m)$.

Теорема 2.8.1. Если одно число класса вычетов $\overline{a} \in \mathbb{Z}_m$ имеет порядок k, то и все числа этого класса имеют порядок k.

□. Пусть $\theta(a \mod m) = k$ т.е. $a^k \equiv 1 \pmod{m}$. Возьмём число $b \in \overline{a} \in \mathbb{Z}_m$ и покажем, что $\theta(b \mod m) = k$. Действительно, $b \equiv a \pmod{m}$. Тогда $b^k \equiv a^k \pmod{m}$. Значит, $b^k \equiv 1 \pmod{m}$. Допустим, что $b^r \equiv 1 \pmod{m}$, $0 < r < k$. Так как $b^r \equiv a^r \pmod{m}$, то $a^r \equiv 1 \pmod{m}$, что противоречит условию.

Таким образом, $\theta(a \mod m) = k$, т.е. все числа класса $\overline{a} \in \mathbb{Z}_m$ имеют порядок k. Число k называется *порядком класса вычетов* $\overline{a}$ и обозначается $\theta(\overline{a} \mod m)$. ⊠

Пример 2.8.1. Найдите $\theta(2 \mod 15)$.

$\square$. $2^1, 2^2, 2^3 \not\equiv 1 \pmod{15}, 2^4 \equiv 1 \pmod{15}$, значит, $\theta(2 \mod 15) = 4$.
Ответ: 4. $\boxtimes$

Теорема 2.8.2. Если $\theta(a \mod m) = k$, то числа $a^0, a^1, a^2, \ldots, a^{k-1}$ попарно несравнимы по модулю m.

$\square$. Доказательство методом от противного. Пусть $a^s \equiv a^t \pmod{m}$ где $0 \leq t < s < k$. Так как НОД$(a, m) = 1$, то НОД$(a^t, m) = 1$. Разделим обе части сравнения на a^t : $a^{s-t} \equiv 1 \pmod{m}$, где $0 < s - t < k$, что невозможно. Допущение неверно. $\boxtimes$

Определение 2.8.2. Если $\theta(a \mod m) = \varphi(m)$, то a называется *первообразным корнем по модулю* m.
Следствие 2.8.1. Если a — первообразный корень по модулю m, то $a^0, a^1, a^2, \ldots, a^{\varphi(m)-1}$ образуют приведённую систему вычетов по модулю m.

$\square$. Действительно, по теореме 2.8.2 эти числа попарно несравнимы по модулю m, кроме того, они взаимно просты с m. $\boxtimes$

Следствие 2.8.2. Если a — первообразный корень по простому модулю p, то $a^0, a^1, a^2, \ldots, a^{p-2}$ образуют приведённую систему вычетов по модулю p.
Теорема 2.8.3. Если $\theta(a \mod m) = k$ и $a^n \equiv 1 \pmod{m}$, то n делится на k.

$\square$. Разделим с остатком n на k :

$$n = kq + r, \ 0 \leq r < k.$$

Покажем, что $r = 0$. По условию $a^k \equiv 1 \pmod{m}$, тогда

$$a^n \equiv (a^k)^q \dot{a}^r \equiv a^r \pmod{m}.$$

Если $0 < r < k$, то $a^r \not\equiv 1 \pmod{m}$. Значит, $r = 0$ и n делится на k. $\boxtimes$

Следствие 2.8.3. Порядок числа a по модулю m является делителем $\varphi(m)$.
Следствие 2.8.4. Порядок числа a по простому модулю p является делителем $p - 1$.

Теорема 2.8.4. Если $\theta(a \mod m) = k$, то

$$a^{k_1} \equiv a^{k_2} \pmod{m} \Leftrightarrow k_1 \equiv k_2 \pmod{k}.$$

□. **Необходимость.** Пусть $a^{k_1} \equiv a^{k_2} \pmod{m}$, где $k_1 \geq k_2$. Так как НОД$(a^{k_2}, m) = 1$, то $a^{k_1-k_2} \equiv 1 \pmod{m}$.

Тогда по теореме 2.8.3 разность $k_1 - k_2$ делится на k, т.е. $k_1 \equiv k_2 \pmod{k}$.

Достаточность. Пусть $k_1 \equiv k_2 \pmod{k}$. Поэтому $k_1 - k_2 = kq$, $q \in \mathbb{Z}$. Значит, $a^{k_1-k_2} \equiv a^{kq} \equiv (a^k)^q \equiv 1 \pmod{m}$. Итак, $a^{k_1-k_2} \equiv 1 \pmod{m}$. Умножая это сравнение на a^{k_2}, имеем $a^{k_1} \equiv a^{k_2} \pmod{m}$. ⊠

Следствие 2.8.5. Если a — первообразный корень по простому модулю p, то $a^{k_1} \equiv a^{k_2} \pmod{p} \Leftrightarrow k_1 \equiv k_2 \pmod{(p-1)}$.

Проверкой можно убедиться, что если m — составное число, то в большинстве случаев не существует первообразных корней по модулю m. Так, например, не существует первообразных корней по модулю 20. Действительно, $\varphi(20) = 8$, но

$\theta(1 \mod 20) = 1 \neq 8$, $\theta(3 \mod 20) = 4 \neq 8$,
$\theta(7 \mod 20) = 4 \neq 8$, $\theta(9 \mod 20) = 2 \neq 8$,
$\theta(11 \mod 20) = 2 \neq 8$, $\theta(13 \mod 20) = 4 \neq 8$,
$\theta(17 \mod 20) = 4 \neq 8$, $\theta(19 \mod 20) = 2 \neq 8$.

Можно доказать, что по простому модулю p всегда существуют первообразные корни, причём число попарно несравнимых по модулю p первообразных корней равно $\varphi(p-1)$, т.е. существует $\varphi(p-1)$ классов первообразных корней по простому модулю p, см. [3]. Более того, если a — первообразный корень по модулю p, то число a^k, НОД$(k, p-1) = 1$ тоже будет первообразным корнем по модулю p.

Заметим, что если $p = 2$, то класс $\overline{1} \in \mathbb{Z}_2$ является единственным классом первообразных корней по модулю 2, так как $\theta(1 \mod 2) = 1 = \varphi(2)$. Если $p > 2$, то число 1 не является первообразным корнем по модулю p, так как

$$\theta(1 \mod p) = 1 \neq \varphi(p) = p - 1.$$

Теорема 2.8.5. Если $p-1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ — каноническое разложение числа $p-1$ (p — простое) и $a^{\frac{p-1}{p_j}} \not\equiv 1 \pmod{p}$, $j = \overline{1,k}$, НОД$(a,p) = 1$,

то a — первообразный корень по модулю p.

$\square$. Покажем, что $\theta(a \mod p) = p-1$. Допустим противное, т.е. $\theta(a \mod p) = d \neq p-1$. Так как НОД$(a,p)=1$, то по теореме Ферма

$$a^{p-1} \equiv 1 \pmod{p}.$$

Следовательно, d — делитель числа $p-1$, т.е. $d = p_1^{\beta_1} \dots p_k^{\beta_k}$, $0 \leq \beta_j \leq \alpha_j$, $j = \overline{1,k}$. Тогда

$$\frac{p-1}{p_j} = (p_1^{\beta_1} \dots p_j^{\beta_j} \dots p_k^{\beta_k}) \cdot (p_1^{\alpha_1-\beta_1} \dots p_j^{\alpha_j-\beta_j-1} \dots p_k^{\alpha_k-\beta_k}) = dq,\ q \in \mathbb{Z},$$

$$\alpha_1 - \beta_1 \geq 0, \dots, \alpha_j - \beta_j - 1 \geq 0, \dots, \alpha_k - \beta_k \geq 0.$$

Значит, $a^{\frac{p-1}{p_j}} \equiv a^{dq} \equiv (a^d)^q \equiv 1 \pmod{p}$, $1 \leq j \leq k$, что противоречит условию. Следовательно, $\theta(a \mod p) = p-1 = \varphi(p)$ и a — первообразный корень по модулю p. Очевидно, что условие $a^{\frac{p-1}{p_j}} \not\equiv 1 \pmod{p}$ для всех простых p_j, входящих в каноническое разложение $p-1$ является не только достаточным, но и необходимым условием того, чтобы a было первообразным корнем по простому модулю p. $\boxtimes$

Таким образом, имеем следующий способ отыскания попарно несравнимых первообразных корней по простому модулю $p > 2$. Путём испытаний чисел из приведённой системы наименьших положительных вычетов по модулю p (кроме 1) находится наименьший положительный первообразный корень a по модулю p. Остальные попарно несравнимые первообразные корни находятся, как наименьшие положительные вычеты степеней a^k по модулю p, где НОД$(k, p-1) = 1,\ 1 < k < p-1$.

Пример 2.8.2. Найдите все попарно несравнимые первообразные корни по модулю 17.

$\square$. Число попарно несравнимых по модулю 17 первообразных корней равно $\varphi(17-1) = \varphi(16) = 8$. Найдём сначала наименьший положительный первообразный корень, испытывая числа из приведённой системы наименьших положительных вычетов по модулю 17: $2^{\frac{17-1}{2}} \equiv 2^8 \equiv 1 \pmod{17}$. Значит, необходимое условие не выполняется, поэтому 2 не является первообразным корнем по модулю 17; $3^8 \equiv -1 \not\equiv 1 \pmod{17}$, т.е. достаточное условие выполняется и 3 – первообразный корень по модулю 17. Остальные первообразные корни найдём,

как наименьшие положительные вычеты степеней 3^k по модулю 17, где

$$k = 3,\ 5,\ 7,\ 9,\ 11,\ 13,\ 15:\ 3^3 \equiv 10 \pmod{17},$$
$$3^5 \equiv 5 \pmod{17},\ 3^7 \equiv 11 \pmod{17},$$
$$3^9 \equiv 14 \pmod{17},\ 3^{11} \equiv 7 \pmod{17},$$
$$3^{13} \equiv 12 \pmod{17},\ 3^{15} \equiv 6 \pmod{17}.$$

Ответ: $3, 5, 6, 7, 10, 11, 12, 14$ — попарно несравнимые первообразные корни по модулю 17. ⊠

Пример 2.8.3. Какой порядок имеет число 5 по модулю 12?

□. Должны быть выполнены следующие требования:

а) искомый порядок надо искать среди делителей числа $\varphi(m)$, где m — модуль;

б) искомый порядок должен быть наименьшим из положительных показателей, удовлетворяющих сравнению $a^z \equiv 1 \pmod{m}$, где a – испытуемое число.

В данном случае имеем:

$$\text{НОД}(5, 12) = 1;\ \varphi(12) = 12 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{3}) = 4.$$

Делителями 4 являются числа 1, 2, 4. Тогда

$$5^1 \equiv 5 \pmod{12},\ 5^2 \equiv 1 \pmod{12}.$$

Следовательно, число 5 имеет порядок 2 по модулю 12.
Ответ: 2. ⊠

Пример 2.8.4. Какой порядок имеет число 4 по модулю 12?

□. Числа 4 и 12 не являются взаимно простыми, а следовательно, сама постановка вопроса является ошибочной. ⊠

Пример 2.8.5. Найти наименьший первообразный корень по модулю 7.

□. Для нахождения наименьшего первообразного корня по простому модулю p необходимо и достаточно:

а) найти все различные простые делители числа $p - 1$ (обозначим их $p_1, p_2, \ldots, p_k$);

б) последовательно проверить числа, взаимно простые с модулем, начиная с числа 1; первое из чисел, которое не удовлетворяет ни одному из сравнений:

$$q^{\frac{p-1}{p_1}} \equiv 1 \pmod{p}, \ldots, q^{\frac{p-1}{p_k}} \equiv 1 \pmod{p}$$

будет искомым первообразным корнем.

Имеем $7-1=6=2\cdot 3$. Так как

$$1^2 \equiv 1 \pmod{7},$$

то число 1 не является первообразным корнем по модулю 7.

Так как $2^2 \equiv 4 \pmod{7}$, $2^3 \equiv 1 \pmod{7}$, то число 2 не является первообразным корнем по модулю 7;

Так как $3^2 \equiv 2 \pmod{7}$, $3^3 \equiv -1 \pmod{7}$, то число 3 — наименьший первообразный корень по модулю 7.

Ответ: 3. ⊠

2.9. Индексы по простому модулю

Пусть a — первообразный корень по простому модулю p.

Определение 2.9.1. Если $a^k \equiv b \pmod{p}$, где k — целое неотрицательное число, то число k называется *индексом числа b по модулю p и первообразному корню (основанию) a* и обозначается $k = \mathrm{ind}_a b$ или $k = \mathrm{ind}\, b$. Таким образом, $a^{\mathrm{ind}_a b} \equiv b \pmod{p}$.

Так как НОД$(a,p)=1$, то НОД$(a^k,p)=1$. Значит, НОД$(b,p)=1$.

Теорема 2.9.1. Любое число b взаимно простое с p имеет бесконечное множество индексов по модулю p и первообразному корню a. Индексы каждого такого числа b представляют собой целые неотрицательные числа некоторого класса вычетов по модулю $p-1$

□. Если a — первообразный корень по модулю p, то $a^0,\ a^1, \ldots,\ a^{p-2}$ $(*)$ образуют приведённую систему вычетов по модулю p. Если число b взаимно просто с p, то в $(*)$ существует некоторое число $a^s,\ 0 \le s \le p-2$, принадлежащее тому же классу, что и b, т.е. $a^s \equiv b \pmod{p}$. Значит, существует, по крайней мере, один $\mathrm{ind}_a b = s$, причём $s \le p-2$. Если s' — другое число, для которого $a^{s'} \equiv b \pmod{p}$, то $a^s \equiv a^{s'} \pmod{p}$, т.е. $s \equiv s' \pmod{(p-1)}$. Следовательно, индексы каждого числа b, взаимно простого с p, являются целыми неотрицательными числами некоторого

класса вычетов по модулю $p-1$. Обычно из всех возможных значений индекса числа b по данному основанию a берут наименьшее; при таком выборе индексов они имеют значения, меньшие чем $p-1$. $\boxtimes$

Теорема 2.9.2. Индекс числа b по модулю p и первообразному корню a является также индексом и всех чисел из класса $\overline{b} \in \mathbb{Z}_p$.

$\square$. Пусть $\alpha \in \overline{b}$, т.е. $\alpha \equiv b \pmod{p}$. Если $\mathrm{ind}_a b = k$, то $a^k \equiv b \pmod{p}$. Тогда $a^k \equiv \alpha \pmod{p}$. Этот значит, что $k = \mathrm{ind}_a \alpha$. Поэтому число k можно назвать индексом класса $\overline{b} \in \mathbb{Z}_p$. $\boxtimes$

Лемма 2.9.1. (свойства индексов).

1. $\mathrm{ind}_a 1 \equiv 0 \pmod{(p-1)}$;
2. $\mathrm{ind}_a a \equiv 1 \pmod{(p-1)}$;
3. $c \equiv d \pmod{p} \Leftrightarrow \mathrm{ind}_a c \equiv \mathrm{ind}_a d \pmod{(p-1)}$;
4. $\mathrm{ind}_a(b_1 \cdot \ldots \cdot b_n) \equiv \mathrm{ind}_a b_1 + \ldots + \mathrm{ind}_a b_n \pmod{(p-1)}$;
5. $\mathrm{ind}_a b^n \equiv n \mathrm{ind}_a b \pmod{(p-1)}$;
6. $\mathrm{ind}_a \dfrac{b}{c} \equiv \mathrm{ind}_a b - \mathrm{ind}_a c \pmod{(p-1)}$.

$\square$. *Докажите самостоятельно.* $\boxtimes$

Очевидно, что понятие индекса аналогично понятию логарифма. Индексы имеют такие же приложения, как и логарифмы. Для практических целей составлены таблицы индексов и антииндексов, по по которым можно находить соответственно индекс по числу, или число по индексу. Эти таблицы помещаются в качестве приложения в конце каждого учебника по теории чисел. Таблицы индексов и антииндексов составлялись многими авторами. В 1839 г. таблицы индексов и антииндексов для простых модулей, меньших 1000, были опубликованы Якоби. Покажем на примере составление таблиц по одному из модулей.

Пример 2.9.1. 1. Построите таблицы индексов и антииндексов по модулю $p = 23$.

$\square$. В качестве основания a возьмём наименьший положительный первообразный корень по модулю 23.

Либо по таблице первообразных корней, либо путём непосредственного вычисления находим, что $a = 5$. Последовательно приводим по модулю 23 все степени 5 до $p - 2 = 21$ включительно:

$$\begin{array}{llll} 5^0 \equiv 1 & 5^5 \equiv 20 & 5^{10} \equiv 9 & 5^{16} \equiv 3 \\ 5^1 \equiv 5 & 5^6 \equiv 8 & 5^{11} \equiv 22 & 5^{17} \equiv 15 \\ 5^2 \equiv 2 & 5^7 \equiv 17 & 5^{12} \equiv 18 & 5^{18} \equiv 6 \\ 5^3 \equiv 10 & 5^8 \equiv 16 & 5^{13} \equiv 21 & 5^{19} \equiv 7 \\ 5^4 \equiv 4 & 5^9 \equiv 11 & 5^{14} \equiv 13 & 5^{20} \equiv 12 \\ & & 5^{15} \equiv 19 & 5^{21} \equiv 14 \end{array}$$

Получим таблицы:

а) таблица индексов

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) таблица антииндексов

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								

2. Найдём 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:

$$243 \equiv 13 \pmod{23}; \ \operatorname{ind} 243 = \operatorname{ind} 13 = 14.$$

3. Найдем числа N_1 и N_2, если известно, что $\operatorname{ind} N_1 = 8$, $\operatorname{ind} N_2 = 17$.

По таблице антииндексов находим, что $N_1 = 16$, $N_2 = 15$. ⊠

2.10. Двучленные сравнения. Квадратичные вычеты

Определение 2.10.1. Сравнение вида

$$ax^n \equiv b \pmod{p},\ a \not\equiv 0 \pmod{p}, n \in \mathbb{N} \tag{2.18}$$

называется *двучленным сравнением n-ой степени с одной переменной x по простому модулю p.*

Индексируем обе части сравнения (2.18) по модулю p и некоторому первообразному корню g. Получим равносильное ему сравнение:

$$\text{ind}_g\ a + n\text{ind}_g\ x \equiv \text{ind}_g\ b \pmod{(p-1)} \text{ или}$$

$$n\text{ind}_g\ x \equiv \text{ind}_g\ b - \text{ind}_g\ a \pmod{(p-1)}. \tag{2.19}$$

Таким образом, решение сравнения (2.18) сводится к решению сравнения (2.19) первой степени.

Если НОД$(n, p-1) = d$ и $c = \text{ind}_g\ b - \text{ind}_g\ a$ делится на d, то сравнение (2.19), а следовательно, и сравнение (2.18), имеет d решений; если же если c не делится на d, сравнение (2.19), а поэтому и сравнение (2.18), решений не имеет.

Пример 2.10.1. Решите сравнение

$$15x^4 \equiv 17 \pmod{23}.$$

□. Индексируем обе части сравнения по модулю 23:

$$\text{ind } 15 + 4\text{ind } x \equiv \text{ind } 17 \pmod{22}.$$

Из таблицы индексов для простого числа 23 находим, что ind $15 =$ $= 17$, ind $17 = 7$. Тогда получим сравнение первой степени относительно ind x, а именно, $4\text{ind } x \equiv 12 \pmod{22}$.

Последнее сравнение имеет два решения ind $x \equiv 3;\ 14 \pmod{22}$.

Теперь из таблицы антииндексов для простого числа 23 находим, что $x \equiv 10; 13 \pmod{23}$ — два решения данного сравнения.

Ответ: $x \equiv 10; 13 \pmod{23}$. ⊠

Умножим обе части сравнения (2.18) на такое число α, что $a\alpha \equiv 1 \pmod{p}$; получим: $a\alpha x^n \equiv b\alpha \pmod{p}$, или

$$x^n \equiv c \pmod{p}, \tag{2.20}$$

где $b\alpha = c$.

Определение 2.10.2. Если сравнение (2.20) имеет решения, то c называется *вычетом степени n по простому модулю p*, в противном случае — *невычетом степени n*. Вычет (невычет) называется: при $n = 2$ *квадратичным*, при $n = 3$ *кубическим*, при $n = 4$ *биквадратным*.

Теорема 2.10.1. Число c является вычетом степени n по простому модулю p тогда и только тогда, когда

$$c^{\frac{p-1}{d}} \equiv 1 \pmod{p}, \tag{2.21}$$

где $d = \text{НОД}(n, p-1)$.

$\square$. Сравнение (2.20) равносильно такому:

$$n\text{ind } x \equiv \text{ind } c \pmod{(p-1)}. \tag{2.22}$$

Сравнение (2.22) первой степени относительно $\text{ind } x$ имеет решение тогда и только тогда, когда $\text{ind } c$ делится на d, $d = \text{НОД}(n, p-1)$. Значит, c есть вычет степени n по простому модулю p тогда и только тогда, когда $\text{ind } c \equiv 0 \pmod{d}$, что равносильно условию:

$$\frac{p-1}{d} \cdot \text{ind } c \equiv 0 \pmod{(p-1)}. \tag{2.23}$$

Но условие (2.23) есть «индексированная» запись условия (2.21). $\boxtimes$

Теорема 2.10.2. (критерий Эйлера). Число c является квадратичным вычетом по простому модулю p тогда и только тогда, когда

$$c^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

и квадратичным невычетом по простому модулю p тогда и только тогда, когда

$$c^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

$p > 2$, p не делит c.

Определение 2.10.3. *Показательным двучленным сравнением* называется сравнение вида

$$a \cdot c^x \equiv b \pmod{p}, \tag{2.24}$$

где p — простое число, $a \not\equiv 0 \pmod{p}$, $c \not\equiv 0 \pmod{p}$.

Индексируем обе части сравнения (2.24) по модулю p и некоторому

первообразному корню:

$$\text{ind } a + x\text{ind } c \equiv \text{ind } b \pmod{(p-1)}$$

или

$$x\text{ind } c \equiv \text{ind } b - \text{ind } a \pmod{(p-1)}. \tag{2.25}$$

Сравнение (2.25) является сравнением первой степени по модулю $p-1$. Решив его, найдем $x \geq 0$.

Пример 2.10.2. Решим сравнение $15 \cdot 7^{2x} \equiv 8 \cdot 3^{3x} \pmod{31}$.

□. Индексируя члены сравнения, получаем:

$$\text{ind } 15 + 2x\text{ind } 7 \equiv \text{ind } 8 + 3x\text{ind } 3 \pmod{30}$$

или $23x \equiv 21 \pmod{30}$.

Решая последнее сравнение, получим $x \equiv 27 \pmod{30}$.

Ответ: $x \equiv 27 \pmod{30}$. ⊠

2.11. Символ Лежандра

При изучении сравнений 2-й степени удобно пользоваться так называемым символом Лежандра. Введение этого символа, как будет видно из дальнейшего, значительно упрощает запись многих результатов и облегчает вычисления. Символ Лежандра для числа a по простому модулю $p > 2$ принято записывать в виде $\left(\frac{a}{p}\right)$, причем этот символ определяется следующим образом.

Определение 2.11.1. Пусть p — простое число, $p > 2$ и p не делит a. Символ Лежандра $\left(\frac{a}{p}\right)$ задается следующим образом:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{если } a \text{ – квадратичный вычет по модулю } p, \\ -1, & \text{если } a \text{ – квадратичный невычет по модулю } p. \end{cases}$$

Другими словами, $\left(\frac{a}{p}\right)$ равно 1, если сравнение $x^2 \equiv a \pmod{p}$ имеет два решения, и $\left(\frac{a}{p}\right)$ равно -1, если это сравнение не имеет решений.

Пример 2.11.1. $\left(\frac{3}{11}\right) = 1$, так как сравнение $x^2 \equiv 3 \pmod{11}$ име-

ет два решения: $x = \pm 5 \pmod{11}$; $\left(\frac{2}{5}\right) = -1$, так как сравнение $x^2 \equiv 2 \pmod 5$ не имеет решений.

Запишем ряд свойств символа Лежандра, непосредственно вытекающих из определения и ранее установленных свойств квадратичных вычетов и невычетов.

Теорема 2.11.1. Если $b \equiv a \pmod p$, то $\left(\frac{b}{p}\right) = \left(\frac{a}{p}\right)$.

$\square$. Если $\left(\frac{a}{p}\right) = 1$, т.е. a — квадратичный вычет по модулю p, то и любое $b \in \overline{a}$ тоже будет квадратичным вычетом по этому модулю, и $\left(\frac{b}{p}\right) = 1$. Если $\left(\frac{a}{p}\right) = -1$, то и весь класс $\overline{a}$ состоит из квадратичных невычетов по модулю p, т.е. при $b \equiv a \pmod p$, верно, что $\left(\frac{b}{p}\right) = -1$. $\boxtimes$

Теорема 2.11.2. $\left(\frac{a^2}{p}\right) = 1$.

$\square$. Сравнение $x^2 \equiv a^2 \pmod p$, p не делит a, имеет два решения: $x \equiv \pm a \pmod p$. В частности, $\left(\frac{1}{p}\right) = 1$. $\boxtimes$

Теорема 2.11.3. (критерий Эйлера).

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p.$$

$\square$. Если $\left(\frac{a}{p}\right) = 1$, т.е. если a — квадратичный вычет по модулю p, то по теореме 2.10.2 имеем:

$$a^{\frac{p-1}{2}} \equiv 1 = \left(\frac{a}{p}\right) \pmod p. \tag{2.26}$$

Если $\left(\frac{a}{p}\right) = -1$, т.е. если a — квадратичный невычет по модулю p, то

по теореме 2.10.2 имеем:

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

Таким образом, сравнение (2.26) верно для любого a, не делящегося на p. ⊠

Пример 2.11.2. $\left(\frac{3}{13}\right) \equiv 3^6 = 729 \equiv 1 \pmod{13}$, так что $\left(\frac{3}{13}\right) = 1$.

$\left(\frac{10}{17}\right) \equiv 10^8 \equiv (-2)^4 = 16 \equiv -1 \pmod{17}$, так что $\left(\frac{10}{17}\right) = -1$.

Теорема 2.11.4. $\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{если } p \equiv 1 \pmod 4, \\ -1, & \text{если } p \equiv 3 \pmod 4. \end{cases}$

□. Согласно теореме 2.11.3 имеем:

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

В левой и правой частях этого сравнения стоят величины, по абсолютной величине равные 1. Две такие величины могут быть сравнимы по модулю $p > 2$, только если они равны, т.е.

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}. \tag{2.27}$$

$(-1)^{\frac{p-1}{2}}$ равно 1 или -1, смотря по тому, будет ли $p \equiv 1 \pmod 4$ или $p \equiv 3 \pmod 4$. ⊠

Теорема 2.11.5.

$$\left(\frac{a_1 \cdot \ldots \cdot a_n}{p}\right) = \left(\frac{a_1}{p}\right) \cdot \ldots \cdot \left(\frac{a_n}{p}\right).$$

□. Согласно теореме 2.11.3 имеем:

$$\left(\frac{a_1 \cdot \ldots \cdot a_n}{p}\right) \equiv (a_1 \cdot \ldots \cdot a_n)^{\frac{p-1}{2}} = a_1^{\frac{p-1}{2}} \cdot \ldots \cdot a_n^{\frac{p-1}{2}} \equiv$$

$$\equiv \left(\frac{a_1}{p}\right) \cdot \ldots \cdot \left(\frac{a_n}{p}\right) \pmod{p}.$$

Очевидно, что $\left(\frac{a_1 \cdot \ldots \cdot a_n}{p}\right)$ и произведение $\left(\frac{a_1}{p}\right) \cdot \ldots \cdot \left(\frac{a_n}{p}\right)$ по абсолютной величине равны 1. Выше отмечено, что два таких числа сравнимы по модулю $p > 2$ только тогда, когда они равны. Следовательно,

$$\left(\frac{a_1 \cdot \ldots \cdot a_n}{p}\right) = \left(\frac{a_1}{p}\right) \cdot \ldots \cdot \left(\frac{a_n}{p}\right).$$

⊠

В частности, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. Таким образом, если $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, то $\left(\frac{ab}{p}\right) = 1$, а если $\left(\frac{a}{p}\right) = -\left(\frac{b}{p}\right)$, то $\left(\frac{ab}{p}\right) = -\left(\frac{a}{p}\right)^2 = -1$, т.е. произведение двух квадратичных вычетов или двух квадратичных невычетов по модулю p представляет собой квадратичный вычет по этому модулю, а произведение квадратичного вычета на невычет представляет собой квадратичный невычет.

Следствие 2.11.1. Если $\left(\frac{a}{p}\right) = 1$, то $\left(\frac{a^s}{p}\right) = 1$ для любого $s \geq 0$, т.е. любая степень квадратичного вычета представляет собой квадратичный вычет по рассматриваемому модулю.

Пример 2.11.3. Найдите все квадратичные вычеты по модулю 23.

□. Так как $5^2 \equiv 2 \pmod{23}$, то 2 является квадратичным вычетом по модулю 23. Беря степени 2, находим последовательно классы квадратичных вычетов по модулю 23:

$$\overline{2}, \overline{4}, \overline{8}, \overline{16}, \overline{2 \cdot 16} = \overline{9}, \overline{2 \cdot 9} = \overline{18}, \overline{2 \cdot 18} = \overline{13}, \overline{2 \cdot 13} = \overline{3}, \overline{2 \cdot 3} = \overline{6}, \overline{2 \cdot 6} = \overline{12},$$

$$\overline{2 \cdot 12} = \overline{1}.$$

Мы нашли $11 = \frac{23-1}{2}$ классов квадратичных вычетов, т.е. все такие классы.

Ответ: $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{6}$, $\overline{8}$, $\overline{9}$, $\overline{12}$, $\overline{13}$, $\overline{16}$, $\overline{18}$. ⊠

Следующий критерий, установленный впервые Гауссом, дает новый, отличный от критерия Эйлера, способ выяснять, является ли некоторое число a квадратичным вычетом или невычетом по простому модулю p.

Теорема 2.11.6. (критерий Гаусса). Для любого a, не делящегося на простой модуль p, $p > 2$, имеем:

$$\left(\frac{a}{p}\right) = (-1)^l,$$

где l – число чисел множества:

$$a,\ 2a,\ \ldots,\ \frac{p-1}{2} \cdot a,$$

у которых наименьший по абсолютной величине вычет по простому модулю p отрицателен.

Пример 2.11.4. Имеет ли решение сравнение $x^2 \equiv 6 \pmod{19}$?

$\square$. Находим наименьший по абсолютной величине вычет чисел $6s$ $(1 \leq s \leq 9)$, подчеркивая те из них, у которых ттакой вычет отрицателен:

$$6 \cdot 1 \equiv 6, \quad 6 \cdot 2 \equiv -7, \quad 6 \cdot 3 \equiv -1, \quad 6 \cdot 4 \equiv 5 \quad 6 \cdot 5 \equiv -8,$$
$$6 \cdot 6 \equiv -2, \quad 6 \cdot 7 \equiv 4, \quad 6 \cdot 8 \equiv -9, \quad 6 \cdot 9 \equiv -3. \pmod{19}.$$

Здесь $l = 6$. Поэтому $\left(\frac{6}{19}\right) = (-1)^6 = 1$. Значит, сравнение $x^2 \equiv 6 \pmod{19}$ имеет два решения.

Ответ: сравнение имеет два решения. $\boxtimes$

Теорема 2.11.7.

$$\left(\frac{2}{p}\right) \equiv \begin{cases} 1, & \text{если } p \equiv 1 \pmod 8 \text{ или } p \equiv 7 \pmod 8, \\ -1, & \text{если } p \equiv 3 \pmod 8 \text{ или } p \equiv 5 \pmod 8. \end{cases}$$

$\square$. Согласно критерию Гаусса (теорема 2.11.6) $\left(\frac{2}{p}\right) = (-1)^l$, где l — число чисел во множестве

$$1 \cdot 2,\ 2 \cdot 2,\ 3 \cdot 2,\ \ldots, \frac{p-1}{2} \cdot 2 = p - 1, \tag{2.28}$$

для которых наименьший по абсолютной величине вычет по модулю p отрицателен.

Числа, лежащие в интервале от 1 до $p-1$, имеют отрицательный наименьший по абсолютной величине вычет, если они больше, чем $\frac{p}{2}$. Согласно теореме 1.15.2 число четных положительных чисел, меньших или равных $\frac{p}{2}$, равно $\left[\frac{p}{4}\right]$. Во множестве (2.28) всего имеется $\frac{p-1}{2}$ чисел

и, таким образом, чисел, больших чем $\frac{p}{2}$, будет

$$l = \frac{p-1}{2} - \left[\frac{p}{4}\right].$$

При

$p = 8n+1 \Rightarrow \quad l = 4n - 2n = 2n,$
$p = 8n+3 \Rightarrow \quad l = (4n+1) - 2n = 2n+1,$
$p = 8n+5 \Rightarrow \quad l = (4n+2) - (2n+1) = 2n+1,$
$p = 8n+7 \Rightarrow \quad l = (4n+3) - (2n+1) = 2(n+1).$

Таким образом, $\left(\frac{2}{p}\right) = (-1)^l$ равно 1, для простых чисел p вида $8n+1$ или $8n+7$ и равно -1, для простых чисел p вида $8n+3$ или $8n+5$. ⊠

2.12. Арифметические приложения теории сравнений

Основные арифметические приложения теории сравнений следующие:

1) вычисление остатка;

2) признаки делимости;

3) обращение обыкновенной дроби в десятичную.

Признаки делимости.

Рассмотрим применение теории сравнений к выводу некоторых признаков делимости на данное натуральное число a. Отметим, что под признаком делимости на a понимают необходимое и достаточное условие делимости произвольного натурального числа n на a. Различают общие признаки, имеющие силу для любого a, и частные — для отдельных значений a.

Французский математик Блез Паскаль (1623–1662) нашел общий признак делимости.

Всякое натуральное число n в десятичной системе счисления можно записать в виде:

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + ... + a_1 \cdot 10 + a_0.$$

Составим число

$$m = a_k \cdot r_k + a_{k-1} \cdot r_{k-1} + ... + a_1 \cdot r_1 + a_0,$$

где $a_i, i = \overline{0,k}$ — цифры числа n, а $r_i, i = \overline{1,k}$ — абсолютно наименьшие вычеты соответствующих степеней 10^i по модулю a.

Теорема 2.12.1. (общий признак делимости Паскаля). Натуральное число n делится на натуральное число a тогда и только тогда, когда m делится на a.

□. **Необходимость.** Если n делится на a, то

$$n \equiv 0 \pmod{a}. \tag{2.29}$$

Кроме того, $10^i \equiv r_i \pmod{a}$, $i = \overline{1,k}$. Поэтому

$$n \equiv m \pmod{a}. \tag{2.30}$$

Из (2.29) и (2.30) следует, что $m \equiv 0 \pmod{a}$, т.е. m делится на a.
Достаточность. *Докажите самостоятельно.* ⊠

Из общего признака Паскаля вытекают различные частные признаки делимости. Рассмотрим некоторые из них, наиболее часто используемые в практике.

1) $a = 2$.

$10 \equiv 0 \pmod{2}$, $10^i \equiv 0 \pmod{2}$, $i = \overline{1,k}$. Тогда $r_i = 0$ и $m = a_0$. Следовательно, по теореме 2.12.1, n делится на 2 тогда и только тогда, когда a_0 делится на 2, т.е. натуральное число n делится на 2 тогда и только тогда, когда его последняя цифра a_0 делится на 2 (последняя цифра чётная).

2) $a = 3$.

$10 \equiv 1 \pmod{3}$, $10^i \equiv 1 \pmod{3}$, $i = \overline{1,k}$. Поэтому $r_i = 1$ и $m = a_k + a_{k-1} + ... + a_1 + a_0$. Тогда по теореме 2.12.1, n делится на 3 тогда и только тогда, когда $a_k + a_{k-1} + ... + a_1 + a_0$ делится на 3, т.е. натуральное число n делится на 3 тогда и только тогда, когда сумма его цифр делится на 3.

3) $a = 4$.

$10 \equiv 2 \pmod{4}$, $10^2 \equiv 0 \pmod{4}$, $10^i = 10^2 10^{i-2} \equiv 0 \pmod{4}$, $i = \overline{2,k}$. Значит, $r_1 = 2$, $r_i = 0$, $i = \overline{2,k}$ и $m = 2a_1 + a_0$. Таким образом, n делится на 4 тогда и только тогда, когда $2a_1 + a_0$ делится на 4, т.е. сумма удвоенной цифры десятков и цифры единиц числа n делится на 4.

4) $a = 5$.

$10 \equiv 0 \pmod 5$, $10^i \equiv 0 \pmod 5$, $i = \overline{1,k}$. Значит, $r_i = 0$ и $m = a_0$. Таким образом, n делится на 5 тогда и только тогда, когда a_0 делится на 5, т.е. последняя цифра числа n есть 0 или 5.

5) $a = 8$.

$10 \equiv 2 \pmod 8$, $10^2 \equiv 4 \pmod 8$, $10^3 \equiv 0 \pmod 8$, $10^i = 10^3 10^{i-3} \equiv 0 \pmod 8$, $i = \overline{3,k}$. Поэтому $r_1 = 2$, $r_2 = 4$, $r_i = 0$, $i = \overline{3,k}$ и $m = 4a_2 + 2a_1 + a_0$.

Таким образом, n делится на 8 тогда и только тогда, когда $4a_2 + 2a_1 + a_0$ делится на 8, т.е. сумма учетверенной цифры сотен, удвоенной цифры десятков и цифры единиц делятся на 8.

Покажите, что $4a_2 + 2a_1 + a_0$ делится на 8 тогда и только тогда, когда $100a_2 + 10a_1 + a_0 = \overline{a_2 a_1 a_0}$ делится на 8.

Поэтому n делится на 8 тогда и только тогда, когда число, записанное последними тремя цифрами числа n, делится на 8.

6) $a = 9$.

$10 \equiv 1 \pmod 9$, $10^i \equiv 1 \pmod 9$, $i = \overline{1,k}$. Значит, $r_i = 1$ и $m = a_k + a_{k-1} + ... + a_1 + a_0$. Таким образом, n делится на 9 тогда и только тогда, когда $a_k + a_{k-1} + ... + a_1 + a_0$ делится на 9, т.е. сумма цифр числа n делится на 9.

7) $a = 11$.

$10 \equiv -1 \pmod{11}$, $10^2 \equiv 1 \pmod{11}, \ldots$, т.е.

$$10^k \equiv \begin{cases} -1, \ k \text{ — нечетное} \\ 1, \ k \text{ — четное} \end{cases} \pmod{11}.$$

Поэтому $r_k = -1$, если k — нечетное; $r_k = 1$, если k — четное, и $m = (a_0 + a_2 + a_4 + ...) - (a_1 + a_3 + a_5 + ...)...$

Итак, по теореме 2.12.1, число n делится на 11 тогда и только тогда, когда разность между суммой цифр, стоящих на чётных местах и суммой цифр, стоящих на нечетных местах числа n, делится на 11.

Признаки делимости на 7 и 13 также следуют из признака Паскаля, но они получаются неудобными для практического использования.

Теорема 2.12.2. (общий признак делимости на 7, 11, 13). Натуральное число n делится на 7, 11, 13 тогда и только тогда, когда разность между числом, записанным последними тремя цифрами числа n и числом, записанным остальными его цифрами, делится на 7, 11, 13, т.е. $n = \overline{a_k a_{k-1} ... a_0}$

делится на 7, 11, 13 тогда и только тогда, когда $(\overline{a_2a_1a_0} - \overline{a_ka_{k-1}...a_3})$ делится на 7, 11, 13.

□. *Докажите самостоятельно.* ⊠

Теорема 2.12.3. (признак делимости на составное число). Если НОД$(a, b) = 1$, то $n \vdots (ab)$ тогда и только тогда, когда $n \vdots a$ и $n \vdots b$.

Обращение обыкновенной дроби в десятичную.

Применим некоторые из рассмотренных свойств сравнений к вопросу об обращении обыкновенной дроби в десятичную.

Утверждение 2.12.1. Несократимая обыкновенная дробь $\frac{a}{b}$ обращается в конечную десятичную дробь тогда и только тогда, когда каноническое разложение её знаменателя содержит лишь простые числа 2 или 5.

□. Доказательство проведем для положительной несократимой обыкновенной дроби.

Необходимость. Пусть дробь $\frac{a}{b}$ представляется в виде конечной десятичной дроби, т.е. $\frac{a}{b} = a_ka_{k-1}...a_0, b_1b_2...b_s = a_k10^k + ... + a_0 + b_110^{-1} + + ... + b_s10^{-s} = \frac{n}{10^s} = \frac{n}{2^s \cdot 5^s}$. Сократим дробь $\frac{n}{2^s \cdot 5^s}$, получим:

$$\frac{a}{b} = \frac{n_1}{2^{s_1} \cdot 5^{s_2}}, s_1, s_2 \in \mathbb{Z}, s_1, s_2 \geq 0. \tag{2.31}$$

Две положительные несократимые дроби равны тогда и только тогда, когда равны их числители и знаменатели (докажите). Поэтому из (2.31) следует, что $b = 2^{s_1} \cdot 5^{s_2}$, т.е. каноническое разложение знаменателя b содержит лишь простые множители 2 или 5.

Достаточность. Пусть каноническое разложение знаменателя дроби $\frac{a}{b}$ имеет вид: $b = 2^{s_1} \cdot 5^{s_2}$, $s_1, s_2 \in \mathbb{Z}, s_1, s_2 \geq 0$. Если $s_1 = s_2 = = s$, то $\frac{a}{b} = \frac{a}{10^s} = a_ka_{k-1}...a_0, b_1b_2...b_s$. Если же $s_1 > s_2$, то

$$\frac{a}{b} = \frac{a \cdot 5^{s_1-s_2}}{2^{s_1} \cdot 5^{s_2} \cdot 5^{s_1-s_2}} = \frac{a \cdot 5^{s_1-s_2}}{2^{s_1} \cdot 5^{s_1}} = \frac{n}{10^{s_1}} = a_ka_{k-1}...a_0, b_1b_2...b_{s_1}.$$

⊠

Следствие 2.12.1. Несократимая обыкновенная дробь $\frac{a}{b}$ обращается в бесконечную десятичную дробь тогда и только тогда, когда каноническое разложение её знаменателя содержит хотя бы одно простое число, отличное от 2 и 5.

Определение 2.12.1. Бесконечная десятичная дробь, у которой, начиная с некоторого десятичного знака, повторяется некоторая совокупность цифр, называется *бесконечной периодической дробью*. Повторяющаяся совокупность цифр называется *периодом*, а число цифр в периоде называется *длиной периода*. Записывается бесконечная периодическая дробь в виде $m, a_1...a_s(b_1...b_k)$, где m — её целая часть.

Определение 2.12.2. Бесконечная периодическая дробь называется *чистой периодической*, если период начинается с первого десятичного знака и *смешанной периодической* — если не с первого десятичного знака.

Обращение обыкновенной дроби в чистую периодическую дробь.

Теорема 2.12.4. Несократимая обыкновенная дробь $\frac{a}{b}$, знаменатель которой взаимно прост с 10, обращается в чистую периодическую дробь, длина периода которой равна порядку 10 по модулю b, т.е $\theta(10 \mod m)$.

$\square$. 1. Пусть $\frac{a}{b}$ — правильная несократимая дробь, знаменатель которой взаимно прост с 10. Тогда b не делится на 2 и b не делится на 5, т.е. каноническое разложение знаменателя не содержит простых множителей 2 и 5. Поэтому дробь $\frac{a}{b}$ обращается в бесконечную десятичную дробь. Покажем, что эта дробь будет чистой периодической, длина периода которой равна k, где $k = \theta\ (10 \mod b)$. Применим следующий алгоритм обращения обыкновенной дроби $\frac{a}{b}$ в десятичную: делим с остатком $10a$ на b : $10a = bq_1 + r_1$.

Так как НОД(b, r_1) = НОД$(10a, b)$ = 1, то $r_1 \neq 0$. Значит, $0 < r_1 < b$;

делим с остатком $10r_1$ на b : $10r_1 = bq_2 + r_2$. Аналогично, $0 < r_2 < b$;

делим с остатком $10r_2$ на b : $10r_2 = bq_3 + r_3$, где $0 < r_3 < b$;

. . . . . .

делим с остатком $10r_{k-1}$ на b : $10r_{k-1} = bq_k + r_k$, $0 < r_k < b$;

делим с остатком $10r_k$ на b : $10r_k = bq_{k+1} + r_{k+1}$, $0 < r_{k+1} < b$.

. . . . . .

Так как остатки в этом алгоритме не обращаются в 0, то он бесконечный. Разделим получающиеся равенства на $10b$:

$$\frac{a}{b} = \frac{q_1}{10} + \frac{r_1}{10b},$$
$$\frac{r_1}{b} = \frac{q_2}{10} + \frac{r_2}{10b},$$
$$\frac{r_2}{b} = \frac{q_3}{10} + \frac{r_3}{10b},$$

. . . . . .

$$\frac{r_{k-1}}{b} = \frac{q_k}{10} + \frac{r_k}{10b},$$

. . . . . .

$$\frac{a}{b} = \frac{q_1}{10} + \frac{q_2}{10^2} + \frac{q_3}{10^3} + \frac{r_3}{10^3 b} = ... =$$
$$= \frac{q_1}{10} + \frac{q_2}{10^2} + \frac{q_3}{10^3} + ... + \frac{q_k}{10^k} + \frac{r_k}{10^k b} = ... \ . \qquad (2.32)$$

Покажем, что все q_i — целые неотрицательные числа, меньше 10. Действительно, из первого равенства в описанном алгоритме $q_1 = \frac{10a - r_1}{b}$, где $0 < a < b$, $0 < r_1 < b$. Поэтому $-1 < q_1 < 10$. Из других равенств в алгоритме получаем $q_i = \frac{10r_{i-1} - r_i}{b}$, где $0 < r_{i-1} < b$, $0 < r_i < b$, $i = 2, 3, ...$ Отсюда $-1 < q_i < 10$.

Таким образом, $q_1, q_2, ..., q_k$ — k первых десятичных знаков бесконечной десятичной дроби, в которую обращается дробь $\frac{a}{b}$.

Покажем, что они будут повторяться, т.е. образуют период десятичной дроби, в которую обращается обыкновенная дробь $\frac{a}{b}$.

Равенство (2.32) умножим на $10^k b$:

$$a \cdot 10^k = b \cdot (q_1 \cdot 10^{k-1} + q_2 \cdot 10^{k-2} + ... + q_k) + r_k, 0 < r_k < b.$$

Значит, r_k — остаток от деления $10^k \cdot a$ на b. Поэтому $10^k \cdot a \equiv r_k \pmod{b}$. Так как $k = \theta(10 \mod b)$, то $10^k \equiv 1 \pmod{b}$.

Следовательно, $a \cdot 10^k \equiv a \pmod{b}$ и $r_k \equiv a \pmod{b}$. Тогда $r_k - a$ делится на b. Отсюда $\mid r_k - a \mid \geq b$ или $r_k - a = 0$. С другой стороны,

учитывая, что $0 < r_k < b$, $0 < a < b$, имеем $-b < r_k - a < b$, т.е. $\mid r_k - a \mid < b$.

Таким образом, $r_k - a = 0$, т.е. $r_k = a$. Поэтому $10r_k = 10a$; следовательно, $q_{k+1} = q_1$ и $r_{k+1} = r_1$. Тогда $10r_{k+1} = 10r_1$, значит, $q_{k+2} = q_2$ и т.д. Итак, десятичные знаки $q_1, q_2, ..., q_k$ будут повторяться. Они образуют период десятичной дроби, в которую обращается обыкновенная дробь $\frac{a}{b}$; длина периода равна k, где $k = \theta(10 \mod b)$.

2. Если дробь $\frac{a}{b}$ неправильная ($a > b$), то при обращении её в десятичную из неё предварительно выделяется целая часть: $\frac{a}{b} = m + \frac{a_1}{b} = m, (q_1, ..., q_k)$ – чистая периодическая дробь, где m — целая часть $\frac{a}{b}$, $\frac{a_1}{b}$ – правильная несократимая дробь. ⊠

Теорема 2.12.5. Несократимая обыкновенная дробь $\frac{a}{b}$, знаменатель которой $b = 2^\alpha \cdot 5^\beta \cdot b_1$, где α, β — целые неотрицательные числа, не равные 0 одновременно, НОД$(b_1, 10) = 1$, $b_1 \neq 1$, т.е. в каноническое разложение b входит хотя бы одно из простых чисел 2 и 5, а также хотя бы одно простое число, отличное от 2 и 5, обращается в смешанную периодическую дробь, у которой число знаков до периода равно наибольшему из чисел α и β, а длина периода равна $\theta(10 \mod b_1)$.

□. Обозначим через n наибольшее из чисел α и β, и рассмотрим дробь:

$$\frac{10^n a}{b} = \frac{2^n \cdot 5^n \cdot a}{2^\alpha 5^\beta b_1} = \frac{2^{n-\alpha} \cdot 5^{n-\beta} \cdot a}{b_1} = \frac{a_1}{b_1}.$$

Так как НОД$(a, b) = 1$, то НОД$(a, b_1) = 1$. По условию НОД$(10, b_1) = 1$. Значит, НОД$(2, b_1) = 1$, НОД$(5, b_1) = 1$. Следовательно, НОД$(2^{n-\alpha}, b_1) = 1$, НОД$(5^{n-\beta}, b_1) = 1$, НОД$(a_1, b_1) = 1$, т.е. дробь $\frac{a_1}{b_1}$ несократима, причем НОД$(b_1, 10) = 1$.

По теореме 2.12.4 дробь $\frac{a_1}{b_1}$ обращается в чистую периодическую дробь, длина периода которой равна $\theta(10 \mod b_1)$, т.е. $\frac{10^n a}{b} = \frac{a_1}{b_1} = l, (q_1 ... q_k)$, где l — целая часть $\frac{a_1}{b_1}$.

Отсюда $\frac{a}{b} = \frac{l,(q_1...q_k)}{10^n} = m,\, m_1...m_n(q_1...q_k)$, где m – целая часть $\frac{a}{b}$. Таким образом, получили смешанную периодическую дробь с n десятичными знаками до периода и длиной периода $k = \theta(10 \mod b_1)$. ⊠

Следствие 2.12.2. Всякая несократимая обыкновенная дробь обращается или в конечную десятичную дробь или в бесконечную периодическую дробь, причём длина периода не зависит от числителя дроби, а зависит только от её знаменателя.

Пример 2.12.1. Найти длину периода при обращении следующих обыкновенных дробей в десятичные:

1) несократимой дроби со знаменателем $b = 41$.

2) несократимой дроби со знаменателем $b = 1260$.

□. 1. Так как НОД$(41, 10) = 1$, то по теореме 2.12.4 данная дробь обращается в чистую периодическую дробь, длина периода которой равна $\theta(10 \mod 41)$. Известно, что $\theta(10 \mod 41)$ является делителем $\varphi(41) = 40$, т.е. одним из чисел $1, 2, 4, 5, 8, 10, 20, 40$. Испытывая эти числа, получаем: $\theta(10 \mod 41) = 5$.

2. $b = 2^2 \cdot 5 \cdot 3^2 \cdot 7$, т.е. каноническое разложение b входят простые числа 2 и 5, а также простые числа 3 и 7. Поэтому по теореме 2.12.5 данная дробь обращается в смешанную периодическую, у которой число десятичных знаков до периода равно 2, а длина периода равна $\theta(10 \mod 63) = 6$.

Ответ: 1) 5; 2) 6. ⊠

2.13. Обращение периодических дробей в обыкновенные

Теорема 2.13.1. Чистая периодическая дробь $0,(b_1 \dots b_k)$ равна обыкновенной дроби, числитель которой есть период, а знаменатель записан столькими девятками, какова длина периода, т.е.

$$0,(b_1 \dots b_k) = \frac{\overline{b_1 \dots b_k}}{\underbrace{9 \dots 9}_{k}}.$$

□. Очевидно, что $0,(b_1 \dots b_k) = 0,b_1 \dots b_k b_1 \dots b_k \dots = 0,\overline{b_1 \dots b_k} +$

$$+ 0,\underbrace{0 \dots 0}_{k} b_1 \dots b_k + 0,\underbrace{0 \dots 0}_{2k} b_1 \dots b_k + \dots = \frac{\overline{b_1 \dots b_k}}{10^k} + \frac{\overline{b_1 \dots b_k}}{10^{2k}} + \frac{\overline{b_1 \dots b_k}}{10^{3k}} +$$

$+\ldots=$ [сумма бесконечно убывающей геометрической прогрессии $S=$ $=\dfrac{a_1}{1-q}$, где $a_1=\dfrac{\overline{b_1\ldots b_k}}{10^k}$, $q=\dfrac{1}{10^k}$] $=\dfrac{\overline{b_1\ldots b_k}}{10^k}\cdot\dfrac{1}{1-\dfrac{1}{10^k}}=\dfrac{\overline{b_1\ldots b_k}}{10^k-1}=$ $=\dfrac{\overline{b_1\ldots b_k}}{\underbrace{9\ldots9}_{k}}$. ⊠

Пример 2.13.1. $0,(321)=\dfrac{321}{999}=\dfrac{107}{333}$.

Теорема 2.13.2. Смешанная периодическая дробь $0,a_1\ldots a_m(b_1\ldots b_k)$ равна обыкновенной дроби, числитель которой есть разность между числом, записанным десятичными знаками до второго периода и числом, записанным десятичными знаками до первого периода, а знаменатель записан столькими девятками, какова длина периода и столькими нулями, сколько десятичных знаков до первого периода, т.е.

$$0,a_1\ldots a_m(b_1\ldots b_k)=\frac{\overline{a_1\ldots a_mb_1\ldots b_k}-\overline{a_1\ldots a_m}}{\underbrace{9\ldots9}_{k}\underbrace{0\ldots0}_{m}}$$

□. $0,a_1\ldots a_m(b_1\ldots b_k)=0,a_1\ldots a_m+0,\underbrace{0\ldots0}_{m}b_1\ldots b_k+0,\underbrace{0\ldots0}_{k+m}b_1\ldots b_k+$ $+\ldots=\dfrac{\overline{a_1\ldots a_m}}{10^m}+\dfrac{\overline{b_1\ldots b_k}}{10^{m+k}}+\dfrac{\overline{b_1\ldots b_k}}{10^{m+2k}}+\dfrac{\overline{b_1\ldots b_k}}{10^{m+3k}}+\ldots=$ [члены, начиная со второго, образуют бесконечно убывающую геометрическую прогрессию со знаменателем $\dfrac{1}{10^k}$ и $a_1=\dfrac{\overline{b_1\ldots b_k}}{10^{m+k}}$] $=\dfrac{\overline{a_1\ldots a_m}}{10^m}+\dfrac{\overline{b_1\ldots b_k}}{10^{m+k}}\cdot\dfrac{1}{1-\dfrac{1}{10^k}}=$ $=\dfrac{\overline{a_1\ldots a_m}}{10^m}+\dfrac{\overline{b_1\ldots b_k}}{10^m(10^k-1)}=\dfrac{\overline{a_1\ldots a_m}\cdot10^k-\overline{a_1\ldots a_m}+\overline{b_1\ldots b_k}}{10^m(10^k-1)}=$ $=\dfrac{\overline{a_1\ldots a_mb_1\ldots b_k}-\overline{a_1\ldots a_m}}{\underbrace{9\ldots9}_{k}\underbrace{0\ldots0}_{m}}$. ⊠

Пример 2.13.2. $0,12(3)=\dfrac{123-12}{900}=\dfrac{111}{900}=\dfrac{37}{300}$.

ЛИТЕРАТУРА

1. Айерлэнд, К. Классическое введение в современную теорию чисел / К. Айерлэнд, М. Роузен - М.: Мир, 1987. — 416 с.

2. Алфутова, Н.Б. Алгебра и теория чисел. Сборник задач для математических школ / Н.Б. Алфутова, А.В. Устинов. — М.: МЦНМО, 2002. — 264 с.

3. Бухштаб, А.А. Теория чисел / А.А. Бухштаб. — М. : Уч.пед.издво, 1966. — 376 с.

4. Виноградов, И.М. Основы теории чисел / И.М. Виноградов. — М.: Наука, 1965. — 172 с.

5. Воробьев, Н. Н. Признаки делимости / Н.Н. Воробьев. — М.: Наука, 1988. — 96 с.

6. Базылев, Д.Ф. Справочное пособие к решению задач: диофантовы уравнения / Д.Ф. Базылев. — Мн.: НТЦ "АПИ 1999. — 160 с.

7. Грибанов, В.У. Сборник задач по теории чисел / В.У. Грибанов, П.И. Титов — М. : Просвещение, 1964. — 144 с.

8. Кострикин, А.И. Введение в алгебру. Основы алгебры : Учебник для вузов. — М. : Физмалит, 1994. — 320 с.

9. Коутинхо, С. Введение в теорию чисел. Алгоритм RSA / С. Коутинхо. — М. : Постмаркет, 2001. — 328 с.

10. Кудреватов, Г.А. Сборник задач по теории чисел / Г.А. Кудреватов. — М.: Просвещение, 1970. — 128 с.

11. Куликов, Л.Я. Алгебра и теория чисел / Л.Я. Куликов. — М. : Высшая школа, 1979. — 559 с.

12. Курош, А.Г. Курс высшей алгебры / А.Г. Курош. М. : Наука, 1975. — 431 с.

13. Монахов, В.С. Алгебра и теория чисел : практикум : учеб. пособие. В 2 ч. Ч. 1 / В.С. Монахов, А.В. Бузланов. — Минск : Изд. центр БГУ, 2007. — 264 с.

14. Монахов, В.С. Числовые функции и классы вычетов : практикум / В.С. Монахов, А.А. Трофимук; Брест. гос. ун-т имени А.С. Пушкина. — Брест : БрГУ, 2012. — 88 с.

15. Нестеренко, Ю.В. Теория чисел : учебник для студ. высш. учеб. заведений / Ю.В. Нестеренко. — М.: Издательский центр «Академия», 2008. — 272 с.

16. Окунев, Л.Я. Краткий курс теории чисел / Л.Я. Окунев. — М.: Уч. пед. изд-во, 1956. — 240 с.

17. Окунев, Л.Я. Целые комплексные числа / Л.Я. Окунев. — М.: Учпедгиз, 1941. — 54 с.

18. Сизый, С.В. Лекции по теории чисел: Учебное пособие для математических специальностей / С.В. Сизый. — Екатеринбург : Уральский государственный университет им. А. М. Горького, 1999. — 136 с.

19. Шмигирев, А.Э. Теория чисел : тексты лекций и индивидуальные задания / А.Э. Шмигирев, Э.Ф. Шмигирев, М.И. Ефремова. — Мозырь : УО МГПУ им. И.П. Шамякина, 2006. — 78 с.

20. Шнеперман, Л.Б. Сборник задач по алгебре и теории чисел / Л.Б. Шнеперман. Минск : Высшая школа, 1983. — 223 с.