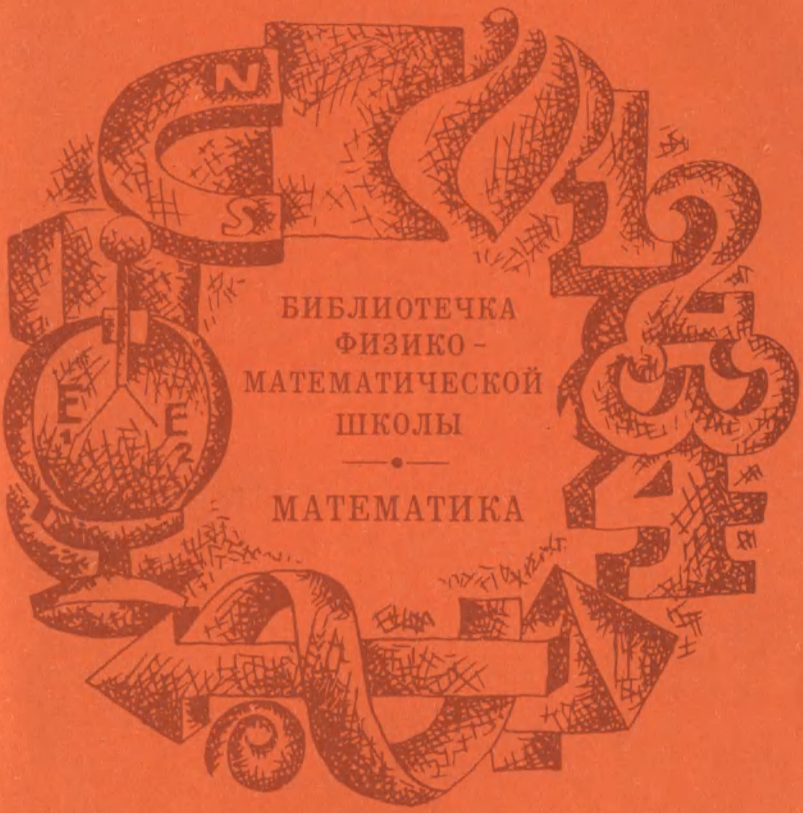

А. А. БЕЛЬСКИЙ, Л. А. КАЛУЖНИН

ДЕЛЕНИЕ С ОСТАТКОМ

БИБЛИОТЕЧКА ФИЗИКО-МАТЕМАТИЧЕСКОЙ ШКОЛЫ
МАТЕМАТИКА

А. А. БЕЛЬСКИЙ, Л. А. КАЛУЖНИН

ДЕЛЕНИЕ С ОСТАТКОМ

Издательское объединение «Вища школа»
Головное издательство
Киев — 1977

517.1
Б44

УДК 511

Деление с остатком. Бельский А. А., Калужнин Л. А. Издательское объединение «Вища школа», 1977, 72 с.

В книге освещены некоторые важные вопросы теории чисел. Приведено доказательство теоремы о единственности разложения на простые множители, рассмотрены алгоритм Евклида, диафантовые уравнения, арифметики целых комплексных чисел и классов вычетов, представление чисел в различных позиционных системах и др.

Рассчитана на учащихся физико-математических школ. Книгой могут пользоваться учителя математики и учащиеся старших классов общеобразовательных школ.

Ил. 3. Список лит. 10

Редакция литературы по математике и физике
Зав. редакцией *А. С. Макуха*

Б $\frac{20203-124}{M211(04)-77}$ 152—77

Глава I

ОСНОВНАЯ ТЕОРЕМА АРИФМЕТИКИ

Эту теорему учащиеся хорошо знают и часто пользуются ею при арифметических вычислениях (например, при нахождении общего знаменателя дробей), не осознавая порой того, что речь идет о важной теореме, требующей строгого и подробного доказательства. Имеется в виду следующее: каждое целое число мы умеем раскладывать в произведение простых чисел. Например,

$$420 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 7. \qquad (1)$$

При этом, если число достаточно велико, то для нахождения соответствующего разложения нужно иногда потратить немало времени, тем не менее, мы всегда это разложение получаем. Но, может быть, нам до сих пор просто везло? Уверены ли мы в том, что любое целое число можно всегда представить в виде произведения простых чисел? Это действительно так, но этот факт требует доказательства. Первую часть основной теоремы как раз и составляет утверждение:

Всякое целое число может быть представлено в виде произведения простых чисел.

Доказательство этого утверждения приводится ниже.

Прежде чем сформулировать второе утверждение теоремы, обратимся опять к примеру разложения числа 420 на простые сомножители. В школе этот процесс записывается так:

420	2
210	2
105	3
35	5
7	7
1	,

что и дает разложение (1). Но может быть существуют и другие методы разложения? Как знать, дадут ли они тот же результат? Естественно, например, пытаться разло-

жить данное число в произведение двух меньших чисел (не обязательно взаимно простых), а затем каждое из них — в произведение меньших чисел и т. д. до тех пор, пока мы не придем к числам, уже не разложимым далее, т. е. к простым. Однако уже после первого шага ясно, что такой процесс неоднозначен. Действительно, для того же числа 420 имеем:

$$420 = 20 \cdot 21, \quad 420 = 15 \cdot 28.$$

Таким образом, совершенно естественен вопрос: быть может существуют целые числа, которые можно разложить различными способами в произведение простых чисел? Оказывается, что таких чисел нет, и соответствующее утверждение — утверждение об однозначности разложения числа в произведение простых сомножителей — составляет как раз вторую часть основной теоремы:

Если некоторое число n разложимо двумя способами в произведение простых сомножителей

$$n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_l,$$

то эти разложения совпадают с точностью до порядка сомножителей: оба они имеют одно и то же число сомножителей, т. е. $k = l$, и каждый сомножитель, встречающийся в первом разложении, встречается столько же раз во втором[1].

Доказательство этого утверждения мы приведем довольно подробно. Оно сложнее, чем доказательство первого утверждения, так как связано с рядом свойств арифметики целых чисел.

§ 1. ДЕЛЕНИЕ С ОСТАТКОМ И НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ (НОД) ДВУХ ЧИСЕЛ

Исходными для наших последующих рассуждений является утверждение о возможности «деления с остатком» в области целых чисел. Это утверждение формулируется так:

---

[1] Если рассматривать любые целые числа (как положительные, так и отрицательные), то под единственностью разложения на простые множители следует понимать, что два разложения $n = p_1 p_2 \dots p_k$ и $n = q_1 q_2 \dots q_l$ могут отличаться не только порядком сомножителей, но и знаками соответствующих сомножителей.

Теорема 1. *Пусть a и b — целые числа и $b \neq 0$. Тогда существуют такие целые числа q и r, причем $0 \leqslant r < |b|$, что*

$$a = qb + r. \tag{1}$$

Числа q и r определяются по a и b однозначно, т. е. если

$$a = q_1 b + r_1 = q_2 b + r_2,$$

где $0 \leqslant r_i < |b|$, $i = 1, 2$, то $q_1 = q_2$ и $r_1 = r_2$. Если в равенстве (1) $r = 0$, то это означает, что число a делится на число b и соответственно записывается

$$b \mid a.$$

Примечание. Для двух целых чисел a и b выражения «число a делится на число b», «число a — кратное числа b», «число b является делителем числа a» или, наконец, «число b делит число a» имеют один и тот же смысл; мы будем пользоваться каждым из них.

Докажем возможность представления (1). Пусть сначала $b > 0$. Заметим, что для каждого рационального числа τ (как, впрочем, и для любого вещественного числа) существует такое целое число t, что $t \leqslant \tau < t + 1$. В частности, предположим, что такое целое t найдено для $\tau = \frac{a}{b}$

$$t \leqslant \frac{a}{b} < t + 1.$$

Отсюда

$$bt \leqslant a < bt + b \text{ и } 0 \leqslant a - bt < b.$$

Пусть $q = t$ и $r = a - bt$, тогда $a = bq + r$ и при этом, как вытекает из последнего неравенства, $0 \leqslant r < b$. Мы получили представление (1) для случая $b > 0$.

Пусть теперь $b < 0$; вновь отметим, что существует такое целое число t, что

$$t < \frac{a}{b} \leqslant t + 1.$$

Умножая это неравенство на b и учитывая, что $b < 0$, получим: $b(t + 1) \leqslant a < bt$, откуда $0 \leqslant a - b(t + 1) < -b$. Пусть $q = t + 1$ и $r = a - b(t + 1)$. Представление (1) вновь получено: $a = bq + r$, где $0 \leqslant r < -b$, т. е. $0 \leqslant r < |b|$.

Остается доказать единственность. Пусть

$$a = q_1 b + r_1 = q_2 b + r_2.$$

Тогда $b(q_1 - q_2) = r_2 - r_1$. Так как $0 \leqslant r_i < |b|$, то разность $r_2 - r_1$ по абсолютной величине будет меньше, чем $|b|$ и, следовательно, деление на b здесь возможно лишь при условии, что $r_2 - r_1 = 0$. Но если $r_1 = r_2$, то $q_1 b = q_2 b$ и, таким образом, $q_1 = q_2$.

Число q называют частным, а число r — остатком от деления числа a на число b.

При помощи теоремы 1 можно ввести понятие наибольшего общего делителя двух чисел и доказать ряд его свойств.

Определение 1. *Если a и b — два целых числа, отличных от нуля, и если число c таково, что $c|a$ и $c|b$, то c называется общим делителем чисел a и b.*

Заметим, что любые два числа всегда имеют общие делители: ими являются числа 1 и -1. Если других общих делителей нет, то числа a и b называются взаимно простыми. О взаимно простых числах речь будет идти ниже.

Определение. 2. *Число d называется наибольшим общим делителем (НОД) чисел a и b, если* 1) *d является общим делителем чисел a и b и* 2) *d делится на любой другой общий делитель чисел a и b.*

Так, например, 6 есть НОД чисел 18 и 30, так как $6|18$ и $6|30$ и, с другой стороны, 6 делится на все общие делители этих чисел: 1, -1, 2, -2, 3, -3, 6, -6.

Из этого определения непосредственно не вытекает, что для произвольных двух чисел a и b НОД всегда существует. Мы сейчас докажем, что это действительно так; при этом мы не будем использовать разложение чисел a и b на простые множители.

Теорема 2. *Для любой пары целых чисел $a \neq 0$ и $b \neq 0$ существует НОД.*

Доказательство. Наряду с числами a и b мы будем рассматривать всевозможные числа вида $xa + yb$, где x и y какие-либо целые числа. Числа такого вида:

$$v = xa + yb \qquad (2)$$

называют *линейными комбинациями* чисел a и b. Например, для $a = 6$, $b = 22$ линейными комбинациями будут числа $28 = 1 \cdot 6 + 1 \cdot 22$, $10 = (-2) \cdot 6 + 1 \cdot 22$, $-92 = 3 \cdot 6 + (-5) \cdot 22$ и т. д. Вообще для заданных чисел a и b существует бесконечно много чисел, являющихся их линейными комбинациями. Обозначим множество таких чисел через M. Заметим, что множество M содержит,

в частности, и сами числа a (при $x = 1$, $y = 0$) и b (при $x = 0$, $y = 1$), а также число 0 (при $x = 0$, $y = 0$). Все числа v из множества M являются, очевидно, целыми числами. Если v принадлежит M, то и $-v$ тоже принадлежит M (если $v = xa + yb$, то $-v = (-x)a + (-y)b$). Отметим еще одно свойство чисел v из M, которое мы будем использовать: *все эти числа делятся на все общие делители чисел a и b*. Действительно, если $c \mid a$ и $c \mid b$ и пусть $a = a' \cdot c$ и $b = b' \cdot c$, то $v = xa + yb = xa'c + yb'c = (xa' + yb')c$, т. е. $c \mid v$. Пусть теперь $d \neq 0$ — наименьшее по модулю число среди всех чисел из M, отличных от 0.

Такое число во множестве M действительно существует. Заметим, что во множестве M содержатся числа, не равные нулю (например, a или b), а их модули — положительные целые, т. е. натуральные, числа. Но одно из основных свойств натуральных чисел, принимаемое обычно за аксиому (см. И. С. Соминский, «Метод математической индукции», с. 9, замечание), состоит в том, что во всякой непустой совокупности натуральных чисел всегда содержится наименьшее число.

Покажем, что d является НОД чисел a и b. Свойством 2) определения НОД оно обладает, так как им обладают все числа из M. Нужно только еще установить, что оно обладает и свойством 1), т. е. что d является общим делителем чисел a и b. Покажем, что $d \mid a$. Так как d принадлежит M, то $d = sa + tb$, где s и t — целые числа. Разделим a на d с остатком, т. е. найдем такие числа q и r, $0 \leqslant r < |d|$, что

$$a = qd + r.$$

Но тогда и остаток r должен принадлежать множеству M. Действительно,

$$r = a - qd = a - q(sa + tb) = (1 - qs)a + tb.$$

Вспомним теперь, что d — наименьшее по модулю число среди отличных от нуля чисел множества M, а число r меньше $|d|$. Следовательно, $r = 0$ и $d \mid a$. Аналогично доказывается, что $d \mid b$. Теорема доказана.

Мы установили существование НОД двух целых чисел, отличных от нуля. Из доказательства теоремы вытекает следующая теорема:

Теорема 3. *НОД чисел a и b можно представить в виде линейной комбинации этих чисел.*

Возникает вопрос: определен ли НОД чисел a и b однозначно? Ответ, конечно, отрицательный: если число

d обладает свойствами 1) и 2) определения НОД, то и $-d$ тоже ими обладает. Но этим неоднозначность исчерпывается. Действительно, пусть d и d' — два НОД чисел a и b. Так как d обладает свойством 2), а d' — свойством 1), то $d' \mid d$. Но аналогично, $d \mid d'$. Итак, $\alpha = \frac{d}{d'}$ и $\frac{d'}{d} = \frac{1}{d/d'} = \frac{1}{\alpha}$ — целые числа. Но единственные целые числа, обратные от которых также целые, — это числа 1 и —1. Итак, $\alpha = 1$ или $\alpha = -1$, откуда $d' = d$ или $d' = -d$. Если бы в определении НОД было условие, что это число должно быть положительным (это иногда бывает удобным), то можно было бы сказать, что НОД двух отличных от нуля целых чисел существует и однозначно определен.

В дальнейшем мы будем обозначать НОД чисел a и b через (a, b), как это обычно принято в литературе по теории чисел.

Перейдем к рассмотрению пар взаимно простых чисел. Мы уже встречались с этим понятием.

Определение 3. *Целые числа $a \neq 0$ и $b \neq 0$ называются взаимно простыми, если их НОД равен* 1.

Иными словами, можно сказать, что взаимно простые числа — это такие числа, единственными общими делителями которых являются числа 1 и —1.

Из сказанного выше (теорема 3) следует, что если $(a, b) = 1$, то 1 можно представить в виде:

$$1 = sa + tb, \tag{3}$$

где s и t — целые числа. Обратно, если равенство (3) выполняется для соответственных s и t, то a и b взаимно просты. Действительно (см. доказательство теоремы 1), $d = (a, b)$ — это наименьшее по модулю число среди отличных от нуля чисел вида $xa + yb$. Следовательно, если (3) выполняется, то $|d| \leqslant 1$ и $d \neq 0$, так что $d = \pm 1$.

Из сказанного непосредственно вытекает важнейшее свойство взаимно простых чисел:

Теорема 4. *Если $a \mid bc$ и $(a, b) = 1$, то $a \mid c$* (это свойство читается так: *если число a делит произведение двух чисел и взаимно просто с одним из сомножителей, то оно делит другой сомножитель*).

Доказательство. Так как $(a, b) = 1$, то найдутся такие числа s и t, что

$$1 = sa + tb. \tag{4}$$

Умножим последнее равенство на c. Имеем:

$$c = (sc)\,a + t\,(bc).$$

Оба слагаемых в правой части делятся на a, следовательно, c делится на a.

Теорема 5. *Если число a взаимно просто с числами b и c, то оно взаимно просто с произведением bc.*

Доказательство. Так как $(a, b) = 1$, то найдутся целые числа s и t, удовлетворяющие равенству

$$1 = sa + tb.$$

Аналогично, так как $(a, c) = 1$, то

$$1 = ua + vc$$

для соответственных u и v. Перемножив почленно два последних равенства, получим:

$$1 = (sa + tb)(ua + vc) = sua^2 + savc + tbua + tbvc = \\ = (sua + svc + tbu)\,a + (tv)\,(bc).$$

Пусть $m = sua + svc + tbu$ и $n = tv$, тогда m и n — целые числа и

$$1 = ma + n\,(bc),$$

следовательно, a и b — взаимно просты.

Утверждение только что доказанной теоремы легко обобщается на произвольное число сомножителей:

Теорема 6. *Если a взаимно просто с числами b_1, $b_2, \ldots, b_k$, то a взаимно просто с произведением b_1, $b_2, \ldots, b_k$.*

Доказательство этой теоремы проводится методом математической индукции по числу k сомножителей.

§ 2. ОСНОВНАЯ ТЕОРЕМА АРИФМЕТИКИ

Теорема. *Любое целое число, отличное от нуля, может быть представлено в виде произведения простых чисел, причем такое представление единственно с точностью до порядка сомножителей и их знаков.*

Доказательство. Существование разложения целого рационального числа в произведение простых чисел. Ограничимся сначала случаем положительных целых чисел.

Примечание. Число 1 по многим причинам не принято считать простым числом, несмотря на то, что оно не разложимо в произведение меньших чисел. Тогда возникает вопрос: в каком же смысле

указанная выше теорема верна для числа 1? Или, иначе, в каком смысле число 1 представимо в виде произведения простых чисел?

Мы будем считать, что $1 = 1$ и есть разложение числа 1 в произведение простых чисел, причем число простых сомножителей в правой части равно 0. Эта условность напоминает определение нулевой степени $a^0 = 1$ (число сомножителей a равно 0). Подобное соглашение мы принимаем и для числа -1.

Воспользуемся методом математической индукции:

а) Для $n = 1$ равенство $1 = 1$ и есть искомое представление: 1 является произведением пустого множества простых чисел.

б) Предположим, что для всех положительных чисел m меньших, чем n, разложимость в произведение простых чисел уже установлена. Докажем тогда, что и для числа n такая разложимость будет иметь место. Если n — простое число, то

$$n = n$$

и есть искомое разложение (один простой сомножитель). Если n сложное составное число, то оно является произведением $n = n_1 \cdot n_2$ двух целых чисел n_1 и n_2, каждое из которых отлично от 1 и от n и, следовательно, $n_1 < n$ и $n_2 < n$. Но тогда, по предположению индукции, разложимость чисел n_1 и n_2 в произведение простых чисел уже установлена:

$$n_1 = p_1 \cdot p_2 \cdot \ldots \cdot p_r,$$

$$n_2 = q_1 \cdot q_2 \cdot \ldots \cdot q_s,$$

где p_j и q_l — простые числа. Имеем: $n = p_1 \cdot p_2 \ldots p_r \times \times q_1 \cdot q_2 \ldots q_s$, т. е. мы получили искомое разложение числа n.

Пусть n — отрицательное целое число, тогда $-n$ — число положительное. Как уже доказано, $-n$ разложимо в произведение простых чисел:

$$-n = p_1 \cdot p_2 \cdot \ldots p_k,$$

$$\text{тогда } n = (-1)\, p_1 \cdot p_2 \cdot \ldots p_k,$$

или, например,

$$n = (-p_1)p_2 \cdot \ldots p_k$$

— искомое разложение числа n. Тем самым первая часть теоремы доказана.

Примечание. Доказательств единственности разложения существует довольно много. То, которое мы приведем, не самое короткое и не совсем простое. Однако наше доказательство имеет то преиму-

щество, что оно непосредственно обобщается на ряд других областей, например на область полиномов от одной переменной и на область целых комплексных чисел.

Доказательство единственности разложения целого рационального числа в произведение простых сомножителей.

Заметим, что по определению простого числа два различных простых числа взаимно просты. Доказательство однозначности разложения будем вести методом математической индукции по абсолютной величине числа n.

а) Если $|n| = 1$, то $n = \pm 1$ и $1 = 1$, $-1 = -1$, т. е. имеет место единственность разложения для чисел 1 и -1.

б) Предположим, что доказываемое свойство уже установлено для всех чисел m, для которых $|m| < |n|$. Пусть

$$n = p_1 \cdot p_2 \dots p_k = q_1 \cdot q_2 \dots q_l$$

— два разложения числа n в произведение простых чисел $p_1, p_2, \dots, p_k$ и $q_1, q_2, \dots, q_l$, соответственно. Мы утверждаем, что простое число p_k встречается среди простых чисел $q_1, \dots, q_l$ или, быть может, противоположно какому-то из них. Действительно, если бы это было не так, т. е. $p_k \neq q_i$, $i = 1, 2, \dots, l$, то p_k было бы взаимно просто со всеми числами q_i, а следовательно, согласно теореме 6, оно было бы взаимно просто с их произведением, т. е. с числом n. Но это невозможно, так как $p_k | n$, т. е. $(p_k, n) = p_k$. Итак, p_k равно какому-то из простых чисел $\pm q_i$. Пусть $p_k = q_i$ (в противном случае этого равенства можно было бы добиться перестановкой сомножителей q_i, а если все же $p_k = -q_i$, то мы изменили бы знаки у q_i и соответственно у какого-либо q_i).

Итак, получаем:

$$n = p_1 \cdot p_2 \dots p_{k-1} \cdot p_k = q_1 \cdot q_2 \dots q_{i-1} \cdot p_k,$$

откуда

$$m = \frac{n}{p_k} = p_1 \cdot p_2 \dots p_{k-1} = q_1 \cdot q_2 \dots q_{i-1}.$$

Но $|m| < |n|$ и, по предположению индукции, для m утверждение теоремы уже доказано, т. е. $k - 1 = l - 1$. Последовательности $p_1, p_2, \dots, p_{k-1}$ и $q_1, q_2, \dots, q_{i-1}$ содержат с точностью до знаков одни и те же простые числа, и соответствующие простые числа входят в оба представления одинаковое число раз, а так как $p_k = q_i$, то это же справедливо и для последовательностей $p_1, p_2, \dots, p_{k-1}, p_k$ и $q_1, q_2, \dots, q_{i-1}, q_i$. Теорема доказана.

§ 3. АЛГОРИТМ ЕВКЛИДА И РЕШЕНИЕ ЛИНЕЙНЫХ ДИОФАНТОВЫХ УРАВНЕНИЙ С ДВУМЯ НЕИЗВЕСТНЫМИ

Согласно теореме 2 два целых числа a и b имеют НОД. Рассмотрим сейчас один из способов нахождения НОД, который был указан еще в «Элементах» Евклида и называется алгоритмом Евклида. При этом будем считать, что $|a| \geqslant |b|$.

Первый шаг. Делим a на b с остатком:

$$(1) \qquad a = q_1 \cdot b + r_1, \quad 0 \leqslant r_1 < |b|.$$

Если $r_1 = 0$, то $b \mid a$ и $(a, b) = b$. Если $r_1 \neq 0$, то делаем следующее:

Второй шаг. Делим b на r_1:

$$(2) \qquad b = q_2 \cdot r_1 + r_2, \quad 0 \leqslant r_2 < r_1.$$

Если $r_2 \neq 0$, то переходим к третьему шагу:

Третий шаг.

$$(3) \qquad r_1 = q_3 \cdot r_2 + r_3, \quad 0 \leqslant r_3 < r_2$$

и т. д. На каждом шаге новый остаток меньше остатка на предыдущем шаге:

$$|b| > r_1 > r_2 > \ldots$$

и на каком-то k-м шаге ($k < |b|$) остаток станет равным нулю:

k-й шаг:

$$(k) \qquad r_{k-2} = q_{k_1} r_{k-1}.$$

Покажем, что последний, не равный нулю, остаток r_{k-1} является искомым НОД чисел a и b. Действительно, мы имеем цепочку равенств:

$$(1) \quad a = q_1 \cdot b + r_1;$$

$$(2) \quad b = q_2 \cdot r_1 + r_2;$$

$$(3) \quad r_1 = q_3 \cdot r_2 + r_3;$$

$$\vdots \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$(k-1) \quad r_{k-3} = q_{k-1} \cdot r_{k-2} + r_{k-1};$$

$$(k) \quad r_{k-2} = q_k \cdot r_{k-1}.$$

Из последнего равенства вытекает, что $r_{k-1} \mid r_{k-2}$, из предпоследнего — $r_{k-1} \mid r_{k-1}$ и $r_{k-1} \mid r_{k-2}$ и, следовательно,

$r_{k-1} | r_{k-3}$ и, поднимаясь, таким образом, к первым равенствам, заключаем, что $r_{k-1} | r_2$, $r_{k-1} | r_1$, $r_{k-1} | b$, $r_{k-1} | a$. Отсюда r_{k-1} является общим делителем чисел a и b.

Пусть теперь $c | a$ и $c | b$. Тогда из равенств (1), (2), ..., $(k-1)$ последовательно получаем: $c | r_1$, $c | r_2$, ..., $c | r_{k-1}$.

Таким образом, r_{k-1} — действительно НОД чисел a и b.

Рассмотрим пример: $a = 858$, $b = 253$. Найти НОД этих чисел.

Имеем:

(1) $858 = 3 \cdot 253 + 99$;

(2) $253 = 2 \cdot 99 + 55$;

(3) $99 = 1 \cdot 55 + 44$;

(4) $55 = 1 \cdot 44 + 11$;

(5) $44 = 4 \cdot 11$,

откуда $(858, 253) = 11$. Как видим, при помощи алгоритма Евклида НОД двух чисел находится без использования разложения этих чисел на простые сомножители.

В теореме 3 мы установили, что $(a, b) = d$ можно записать в виде:

$$d = s \cdot a + t \cdot b,$$

но в доказательстве не было никакого указания на то, как найти соответствующие числа s и t. Это очень просто сделать, применяя алгоритм Евклида. Мы не будем излагать это решение в общем случае, а разберем его на вышеприведенном примере.

Итак, нужно найти такие целые числа s и t, что

$$11 = s \cdot 858 + t \cdot 253.$$

Из равенств (4), (3), (2), (1) последовательно получаем:

$$11 = 55 + (-1) \cdot 44,$$
$$44 = 99 + (-1) \cdot 55,$$
$$55 = 253 + (-2) \cdot 99,$$
$$99 = 858 + (-3) \cdot 253.$$

Подставляя теперь в первое равенство выражение для 44 из второго, затем для 55 — из третьего и т. д., получим:

$$11 = 55 + (-1) \cdot (99 + (-1) \cdot 55) = 2 \cdot 55 + (-1) \cdot 99 =$$
$$= 2 \cdot (253 + (-2) \cdot 99) + (-1) \cdot 99 = 2 \cdot 253 + (-5) \cdot 99 =$$
$$= 2 \cdot 253 + (-5) \cdot (858 + (-3) \cdot 253) = (-5) \cdot 858 + 17 \cdot 253.$$

Следовательно, $s = -5$, $t = 17$.

Равенства, появляющиеся в алгоритме Евклида при нахождении НОД чисел a и b, позволяют решить в целых числах уравнение вида

$$d = xa + yb,$$

где $d = (a, b)$.

Вообще, уравнение вида

$$xa + yb = c,$$

где a, b, c — заданные целые числа, для которого надо найти целочисленное решение x, называется *линейным диофантовым уравнением* с двумя неизвестными. Линейным оно называется потому, что неизвестные x и y входят в него в первой степени. Термин «диофантово» указывает на то, что коэффициенты уравнения — целые числа и что решения также находятся целочисленные.

Примечание. «Диофантово» — по имени древнегреческого математика Диофанта, около 250 г. до н. э., который в своей книге «Арифметика» исследовал целочисленные уравнения; ниже мы остановимся на квадратичных диофантовых уравнениях.

Заметим, что мы уже умеем решать линейные диофантовы уравнения вида

$$xa + yb = c. \tag{1}$$

Но мы должны рассмотреть вопрос о всех решениях этого уравнения более детально. Отметим сначала, что не всякое уравнение такого вида имеет решение. Действительно, если уравнение (1) имеет решение в целых числах, например $x = x_0$, $y = y_0$, т. е. $c = x_0a + y_0b$, и если $d = (a, b)$, то, так как $d \mid a$, $d \mid b$, число d делит оба слагаемых в правой части и, следовательно, также делит c. Отсюда делаем вывод:

Для существования целочисленного решения уравнения (1) *необходимо, чтобы правая часть этого уравнения делилась на НОД чисел a и b.*

Например, уравнение

$$9x + 15y = 7$$

целочисленного решения не имеет, так как 7 не делится на $3 = (9, 15)$. Если же в уравнении (1) $d \mid c$, то это уравнение имеет целочисленное решение, и мы даже знаем, как такое решение найти. Действительно, пусть $c = c' \times d$ и пусть s и t — такие целые числа, что

$$d = a \cdot s + b \cdot t.$$

Тогда

$$c = c' \cdot d = a(sc') + b(t \cdot c'),$$

т. е. $x_0 = sc'$, $y_0 = t \cdot c'$ — решение уравнения (1).

Решим, например, диофантово уравнение

$$33 = 858x + 253y. \tag{2}$$

Выше мы показали, что

$$11 = 858 \cdot (-5) + 253 \cdot 17.$$

Умножая это равенство почленно на 3, получаем

$$33 = 858 \cdot (-15) + 253 \cdot 51.$$

Итак, $x = -15$, $y = 51$ — решение уравнения (2). Не следует думать, что найденное решение единственно. Вообще, оказывается, что если диофантово уравнение вида (1) имеет решение, то оно имеет бесконечно много решений. Мы сейчас исследуем этот вопрос более подробно: докажем сформулированное утверждение и найдем общий вид всевозможных решений уравнения (1).

Найдем сначала общий вид решения. Предположим, что уравнение (1) наряду с целочисленным решением x_0, y_0 имеет еще и решение x_1, y_1. Тогда

$$c = ax_0 + by_0;\ c = ax_1 + by_1.$$

Вычитая второе равенство из первого, получим:

$$a(x_0 - x_1) + b(y_0 - y_1) = 0,$$

или

$$a(x_0 - x_1) = b(y_1 - y_0). \tag{3}$$

Если $d = (a, b)$, то положим $a' = \frac{a}{d}$, $b' = \frac{b}{d}$, т. е.

$$a = a'd;$$
$$b = b'd,$$

где a' и b' — взаимно простые числа. Сокращая равенство (3) на d, приходим к равенству

$$a'(x_0 - x_1) = b'(y_1 - y_0).$$

Но так как a', b' взаимно просты, то $a' \mid (y_1 - y_0)$ и, аналогично, $b' \mid (x_0 - x_1)$. Пусть

$$y_1 - y_0 = a'k_1;$$
$$x_0 - x_1 = b'k_2,$$

имеем: $a'b' \cdot k_1 = a'b'k_2$, откуда $k_1 = k_2 = k$. Таким образом, окончательно получаем

$$y_1 = y_0 + a'k = y_0 + \frac{a}{d}k; \tag{4}$$

$$x_1 = x_0 - b'k = x_0 - \frac{b}{d}k, \tag{5}$$

где k — некоторое целое число. Обратно, легко проверить, что если x_0, y_0 — целочисленное решение уравнения (1), то все пары чисел вида (4) и (5) при любом целочисленном k дают решение уравнения (1). Действительно,

$$ax_1 + by_1 = a\left(x_0 - \frac{b}{d}k\right) + b\left(y_0 + \frac{a}{d}k\right) =$$

$$= ax_0 + by_0 + \left(-\frac{ab}{d}k + \frac{ab}{d}k\right) = c + 0 = c.$$

Итак, если x_0, y_0 — целочисленные решения уравнения (1), то все числа вида $x_0 - \frac{b}{d}k$, $y_0 + \frac{a}{d} \cdot k$, где k — любое целое число, являются также решениями этого уравнения (решений бесконечно много — по одному для каждого k) и других решений нет.

§ 4. ПИФАГОРОВЫ ТРОЙКИ

Метод, по которому были найдены решения линейного диофантова уравнения с двумя неизвестными, а главное — форма, в которой был дан ответ, применяются при решении следующей классической задачи:

Найти все тройки целых чисел a, b, c, для которых

$$a^2 + b^2 = c^2. \tag{1}$$

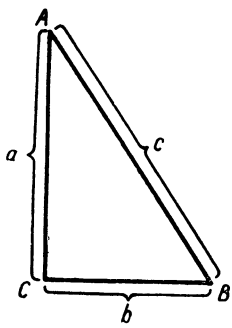

Рис. 1

Тройка таких чисел называется пифагоровой, потому что при ненулевых a, b, c, удовлетворяющих условию (1), всегда существует, и притом единственный, прямоугольный треугольник со сторонами a, b, c. В самом деле, если отложить отрезки a и b на сторонах прямого угла, как это показано на рис. 1, и соединить их концы A и B, то по теореме Пифагора $AB^2 = a^2 + b^2 = c^2$, т. е. $AB = c$. Единственность треугольника ABC при данных

a, b и c вытекает из признака равенства треугольников по трем сторонам. Итак, рассмотрим подробно пифагоровы тройки a, b, c, считая выполненным равенство (1).

Если $c = 0$, то обязательно $a = b = 0$. Поэтому достаточно взять лишь случай $c \neq 0$. Из равенства (1) получаем:

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1. \tag{2}$$

Положим $\frac{a}{c} = x$ и $\frac{b}{c} = y$. Тогда соотношение (2) принимает вид

$$x^2 + y^2 = 1. \tag{3}$$

Если мы сможем найти все рациональные (а не только целые) решения уравнения (3), то тем самым будет получен ответ на задачу о пифагоровых тройках. Действительно, если (x, y) — решение уравнения (3), то всякая тройка чисел $(\alpha x, \alpha y, \alpha)$ (где α такое целое число, что αx и αy тоже целые) будет пифагоровой: равенство $\alpha^2 x^2 + \alpha^2 y^2 = \alpha^2$ получается из (3) умножением его на α^2. Поэтому рассмотрим все рациональные решения уравнения (3).

Прежде всего, уравнение (3) эквивалентно уравнению

$$x^2 = 1 - y^2. \tag{3'}$$

Если из множества всех решений этого уравнения исключить решения $x = 0$, $y = \pm 1$, то все оставшиеся решения будут составлять множество решений уравнения

$$\frac{x}{1-y} = \frac{1+y}{x}. \tag{4}$$

Пусть

$$\frac{x}{1-y} = u, \quad \frac{1+y}{x} = v. \tag{5}$$

Числа u и v, очевидно, тоже рациональные, причем x и y выражаются через них так:

$$x = \frac{2u}{uv+1}, \quad y = \frac{uv-1}{uv+1}. \tag{6}$$

(Читатель легко проверит справедливость равенств (6), решив систему (5) относительно x и y). Уравнение (4) в терминах u и v выглядит совсем просто:

$$u = v. \tag{7}$$

Таким образом, если $(x = x_0,\ y = y_0)$ — решение уравнения (4), то $\left(u_0 = \frac{x_0}{1 - y_0},\ v_0 = \frac{1 + y_0}{x_0}\right)$ — решение уравнения (7) и обратно, если $(u_0,\ v_0)$ — решение уравнения (7), то (см. формулы (6) $\left(x_0 = \frac{2v_0}{u_0v_0 + 1},\ y_0 = \frac{u_0v_0 - 1}{u_0v_0 + 1}\right)$ — решение уравнения (4).

Но все решения уравнения (7) получаются так: надо неизвестным u и v придавать одинаковые и всевозможные рациональные значения. Следовательно, все решения уравнения (4) задаются формулами (6) при u и v, равных одному и тому же, но произвольному рациональному числу t:

$$\begin{cases} x = \frac{2t}{t^2 + 1}, \\ y = \frac{t^2 - 1}{t^2 + 1}. \end{cases} \tag{8}$$

Пусть $t = \frac{m}{n}$ — несократимая дробь. Тогда система (8) принимает вид

$$\begin{cases} x = \frac{2mn}{m^2 + n^2}, \\ y = \frac{m^2 - n^2}{m^2 + n^2}. \end{cases} \tag{9}$$

Таковы все рациональные числа x и y, которые удовлетворяют уравнению (4). Подставляя вместо m и n произвольные целые значения, одновременно не равные нулю, мы получаем решение уравнения (4). Заметим, что при $m = 0,\ n = 1$ имеем решение: $x = 0,\ y = -1$, а при $m = 1,\ n = 0$ — решение $x = 0,\ y = 1$. Оба эти решения раньше были исключены для законного выполнения преобразований, но теперь, как мы видим, они не утеряны. Итак, при любых целых m и n, одновременно не равных нулю, тройка целых чисел

$$2mn,\ m^2 - n^2,\ m^2 + n^2 \tag{10}$$

— пифагорова. Более того, как уже было сказано, пифагоровой является всякая тройка целых чисел

$$2\alpha mn,\quad \alpha(m^2 - n^2),\quad \alpha(m^2 + n^2) \tag{10'}$$

при любом допустимом рациональном числе α (в частности, и при $\alpha = 0$). Напомним, мы начали с равенства

(1) и затем последовательно перешли от него через равенства (2)—(8) к равенству (9), т. е. к равенствам

$$\frac{a}{c} = \frac{2mn}{m^2+n^2}, \qquad (9')$$
$$\frac{b}{c} = \frac{m^2-n^2}{m^2+n^2}.$$

Положим $a = 2mn\rho_1$, $b = (m^2 - n^2)\rho_2$, $c = (m^2 + n^2)\rho_3$ при некоторых рациональных числах ρ_1, ρ_2, ρ_3. Тогда из первого равенства в (9′) следует, что $\frac{\rho_1}{\rho_2} = 1$, а из второго — $\frac{\rho_2}{\rho_3} = 1$, т. е. $a = 2mn\alpha$, $b = (m^2 - n^2)\alpha$, $c = (m^2 + n^2)\alpha$ при некотором рациональном α.

Остается выяснить, каким может быть знаменатель рационального числа α. Так как число $2mn\alpha$ — целое, то делителями знаменателя α могут быть лишь делители чисел m, n и 2. С другой стороны, так как $(m^2 - n^2)\alpha$ — целое число, то делители знаменателя числа α должны быть делителями числа $m^2 - n^2$, а потому среди них нет делителей чисел m и n: ведь $(m, n) = 1$ по условию. Итак, число α — либо целое, либо рациональное со знаменателем 2. В последнем случае числа m и n одновременно нечетны.

Таким образом, мы пришли к теореме:

Теорема. *Тройка целых чисел (a, b, c) является пифагоровой тогда и только тогда, когда она имеет вид $(2\alpha mn, \alpha(m^2 - n^2), \alpha(m^2 + n^2))$, где m и n — целые взаимно простые числа, а α — любое целое число; если m и n — нечетные числа, то число α может быть не только целым, но и числом вида $\frac{p}{2}$, где p —* нечетное число.

Например, положив $m = 2$, $n = 1$, $\alpha = 1$, мы получаем пифагорову тройку 4, 3, 5, а с ней и пифагоровы тройки при тех же m и n, но других α: (12, 9, 15); (20, 15, 25) и т. д.

В Древнем Египте пифагоровы тройки использовались для построения прямых углов. Если числа a, b, c связаны соотношением (1), то треугольник со сторонами a, b и c — прямоугольный. Построение же треугольника по трем сторонам легко проводится циркулем и линейкой: на концах отрезка c как из центров описываются дуги радиусов a и b соответственно, и точка их пересечения соединяется с концами отрезка c. На практике отрезки

a, b и c были кусками веревки, длины которых относились друг к другу как числа какой-нибудь пифагоровой тройки. Например, 3 : 4 : 5.

Упражнения

1. Найти все целые числа x такие, что выражение $x^3 + 2x + 7$ при делении на 5 дает остаток 2.

2. Пусть m — натуральное число $m > 1$, а $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ — полином с целыми коэффициентами $a_0, a_1, \ldots, a_n$. Доказать, что если x целое число, то остаток при делении $f(x)$ на m зависит лишь от остатка числа x при делении на m.

3. Докажите, что $d = \text{НОД}(a, b)$ и $-d$ единственные общие делители чисел a и b, которые можно представить в виде линейной комбинации чисел a и b.

4. Покажите, что число шагов в алгоритме Евклида может быть сколь угодно велико.

5. Найти НОД (a, b) и представить его в виде $\alpha a + \beta b$ для: а) $a = 127$, $b = 211$; б) $a = 111\,111$, $b = 111$; в) $a = 191$, $b = 291$.

6. Доказать, что НОД $(a, b) = \text{НОД}(a, a + b) = \text{НОД}(a, a - b)$.

7. Найти все целочисленные решения уравнений:
а) $2x + 3y = 5$; б) $10x + 2y = 5$; в) $121x + 1331y = 11$.

8. Доказать, что если p — простое число, то $\sqrt{p}$ — число иррациональное.

9. Найти все пифагоровы тройки a, b, c, для которых $|c| < 100$.

Глава II
АРИФМЕТИКА ГАУССОВЫХ ЧИСЕЛ

§ 1. ГАУССОВЫ ЧИСЛА И ЦЕЛЫЕ ГАУССОВЫ ЧИСЛА

Естественным обобщением целых рациональных чисел являются «целые комплексные числа», или, как их обычно называют, «целые гауссовы числа» по имени великого немецкого математика К. Ф. Гаусса, который их впервые подробно изучал.

Определение 1. *Целым гауссовым числом называется комплексное число, вещественной и мнимой частью которого являются целые рациональные числа. Иначе говоря, это комплексные числа α вида*

$$\alpha = a + bi, \tag{1}$$

где a и b — целые рациональные числа. Наряду с целыми гауссовыми числами нам понадобятся также (просто) гауссовы числа, т. е. комплексные числа, у которых вещественная и мнимая части — числа рациональные.

Связь между областями гауссовых чисел и целых гауссовых чисел аналогична связи между рациональными числами и целыми рациональными числами. Более точно, имеются в виду следующие утверждения, которыми в дальнейшем мы будем часто пользоваться без особой оговорки и которые читатель легко проверит непосредственно:

I. *Сумма, разность и произведение двух целых гауссовых чисел также являются целыми гауссовыми числами* (это свойство выражают кратко, говоря, что целые гауссовы числа образуют кольцо).

II. *Сумма, разность, произведение и частное (в случае, если делитель не равен нулю) двух гауссовых чисел также являются гауссовыми числами* (это свойство выражают кратко, говоря, что гауссовы числа образуют поле).

III. *Частное двух целых гауссовых чисел является гауссовым числом и, обратно, всякое гауссово число представимо как частное двух целых гауссовых чисел.*

Это утверждение требует небольшого пояснения: пусть $\alpha = a + bi$ и $\beta = c + di$ — целые гауссовы числа (т. е. a, b, c, d — целые рациональные числа) и пусть $\beta \neq 0$. Покажем, что $\gamma = \alpha/\beta$ — гауссово число. Действительно,

$$\gamma = \frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{ac+bd+bci-adi}{c^2+d^2} =$$

$$= \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}\,i.$$

Числа $\frac{ac+bd}{c^2+d^2}$ и $\frac{bc-ad}{c^2+d^2}$ (вещественная и мнимая части числа γ) — числа рациональные и, следовательно, γ — гауссово число.

Отметим, наконец, что, очевидно, всякое рациональное число является гауссовым (мнимая часть равна 0) и что всякое целое рациональное число является целым гауссовым числом.

Рассмотрим расположение целых гауссовых чисел на комплексной плоскости. По определению целые гауссовы числа изображаются точками с целочисленными координатами (рис. 2). Они лежат в вершинах сетки квадратов со стороной, равной 1, покрывающей комплексную плоскость.

В дальнейшем нам из теории комплексных чисел нужны будут понятия нормы и модуля комплексного числа. Напомним, что нормой комплексного числа $\alpha = x + iy$

называется неотрицательное вещественное число $N(\alpha) = x^2 + y^2$; модулем комплексного числа α (обозначается $|\alpha|$) называется вещественное число $\sqrt{x^2+y^2}$. Геометрически модуль комплексного числа — это расстояние соответствующей точки на комплексной плоскости от начала координат. Норма $N(\alpha)$ числа α представима как произведение $N(\alpha) = \alpha \cdot \bar{\alpha}$, где $\bar{\alpha}$ — комплексно сопряженное число $x - iy$ числа α. Известным предполагается также свойство мультипликативности нормы, т. е. что

$$N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta). \qquad (2)$$

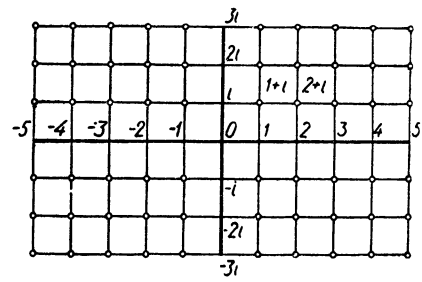

Рис. 2

Отметим сразу, что если α — гауссово число, то $N(\alpha)$ — неотрицательное рациональное число, а если α — целое гауссово число, то $N(\alpha)$ — неотрицательное целое число.

Примечание. Модуль $|\alpha|$ гауссова числа уже не всегда будет рациональным числом, поэтому в дальнейшем мы в основном будем пользоваться не модулем, а нормой.

Однако не всякое положительное целое рациональное число является нормой целого гауссового числа. Действительно, докажем следующую теорему:

Теорема 1: *Положительное целое рациональное число c является нормой некоторого целого гауссова числа тогда и только тогда, когда число c представимо в виде суммы двух квадратов целых чисел.*

Доказательство. Если $\alpha = a + bi$ — целое гауссово число, то $N(\alpha) = a^2 + b^2$ — сумма квадратов целых чисел a и b. Наоборот, если $c = x^2 + y^2$, где x и y — целые рациональные числа, то $c = N(x + yi)$, где $x + iy$ — целое гауссово число. Теорема доказана.

Нетрудно показать, что не всякое положительное целое число представимо в виде суммы двух квадратов. Так, например, если нечетное положительное целое число t представимо в виде суммы двух квадратов целых чисел, то оно дает при делении на 4 остаток, равный 1, т. е. является числом вида $t = 4k + 1$. Действительно, пусть

$t = x^2 + y^2$, тогда одно из чисел, скажем x, должно быть четным, другое — y — нечетным. Пусть $x = 2m$ и $y = 2n + 1$. Следовательно, $x^2 = 4m^2$ и $y^2 = 4(n^2 + n) + 1$ и, окончательно, $t = 4(m^2 + n^2 + n) + 1$, что и доказывает наше утверждение. Таким образом, числа 7, 11, 15 и др. не представимы в виде суммы двух квадратов и не являются поэтому нормами гауссовых чисел.

Вопрос о том, какие целые числа представимы в виде суммы двух квадратов или, что то же самое, какие числа являются нормами целых гауссовых чисел, мы выясним в результате исследования арифметики целых гауссовых чисел.

Как и в области (кольце) целых рациональных чисел, так и в области целых гауссовых чисел основной интерес представляет вопрос делимости.

Будем говорить, что *целое гауссово число* α *делит целое гауссово число* β (*и записывать это так:* $\alpha \mid \beta$), *если для некоторого целого гауссова числа* γ *имеет место равенство*

$$\beta = \alpha \cdot \gamma. \tag{3}$$

Так как из (3) следует: $N(\beta) = N(\alpha) \cdot N(\gamma)$, то необходимым условием для $\alpha \mid \beta$ является делимость $N(\alpha) \mid N(\beta)$, где $N(\alpha)$ и $N(\beta)$ — целые рациональные числа.

В случае целых рациональных чисел имеются только два числа, которые делят все целые числа: $+1$ и -1; в случае целых гауссовых чисел таких чисел имеется четыре: $+1$, -1, $+i$, $-i$. Действительно,

$$\alpha = \alpha \cdot 1,$$
$$\alpha = (-\alpha)(-1),$$
$$\alpha = (-\alpha i) \cdot i,$$
$$\alpha = (\alpha i) \cdot (-i).$$

Других чисел с данными свойствами среди целых гауссовых чисел нет. В самом деле, если некоторое целое гауссово число ξ делит все целые гауссовы числа, то оно, в частности, должно делить число 1 (поэтому такие числа называются *делителями единицы*). Из $N(\xi) \mid 1$ следует, что $N(\xi) = 1$. Если $\xi = x + iy$, то $x^2 + y^2 = 1$. Очевидно, что это уравнение имеет в целых рациональных числах в точности четыре решения: $x = 1, y = 0$; $x = -1$, $y = 0$; $x = 0$, $y = 1$; $x = 0$, $y = -1$, которые и соответствуют целым гауссовым числам $+1$, -1, i, $-i$.

Для целых гауссовых чисел, аналогично тому, как это делалось для целых рациональных чисел, определяются понятия общего делителя, наибольшего общего делителя, взаимно простых чисел и простых чисел. Первые три понятия дословно определяются как и в случае целых рациональных чисел. Однако на определении простого целого гауссова остановимся более подробно.

Определение 2. *Целое гауссово число* π *называется простым, если в любом его разложении* $\pi = \tau \cdot \sigma$ *в произведение двух целых гауссовых чисел один из сомножителей* (τ *или* σ) *является делителем единицы* (*при этом делители единицы простыми числами не считаются*).

Иначе это свойство можно выразить так: *простое гауссово число* π *— это такое целое гауссово число, отличное от нуля, норма которого больше единицы и которое не разложимо в произведение двух целых гауссовых чисел, нормы которых меньше, чем норма числа* π.

Согласно этому определению простыми гауссовыми числами будут, например, числа $\pi_1 = 2 + i$, $(N(\pi_1) = 5)$; $\pi_2 = 3 + 2i$, $(N(\pi_2) = 13)$. Вообще, простыми числами будут все числа, нормы которых являются простыми рациональными числами. В дальнейшем мы увидим, что этими примерами простые гауссовы числа не исчерпываются. В ходе наших исследований мы опишем все простые гауссовы числа. Теперь же перейдем к формулировке и к доказательству основной теоремы арифметики целых гауссовых чисел:

Теорема. *Любое целое гауссово число* $\alpha \neq 0$ *разложимо в произведение простых гауссовых чисел*

$$\alpha = \pi_1 \cdot \pi_2 \ldots \pi_k \tag{4}$$

(π_i *— простые гауссовы числа, не обязательно все различные*). *Такое разложение однозначно в следующем смысле: если*

$$\alpha = \sigma_1 \cdot \sigma_2 \ldots \sigma_l \tag{5}$$

— другое разложение числа α *в произведение простых гауссовых чисел* σ_j, *то оба разложения имеют одно и то же число сомножителей,* $k = l$, *и разложения* (4) *и* (5) *могут отличаться друг от друга только порядком сомножителей и множителями, являющимися делителями единицы.*

Относительно части формулировки, касающейся однозначности разложения, сделаем еще одно замечание. Если, скажем, $\alpha = \pi_1 \cdot \pi_2 \cdot \pi_3$ есть произведение простых чисел π_1, π_2, π_3, то, например, $\alpha = (-\pi_3) \cdot (i\pi_2) \cdot (i\pi_1)$ есть «дру-

гое» представление числа α в виде произведения простых чисел $-\pi_3$, $i\pi_2$, $i\pi_1$, отличных от простых чисел π_1, π_2, π_3. Однако легко замстить, что любое из чисел $-\pi_3$, $i\pi_2$, $i\pi_1$ получается умножением какого-то из чисел π_1, π_2, π_3 на некоторый делитель единицы, при этом изменен также первоначальный порядок чисел. Такие различия в разложениях одного и того же числа допускаются. Вторая часть формулировки теоремы как раз и утверждает, что подобного рода различными разложениями неоднозначность представления исчерпывается. Это обстоятельство ничем не отличается от ситуации в арифметике целых рациональных чисел. Оно усложняется тем, что в случае арифметики целых гауссовых чисел мы располагаем большим числом делителей единицы.

Примечание. Отметим, что однозначность разложения с точностью до знаков сомножителей, о которой шла речь в случае целых рациональных чисел, и означает как раз однозначность с точностью до множителей, являющихся делителями единицы, так как $+1$ и -1— единственные делители единицы в этом случае.

Утверждение об однозначности разложения можно сформулировать короче, если ввести понятие ассоциированности целых гауссовых чисел.

Определение 3. *Два целых гауссовых числа называются ассоциированными, если они отличаются друг от друга на сомножитель, равный делителю единицы, т. е.* β, $-\beta$, $i\beta$, $-i\beta$ — *ассоциированные целые гауссовы числа, если* β — *произвольное целое гауссово число.*

С использованием этого определения утверждение об однозначности в основной теореме формулируется так:

Если $\alpha = \pi_1 \cdot \pi_2 \ldots \pi_k$ *и* $\alpha = \sigma_1 \cdot \sigma_2 \ldots \sigma_l$ — где $\pi_i (i = 1, 2, \ldots, k)$ *и* $\sigma_j (j = 1, 2, \ldots, l)$ — *простые числа, то* $l = k$ *и сомножители* σ_j *можно так переставить, что каждое* σ_j *будет ассоциировано с соответствующим простым числом* π_j.

Доказательство основной теоремы арифметики целых гауссовых чисел проводится так же, как и доказательство соответствующих утверждений для целых рациональных чисел. Поэтому мы не будем подробно излагать его, а рекомендуем читателю сделать это самостоятельно.

Первое утверждение теоремы (о существовании разложения) можно провести индукцией по норме числа:

а) Если $N(\alpha) = 1$, то $\alpha = 1$, -1, i, $-i$, т. е. число разложимо в произведение пустого множества простых чисел.

Примечание. Относительно «разложимости» делителей единицы в произведение простых сомножителей мы принимаем то же положение, что и для ± 1 в случае целых рациональных чисел.

б) Пусть $N(\alpha) = n$, а для всех целых гауссовых чисел с меньшей нормой утверждение уже доказано. Тогда или α простое число и все доказано, или $\alpha = \rho \cdot \tau$, где $N(\rho) < n$ и $N(\tau) < n$. По предположению индукции для ρ и τ существуют разложения: $\rho = \pi_1 \cdot \pi_2 \ldots \pi_k$ и $\tau = \sigma_1 \cdot \sigma_2 \ldots \sigma_l$, тогда $\alpha = \pi_1 \cdot \pi_2 \ldots \pi_k \cdot \sigma_1 \cdot \sigma_2 \ldots \sigma_l$ — разложение для α.

Доказательство утверждения об однозначности можно вести по пути установления свойств наибольшего общего делителя и свойств взаимно простых чисел в области целых гауссовых чисел. Ключом для всего доказательства является утверждение о возможности деления с остатком в области целых гауссовых чисел. Оно формулируется здесь так:

Пусть α, β $(\beta \neq 0)$ — *два целых гауссовых числа; тогда существуют такие целые гауссовы числа* γ *и* ρ, *причем* $N(\rho) < N(\beta)$, *что*

$$\alpha = \gamma \cdot \beta + \rho.$$

Примечание. Число γ называют частным, а число ρ — остатком от деления α на β. В теореме 1 на стр. 5 эти понятия вводились для обычных целых чисел, но при этом остаток должен был быть неотрицательным $(r \geqslant 0)$. Однако это требование несущественно. Если от него отказаться и принять лишь неравенство $|r| < b$, то определение частного и остатка для гауссовых чисел будет естественным обобщением определения в обычной ситуации.

Доказательство основано на очень простом геометрическом факте: если P — точка, лежащая внутри квадрата со стороной a или на одной из его сторон, то расстояние от точки P до ближайшей вершины меньше, чем a. Действительно, точка, наиболее удаленная от всех вершин, — это центр квадрата. Но расстояние от нее до любой вершины равно $\frac{1}{\sqrt{2}}a < a$. Любая другая точка квадрата удалена от ближайшей вершины еще меньше.

Из этого простого утверждения непосредственно вытекает, что для любой точки τ комплексной плоскости найдется точка γ с целыми координатами — точка, представляющая целое гауссово число, — удаленная от τ меньше чем на 1 (рис. 3). Иначе говоря, для всякого комплексного числа τ существует такое целое гауссово число γ, что $N(\tau - \gamma) < 1$. Найдем такое γ для числа

$\tau = \frac{\alpha}{\beta}$ и положим $\rho = \alpha - \gamma\beta$. Тогда ρ — целое гауссово число,

$$N(\rho) = N(\beta) \cdot N\left(\frac{\alpha}{\beta} - \gamma\right) < N(\beta)$$

и

$$\alpha = \gamma\beta + \rho.$$

Утверждение доказано.

Имея уже теорему о делении с остатком, все остальные свойства можно доказать так же, как мы это делали выше в случае рациональных чисел: 1) доказывается существование НОД двух целых гауссовых чисел α, β, как числа $\delta \neq 0$ с наименьшей нормой из множества чисел, представимых в виде $\alpha\xi + \beta\eta$ (ξ и η — целые гауссовы числа); 2) вводится понятие взаимно простых целых гауссовых чисел и доказывается основная лемма: *если α взаимно просто с β_1 и α взаимно просто с β_2, то α взаимно просто с $\beta_1 \cdot \beta_2$*. Затем уже совсем просто индукцией по норме доказывается однозначность разложения на простые сомножители.

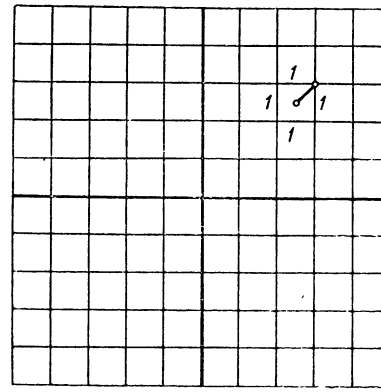

Рис. 3

§ 2. ПРОСТЫЕ ГАУССОВЫ ЧИСЛА И ПРЕДСТАВЛЕНИЕ ЦЕЛЫХ РАЦИОНАЛЬНЫХ ЧИСЕЛ В ВИДЕ СУММЫ ДВУХ КВАДРАТОВ

Перейдем теперь к описанию всех простых гауссовых чисел. Докажем сначала несколько вспомогательных утверждений.

Лемма 1. *Всякое простое гауссово число является делителем простого рационального числа.*

Примечание. Заметим, что простое рациональное число является всегда и целым гауссовым числом, но как гауссово число оно не

обязательно простое, а может делиться на целые гауссовы числа с меньшей нормой. Так, например, число 2— простое, если его рассматривать как целое рациональное число, но оно не простое, если его рассматривать как целое гауссово число. Действительно, в области целых гауссовых чисел число 2 допускает разложение $2 = (1 + i) \times (1 - i)$ и ни один из сомножителей $1 + i$ и $1 - i$ не является делителем единицы. Очевидно, что и 5 не является простым в области гауссовых чисел, так как $5 = (2 + i) \cdot (2 - i)$.

Доказательство. Действительно, так как $N(\alpha) = \alpha \cdot \bar{\alpha}$, то всякое целое гауссово число делит свою норму: $\alpha \mid N(\alpha)$. Пусть теперь π — простое гауссово число, тогда $\pi \mid N(\pi)$, и пусть $N(\pi) = p_1 \cdot p_2 \ldots p_r$ — разложение числа $N(\pi)$ в произведение простых рациональных чисел. Имеем: $\pi \mid p_1 \cdot p_2 \ldots p_r$, следовательно, π делит одно из простых чисел p_i. В самом деле, если бы простое целое гауссово число π не делило бы ни одно из чисел p_i, то оно было бы взаимно просто с каждым из них, а следовательно, и с их произведением $N(\pi)$. Но это невозможно, так как $\pi \mid N(\pi)$. Итак, число π является делителем одного из простых целых рациональных чисел p_i. Лемма доказана.

Лемма 2. *Норма $N(\pi)$ простого гауссова числа π является или простым рациональным числом, или квадратом простого рационального числа.*

Доказательство. Как мы уже знаем, π делит некоторое простое рациональное число p. Пусть $p = \pi \cdot \gamma$. Перейдем к нормам: $N(\pi) \cdot N(\gamma) = p^2$. Возможны только два случая: 1) $N(\pi) = N(\gamma) = p$ и 2) $N(\pi) = p^2 = N(p)$, а $N(\gamma) = 1$. Лемма доказана.

Случай 2) означает, что γ — делитель единицы и что справедливо одно из равенств: $\pi = p$, $\pi = -p$, $\pi = ip$, $\pi = -ip$. Следовательно, p — такое простое рациональное число, которое одновременно является и простым гауссовым числом. В случае 1) γ — простое гауссово число, так как $N(\gamma) = p$. Можно утверждать, что $\gamma = \bar{\pi}$. Действительно, $N(\pi) = p = \pi \cdot \bar{\pi}$ и $\bar{\pi}$ — простое число. Но мы имеем также $p = \pi \cdot \gamma$, так что $\bar{\pi} = \gamma$.

Если же p такое простое рациональное число, которое не является простым гауссовым числом, то оно делится на какое-либо простое гауссово число, отличное от p, и при этом, как мы видели, $p = \pi \cdot \bar{\pi}$, т. е. p является произведением двух простых гауссовых комплексно сопряженных чисел. В этом случае p является нормой целого гауссового числа и, следовательно, представимо

в виде суммы двух квадратов. Такое простое число, если оно нечетное (т. е. $p \neq 2$), — число вида $4n+1$. Можно показать, что все простые числа вида $4n+1$ представимы в виде суммы двух квадратов, т. е. являются нормами некоторых целых гауссовых чисел, а потому не являются простыми гауссовыми числами и, следовательно, принадлежат к классу тех простых рациональных чисел, которые разложимы в произведение двух комплексно сопряженных простых гауссовых чисел. Доказательство этого утверждения мы приведем ниже (гл. III, § 3). Все простые рациональные числа, отличные от чисел вида $4n+1$ и от числа 2, т. е. числа вида $4n+3$, и составляют как раз множество простых рациональных чисел, остающихся простыми и в области гауссовых чисел.

Несколько особое положение занимает простое число 2. Легко видеть, что

$$2 = i \cdot (1-i)^2$$

$N(1-i) = 2$. Таким образом, 2 делится на квадрат простого гауссова числа $(1-i)$.

Предполагая известным, что все простые числа вида $4n+1$ представимы в виде суммы двух квадратов, мы можем теперь установить, каковы все целые рациональные числа, представимые в виде суммы двух квадратов. Как мы уже знаем, для всякого числа t с таким свойством необходимо и достаточно, чтобы оно было нормой некоторого целого гауссова числа α: $t = N(\alpha)$.

Число α раскладывается в произведение простых гауссовых чисел:

$$\alpha = \pi_1 \cdot \pi_2 \dots \pi_r. \tag{6}$$

Разобьем все простые числа π_i ($i = 1, 2, \dots, r$) на два класса: к первому классу отнесем те числа π_i, нормы которых — простые числа, а ко второму соответственно числа, нормы которых — квадраты простых чисел (может оказаться, что один из классов пуст, но это не повлияет на ход наших рассуждений, надо только иметь в виду, что все числа a_i или все b_k в разложениях (7) и (8) могут быть нулями). Обозначим различные числа первого класса через σ_j ($j = 1, 2, \dots, l$), а все различные числа второго класса — через ρ_k ($k = 1, 2, \dots, s$). Имеем: $N(\sigma_j) = p_j$, $N(\rho_k) = q_k^2$, где p_j — простое число вида $4n+1$ или 2, а q_k — простое число вида $4n+3$. Объединяя равные

простые числа в правой части равенства (6), запишем это произведение в виде степеней простых чисел σ_j и ρ_k:

$$\alpha = \sigma_1^{a_1} \dots \sigma_l^{a_l} \cdot \rho_1^{b_1} \dots \rho_s^{b_s} \tag{7}$$

и, переходя к нормам, имеем:

$$t = p_1^{a_1} \dots p_l^{a_l} q_1^{2b_1} \dots q_s^{2b_s}. \tag{8}$$

Мы видим, что простые числа q_k входят в разложение числа в четных степенях.

Обратно, пусть число t представимо в виде (8), где каждое p_j — простое число вида $4n+1$ или число 2, q_k — простые числа вида $4n+3$ и $a_1, \dots, a_l$, $b_1, \dots, b_s$ — целые неотрицательные числа. Поскольку каждое p_j является суммой двух квадратов, то можно подобрать σ_j так, чтобы $N(\sigma_j) = p_j$. Положив далее $\rho_k = q_k$ и, наконец, $\alpha = \sigma_1^{a_1} \dots \sigma_l^{a_l} \rho_1^{b_1} \dots \rho_s^{b_s}$, получим $t = N(\alpha)$, т. е. t представимо в виде суммы двух квадратов. Окончательно имеем следующую теорему:

Теорема 2. *Для того чтобы целое рациональное число было представимо в виде суммы двух квадратов, необходимо и достаточно, чтобы простые числа вида* $4n+3$ *входили в разложение этого числа на простые сомножители в четных степенях.*

Примечание. Такая формулировка охватывает и случай, когда простых чисел вида $4n+3$ нет в разложении рассматриваемого числа,— ведь число 0 также является четным.

Как видим, эта теорема дает критерий того, чтобы диофантово уравнение второй степени вида

$$x^2 + y^2 = t$$

имело решение (целочисленное). Вообще изучение диофантовых уравнений вида

$$ax^2 + 2bxy + cy^2 = t$$

тесно связано с арифметиками в областях чисел, аналогичных области целых гауссовых чисел.

Существенным в таких исследованиях оказывается следующий удивительный факт: не во всех подобных арифметиках имеет место теорема об однозначности разложения чисел в произведение простых чисел. Приведем пример такой «арифметики».

Рассмотрим комплексные числа вида

$$\alpha = x + y\sqrt{-5}, \tag{1}$$

где x и y — целые рациональные числа. Легко видеть, что сумма, разность и произведение чисел вида (1) являются числами такого же вида. Обозначим совокупность всех чисел вида (1) через Γ. Очевидно, что Γ содержит все целые рациональные числа (при $y = 0$). Так же, как в случаях целых рациональных и целых гауссовых чисел, можно говорить о делимости в Γ: α делит β ($\alpha|\beta$), если $\frac{\beta}{\alpha}$ — число из Γ т. е. представимо в виде (1). Как и в случае целых гауссовых чисел, в вопросе делимости важную роль играют нормы чисел из Γ:

$$N(\alpha) = N(x + y\sqrt{-5}) = (x + y\sqrt{-5})(x - y\sqrt{-5}) = x^2 + 5y^2.$$

Таким образом норма всякого числа из Γ есть целое рациональное число и, так как $N(\xi \cdot \eta) = N(\xi) \cdot N(\eta)$, то необходимым (но, вообще говоря, не достаточным) условием для $\alpha \mid \beta$ является условие $N(\alpha) \mid N(\beta)$.

Так же, как и в случае целых гауссовых чисел, естественно вводится понятие делителей единицы и простых чисел. В отношении делителей единицы дело обстоит здесь даже проще, чем для целых гауссовых чисел. А именно, делителями единицы являются только числа ± 1. Действительно, для делителей единицы $\xi = u + v\sqrt{-5}$ должно выполняться условие $N(\xi) = u^2 + 5v^2 = 1$. Но это диофантово уравнение, очевидно, не может иметь решений, отличных от $u = \pm 1$ и $v = 0$.

Тот факт, что каждое число из Γ представимо в виде произведения простых чисел из Γ, доказывается индукцией по норме точно так же, как и в случае целых гауссовых чисел. А вот утверждение об однозначности такого разложения здесь уже не верно, и мы это покажем на таком примере.

Покажем сначала, что числа $2 = 2 + 0 \cdot \sqrt{-5}$, $3 = 3 + 0 \cdot \sqrt{-5}$, $1 + \sqrt{-5}$, $1 - \sqrt{-5}$ — простые числа в Γ. Действительно, $N(2) = 4$, $N(3) = 9$, $N(1 + \sqrt{-5}) = N(1 - \sqrt{-5}) = 6$. Если бы одно из этих чисел не было простым в Γ, то оно могло бы делиться только на некоторое число $\alpha = x + y\sqrt{-5}$, для которого $N(\alpha) = x^2 + 5y^2 = 2$, или $N(\alpha) = x^2 + 5y^2 = 3$. Но таких чисел в Γ нет, так как очевидно, что уравнения

$$x^2 + 5y^2 = 2$$

и

$$x^2 + 5y^2 = 3$$

не имеют целочисленных решений.

Итак, указанные четыре числа — простые числа в Γ. Отметим теперь легко проверяемое равенство

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

Оно показывает, что число 6 из Γ имеет два различных представления в виде произведения простых чисел.

С этим фактом столкнулся немецкий математик Э. Куммер (1810—1893) при попытках решить так называемую великую теорему Ферма. В дальнейшем трудности, возникающие в связи с невыполнением основной теоремы арифметики в некоторых областях чисел, были успешно преодолены как самим Куммером, так и другими математиками — Р. Дедекиндом, Е. Золотаревым, Л. Кронеккером и др. Возникла большая новая область в математике — теория алгебраических чисел.

Упражнения

1. Разделить с остатком целое гауссово число a на целое гауссово число b, если: а) $a = 2 + 3i$, $b = 1 - i$; б) $a = 1 + i$, $b = 2 + i$.

2. Разложить на простые множители целые гауссовы числа: $1 + i$. $2 + 5i$; 5; 10.

3. Представимы ли в виде суммы двух квадратов целых рациональных чисел числа: а) 197; б) 1472; в) 111 112?

4. Докажите, что для комплексных чисел вида $a + b\sqrt{-2}$, где a и b — целые рациональные числа, выполняется основная теорема арифметики.

5. Докажите, что в кольце чисел вида $a + b\sqrt{-5}$, где a и b — целые рациональные числа, 7, $1 + 2\sqrt{-5}$ и $1 - \sqrt{-5}$ — простые.

Глава III
КОНЕЧНЫЕ АРИФМЕТИКИ

С первыми применениями деления с остатком мы познакомились, доказывая основную теорему арифметики и решая несложные диофантовы уравнения. Обратимся теперь к важнейшей конструкции, связанной с делением целых чисел, — классам вычетов.

Основная идея состоит в следующем: различных остатков от деления на данное натуральное число n всего лишь n: это числа 0, 1, 2, ..., —1. Поэтому бесконечное множество целых чисел можно разбить на конечное число (на n) подмножеств, в каждое из которых входят числа с одним и тем же остатком от деления на n. Такие подмножества называются *классами вычетов по модулю n*. Оказывается, что на них естественным образом переносятся обычные действия арифметики (умножение, сложение, вычитание), и это приводит к новой интересной «арифметике», которую называют конечной.

§ 1. КЛАССЫ ВЫЧЕТОВ

Условимся, что если нет специальных оговорок, то под «числами» подразумеваются «целые числа». Их множество представляет собой «кольцо», которое всюду будет обозначаться через $\boldsymbol{Z}$.

Определение 1. *Числа x и y называются сравнимыми по модулю n, где n — число, отличное от нуля, если их разность $x - y$ делится на n.*

В этом случае пишут:

$$x \equiv y \bmod (n) \text{ или } y \equiv x \bmod (n).$$

Для несравнимых по модулю n чисел пишут:

$$x \not\equiv y \bmod (n) \text{ или } y \not\equiv x \bmod (n).$$

Например, $12 \equiv 15 \bmod (3)$, потому что $12 - 15 = -3$ делится на 3, и $21 \not\equiv 10 \bmod (5)$, потому что $21 - 10 = 11$ не делится на 5.

Пусть $n = 3$. Каково множество всех чисел из Z, сравнимых с числом 5 по модулю 3? Во-первых, в это множество входит само число 5: $5 = 5 \bmod (3)$. Далее, если $x \equiv 5 \bmod (3)$, то $x - 5 = 3k$ при некотором k из Z, т. е. $x = 5 + 3k$. Наоборот, при любом k число $x = 5 + 3k$ будет сравнимо с 5 по модулю 3, потому что $x - 5 = 3k$, а это кратно 3. Следовательно, придавая k в формуле $x = 5 + 3k$ всевозможные значения из Z. мы получим множество всех чисел, сравнимых с 5 по модулю 3. Это множество (обозначим его 5) — является обычной арифметической прогрессией, бесконечной в обе стороны и разность которой равна 3; вот несколько ее последовательных членов: при $k = -3, -2, -1, 0, 1, 2, 3$ имеем

$$\ldots, -4, -1, 2, 5, 8, 11, \ldots$$

Определение 2. *Множество X всех тех чисел из Z, которые сравнимы с числом x по модулю n, называется классом вычетов числа x по модулю n и обозначается одним из трех способов: $x \bmod (n)$ или x или $\bar{x}$, если число n фиксировано.* Числа из X называются *вычетами* числа x по модулю n или *представителями* класса X.

Таким образом, в рассмотренном выше примере был описан класс вычетов $5 \bmod (3)$ числа 5 по модулю 3. Очевидно, что $8 \bmod (3) = 5 \bmod (3)$ и, вообще, класс вычетов $x = x \bmod (3)$ любого представителя x из $5 \bmod (3)$ равен 5.

Теорема 1. *Пусть $x = qn + r$, где $0 \leqslant r < n$. Тогда $x \bmod (n) = r \bmod (n)$.*

Доказательство. I *способ.* Достаточно заметить, что $x \bmod (n)$ и $r \bmod (n)$ — это одна и та же бесконечная в обе стороны арифметическая прогрессия $x + kn$ или $r + kn$ с разностью n, потому что $x + kn = r + (k + q)n$.

II *способ.* Каждое число z, сравнимое с x по $\bmod(n)$, сравнимо и с r по модулю $\bmod(n)$, потому что если $z-x=kn$, то $z-r=z-x-qn=kn-qn=(k-q)n$. И наоборот, если $z-r=kn$, то $z-x=r-x+qn=(k+q)n$.

Остаток r от деления числа x на n называется каноническим представителем класса $x \bmod(n)$. В рассмотренном выше примере класса $5 \bmod(3)$ каноническим представителем будет, следовательно, число 2.

Следствие. *Всевозможные классы вычетов по модулю n таковы:*

$0 \bmod(n)$, $1 \bmod(n)$, $2 \bmod(n)$, ..., $(n-1) \bmod(n)$,

то есть, это $\mathbf{0}$, $\mathbf{1}$, $\mathbf{2}$, ..., $\boldsymbol{n-1}$.

Действительно, числа $0, 1, 2, \ldots, n-1$ составляют множество всевозможных остатков от деления на n — поэтому других классов вычетов кроме $\mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots, \boldsymbol{n-1}$, быть не может. Но нет ли среди этих классов совпадающих? Если бы $\boldsymbol{a=b}$, где a и b — различные остатки от деления на n, то при некотором целом k выполнялось бы равенство $a-b=kn$, а это при $k \neq 0$ невозможно, так как $|a-b|<n$, а $|kn| \geqslant n$. Следовательно, $a=b$, и все классы $\mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots, \boldsymbol{n-1}$ различны.

В дальнейшем мы будем обозначать через Z_n множество классов вычетов по модулю n.

Упражнения

1. Докажите, что если какое-либо целое число a принадлежит двум классам вычетов X и Y по модулю n, то $X=Y$.

Указание. Заметить, что если $x \equiv a \bmod(n)$ и $y \equiv a \bmod(n)$, то $x \equiv y \bmod(n)$ и, следовательно, $x \bmod(n) = y \bmod(n)$.

2. Доказать, что если $n=ml$, где m, l — натуральные числа, то каждый класс вычетов по модулю m состоит из l классов вычетов по модулю n.

3. Доказать, что Z_n и Z_{-n}, $n \neq 0$ — одно и то же множество.

§ 2. АРИФМЕТИКА КЛАССОВ ВЫЧЕТОВ

Изучая делимость целых или целых гауссовых чисел, мы пользовались тем, что они образуют кольцо, т. е. тем, что сумма, разность и произведение двух любых чисел рассматриваемого множества ему принадлежат, и упомянутые операции подчинены привычным законам — переместительному, сочетательному и распределительному. Свойства кольца целых чисел составляют арифметику или,

точнее говоря, арифметику целых чисел. В предыдущей главе мы познакомились с арифметикой целых гауссовых чисел. Сейчас мы введем арифметические операции на множестве $\mathbf{Z}_n$ и познакомимся с арифметикой классов вычетов. Для определенности условимся, что в понятии «по модулю n» число n — натуральное.

Определение 3. *Суммой двух классов вычетов по модулю n — $\bar{x}$ и $\bar{y}$ — называется класс $\overline{x+y}$.* В этом случае пишут:

$$\bar{x}+\bar{y}=\overline{x+y}.$$

Но тут может возникнуть сомнение: ведь классы $\bar{x}$ и $\bar{y}$ — множества, даже — бесконечные множества. Представители x и y, с помощью которых мы определили сумму $\bar{x}+\bar{y}$, внутри своих классов равноправны со всеми другими представителями; поэтому, если определение 3 не таит в себе никаких противоречий, то, выбрав в $\bar{x}$ и $\bar{y}$ другие представители, скажем, x' и y', мы должны в качестве класса $\bar{x}'+\bar{y}'$ получить тот же самый класс $\overline{x+y}$, т. е. необходимо выполнение равенства: $\overline{x'+y'}=\overline{x+y}$ (если бы $\overline{x'+y'}\neq\overline{x+y}$, то определение таило бы в себе следующее противоречие: $\overline{x'+y'}=\bar{x}'+\bar{y}'=\bar{x}+\bar{y}=\overline{x+y}$ вопреки $\overline{x'+y'}\neq\overline{x+y}$). Проверку равенства $\overline{x'+y'}=\overline{x+y}$ математики называют *проверкой определения на корректность.*

Действительно, пусть r_x и r_y — остатки от деления на n чисел x и y, соответственно. Тогда класс $\bar{x}+\bar{y}$ состоит из всех тех чисел, которые при делении на n дают тот же остаток, что и r_x+r_y. С другой стороны, класс $\bar{x}'+\bar{y}'$ состоит из тех же самых чисел, потому что остатки от деления на n чисел x' и y' есть r_x и r_y. Корректность определения 3 доказана.

Рассмотрим несколько примеров. Пусть $n=2$. Тогда классов вычетов всего лишь два: **0** и **1**. Их сложение описать легко:

$$\mathbf{0}+\mathbf{0}=\mathbf{0},$$
$$\mathbf{1}+\mathbf{0}=\mathbf{0}+\mathbf{1}=\mathbf{1},$$
$$\mathbf{1}+\mathbf{1}=\mathbf{0}.$$

Удобней, однако, эти результаты описать таблицей:

Табл. 1

	0	1
0	0	1
1	1	0

Читать ее следует так: допустим, надо найти сумму $0 + 1$. В левом столбце отыскиваем первое слагаемое (т. е. **0**), а в верхней строке — второе (т. е. **1**). На пересечении той строки, где стоит первое слагаемое, и того столбца, где стоит второе, указана их сумма: **1**. Эту таблицу называют таблицей сложения для Z_2.

Пусть $n = 3$. Тогда классы таковы: **0**, **1** и **2**. Соответствующая им таблица сложения имеет вид:

Табл. 2

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Читателю будет полезно проверить и следующие таблицы сложения для $n = 7$ и для $n = 10$:

Табл. 3

Таблица сложения в Z_7

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

Табл. 4

Таблица сложения в Z_{10}

	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Итак, сложение классов вычетов в Z_n определяется через сложение представителей этих классов. Аналогично определяются вычитание и умножение. Вот точные определения:

Определение 4. *Разностью двух классов вычетов по модулю* n — $\bar{x}$ и $\bar{y}$ — называется класс $\overline{x-y}$. В этом случае пишут:

$$\bar{x}-\bar{y}=\overline{x-y}.$$

Определение 5. *Произведением двух классов вычетов по модулю* n — $\bar{x}$ и $\bar{y}$ — называется класс $\overline{xy}$. В этом случае пишут:

$$\bar{x}\bar{y}=\overline{xy}, \text{ или } \bar{x}\cdot\bar{y}=\overline{xy}.$$

Читатель, вероятно, уже заметил, что определения 4 и 5, как и определение 3, нуждаются в проверке на корректность. Доказательство соответствующих равенств — $\overline{x'-y'}=\overline{x-y}$ и $\overline{x'y'}=\overline{xy}$ — несложно. Первое из них мы оставляем в качестве упражнения, а второе устанавливается так. Имеем: $x'=x+k_xn$ и $y'=y+k_yn$, где k_x и k_y — целые числа. Тогда $x'y'=xy+n(xk_y+yk_x+k_xk_yn)$. Поэтому

$$x'y'\equiv xy \bmod (n).$$

Таблицы сложения (см., например, таблицы 1—4) удобны не только для описания сложения, но и для описания вычитания. Связано это со следующим простым наблюдением: если $a=b-c$, то $b=a+c$. Действительно, прибавим к обеим частям равенства $a=b-c$ класс c. Получим:

$$a+c=(b-c)+c.$$

Очевидно, что $b-c=b+(-c)$ (и то, и другое — класс $(b-c) \bmod (n)$). Поэтому $(b-c)+c=(b+(-c))+c$. Но для трех любых классов x, y, z справедлив сочетательный закон:

$$(x+y)+z=x+(y+z)$$

(и то, и другое — класс $(x+y+z) \bmod (n)$). Поэтому $(b+(-c))+c=b+(-c+c)=b+0=b$, так что $a++c=b$.

Следовательно, чтобы по таблице сложения найти разность $a-b$, достаточно в левом столбце найти вычитаемое b, затем в этой же строке таблицы найти умень-

шаемое a, и тогда разность $a - b$ будет указана вверху столбца, в котором было найдено a. Так, по таблице 3 легко найти, что $4 \bmod (7) - 6 \bmod (7) = 5 \bmod (7)$, или, скажем, по таблице 4 $4 \bmod (10) - 6 \bmod (10) = 8 \bmod (10)$ и $6 \bmod (10) - 4 \bmod (10) = 2 \bmod (10)$.

Что касается умножения в Z_n, то и его удобно описывать таблицами, аналогичными таблицам сложения — только вместо того, чтобы указывать сумму классов вычетов, в них мы будем указывать произведение.

Табл. 5

Таблица умножения в Z_2

	0	1
0	0	0
1	0	1

Табл. 6

Таблица умножения в Z_3

	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Табл. 7

Таблица умножения в Z_7

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

Табл. 8

Таблица умножения в Z_{10}

	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Итак, классы вычетов в Z_n можно складывать, вычитать и умножать. Переместительный, сочетательный и распределительный законы, действующие при сложении и умножении чисел, переносятся и на классы вычетов. Доказательство соответствующих равенств мы оставляем читателю. Множество Z_n с введенными выше сложением,

вычитанием и умножением является кольцом, которое принято называть *кольцом классов вычетов по модулю n*. Элементы **0** и **1** из $\mathbf{Z}_n$ естественно называть нулем и единицей кольца $\mathbf{Z}_n$.

Наконец, обратимся к делению в кольце $\mathbf{Z}_n$. Пусть $\boldsymbol{a} = a \bmod (n)$ и $\boldsymbol{b} = b \bmod (n)$; говорят, что класс $\boldsymbol{b}$ делит класс $\boldsymbol{a}$ (и пишут $\boldsymbol{b} \mid \boldsymbol{a}$), если существует такой класс $c = c \bmod (n)$, что $\boldsymbol{a} = \boldsymbol{b} \cdot c$. Например, при $n = 10$ (см. табл. 8) класс **2** делит класс **4**, а класс **4** делит класс **6**. Если $\boldsymbol{b} \mid \boldsymbol{a}$, то $\boldsymbol{b}$ называют также делителем класса $\boldsymbol{a}$.

В кольце целых чисел **Z** делителями числа 0 являются все числа, потому что $x \cdot 0 = 0$ для любого x, а делителями числа 1 являются лишь два числа: 1 и —1. Конечно, и в кольце **Z** все классы $\boldsymbol{x}$ делят 0, а классы **1** и —1 делят **1**. Но, в отличие от кольца **Z**, здесь при том или ином n можно установить и несколько специфических, не свойственных кольцу **Z** качеств.

Так, в кольце **Z** равенство $xy = 0$ возможно лишь тогда, когда, по крайней мере, один из элементов x или y равен 0. А вот в кольце $\mathbf{Z}_{10}$ имеем: $2 \cdot 5 = 0$, хотя $2 \neq 0$ и $5 \neq 0$! Далее, в кольце **Z** делителями числа 1 являются лишь 1 и —1, а в том же кольце $\mathbf{Z}_{10}$ класс **1** делят сразу четыре элемента: **1**, **3**, **7**, **9**, потому что $1 = 1 \cdot 1 = 3 \cdot 7 = 7 \cdot 3 = 9 \cdot 9$. Наконец, в кольце **Z** можно смело производить сокращения (т. е. гарантировать, что из равенства $ax = ay$ и условия $a \neq 0$ следует равенство чисел $x = y$), а в кольце $\mathbf{Z}_n$ — нет; например, в $\mathbf{Z}_{10}$ из равенства $2 \cdot 7 = 2 \cdot 2$ и условия $2 \neq 0$ не следует, что $7 = 2$.

Сейчас мы докажем основную в этом плане теорему о кольцах $\mathbf{Z}_n$. Введем два термина:

Класс $\boldsymbol{x}$ кольца $\mathbf{Z}_n$ называется делителем нуля, если $\boldsymbol{x} \neq 0$ и существует такой класс $\boldsymbol{y} \neq 0$ в $\mathbf{Z}_n$, что $\boldsymbol{xy} = 0$.

Класс $\boldsymbol{x}$ из $\mathbf{Z}_n$ называется делителем единицы, если существует такой класс $\boldsymbol{y}$ в $\mathbf{Z}_n$, что $\boldsymbol{x} \cdot \boldsymbol{y} = 1$.

Делители единицы называют также обратимыми элементами.

Теорема 2. (1) *Класс $\boldsymbol{x}$ кольца $\mathbf{Z}_n$ является делителем единицы тогда и только тогда, когда числа x и n взаимно просты.*

(2) *Класс $\boldsymbol{x}$ кольца $\mathbf{Z}_n$ является делителем единицы тогда и только тогда, когда он не является делителем нуля.*

Следует отметить, что наибольший общий делитель чисел x и n не зависит от выбора представителя в клас-

се x. Действительно, если $x' \equiv x \bmod (n)$, то $x' = x + kn$ и каждый (в частности, наибольший) общий делитель x и n является общим делителем для x' и n. Поэтому $(x, n) \mid (x', n)$ и, конечно, наоборот: $(x', n) \mid (x, n)$. Таким образом, формулировка теоремы 2 в части (1) корректна.

Доказательство. (1) Пусть x и n взаимно просты. Согласно теореме 3, главы I, это означает, что $xs + nt = 1$ при некоторых s и t из $\mathbf{Z}$. Но тогда, переходя к вычетам по модулю n, мы получаем:

$$\boldsymbol{xs} + \boldsymbol{nt} = \mathbf{1}$$

или

$$(xs) \bmod (n) + (nt) \bmod n = 1 \bmod (n),$$

т. е. $\boldsymbol{xs} = \mathbf{1}$, поскольку $\boldsymbol{nt} = \mathbf{0}t = \mathbf{0}$ и $\boldsymbol{x}$ — обратим в $\mathbf{Z}_n$.

Обратно, пусть $\boldsymbol{xs} = \mathbf{1}$ в $\mathbf{Z}_n$ при некотором классе $\boldsymbol{s}$. Тогда $xs - 1 \equiv 0 \bmod (n)$, т. е. $xs - 1 = k \cdot n$ и, следовательно, x и n взаимно просты.

(2) Пусть $\boldsymbol{x}$ не является делителем нуля. Рассмотрим наибольший общий делитель d чисел x и n. Пусть

$$d = xs + nt$$

при некоторых целых s и t и $n = d \cdot n'$. Если $d = 1$, то из доказанного выше, x обратим в $\mathbf{Z}_n$. Если же $d \neq 1$, то $\boldsymbol{n'} \neq \mathbf{0}$, и, кроме того, для $x = x' \cdot d$

$$\boldsymbol{xn'} = \boldsymbol{x'd} \cdot \boldsymbol{n'} = \boldsymbol{x'} \cdot \boldsymbol{n} = \mathbf{0} \qquad (1)$$

и $\boldsymbol{x}$ — делитель нуля в противоречии с предположением. Следовательно, $d = 1$ и $\boldsymbol{x}$ обратим в $\mathbf{Z}_n$.

Обратно, пусть $\boldsymbol{x}$ обратим в $\mathbf{Z}_n$, т. е. $\boldsymbol{xy} = \mathbf{1}$ при некотором $\boldsymbol{y}$ из $\mathbf{Z}_n$. Если бы $\boldsymbol{xz} = \mathbf{0}$ при $\boldsymbol{z} \neq \mathbf{0}$, то из последнего равенства следовало бы, что $\boldsymbol{yxz} = \boldsymbol{y0} = \mathbf{0}$, т. е. $(\boldsymbol{yx})\boldsymbol{z} = \mathbf{0}$ или $\mathbf{1} \cdot \boldsymbol{z} = \mathbf{0}$, но $\boldsymbol{z} \neq \mathbf{0}$ по предположению. Теорема доказана.

Следствие 1. *Класс $\boldsymbol{x}$ из $\mathbf{Z}_n$, $\boldsymbol{x} \neq \mathbf{0}$ является делителем нуля тогда и только тогда, когда числа x и n не взаимно просты.*

Следствие 2. *В кольце $\mathbf{Z}_p$, где p — простое число, нет делителей нуля.*

Действительно, каждое из чисел 1, 2, ..., $p - 1$ взаимно просто с p, если p — простое; поэтому классы $\mathbf{1}$, $\mathbf{2}$, ..., $\boldsymbol{p} - \mathbf{1}$ обратимы в $\mathbf{Z}_p$.

В заключение этого параграфа мы приведем еще две теоремы, посвященные «необычным» фактам конечной арифметики.

Теорема 3. *Если p — простое число и $\boldsymbol{a} = a \bmod (p)$ $\boldsymbol{b} = b \bmod (p)$, то $(\boldsymbol{a} + \boldsymbol{b})^p = \boldsymbol{a}^p + \boldsymbol{b}^p$.*

Доказательство. Напомним прежде всего, что для любых чисел x и y бином $(x + y)^p$ раскладывается по следующей формуле Ньютона:

$$(x + y)^p = x^p + C_p^1 x^{p-1} y + \ldots + C_p^k x^{p-k} y^k + \\ + \ldots + C_p^{p-1} x y^{p-1} + y^p,$$

где

$$C_p^k = \frac{p(p-1)\ldots(p-k+1)}{1 \cdot 2 \ldots k}, \quad k = 1, 2, \ldots, p-1.$$

Биномиальный коэффициент C_p^k при любом k делится на p, потому что p, будучи простым, взаимно просто с каждым из чисел 1, 2, ..., k при $k < p$. Следовательно, разность $(x + y)^p - x^p - y^p$ представляется в виде суммы чисел, каждое из которых делится на p; поэтому $(x + y)^p \equiv (x^p + y^p) \bmod (p)$, откуда при $x = a$ и $y = b$ получается требуемое:

$$(\boldsymbol{a} + \boldsymbol{b})^p = \boldsymbol{a}^p + \boldsymbol{b}^p.$$

Не менее интересным является следующий факт, носящий название «малой теоремы Ферма»:

Теорема 4. *Если p — простое число и $\boldsymbol{x} = x \bmod (p)$, то $\boldsymbol{x}^p = \boldsymbol{x}$.*

Доказательство. Если $\boldsymbol{x} = 0$, то утверждение очевидно. Пусть $\boldsymbol{x} \neq 0$. Это означает, что число x не делится на p, а так как p — простое, то числа x и p взаимно просты. Следовательно, классы $\boldsymbol{x}$, $2\boldsymbol{x}$, ..., $(\boldsymbol{p} - 1)\boldsymbol{x}$ — попарно различны: равенство $\boldsymbol{lx} = \boldsymbol{kx}$ означало бы, что $l = k$ (по теореме 2 этой главы элемент $\boldsymbol{x}$ обратим, и если $\boldsymbol{xy} = 1$, то, умножив обе части равенства $\boldsymbol{lx} = \boldsymbol{kx}$ на $\boldsymbol{y}$, мы получим, что $\boldsymbol{l} = \boldsymbol{k}$), а это невозможно, если $0 < l, k < p$ и $l \neq k$. Таким образом, $\boldsymbol{x}$, $2\boldsymbol{x}$, ..., $(\boldsymbol{p} - 1)\boldsymbol{x}$ — это в каком-то порядке переставленные классы 1, 2, ..., $\boldsymbol{p} - 1$, а потому произведение $\boldsymbol{x} \cdot 2\boldsymbol{x} \cdot \ldots \times \times (\boldsymbol{p} - 1)\boldsymbol{x}$ равно $1 \cdot 2 \ldots (\boldsymbol{p} - 1)$, т. е. $1 \cdot 2 \ldots (\boldsymbol{p} - 1) \times \times \boldsymbol{x}^{p-1} = 1 \cdot 2 \ldots (\boldsymbol{p} - 1)$. Следовательно, если последнее равенство сократить на $1 \cdot 2 \ldots \cdot (\boldsymbol{p} - 1)$, то получится $\boldsymbol{x}^{p-1} = 1$, или после домножения на x имеем $\boldsymbol{x}^p = \boldsymbol{x}$. Теорема доказана.

Множество ненулевых классов вычетов 1, 2, ..., $\boldsymbol{p} - 1$ по простому модулю p обладает многими интересными

свойствами. Одно из них состоит в следующем: среди этих классов всегда есть такой класс a, что любой другой класс является некоторой его степенью, т. е. для любого другого класса x существует такое натуральное t, что $a^t = x$.

Упражнения

1. По таблице 7 найти для каждого x из Z_7 обратный класс (т. е. такой y, что $xy = 1$).

2. Доказать, что если класс x кольца Z_n обратим, то существует ровно один класс y, для которого $xy = 1$ (предположив противное, т. е. существование равенства $1 = xy_1 = xy_2$, надо последнее из них домножить на y_1 или на y_2).

3. Доказать, что на элемент $a \neq 0$ кольца Z_n можно сокращать (т. е. гарантировать, что из $ax = ay$ следует $x = y$), тогда и только тогда, когда a является делителем единицы.

Указание. Достаточность этого условия почти очевидна, а необходимость следует установить от противного: если a не является делителем единицы, то $ab = 0$ при некотором $b \neq 0$ из Z_n; после этого нужно представить b в виде $x - y$ при некоторых $x \neq y$ из Z_n и рассмотреть равенство $a(x - y) = 0$.

4. Составить таблицы сложения и умножения для Z_8 и найти в этом кольце все делители нуля и все делители единицы.

5. Пусть N — произвольное натуральное число и r — число, равное количеству взаимно простых с N чисел ряда $1, 2, \ldots, N-1$. Доказать, что для любого целого числа a, взаимно простого с N, в кольце Z_n имеет место равенство: $a^r = 1$ (теорема Эйлера).

§ 3. ДИОФАНТОВЫ УРАВНЕНИЯ И ВЫЧЕТЫ

Теперь мы уже можем приступить к исследованию диофантовых уравнений более общего типа, чем рассматривались в главе I.

Сначала введем понятие целочисленного полинома от n переменных. Будем говорить, что $x_1, x_2, \ldots, x_n$ — независимые переменные, если каждая из них принимает целочисленные значения независимо от всех остальных. Мономом от переменных $x_1, x_2, \ldots, x_n$ называется всякое выражение вида

$$ax_1^{m_1}x_2^{m_2} \ldots x_n^{m_n}, \qquad (1)$$

где $m_1, m_2, \ldots, m_n$ — целые неотрицательные числа, а a — произвольное целое число, называемое коэффициен-

том монома. Если вместо каждой из букв $x_1, x_2, \ldots, x_n$ подставить в моном конкретные числа, например $x_1 = a_1, x_2 = a_2, \ldots, x_n = a_n$, то моном обратится в определенное целое число $a \cdot a_1^{m_1} a_2^{m_2} \ldots a_n^{m_n}$.

Два монома от одних и тех же переменных $ax_1^{m_1} x_2^{m_2} \ldots x_n^{m_n}$ и $bx_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ можно «умножать» и снова получать моном по следующему правилу:

$$(ax_1^{m_1} x_2^{m_2} \ldots x_n^{m_n})(bx_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}) = \\ = abx_1^{m_1+k_1} x_2^{m_2+k_2} \ldots x_n^{m_n+k_n}. \quad (2)$$

Конечно, равенство (2) остается верным, если вместо $x_1, x_2, \ldots, x_n$ подставить конкретные числовые значения.

Условимся и о том, как «складывать» мономы: под суммой двух мономов $ax_1^{m_1} x_2^{m_2} \ldots x_n^{m_n}$ и $bx_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ мы будем подразумевать выражение

$$ax_1^{m_1} \cdot x_2^{m_2} \ldots x_n^{m_n} + bx_1^{k_1} x_2^{k_2} \ldots x_n^{k_n},$$

которое при конкретных целочисленных значениях $x_1, x_2, \ldots, x_n$, скажем, $x_1 = a_1, x_2 = a_2, \ldots, x_n = a_n$, принимает целочисленное значение $aa_1^{m_1} a_2^{m_2} \ldots a_n^{m_n} + ba_1^{k_1} a_2^{k_2} \ldots \ldots a_n^{k_n}$. После этого нетрудно определить сумму любого конечного числа мономов от переменных $x_1, x_2, \ldots, x_n$.

Определение 6. *Целочисленным полиномом от переменных $x_1, x_2, \ldots, x_n$ называется любая сумма конечного числа мономов от переменных $x_1, x_2, \ldots, x_n$. Коэффициенты мономов-слагаемых называются коэффициентами полинома. Полином от n переменных мы будем обозначать через $f(x_1, x_2, \ldots, x_n)$.*

Так, например, $f(x_1, x_2) = x_1 + x_2$ — полином от двух переменных; его коэффициенты равны единице; для полинома $g(x_1, x_2) = x_1^2 + 2x_1x_2 + x_2^2$ характерно, конечно, то, что все его значения (т. е. числа, получающиеся при замене x_1 и x_2 на конкретные целые числа) являются квадратами — ведь

$$g(x_1, x_2) = (x_1 + x_2)^2.$$

Само собой разумеется, что многократное повторение слова «целочисленный» во всей проведенной конструкции обусловлено конкретностью наших целей; мы построили полином от n переменных $x_1, x_2, \ldots, x_n$, который при

целочисленных значениях последних принимает целочисленные значения. Но можно было говорить и о вещественных или о комплексных полиномах от n переменных, только коэффициенты мономов следовало бы тогда брать вещественными или, соответственно, комплексными и, аналогично, — значения переменных $x_1, x_2, \ldots, x_n$. Более того, можно построить (и это нам понадобится) полином от n переменных $x_1, x_2, \ldots, x_n$, коэффициенты которого являются классами вычетов по фиксированному модулю m и чьи переменные принимают значения из $\mathbf{Z}_m$. Такой полином мы будем называть (в отличие от целочисленного полинома) *полиномом над кольцом классов вычетов по модулю m*.

Рассмотрим связь между целочисленными полиномами и полиномами над кольцом классов вычетов. Пусть $f(x_1, x_2, \ldots, x_n)$ — целочисленный полином от n переменных и m — целое положительное число. Придадим переменным $x_1, x_2, \ldots, x_n$ какие-нибудь числовые значения, например $x_1 = a_1, \ x_2 = a_2, \ldots, x_n = a_n$, тогда полином обратится в число $f(a_1, a_2, \ldots, a_n)$. Обозначим теперь через $\bar{f}(x_1, x_2, \ldots, x_n)$ полином над кольцом классов вычетов по модулю m, который получается из $f(x_1, x_2, \ldots, x_n)$ заменой коэффициентов на их классы вычетов по модулю m. Тогда, как следует из § 2,

$$\overline{f(a_1, a_2, \ldots, a_n)} = \bar{f}(\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n),$$

где $\overline{f(a_1, a_2, \ldots, a_n)} = f(a_1, a_2, \ldots, a_n) \bmod (m)$ и $\bar{a}_i = a_i \bmod (m)$ $(i = 1, 2, \ldots, n)$. Мы будем называть полином $\bar{f}(x_1, x_2, \ldots, x_n)$ редукцией полинома $f(x_1, x_2, \ldots, x_n)$, по модулю m.

Например, если $m = 9$, $n = 2$ и $f(x_1, x_2) = 15x_1^3 + 9x_1^2x_2 + 8x_1x_2 + 11x_2^2$, то

$$\bar{f}(x_1, x_2) = \bar{6}x_1^3 + \bar{0}x_1^2x_2 + \bar{8}x_1x_2 + \bar{2}x_2^2 = \bar{6}x_1^3 + \bar{8}x_1x_2 + \bar{2}x_2^2.$$

Определение 7. *Диофантовым уравнением от n неизвестных называется уравнение вида*

$$f(x_1, x_2, \ldots, x_n) = 0, \tag{3}$$

где $f(x_1, x_2, \ldots, x_n)$ — целочисленный полином от n переменных и $x_1, x_2, \ldots, x_n$ принимают только целые значения.

Отметим, что если $x_1 = a_1$, $x_2 = a_2$, ..., $x_n = a_n$ — решение диофантова уравнения (3), т. е. $f(a_1, a_2, \ldots, a_n) = 0$, то

$$\bar{f}(\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n) = \bar{0} \qquad (4)$$

для редукции по любому модулю m. Следовательно, если при каком-либо m равенство (4) не выполняется для всевозможных вычетов $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n$ по модулю m, то уравнение (3) решений не имеет. Иными словами, справедлива теорема:

Теорема 5. *Необходимым условием существования решения уравнения* (3) *является выполнимость равенств* (4) *при всех модулях m и каких-либо вычетах $\bar{a}_i = a_i \bmod (m)$, $i = 1, 2, \ldots, n$.*

Примеры 1. Найти все решения диофантова уравнения

$$x^2 + 21xy + 14y^2 - 3 = 0.$$

Редукция по модулю 7 этого уравнения выглядит так:

$$x^2 = \bar{3}.$$

Но среди классов вычетов $\bar{0}$, $\bar{1}$, $\bar{2}$, $\bar{3}$, $\bar{4}$, $\bar{5}$, $\bar{6}$ по модулю 7 квадратами являются лишь классы $\bar{0}$, $\bar{1}$, $\bar{2}$, $\bar{4}$ — это проверяется непосредственно $\bar{0}^2 = \bar{0}$, $\bar{1}^2 = \bar{1}$, $\bar{2}^2 = \bar{4}$, $\bar{3}^2 = \bar{2}$, $\bar{4}^2 = \bar{2}$, $\bar{5}^2 = \bar{4}$ и $\bar{6}^2 = \bar{1}$; поэтому равенство $x^2 = \bar{3}$ никогда не выполняется и заданное уравнение не имеет решений.

2. Найти все решения диофантова уравнения:

$$15x^2 - 7y^2 = 9.$$

Пусть $x = m$, $y = n$ — решение. Из рассмотрения делимости на 3 и на 9 следует, что m^2 и n^2 делятся на 9; при этом частным от деления будут тоже квадраты, что легко получается из основной теоремы арифметики. Итак, $m^2 = 9m_1^2$ и $n^2 = 9n_1^2$. Данное уравнение приводится теперь к виду:

$$15m_1^2 - 7n_1^2 = 1,$$

а редукция по модулю 5 дает

$$-\bar{2}\bar{n}_1^2 = \bar{1}.$$

Учитывая, что $-\bar{2}\bar{2} = -\bar{4} = \bar{1}$, получаем

$$\bar{n}_1^2 = \bar{2}.$$

Но среди вычетов по модулю 5 квадратами являются лишь $\bar{0}$, $\bar{1}$ и $\bar{4}$. Поэтому данное уравнение не имеет решений.

Естественно задать следующий вопрос: является ли условие разрешимости редукций данного диофантова

уравнения по всевозможным модулям достаточным для того, чтобы само диофантово уравнение имело решение? В общем случае ответ на этот вопрос отрицательный. Можно показать, что, например, диофантово уравнение

$$(x^2 - 13)(x^2 - 17)(x^2 - 221) = 0,$$

не имеющее, очевидно, решений (ведь ни 13, ни 17, ни 221 не являются квадратами в кольце $\mathbf{Z}$) при редукции по любому модулю m приобретает решение среди соответствующих классов вычетов. Наших сведений, однако, для этой цели сейчас недостаточно: необходимо подробное описание подмножества квадратов в кольце классов вычетов по модулю m. Вот как его получить, по крайней мере, при простых m.

Пусть p — простое число, отличное от 2 (следовательно, — нечетное), $-\frac{p-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2}$ — все элементы из $\mathbf{Z}_p$. Если каждый из них возвести в квадрат, то получится не больше $\frac{p-1}{2}$ различных ненулевых элементов: ведь все они содержатся во множестве

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

Кроме того, все квадраты $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ попарно различны: если бы $\alpha^2 = \beta^2$, то обязательно $(\alpha - \beta)(\alpha + \beta) = 0$, и либо (ведь в $\mathbf{Z}_p$ нет делителей нуля) $\alpha = \beta$, либо $\alpha = -\beta$; первое невозможно, так как по условию α и β различны, второе исключено, так как α и β различные элементы множества $1, 2, \ldots, \frac{p-1}{2}$. Следовательно, в $\mathbf{Z}_p$ ровно $\frac{p-1}{2}$ ненулевых квадратов.

Когда среди этих элементов находится -1? По малой теореме Ферма $a^{p-1} = 1$ для всех $a \neq 0$ из $\mathbf{Z}_p$. Если a — квадрат, т. е. $a = b^2$ при некотором b, то $a^{\frac{p-1}{2}} = (b^2)^{\frac{p-1}{2}} = b^{p-1} = 1$. Вообще, $x^{\frac{p-1}{2}}$ равно 1 или -1 в зависимости от того, является ли x квадратом или нет. Действительно, если x — квадрат, то, как мы уже видели, это так; если же x не является квадратом, то $x^{\frac{p-1}{2}} = r$, но уже

$r^2 = 1$, или $r^2 - 1 = 0$. Последнее, в силу соотношения $r^2 - 1 = (r - 1)(r + 1)$ и отсутствия в Z_p делителей нуля, возможно лишь при $r = 1$ или $r = -1$. Если бы $r = 1$, то полином $z^{\frac{p-1}{2}} - 1$ над Z_p обращался бы в нуль более, чем при $\frac{p-1}{2}$ значениях z. Это, однако, невозможно по следующей причине:

Пусть $f(z) = a_0 z^n + \ldots + a_n$ — произвольный полином над Z_p и $f(c) = 0$ при некотором c из Z_p; тогда обязательно $f(z) = (z - c)\, g(z)$ при некотором полиноме $g(z)$ над Z_p. Действительно, проведем индукцию по числу n, называемому степенью полинома $f(x)$. При $n = 1$ полином $f(z)$ имеет вид $a_0 z + a_1$ и, так как $f(c) = 0$, т. е. $a_0 c + a_1 = 0$, обязательно $f(z) = a_0 z - a_0 c$. Следовательно, $f(z) = (z - c)\, a_0$. Предположим, что утверждение доказано для всех степеней, меньших n. Полином $g_1(z) = f(z) - a_0 z^{n-1}(z - c)$ имеет степень меньшую, чем n и, очевидно, обращается в нуль при $z = c$. Поэтому по предположению индукции, $g_1(z) = (z - c)\, g_2(z)$ и, следовательно, $f(z) = g_1(z) + a_0 z^{n-1}(z - c) = (z - c)(a_0 z^{n-1} + g_2(z))$. Утверждение доказано. Из него вытекает, что если $c_1, \ldots, c_k$ — разные элементы из Z_p, для которых $f(c_1) = \ldots = f(c_k) = 0$, то $f(z) = (z - c_1)\ldots(z - c_k) g(z)$. Надо рассуждать так же, как выше, выделяя сначала в $f(z)$ множитель $z - c_1$ (получается $f(z) = (z - c_1)\, g_1(z)$ и, следовательно, $g_1(c_2) = 0$), затем $z - c_2$ в $g_1(z)$ и т. д. Так как степени полиномов при умножении складываются, то в выражении $f(z) = (z - c_1)\ldots(z - c_k)\, g(z)$ справа не может быть больше множителей вида $(z - c_l)$, чем степень полинома $f(z)$. Вот почему полином $z^{p-1} - 1$, упомянутый в предыдущем абзаце, не может иметь более, чем $\frac{p-1}{2}$ значений z, для которых его значение равно 0.

Следовательно, $x^{\frac{p-1}{2}} = -1$. Отсюда принципиально важный вывод: элемент x из Z_p является квадратом тогда и только тогда, когда $x^{\frac{p-1}{2}} = 1$ и не является квадратом тогда и только тогда, когда $x^{\frac{p-1}{2}} = -1$. Таким образом, -1 является квадратом, когда $(-1)^{\frac{p-1}{2}} = 1$, и не является квадратом, когда $(-1)^{\frac{p-1}{2}} = -1$. Число p — нечетное; следовательно, либо $p = 4k + 1$, либо $p = 4k - 1$. В первом случае обязательно $(-1)^{\frac{p-1}{2}} = (-1)^{2k} = 1$ и (-1) — квадрат; во втором случае обязательно $(-1)^{\frac{p-1}{2}} = (-1)^{2k-1} = -1$ и -1 не является квадратом. И еще одно утверждение: если x и y из Z_p не являются квадратами, то обязательно xy — квадрат (докажите это самостоятельно).

В диофантовом уравнении $(x^2 - 13)(x^2 - 17)(x^2 - 221) = 0$ замечаем, что $221 = 13 \cdot 17$; следовательно, в редукции по простому

модулю это уравнение имеет решение (хотя один из классов 13, 17 или 13 · 17 — квадрат).

Теперь можно доказать утверждение, сформулированное еще в гл. II: всякое простое число p вида $p = 4k + 1$, где k — целое, является нормой целого гауссового числа (и, следовательно, представимо в виде суммы двух целых квадратов): $p = x^2 + y^2$. Доказательство проведем индукцией по p. При $p = 5$ (это самое маленькое p вида $4k + 1$) утверждение очевидно: $5 = 2^2 + 1^2$. Допустим, что утверждение доказано для всех простых чисел вида $4k + 1$, меньших простого числа p такого же вида: $p = 4k + 1$. В кольце Z_p класс -1 является квадратом (это было доказано выше), т. е. $x^2 + 1 = 0$ при некотором x из Z_p. Это означает, что в кольце целых чисел Z $x^2 + y^2 = lp$, где x и y — целые числа и где класс вычетов числа y — это класс 1. Поскольку все квадраты в Z_p получаются из серии $0^2, 1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$, можно считать, что $0 < x, y < \frac{p}{2}$ и, следовательно, $l < p$. Конечно, будем считать, что x и y — взаимно простые целые числа (в противном случае мы сократили бы равенство $x^2 + y^2 = lp$ на их общие делители).

Пусть $l = p_1 \cdot p_2 \ldots p_r$ — разложение числа l на простые множители в кольце Z. Так как $(x, y) = 1$ и $x^2 + y^2$ делится на p_j ($j = 1, 2, \ldots, r$), класс $-1 \bmod p_j$ является квадратом в Z_{p_j}, то $p_j = 4m_j + 1$ при некотором целом m_j ($j = 1, 2, \ldots, r$). Поскольку $p_j < p$, то по предположению индукции

$$p_j = x_j^2 + y_j^2 = (x_j + iy_j)(x_j - iy_j) = t^{(j)} \cdot \bar{t}^{(j)},$$

где $t^{(j)}$, $\bar{t}^{(j)}$ — простые множители в кольце целых гауссовых чисел, и, как обычно, $\overline{a + bi} = a - bi$ — сопряженное число.

Следовательно,

$$(x + iy)(x - iy) = pt^{(1)} \ldots t^{(r)}\bar{t}^{(1)} \ldots \bar{t}^{(r)}.$$

В правой части равенства имеем произведение простых гауссовых чисел. Пользуясь справедливостью основной теоремы арифметики в кольце целых гауссовых чисел, сократим правую и левую части последнего равенства на простые числа $t^{(1)}, \bar{t}^{(1)} \ldots t^{(r)}, \bar{t}^{(r)}$, в результате получим представление простого целого числа p в виде произведения сопряженных гауссовых чисел. Теорема доказана.

Изучение уравнений над кольцами классов вычетов имеет важное значение в теории чисел именно потому, что позволяет во многих случаях «предугадать» исход решения той или иной диофантовой задачи.

Мы закончим эту главу примером изучения редукций одного частного диофантова уравнения:

$$f(x, y) = ax^2 + 2bxy + cy^2 = 0.$$

Условимся символом $\bar{f}_p(x, y)$ обозначать редукцию полинома $f(x, y)$ по модулю p.

Теорема 6. *Пусть $p \neq 2$ — простое число. Уравнение*

$$f_p(x, y) = \bar{0}$$

имеет решение, отличное от $x = y = \bar{0} = 0 \bmod (p)$, тогда и только тогда, когда $\bar{b}^2 - \bar{a} \cdot \bar{c} = (b^2 - ac) \bmod (p)$ является квадратом в кольце $\mathbf{Z}_p$.

Доказательство. Пусть $\bar{b} - \overline{ac} = \bar{z}^2$ и допустим, что $\bar{a} \neq \bar{0}$. Поскольку среди ненулевых классов вычетов по простому модулю возможно деление, то в результате алгебраических преобразований можно получить следующее равенство:

$$\bar{a}x^2 + \overline{2b}xy + \bar{c}y^2 = \bar{a}\left(x - \frac{-\bar{b} + \bar{z}}{\bar{a}} y\right)\left(x - \frac{-\bar{b} - \bar{z}}{\bar{a}} y\right)$$

(в его справедливости можно убедиться непосредственно, на основании определения действий над мономами). Следовательно, достаточно найти решение уравнения:

$$\left(x - \frac{\bar{z} - \bar{b}}{\bar{a}} y\right)\left(x + \frac{\bar{b} + \bar{z}}{\bar{a}} y\right) = 0.$$

Эти решения, ввиду отсутствия делителей нуля в кольце классов вычетов по простому модулю, описываются двумя независимыми равенствами:

$$x = \frac{-\bar{b} + \bar{z}}{\bar{a}} y \quad \text{и} \quad x = \frac{-\bar{b} - \bar{z}}{\bar{a}} y.$$

Если $\bar{a} = \bar{0}$, а $\bar{c} \neq \bar{0}$, то все сказанное выше легко переносится и на этот случай. Если же $\bar{a} = \bar{c} = \bar{0}$, то ненулевым решением данного уравнения будет, например, $x = \bar{1}$, $y = \bar{0}$.

Обратно, пусть $x = \bar{x}$, $y = \bar{y}$ — решение, причем либо $\bar{x} \neq \bar{0}$, либо $\bar{y} \neq \bar{0}$. Если $\bar{a} = \bar{c} = \bar{0}$, то утверждение очевидно: $\bar{b}^2$ является квадратом. Пусть $\bar{a} \neq \bar{0}$. Тогда

$$\bar{0} = \bar{a}\bar{x}^2 + 2\bar{b}\bar{x}\bar{y} + \bar{c}\bar{y}^2 = \bar{a}^2\left(\bar{x}^2 + \frac{\overline{2b}}{\bar{a}} \bar{x}\bar{y} + \frac{\bar{c}}{\bar{a}} \bar{y}^2\right) =$$

$$= \bar{a}\left(\left(\bar{x} + \frac{\bar{b}}{\bar{a}} \bar{y}\right)^2 - \frac{\bar{b}^2 - \overline{ac}}{\bar{a}^2} \bar{y}^2\right).$$

Следовательно,

$$\left(\bar{x} + \frac{\bar{b}}{\bar{a}} \bar{y}\right)^2 = \frac{\bar{b}^2 - \overline{ac}}{\bar{a}^2} \bar{y}^2.$$

Так как $\bar{a} \neq \bar{0}$, то класс $\bar{y}$ отличен от $\bar{0}$; если бы $\bar{y} = 0$, то и $\bar{x} = 0$, а это противоречит условию. Следовательно,

$$\bar{b}^2 - \bar{a} \cdot \bar{c} = \frac{\bar{a}^2}{\bar{y}^2}\left(\bar{x} + \frac{\bar{b}}{\bar{a}}\bar{y}\right)^2 = \left[\frac{\bar{a}}{\bar{y}}\left(\bar{x} + \frac{\bar{b}}{\bar{a}}\bar{y}\right)\right]^2.$$

Теорема доказана.

В условии предполагалось, что $p \neq 2$. Однако это было сделано не потому, что при $p = 2$ теорема не верна: в этом случае ее утверждение тривиально, потому что редукция $\bar{f}_2(x, y)$ равна $\bar{a}x^2 + \bar{c}y^2$, а оба класса вычетов по модулю 2 являются квадратами и в то же время уравнение $\bar{a}x^2 + \bar{c}y^2 = \bar{0}$ обязательно обладает решениями — это устанавливается просто перебором всевозможных значений полинома $\bar{f}_2(x, y)$.

Глава IV
СИСТЕМЫ СЧИСЛЕНИЯ

При записи чисел мы обычно пользуемся десятью символами: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. Их называют *десятичными цифрами*. В этой главе мы рассмотрим роль числа 10 в традиционной записи чисел и опишем возможные способы замены «десятки» на другие натуральные числа. Особенно важной в наше время стала такая форма записи, в которой роль десятки играет двойка: в электронных вычислительных машинах применяют не десятичную, а так называемую д в о и ч н у ю систему записи.

§ 1. ДЕСЯТИЧНАЯ СИСТЕМА СЧИСЛЕНИЯ

Под десятичной системой счисления понимают всю систему чисел, записанных в обычной форме с помощью десятичных цифр — символов 0, 1, 2, ..., 9, каждый из которых обозначает и некоторое целое неотрицательное число. Подобные системы записи чисел называются «позиционными» — в них цифра означает различные числа в зависимости от того, какое место она занимает в записи. Конечно, вместо этих десяти символов можно было бы взять и другие, но если бы этих других было снова десять и употреблялись они аналогично традиционным цифрам,

то систему чисел все равно следовало бы назвать десятичной.

В чем же состоит роль числа десять? Дело в том, что мы записываем числа с помощью всевозможных остатков от деления на 10; именно как остатки от деления на 10 ведут себя десятичные цифры во всех арифметических операциях над числами. Действительно, расшифруем десятичную запись числа:

Пусть сначала N — натуральное число. Из алгоритма деления с остатком следует, что $N = 10q_0 + r_0$, где $0 \leqslant r_0 \leqslant 9$ и $0 \leqslant q_0 < N$ (если, например, $N = 6$, то $q_0 = 0$ и $r_0 = 6$). Если частное $q_0 > 0$, то точно так же $q_0 = 10q_1 + r_2$, где $0 \leqslant r_1 \leqslant 9$ и

$$N = 10q_0 + r_0 = 10^2q_1 + 10r_1 + r_0.$$

Если $q_1 > 0$, то этот процесс можно продолжить, получив

$$N = 10^3q_2 + 10^2r_2 + 10r_1 + r_0.$$

Частное q_2 будет меньше, чем q_1, а q_1 — меньше, чем q_0, которое меньше, чем N. Поэтому после конечного числа шагов n мы получим, что $q_n = 0$ и

$$N = 10^nr_n + 10^{n-1}r_{n-1} + \ldots + 10r_1 + r_0, \qquad (1)$$

где $r_0, \ldots, r_n$ — неотрицательные целые числа, не превосходящие 9. Запись (1), полученная вполне конкретным образом по числу N, называется десятичным представлением (или десятичным разложением) числа N.

Следует заметить, что если бы существовало второе выражение

$$N = 10^{n'}r'_{n'} + 10^{n'-1}r'_{n'-1} \ldots + 10r'_1 + r'_0, \qquad (1')$$

полученное каким-то иным способом, и в котором $r'_{n'}, \ldots, r'_0$ — неотрицательные целые числа, не превосходящие 9, то оказалось бы, что $n' = n$ и $r'_i = r_i$ для $i = 1, 2, \ldots, n$. Действительно, остаток от деления на 10 числа N определен однозначно и, как следует из представлений (1) и (1'), равен r_0 и r'_0. Поэтому $r_0 = r'_0$. Равенство чисел r_1 и r'_1 получается из единственности остатка от деления на 10 числа $\frac{N - r_0}{10}$. Предоставляем читателю самостоятельно завершить доказательство.

Если принять, что символ $\overline{a_na_{n-1} \ldots a_0}$ обозначает записанные подряд десятичные цифры $a_n, a_{n-1}, \ldots, a_0$

то, конечно, число N, записанное десятичными цифрами, имеет вид:

$$N = \overline{r_n r_{n-1} \ldots r_0}.$$

С представлением (1) связано немало интересных фактов. Вот некоторые из них:

Теорема 1. *Разность между числом и суммой его цифр делится на 9.*

Доказательство. Пусть имеем число N, представленное в виде (1). Тогда

$$N - (r_0 + \ldots + r_n) = 10^n r_n + 10^{n-1} r_{n-1} + \ldots + 10 r_1 +$$

$$+ r_0 - r_n - r_{n-1} - \ldots - r_1 - r_0 =$$

$$= (10^n - 1) r_n + (10^{n-1} - 1) r_{n-1} + \ldots + (10 - 1) r_1.$$

Но $10 \bmod (9) = 1 \bmod (9)$, так что и $10^n \bmod (9) = 1 \bmod (9)$, благодаря чему $N \bmod (9) = (r_n + \ldots + r_0) \bmod (9)$ и, следовательно, $N - (r_n + \ldots + r_0) \equiv 0 \bmod (9)$. Утверждение доказано.

Следствие. *Если сумма цифр числа N делится на 9, то и само число делится на 9.*

Обратно, если число делится на 9, то кратна девяти и сумма его цифр.

Действительно, если M — сумма цифр числа N, делящаяся на 9, то из $N \equiv M \bmod (9)$ следует, что $N \equiv 0 \bmod (9)$. Аналогично, если $N \equiv 0 \bmod (9)$, то из $N \equiv M \bmod (9)$ следует, что и $M \equiv 0 \bmod (9)$.

Точно так же формулируется и доказывается признак делимости на 3.

Теорема 2. *Если разность между суммой цифр числа N, стоящих на четных местах, и суммой цифр этого же числа, стоящих на нечетных местах, делится на 11, то и число N делится на 11.* Верно и обратное: *если число N кратно 11, то разность между суммами указанных цифр делится на 11.*

Доказательство. Заметим, что $10^{2k} \equiv 1 \bmod (11)$ и $10^{2k+1} \equiv 10 \bmod (11)$. Поэтому, переходя от выражения (1) к вычетам по модулю 11, получаем:

$$N \equiv r_0 + 10 n_1 + r_2 + 10 r_3 \ldots \bmod (11),$$

откуда

$$N \equiv (r_0 + r_2 + \ldots) + 10 (r_1 + r_3 + \ldots) \bmod (11).$$

Если $(r_0 + r_2 + \ldots) \equiv (r_1 + r_3 + \ldots) \bmod (11)$, то, конечно

$$N \equiv (r_1 + r_3 + \ldots) + 10 (r_1 + r_3 + \ldots) \bmod (11) \equiv$$

$$\equiv 0 \bmod (11).$$

Обратно, если $N \equiv 0 \bmod (11)$, то, учитывая сравнение $10 \equiv -1 \bmod (11)$, получаем:

$$(r_0 + r_2 + \ldots) + 10\,(r_1 + r_3 + \ldots) \equiv 0 \bmod (11)$$

и

$$(r_0 + r_2 + \ldots) - (r_1 + r_3 + \ldots) \equiv 0 \bmod (11).$$

Как видим, при десятичной записи натурального числа цифры стоят в совершенно строгом порядке как остатки от деления на 10. Любое целое число записывается точно так же, только перед записью отрицательного числа ставится знак минус.

Перейдем к числам рациональным — несократимым дробям вида $R = \frac{N}{M}$, где для начала будем считать N и M натуральными числами, а потом рассмотрим и отрицательные рациональные числа. Наша ближайшая цель получить для такого числа разложение вида (1), совпадающее с ним при $M = 1$.

Будем считать, что дробь $R = \frac{N}{M}$ — правильная, т. е. $N < M$. В противном случае мы могли бы выделить целую часть, десятичное представление которой уже описано, и после этого рассматривать правильную дробь.

Пусть $10N = q_1 M + a_1$, где $0 \leqslant a_1 < M$. Тогда $0 \leqslant q_1 < 9$, потому что $10N < 10M$ и

$$R = \frac{N}{M} = \frac{10N}{10M} = \frac{q_1 M + a_1}{10M} = 10^{-1} q_1 + 10^{-1} \frac{a_1}{M}.$$

Если $a_1 = 0$, то десятичное представление для R выглядит так:

$$R = 10^{-1} q_1. \tag{2}$$

Если $a_1 \neq 0$, то, аналогично,

$$\frac{a_1}{M} = 10^{-1} q_2 + 10^{-1} \frac{a_2}{M},$$

где опять $0 \leqslant q_2 \leqslant 9$ и $0 \leqslant a_2 < M$. При $a_2 = 0$ десятичное представление для R имеет вид

$$R = 10^{-1} q_1 + 10^{-2} q_2.$$

Если $a_2 \neq 0$, то

$$\frac{a_2}{M} = 10^{-1} q_3 + 10^{-1} \frac{a_3}{M},$$

где $0 \leqslant q_3 \leqslant 9$ и $0 \leqslant a_3 < M$ и т. д.

Возможны два случая: либо на одном из шагов остаток обратится в 0, и мы получим конечную десятичную дробь

$$R = 0, \overline{q_{-1}q_{-2} \ldots q_{-k}} = q_{-1}10^{-1} + q_{-2}10^{-2} + \ldots + q_{-k}10^{-k} \quad (3)$$

либо a_k никогда не обратится в 0. Но так как остатков от деления на число M всего лишь M, остатки a_k (а следовательно, частные q_k) начнут повторяться: мы получим бесконечную периодическую десятичную дробь:

$$R = 10^{-1}q_{-1} + 10^{-2}q_{-2} + \ldots + 10^{-k}q_{-k} + \ldots$$

Остановимся на этом случае несколько подробнее, чтобы установить длину периода. Пусть таблица вычисления остатков имеет вид:

$$\begin{aligned} 10a_0 &= Mq_1 + a_1, \\ 10a_1 &= Mq_2 + a_2, \\ &\ldots\ldots\ldots \\ 10a_{k-2} &= Mq_{k-1} + a_{k-1}, \\ 10a_{k-1} &= Mq_k + a_0. \end{aligned} \quad (4)$$

Здесь для простоты нумерация букв сразу выбрана такой, чтобы первая цифра периода (т. е. некоторое частное q_i, полученное в описанном выше процессе) имела номер 1; в последней строке таблицы вновь во второй раз появляется остаток a_0, с которого было начато перечисление в (4). Напоминаем, что остатки $a_0, a_1, \ldots, a_{k-1}$ все отличны от 0, чего, конечно, нельзя сказать о цифрах q_i. Схематически соответствующий кусок десятичной дроби выглядит так:

$$0, \overline{\ldots q_1q_2 \ldots q_{k-1}q_k \ldots}$$

После того как мы запишем цифру q_k, следующей вычисленной цифрой будет вновь q_1; следовательно, период дроби начинается с цифры q_1 и заканчивается на q_k. Всего таких цифр k. Рассмотрим (4) по модулю M:

$$\begin{aligned} 10a_0 &\equiv a_1, \\ 10a_1 &\equiv a_2, \\ &\ldots\ldots \\ 10a_{k-2} &\equiv a_{k-1} \\ 10a_{k-1} &\equiv a_0; \end{aligned} \quad (5)$$

подставляя a_1 из первого сравнения во второе, затем a_2 из второго в третье и т. д., получим:

$$10^k a_0 \equiv a_0.$$

Возможны два случая: $(10,\ M) = 1$ и $(10,\ M) \neq 1$. В первом случае в равенстве $10N = Mq + a$, где $0 \leqslant a < M$, числа a и M взаимно простые, потому что любой их общий делитель, будучи взаимно простым с 10, должен делить и N, а $(N,\ M) = 1$ по условию. Следовательно, при $(10,\ M) = 1$ все остатки a_i взаимно просты с M и, в частности, $(a_0,\ M) = 1$. Это означает, что класс $a_0 \bmod (M)$ обратим, а потому

$$10^k \equiv 1 \bmod (M).$$

Число k, для которого $10^k \equiv 1 \bmod (M)$, является наименьшим среди натуральных чисел n, для которых $10^n \equiv 1 \bmod (M)$. Действительно, если бы $10^n \equiv 1 \bmod (M)$ при $n < k$, то из сравнений (5) следовало бы, что

$$a_n \equiv 10^n a_0 \equiv a_0 \bmod (M).$$

Но a_n и a_0 — остатки от деления на M, поэтому сравнение $a_n \equiv a_0 \bmod (M)$ означает равенство $a_n = a_0$, а это противоречит тому, что все остатки $a_0,\ a_1,\ \ldots,\ a_{k-1}$ попарно различны (на этом были основаны равенства (4)).

Рассмотрим случай $(10,\ M) \neq 1$. Пусть $M = 2^r 5^s M'$, где уже $(10,\ M') = 1$. Тогда $R = \frac{N}{M} = \frac{N}{2^r 5^s M'}$, домножим числитель и знаменатель дроби R на такие степени двойки и пятерки, чтобы знаменатель принял вид $10^l M'$ (например, $\frac{29}{140} = \frac{29}{2^2 \cdot 5 \cdot 7} = \frac{2^0 \cdot 5 \cdot 29}{10^2 \cdot 7} = \frac{145}{10^2 \cdot 7}$). Получим: $R = 10^{-l} \frac{N'}{M'}$, где $(M',\ N') = 1$ и $(M',\ 10) = 1$. По доказанному период дроби $R' = \frac{N'}{M'}$ равен тому наименьшему натуральному числу k, для которого $10^k \equiv 1 \bmod (M')$. Но период дроби $R = 10^{-l} \cdot R'$ таков же, он лишь начинается на l знаков правее.

Мы доказали такую теорему:

Теорема 3. *Пусть* $R = \frac{N}{M}$ *и* $M = 2^r 5^s M'$, *где* $(N,\ M) = 1$ *и* $(10,\ M') = 1$. *Тогда период дроби равен тому наименьшему натуральному* k, *при котором*

$$10^k \equiv 1 \bmod (M').$$

Прежде чем описать восстановление десятичных цифр рациональных дробей, основанное, как и в случае натуральных чисел, на десятичном разложении

$$R = r_{-1} \cdot 10^{-1} + \ldots + r_{-n} \cdot 10^{-n} + \ldots, \qquad (6)$$

где $0 \leqslant r_{-l} \leqslant 9$, отметим следующее обстоятельство, благодаря которому будет введена однозначность представления (6):

$$10^{-s} = 9 \cdot 10^{-s-1} + 9 \cdot 10^{-s-2} + \ldots + 9 \cdot 10^{-s-n} + \ldots$$

(т. е. 0, 0 ... 0 1 = 0, 0 ... 0 9 9 ... 9...).

Доказательство. В соответствии с правилом суммирования бесконечно убывающей геометрической прогрессии имеем

$$9 \cdot 10^{-s-1} + 9 \cdot 10^{-s-2} + \ldots = 9 \cdot 10^{-s}(10^{-1} + \\ + 10^{-2} + \ldots) = 9 \cdot 10^{-s} \cdot \frac{10^{-1}}{1 - 10^{-1}} = 10^{-s}.$$

Поэтому естественно предположить, что всюду вместо «девятки в периоде» можно писать единицу в предшествующем периоду разряде, т. е.

$$0, \overline{r_{-1} \ldots r_{-k}\, 9\, 9 \ldots} = 0, \overline{r_{-1} \ldots r_{-k}} + 0, \underbrace{0 \ldots 0}_{k} 1.$$

Восстановление десятичных знаков дроби R можно теперь описать так.

Пусть

$$R = r_{-1} \cdot 10^{-1} + r_{-2} \cdot 10^{-2} + \ldots + r_{-k} \cdot 10^{-k} + \ldots$$

Тогда r_{-1} — это целая часть числа $10R$, r_{-2} — целая часть числа $10(10R - r_{-1})$ и т. д. r_{-k} — целая часть числа

$$10^k R - 10^{-k-1} r_{-1} - \ldots - 10 r_{-k+1}.$$

Рассмотрим на примерах полученный результат. Пусть $R = \frac{2}{3}$. Длина периода l этой дроби в десятичном представлении равна наименьшему из таких чисел k, что $10^k \equiv 1 \bmod (3)$. Очевидно, $l = 1$. Сам период легко определяется: $R = 0, 6\,6\,6 \ldots$.

А вот пример дроби с большей длиной периода в десятичном представлении: $R_l = \frac{1}{7}$. Здесь отыскать наименьшее число l, для которого $10^l \equiv 1 \bmod (z)$ лучше всего так. Символ $\bmod (7)$ в записях будем для удобства

опускать. В кольце $\mathbf{Z}_7$ имеем: $10 \equiv 3$. Поэтому $10^n \equiv 3^n$ и, следовательно,

$$3^1 \equiv 3,$$
$$3^2 \equiv 2,$$
$$3^3 \equiv 3 \cdot 2 \equiv 6,$$
$$3^4 \equiv 3 \cdot 6 \equiv 4,$$
$$3^5 \equiv 3 \cdot 4 \equiv 5,$$
$$3^6 \equiv 3 \cdot 5 \equiv 1.$$

Таким образом, длина периода l равна 6.

Упражнения

1. Найти длину периода дроби $R = \frac{1}{23}$ в десятичном представлении.

Ответ. Длина периода равна 22.

2. Доказать, что существуют десятичные дроби с как угодно большой длиной периода.

Указание. Пусть N — произвольное натуральное число. Запишем десятичную дробь R за несколько шагов по следующему правилу: 1-й шаг — 0,10, 2-й шаг — 0,101100, 3-й шаг — 0,101100111000, ... и т. д. до тех пор, пока число цифр в дробной части не превзойдет N. После этого припишем к полученной дроби ее дробную часть еще и еще раз, и т. д. Полученная бесконечная дробь будет, конечно, периодической. Остается лишь доказать, что ее период равен переписываемой части.

Подводя итог, можно сказать, что любое рациональное число записывается либо в виде конечной, либо в виде бесконечной, но обязательно периодической десятичной дроби (целая часть которой может быть равна 0 или отлична от 0). Разумеется, верно и обратное: всякая конечная десятичная или бесконечная, но периодическая десятичная дробь есть рациональное число. Для конечной дроби это утверждение просто очевидно, а для периодической доказывается так. Данную периодическую дробь можно представить в виде суммы конечной десятичной дроби и дроби вида:

$$p = 0, \underbrace{0 \ldots 0}_{s} \overline{q_1 \ldots q_n q_1 \ldots q_n},$$

где $\overline{q_1 \ldots q_n}$ — период. Как уже говорилось, первое слагаемое (т. е. конечная дробь) — число рациональное; что

касается второго, то, положив $\overline{q_1 \ldots q_n} = q$, представим его в виде:

$$\rho = q \cdot 10^{-n-s} + q \cdot 10^{-2n-s} + q \cdot 10^{-3n-s} + \ldots =$$
$$= q \cdot 10^{-s}(10^{-n} + 10^{-2n} + 10^{-3n} + \ldots).$$

Согласно правилу суммирования бесконечно убывающей геометрической прогрессии, имеем

$$10^{-n} + 10^{-2n} + \ldots = \frac{10^{-n}}{1 - 10^{-n}} = \frac{1}{10^n - 1}.$$

Таким образом, ρ — рациональное число, а потому рациональна и данная дробь.

Обратимся, наконец, к иррациональным числам, под которыми принято подразумевать бесконечные непериодические десятичные дроби. Восстановление десятичных цифр такого числа проводится в два этапа: сначала восстанавливаются цифры целой части (по правилу, описанному для целых чисел), а потом цифры дробной части.

Итак, произвольное (будем считать, что неотрицательное) вещественное число R в десятичной системе счисления записывается в виде

$$R = 10^n a_n + \ldots + 10a_1 + a_0 + 10^{-1}a_{-1} + \ldots + 10^{-k}a_{-k} + \ldots, \quad (7)$$

где $a_n, \ldots, a_1, a_0, a_{-1}, \ldots, a_{-k}$ — десятичные цифры. С учетом замечания, сделанного на стр. 56, запись (7) числа R единственна. Мы будем называть (7) десятичным представлением (или десятичным разложением) числа R.

Предположим, что P и Q — вещественные числа, записанные в виде (7) и, как обычно, $P \geqslant 0$, $Q \geqslant 0$. Опишем разложение (7) числа $P + Q$. Строго говоря, получить десятичное разложение числа $P + Q$ можно лишь постепенно «повышая точность задания» слагаемых P и Q. Но, поскольку мы не ставим своей целью развить сейчас арифметику вещественных чисел, а хотим всего лишь проиллюстрировать поведение цифр при сложении, нам достаточно будет считать P и Q — конечными десятичными дробями:

$$P = 10^n p_n + \ldots + 10^r p_r + \ldots + p_0 + 10^{-1}p_{-1} + \ldots + 10^{-m}p_{-m},$$
$$Q = 10^l q_l + \ldots + 10^r q_r + \ldots + q_0 + 10^{-1}q_{-1} + \ldots + 10^{-m}q_{-m} \quad (8)$$

(среди цифр p_{-m} и q_{-m} хотя бы одна не равна 0).

В разложении (7) числа $P+Q$ при 10^{-k}, $k>m$ стоят нулевые цифры. При 10^{-m} стоит остаток от деления на 10 числа $p_{-m}+q_{-m}$; пусть $p_{-m}+q_{-m}=10a_{-m}+b_{-m}$, $0\leqslant b_{-m}\leqslant 9$. Тогда при 10^{-m+1} стоит остаток от деления на 10 числа $p_{-m+1}+q_{-m+1}$, сложенный с частным a_{-m} и вновь приведенный по модулю 10, и т. д. Цифры p_r и q_r оказываются, таким образом, подчиненными сложению арифметики вычетов по модулю 10.

Обратимся к десятичному представлению числа $P-Q$, не считая, что P и Q заданы в виде (8), но зато предполагая известным процесс сложения в общем случае.

Пусть $10^n\leqslant Q<10^{n+1}$ и $Q=10^{n+1}-Q'$. Таким образом, $P-Q=-10^{n+1}+P+Q'$ и десятичное разложение числа $P-Q$ легко получить из десятичного разложения числа $P+Q'$. Действительно, пусть a_{n+1} — цифра числа $P+Q'$, стоящая в разложении (7) при 10^{n+1}. Если $a_{n+1}\geqslant 1$, то ответ очевиден. Если же $a_{n+1}=0$, то надо рассмотреть два случая: $10^{n+1}>P+Q'$ и $10^{n+1}<P+Q'$. В первом случае число $P+Q'-10^{n+1}$ отрицательное и его десятичная запись получается на основе представления

$$10^{n+1}=9\cdot 10^n+9\cdot 10^{n-1}+\ldots+9\cdot 10+9+$$
$$+9\cdot 10^{-1}+9\cdot 10^{-2}+9\cdot 10^{-3}+\ldots \qquad (9)$$

Вычитать из такого представления число $P+Q'$ можно просто поразрядно, а потом, при необходимости, воспользоваться замечанием, сделанным на стр. 56. Что касается случая $10^{n+1}<P+Q'$ и $a_{n+1}=0$, то он разбирается так. Пусть a_{n+k} — ближайшая слева к a_{n+1} цифра, отличная от 0 (такая цифра существует ввиду неравенства $10^{n+1}<P+Q'$). Тогда вместо слагаемого $a_{n+k}\cdot 10^{n+k}$ можно написать сумму двух слагаемых: $(a_{n+k}-1)\,10^{n+k}$ и 10^{n+k}, но 10^{n+k} представляется в виде, аналогичном (9). После этого десятичная запись числа $P+Q'-10^{n+k}$ получается в соответствии с правилами, указанными для суммирования.

Уже на примере этих двух основных арифметических операций над числами мы видим, что десятичные цифры ведут себя как остатки от деления на 10. Умножение и деление вещественных чисел в десятичной записи определяются на основе операций сложения и вычитания, и поэтому цифры оказываются вновь подчиненными арифметике вычетов по модулю 10.

§ 2. N-ИЧНАЯ СИСТЕМА СЧИСЛЕНИЯ

Из предыдущего параграфа можно заметить, что число и способ, по которому его записывают (формула (7)), связаны в основном лишь традицией. Мы начали с алгоритма вычисления десятичных цифр, взяв произвольное натуральное число N, а не то, как это число записано.

Заменим теперь десятку другим, произвольно фиксированным натуральным числом N и повторим, по крайней мере в существенных чертах, построения предыдущего параграфа.

Во-первых, нужны цифры — всевозможные остатки от деления на N, т. е. числа $0, 1, \ldots, N-1$. Кстати, если $N=1$ (это ведь тоже натуральное число), то 0 — единственная цифра; конечно, располагая всего одной цифрой, записывать бесконечное множество чисел нельзя. Поэтому будем полагать, что $N \geqslant 2$.

Пусть A — произвольное натуральное число. Запишем его с помощью остатков от деления на N, т. е. с помощью чисел $0, 1, \ldots, N-1$. Для этого разделим A на N с остатком:

$$A = Nq_0 + r_0, \quad 0 \leqslant r_0 < N.$$

Если $q_0 = 0$, то равенство

$$A = r_0$$

и будет искомым N-ичным представлением числа A. Если же $q_0 \neq 0$, то разделим q_0 на N с остатком:

$$q_0 = Nq_1 + r_1, \quad 0 \leqslant r_1 < N.$$

Тогда

$$A = N^2q_1 + Nr_1 + r_0.$$

Если $q_1 = 0$, то искомым N-ичным представлением числа A будет

$$A = r_1N + r_0.$$

Если же $q_1 \neq 0$, то процесс следует продолжить. Поскольку q_1 меньше q_0, а q_0 меньше A, постольку частные q_0, q_1 и т. д. уменьшаются, оставаясь целыми неотрицательными числами; следовательно, на каком-то этапе мы получим нулевое частное q_k и одновременно N-ичное представление натурального числа A:

$$A = r_kN^k + r_{k-1}N^{k-1} + \ldots + r_1N + r_0, \qquad (10)$$

где $r_0, r_1, \ldots, r_{k-1}, r_k$ — целые неотрицательные числа, не превосходящие $N-1$; мы условились называть их N-ичными цифрами.

Представление (10) натурального числа A единственно, т. е. не зависит от описанного способа вычисления цифр $r_0, r_1, \ldots, r_{k-1}, r_k$. Если бы

$$A = r'_{k'}N^{k'} + r'_{k'-1}N^{k'-1} + \ldots + r'_1 N + r_0 \qquad (10')$$

и $r'_{k'}, r'_{k'-1}, \ldots, r'_1, r_0$ были бы целыми неотрицательными числами, не превосходящими $N-1$, то r_0 и r_0 совпадали бы как остатки от деления на N числа A, r'_1 и r_1 — как остатки от деления на N числа $\frac{A-r_0}{N}$ и т. д.

Примеры

1. Записать число $A = 722$ в двоичной системе.

Цифры 2-ичной системы — это числа 0 и 1. Нам, следовательно, нужно записать $A = 722$ с помощью чисел 0 и 1. Чтобы было удобней вычислять остатки $r_0, r_1, \ldots, r_k$, мы будем последовательно заполнять таблицу из двух столбцов: в левом будут стоять частные $q_0, q_1, \ldots, q_k$, а в правом — остатки $r_0, r_1, \ldots, r_k$. Итак,

722	0
361	

т. е. $r_0 = 0$, частное q_0 равно 361. Следующий шаг:

722	0
361	1
180	

т. е. $r_1 = 1$ и $q_1 = 180$. Далее:

722	0
361	1
180	0
90	

т. е. $r_1 = 0$, $q_1 = 90$. Далее:

722	0
361	1
180	0
90	0
45	1
22	0
11	1
5	1
2	0
1	1
0	

(11)

Итак, в двоичной системе число 722 запишется так: «1011010010» (правый столбец записи (11) нужно повернуть на 90° вокруг основания по часовой стрелке — и получится ответ). А вот разложение (10) в этом случае:

$$722 = 0 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4 + 0 \cdot 2^5 + 1 \cdot 2^6 + \\ + 1 \cdot 2^7 + 0 \cdot 2^8 + 1 \cdot 2^9 = 2^9 + 2^7 + 2^6 + 2^4 + 2.$$

2. Записать число $A = 722$ в 12-ичной системе ($N = 12$).

Цифрами будут числа 0, 1, 2, ... 11. Вычисление остатков $r_0, r_1, \ldots$ и частных $q_0, q_1, \ldots$ вновь удобно располагать в виде таблицы (11).

$$\begin{array}{r|l} 722 & 2 \\ 60 & 0 \\ 5 & 5 \\ 0 & \end{array} \qquad (11')$$

Следовательно, в 12-ичной системе число 722 имеет вид: «502», т. е.

$$722 = 2 \cdot 12^0 + 0 \cdot 12 + 5 \cdot 12^2 = 5 \cdot 12^2 + 2.$$

3. Записать число $A = 722$ в 722-ичной системе ($N = 722$).

Таблица (11) здесь такова:

$$\begin{array}{r|l} 722 & 0 \\ 1 & 1 \\ 0 & \end{array}$$

Следовательно, число 722 в этой системе имеет вид: «10», т. е. $722 = 0 \cdot 722^0 + 1 \cdot 722$. Чтобы запись «10» не путать с числом десять, будем писать $\overline{1}\ \overline{0}$, указывая на то, что $\overline{1}$ и $\overline{0}$ рассматриваются как вычеты по модулю 722.

Любопытно отметить следующий факт:

В N-ичной системе число N записывается как $\overline{1}\overline{0}$.

Разумеется, записывать число A в десятичной системе по его представлению в N-ичной системе надо на основе равенства (10), т. е. осуществив серию умножений и сложений, а не делений с остатком. Объяснить это можно тем, что в любом случае мы оперируем числами, записанными в традиционной десятичной системе — ведь у нас нет цифр ни для какой другой системы. Например, 2-ичное число $\overline{1}\overline{0}\overline{1}\overline{1}\overline{0}\overline{1}\overline{0}\overline{0}\overline{1}\overline{0}$ — это, конечно, обычное $2 + 2^4 + 2^6 + 2^7 + 2^9 = 722$. Но если бы мы попытались получить запись этого числа в десятичной системе с помощью описанного выше процесса деления с остатком, то нам пришлось бы делить $\overline{1}\overline{0}\overline{1}\overline{1}\overline{0}\overline{1}\overline{0}\overline{0}\overline{1}\overline{0}$ на число 10, которое, кстати, в двоичной системе выглядит так: $\overline{1}\overline{0}\overline{1}\overline{0}$.

Для наглядности мы приведем соответствующую таблицу вычисления остатков от деления на $\overline{1}\overline{0}\overline{1}\overline{0}$.

$$\begin{array}{l|l}
\overline{1}\overline{0}\overline{1}\overline{1}\overline{0}\overline{1}\overline{0}\overline{0}\overline{1}\overline{0} & \overline{1}\overline{0}\overline{1}\overline{0} \\
\overline{1}\overline{0}\overline{1}\overline{0} & \overline{1}\overline{0}\overline{0}\overline{1}\overline{0}\overline{0}\overline{0} \\
\overline{1}\overline{0}\overline{1}\overline{0} & \\
\overline{1}\overline{0}\overline{1}\overline{0} & \\
\overline{0}\overline{1}\overline{0} &
\end{array}$$

Следовательно, частное равно 1001000, а остаток — $\overline{1}\overline{0}$. Следующий этап:

$$\begin{array}{l|l}
\overline{1}\overline{0}\overline{0}\overline{1}\overline{0}\overline{0}\overline{0} & \overline{1}\overline{0}\overline{1}\overline{0} \\
\overline{1}\overline{0}\overline{1}\overline{0} & \overline{1}\overline{1}\overline{1} \\
\overline{1}\overline{0}\overline{0}\overline{0}\overline{0} & \\
\overline{1}\overline{0}\overline{1}\overline{0} & \\
\overline{1}\overline{1}\overline{0}\overline{0} & \\
\overline{1}\overline{0}\overline{1}\overline{0} & \\
\overline{1}\overline{0} &
\end{array}$$

Частное в этом случае равно $\overline{1}\overline{1}\overline{1}$, а остаток — $\overline{1}\overline{0}$. Наконец, объединим это все в традиционной таблице остатков и частных:

$$\begin{array}{r|l}
\overline{1}\overline{0}\overline{1}\overline{1}\overline{0}\overline{1}\overline{0}\overline{0}\overline{1}\overline{0} & \overline{1}\overline{0} \\
\overline{1}\overline{0}\overline{0}\overline{1}\overline{0}\overline{0}\overline{0} & \overline{1}\overline{0} \\
\overline{1}\overline{1}\overline{1} & \overline{1}\overline{1}\overline{1} \\
\overline{0} &
\end{array}$$

Запись $\underbrace{\overline{1}\overline{1}\overline{1}}_{7}\ \underbrace{\overline{1}\overline{0}}_{2}\ \underbrace{\overline{1}\overline{0}}_{2}$, конечно, означает 722, только цифры здесь записаны в двоичной системе (об этом свидетельствуют верхние надстрочные черты).

Этот пример, показывающий способ перевода числа из двоичной системы в десятичную, свидетельствует о том, что обычные арифметические операции над числами можно производить в той системе, в которой они записаны, не прибегая к десятичной системе.

Обобщим теперь наши рассуждения.

Пусть $A = \overline{a}_n\overline{a}_{n-1} \ldots \overline{a}_1\overline{a}_0$ и $B = \overline{b}_m\overline{b}_{m-1} \ldots \overline{b}_1\overline{b}_0$ — два натуральных числа, записанных в N-ичной системе (так, что $\overline{a}_n, \ldots, \overline{a}_0, \overline{b}_m \ldots, \overline{b}_0$ — N-ичные цифры).

Записать сумму $A+B$ удобнее всего, выполняя сложение «столбиком»:

$$\begin{array}{r} \overline{a_n}\,\overline{a_{n-1}}\ \ldots\ \overline{a_1}\,\overline{a_0} \\ +\quad \overline{b_m}\ \ldots\ \overline{b_1}\,\overline{b_0} \\ \hline \end{array} \qquad (12)$$

Складывая $\overline{a_0}$ и $\overline{b_0}$, получим Nd_0+c_0, где $0 \leqslant c_0 < N-1$ и $0 \leqslant d_0 \leqslant 1$; поэтому под $\overline{a_0}$ и $\overline{b_0}$ в записи (12) надо записать $\overline{c_0}$. Затем сложим $\overline{a_1}$, $\overline{b_1}$ и d_0, вновь представив сумму в виде Nd_1+c_1; под $\overline{a_1}$ и $\overline{b_1}$ в (12) запишем $\overline{c_1}$ и т. д.

Пример. Пусть $N=3$, $A=\overline{2111001}$, и $B=\overline{2010212}$. Найти сумму A и B

$$\begin{array}{r} \overline{2111001} \\ +\ \overline{2010212} \\ \hline \overline{11121220} \end{array}$$

Обратимся к вычитанию. Здесь прежде всего нужно выяснить, что больше: A или B. Если $n>m$, то, как следует из представления (10), $A>B$; если же $n<m$, то, конечно, $A<B$. При $n=m$ надо сравнить $\overline{a_n}$ и $\overline{b_n}$. Если $\overline{a_n}>\overline{b_n}$, то $A>B$, если $\overline{a_n}<\overline{b_n}$, то $A<B$. При $\overline{a_n}=\overline{b_n}$ надо сравнить $\overline{a_{n-1}}$ и $\overline{b_{n-1}}$ и т. д. Если выяснится, что $\overline{a_n}=\overline{b_n}$, $\overline{a_{n-1}}=\overline{b_{n-1}}$, $\ldots$, $\overline{a_1}=\overline{b_1}$, $\overline{a_0}=b_0$, то окажется, что $A=B$. Например, при $N=2$ число 101101001001 больше числа 101101000111.

Для вычисления разности $A-B$ нужно сначала решить, какое из неравенств имеет место: $A \geqslant B$ или $A<B$. Если имеет место второе, то надо искать разность $B-A$, а затем перед ответом поставить знак минус. Будем считать, что $A \geqslant B$. Вычисление разности $A-B$ также удобнее всего описать «столбиком»

$$\begin{array}{r} \overline{a_n}\,\overline{a_{n-1}}\ \ldots\ \overline{a_2}\,\overline{a_1}\,\overline{a_0} \\ -\quad \overline{b_m}\ \ldots\ \overline{b_2}\,\overline{b_1}\,\overline{b_0} \\ \hline \end{array},$$

подразумевая под каждой из строчек сокращенно записанную правую часть формулы (10). Если $\overline{a_0} \geqslant \overline{b_0}$, то под $\overline{a_0}$ и $\overline{b_0}$ запишем N-ичную цифру $c_0=a_0-b_0$. Если же $a_0<b_0$ и $a_1>0$, то «займем» у a_1 «одну единичку» и положим $c_0=N+a_0-b_0$. После этого, конечно, в таблице вместо $\overline{a_1}$ уже будет цифра $\overline{a_1-1}$. Если же $a_1=$

$= 0$ и $a_2 > 0$, то «занять единичку» нужно у a_2, т. е. представить число в виде:

$$A = \ldots + (a_2 - 1)N^2 + N^2 + a_0 =$$
$$= \ldots + (a_2 - 1)N^2 + N^2 - N + N + q_0 =$$
$$= \ldots + (a_2 - 1)N^2 + (N-1)N + N + a_0.$$

Тогда $c_0 = N + a_0 - b_0$, а C_1 — цифра, стоящая под a_1 и b_1 будет равна $N - 1 - b_1$. Если же и $a_2 = 0$, но $a_3 > 0$, то надо вновь повторить эти рассуждения, представляя A в виде

$$A = \ldots + a_3N^3 + a_0 = \ldots + (a_3 - 1)N^3 + N^3 + a_0 =$$
$$= + (a_3 - 1)N^3 + N^3 - N^2 + N^2 - N + N + a_0 =$$
$$= + (a_3 - 1)N^3 + (N-1)N^2 + (N-1)N + N + a_0,$$

если же $a_3 = 0$, то читатель уже, очевидно, догадался, что нужно сделать.

Пример. Пусть $N = 8$, $A = \overline{724135}$ и $B = \overline{2635410}$. Найти $A - B$. Поскольку $B > 0$, то:

$$\begin{array}{r} \overline{2635410} \\ -\ \overline{724135} \\ \hline \overline{1711253} \end{array}$$

Ответ: $-\overline{1711253}$.

Мы рассмотрели сложение и вычитание натуральных чисел в N-ичной системе. Поскольку умножение и деление с остатком основаны на сложении и вычитании, то у нас есть теперь все необходимое для осуществления и этих операций в N-ичной системе.

Обратимся к дробям:

$$R = r_{-1} \cdot 10^{-1} + r_{-2} \cdot 10^{-2} + \ldots$$

Восстановление их десятичных знаков было описано в предыдущем параграфе. Наша ближайшая цель — предсгавить указанную дробь R в виде

$$R = a_{-1}N^{-1} + a_{-2}N^{-2} + \ldots,$$

где a_{-1}, a_{-2}, $\ldots$ — N-ичные цифры. Очевидно, a_{-1} — это целая часть числа NR (конечно, $a_{-1} < N$, т. к. $R < 1$ и поэтому $NR < N$; отсюда a_{-1} — N-ичная цифра). Аналогично, a_2 — целая часть числа $N(NR - a_{-1})$, т. е. $N^2R - Na_{-1}$ и, вообще, a_{-k} — целая часть числа

$$N^{-k}R - N^{k-1}a_{-1} - N^{k-2}a_{-2} - \ldots - Na_{-k+1}.$$

Пример. Записать дробь $R = 0{,}0875$ в девятичной системе ($N=9$). Результаты вычислений и здесь удобно заносить в таблицу из двух столбцов: слева будут указываться дроби, а справа — целые части их произведений с числом $N = 9$. Итак,

0875	0
7875	7
0875	0
7875	7
0875	

Следовательно, в девятичной системе конечная десятичная дробь $R = 0{,}0875$ — является бесконечной периодической дробью

$$\overline{0,\ 0707}\ \ldots$$

длина периода которой равна 2 — наименьшему натуральному числу из таких чисел n, для которых $9^n \equiv 1 \bmod (M)$, где M — знаменатель дроби R, представленной в рациональном виде $\left(\text{т. е. } R = \frac{7}{80}\right.$ и $\left.M = 80\right)$, являющийся взаимно простым с числом 9.

Превращение конечной десятичной дроби в бесконечную периодическую в другой системе записи заслуживает специального внимания. Прежде всего отметим, что если рациональное число $R = \frac{A}{B}$, $(A,\ B) = 1$ является бесконечной периодической десятичной дробью, то в B-ичной системе эта дробь уже будет конечной. Согласно теореме 3 из § 1, длину периода дроби R в десятичной системе надо определять так: представить B в виде $2^r \cdot 5^s \cdot B'$, где $(10,\ B') = 1$, а затем найти такое наименьшее натуральное n, при котором $10^n \equiv 1 \bmod (B')$. Имеет место следующая теорема:

Теорема 4. *Пусть $N \geqslant 2$ — натуральное число и $R = \frac{A}{B}$ — рациональное число в несократимой записи. Пусть $B = B'B''$ — такое представление числа B, что $(B',\ N) = 1$ и каждый простой делитель сомножителя B'' делит N. Тогда период N-ичной дроби, представляющей число R, равен наименьшему из таких натуральных чисел n, что $N^n \equiv 1 \bmod (B')$.*

Предлагаем читателю самостоятельно доказать эту теорему, основываясь на доказательстве теоремы 3.

Таким образом, рациональное число в любой N-ичной системе будет конечной или бесконечной периодической дробью; иррациональное же число в любой системе представляется как непериодическая дробь, потому что если бы

его можно было хотя бы в одной системе представить периодической дробью, то преобразования, аналогичные проведенным на стр. 58, привели бы нас к представлению этого числа в виде отношения двух целых чисел, а это из-за иррациональности невозможно.

Складывать и вычитать N-ичные конечные дроби удобнее «столбиком» как целые числа.

Рассмотрим теперь признаки делимости. В теореме 1 этой главы заключена именно та информация, которую успешно можно обобщить на случай N-ичной системы:

Теорема 5. *Разность между натуральным числом A и суммой его N-ичных цифр делится на $N-1$.*

Для доказательства достаточно воспользоваться представлением (10), из которого следует, что

$$A - M = r_k(N^k - 1) + r_{k-1}(N^{k-1} - 1) + \ldots + r_1(N - 1),$$

где $M = r_0 + \ldots + r_k$.
Но

$$N^s - 1 = (N - 1)(N^{s-1} + N^{s-2} + \ldots + N + 1),$$

откуда следует требуемое.

Вот почему число A делится на какой-либо делитель числа $N-1$ тогда и только тогда, когда этому делителю кратна сумма N-ичных цифр числа A. Например, располагая восьмеричным представлением любого числа A, легко узнать делится ли оно на 7: надо сложить цифры и определить, кратна ли 7 их сумма. Так, число 76125, заданное в восьмеричной системе, конечно, делится на 7 (сумма цифр равна 21). В десятичной системе это число записывается так: 31829.

При $N = 2$ только что описанные сведения становятся тривиальными: ведь $N - 1 = 1$. Поэтому в смысле теоремы 5 двоичная система оказывается неудобной: для проверки той или иной делимости здесь лучше всего провести соответствующее деление с остатком или перейти в другую систему, где получить ответ будет проще.

§ 3. N-ИЧНАЯ И N^k-ИЧНАЯ СИСТЕМЫ

Такие системы при $N = 2$ приобрели большое значение в связи с электронными вычислительными машинами. Каждое двоичное число записывается всего лишь двумя цифрами: 0 и 1. Так как простая электронная лампа может находиться в одном из двух состояний:

быть выключенной и быть включенной, то если условиться первое состояние считать воспроизведением нуля, а второе — воспроизведением единицы, то набором из n ламп можно будет воспроизводить любое n-значное двоичное число. На этом принципе и основана работа электронных вычислительных машин: числа вводятся в них в двоичной системе, а потом подвергаются определенным арифметическим операциям.

При разборе примеров двоичной записи числа в предыдущем параграфе читатель, наверное, заметил, что даже небольшое число требует для своего изображения довольно много двоичных знаков; так, число 722 в двоичной системе является десятизначным. Естественно поэтому представлять числа в двоичной системе лишь перед их вводом в машину, а до этого записывать их в такой системе, где, во-первых, для их изображения потребуется меньше знаков, и, во-вторых, переход к двоичной системе окажется более непосредственным, чем, скажем, в десятичной.

Пусть, например, $A = 30213$ — число в четверичной системе. Как записать его в двоичной системе? Воспользуемся представлением (10):

$$A = 3 \cdot 4^4 + 2 \cdot 4^2 + 1 \cdot 4 + 3 = (2 + 1) \cdot 2^8 + 2 \cdot 2^4 + 1 \cdot 2^2 + \\ + (2 + 1) = 2^9 + 2^8 + 2^5 + 2^2 + 2 + 1.$$

Следовательно, $A = 1100100111$ — запись в двоичной системе. Иными словами, мы записали каждую четвертичную цифру числа A двоичными цифрами и получили ответ. Это легко проверить исходя из ответа.

Проведем соответствующие рассуждения в общем виде. Пусть

$$A = a_{2n} \cdot 2^{2n} + a_{2n-1} 2^{2n-1} + \ldots + a_3 \cdot 2^3 + \\ + a_2 \cdot 2^2 + a_1 \cdot 2 + a_0, \qquad (12)$$

где, возможно, $a_{2n} = 0$ (нам нужно четное число цифр) и $a_0, a_1, \ldots, a_{2n-1}, a_{2n}$ — двоичные цифры, т. е. числа 0 и 1. Число $a_1 \cdot 2 + a_0$ не превосходит 3, а потому служит четвертичной цифрой. Рассмотрим следующую пару слагаемых: $a_3 \cdot 2^3 + a_2 \cdot 2^2 = (a_3 \cdot 2 + a_2) 2^2$, т. е. это четвертичная цифра, умноженная на 4. Следующая пара будет четвертичной цифрой, умноженной на $2^4 = 4$ и т. д.

Используя представление, аналогичное представлению (12), легко вывести следующее правило.

Правило. *Чтобы перейти от N-ичной записи натурального числа A к записи в N^k-ичной системе, нужно разделить N-ичные цифры числа A в группы по k штук справа налево и после этого каждую из групп записать одной N^k-ичной цифрой. Обратный переход делается так: каждую N^k-ичную цифру числа A надо записать в N-ичной системе с помощью N-ичных цифр — тогда получится N-ичное представление для A.*

Примечание. Каждое целое неотрицательное число $M < N^k$ (т. е. N^k-ичная цифра) записывается не более, чем kN-ичными цифрами, потому что N^k в N-ичной системе — это $\underbrace{100\ldots0}_{k\text{ нулей}}$. В данном случае предполагается, что если для M нужно $l < k$ N-ичных цифр, то перед N-ичной записью приписывается $k - l$ нулей. Это находится в полном согласии с представлением (10).

Вместо доказательства, которое легко проводится после введения соответствующих обозначений, мы проиллюстрируем это правило двумя примерами.

Пусть $A = \overline{9\,7\,5}$ — число в 27-ичной системе. Представим его в троичной системе. Имеем: 27-ичное $\overline{9}$ — это троичное $\overline{1\,0\,0}$; 27-ичное $\overline{7}$ — это троичное $\overline{0\,2\,1}$, 27-ичное $\overline{5}$ — это троичное $\overline{0\,1\,2}$. Таким образом, 27-ичное $\overline{9\,7\,5}$ запишется как троичное $\overline{1\,0\,0\,0\,2\,1\,0\,1\,2}$.

Пусть $A = \overline{7\,8\,10\,15\,10\,9}$ — число в 16-ичной системе. Запишем его в 256-ичной системе. Имеем: 16-ичное $\overline{10\,9}$ — это 256-ичное $\overline{169}$; 16-ичное $\overline{10\,15}$ — это 256-ичное $\overline{175}$, 16-ичное $\overline{7\,8}$ — это 256-ичное $\overline{120}$. Следовательно, запись числа A такова: $\overline{120\,175\,169}$.

Литература

1. Хинчин А. Я. Элементы теории чисел. ЭЭМ, кн. I, Арифметика. М., Гостехиздат, 1951.
2. Маркушевич А. И. Деление с остатком в арифметике и в алгебре. Сер. «Педагогическая библиотека учителя». Изд. Академии педагогических наук РСФСР, 1949.
3. Дэвенпорт Г. Высшая арифметика. М., «Наука». 1965.
4. Виноградов И. М. Основы теории чисел. М., «Наука», 1965.
5. Арнольд И. В. Теоретическая арифметика. М., Учпедгиз, 1939.
6. Бухштаб А. А. Теория чисел. М., «Просвещение», 1966.
7. Хассе Г. Лекции по теории чисел. Изд-во иностр. лит. 1953.
8. Воробьев Н. Н. «Признаки делимости». Сер. «Популярные лекции по математике». М., «Наука», 1968.
9. Фомин С. В. «Системы счисления», Сер. «Популярные лекции по математике». М., «Наука», 1968.
10. Дынкин Е. Б., Успенский В. А. «Математические беседы». М — Л., Гостехиздат, 1952.

ОГЛАВЛЕНИЕ

Библиотечка физико-математической школы

Математика

Аркадий Александрович Бельский,
Лев Аркадиевич Калужнин

Деление с остатком

Издательское объединение «Вища школа»
Головное издательство
Киев — 1977

Редактор Г. Ф. Трофимчук
Обложка художника Е. В. Попова
Художественный редактор С. Р. Ойхман
Технический редактор И. И. Каткова
Корректор Н. В. Волкова

Сдано в набор 2.09.1976 г. Подписано к печати 6.12.1976 г. Формат бумаги 84×108¹/₃₂. Бумага тип № 2. Усл. печ. л. 3,78. Уч.-изд. л. 3,58. Тираж 25 000. Изд. № 2706. Цена 11 коп Зак. 6-364.

Головное издательство издательского объединения «Вища школа», 252054, Киев-54, Гоголевская, 7

Харьковская книжная фабрика «Коммунист» республиканского производственного объединения «Полиграфкнига» Госкомиздата УССР. Харьков, Энгельса, 11.

11 коп.