

ВШЭ
K14

МИНИСТЕРСТВО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ЯРОСЛАВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМ. П.Г. ДЕМИДОВА

Л.С. Казарин

В.К. Шалашов

ТЕОРИЯ ЧИСЕЛ
ЧАСТЬ I

УЧЕБНОЕ ПОСОБИЕ

Ярославль 2003



2/3
258903

ББК В13я73
УДК 511(075.8)
К14

Казарин Л.С., Шалашов В.К.

Теория чисел. Часть I: Учебное пособие / Яросл. гос. ун-т.
Ярославль, 2003. 76 с.
ISBN 5-8393-0263-3

Пособие представляет собой первую часть курса лекций по дисциплине "Теория чисел" для студентов, обучающихся по специальности 010100 - Математика. Напоминаются необходимые предварительные факты общематематического характера (математическая индукция, элементы комбинаторики, исторические сведения); изложена теория делимости целых чисел, основная теорема арифметики, простые числа, их распределение, некоторые открытые проблемы. Ко всем разделам предложены задачи.

Библиогр. : 7 назв.

Рецензенты:

Доктор физико-математических наук, профессор В.М. Сидельников,

Доктор педагогических наук, профессор А.В. Ястребов,

кафедра алгебры Ярославского государственного педагогического университета.

*Печатается по решению редакционно-издательского совета
Ярославского государственного университета*

ISBN ISBN 5-8393-0263-3 © Ярославский государственный
университет, 2003

© Л.С. Казарин,
В.К. Шалашов, 2003



Глава 1

Некоторые предварительные соображения

Числа были рождены в суеверии и возвышены в тайну, числа однажды сделались основой религии и философии, а фокусы с цифрами оказывают удивительный эффект на доверчивых людей.

Ф.В. Паркер

1.1. Математическая индукция

В теории чисел (по крайней мере на элементарном уровне) рассматривают свойства целых чисел \mathbb{Z} и чисел $\mathbb{N} = \{1, 2, 3, \dots\}$ (натуральных чисел). Напомним, что в древней Греции слово "число" означало положительное целое и ничего другого. Натуральные числа известны нам столь давно, что Кронекер однажды заметил: "Бог создал натуральное число, а все остальное — творение человека". Будучи даром Небес, теория чисел имела долгую и иногда болезненную историю, историю, которую мы надеемся рассказать на следующих страницах.

Мы не будем прибегать к аксиоматической конструкции целых чисел, но предполагаем, что она уже дана и читатели знакомы с элементарными фактами о них. В их число мы включаем принцип полной упорядоченности. Чтобы освежить память, мы сформулируем его.

Принцип полной упорядоченности. Каждое непустое множе-

ство S неотрицательных целых чисел содержит наименьший элемент, т.е. существует число a из S , такое что $a \leq b$ для всех чисел b , принадлежащих S .

В качестве применения этого принципа докажем следующее утверждение.

Теорема 1.1 (Свойство Архимеда). Если a и b — два произвольных натуральных числа, то существует натуральное число n , такое, что $na \geq b$.

Доказательство. Предположим, что утверждение теоремы неверно, следовательно, для некоторых a и b выполняется неравенство $na < b$ для каждого натурального n . Таким образом, множество

$$S = \{b - na \mid n \in \mathbb{N}\}$$

есть подмножество множества \mathbb{N} . В силу принципа полной упорядоченности S обладает наименьшим элементом. Обозначим его через $b - ma$. По определению множества S число $b - (m+1)a$ также принадлежит ему. С другой стороны,

$$b - (m+1)a = b - ma - a < b - ma,$$

что противоречит выбору $b - ma$ как наименьшему элементу в S . Теорема доказана.

Перейдем к принципу конечной индукции, который даёт основу для доказательства методом математической индукции. Этот принцип утверждает, что если некоторое множество, состоящее из положительных целых чисел, обладает двумя специфическими свойствами, то оно совпадает с \mathbb{N} .

Теорема 1.2 (Принцип конечной индукции). Пусть $S \subset \mathbb{N}$ и обладает двумя свойствами:

$$1 \in S, \tag{1.1}$$

$$\text{если } k \in S, \text{ то } k+1 \in S. \tag{1.2}$$

Тогда $S = \mathbb{N}$.

Доказательство. Пусть $T = \mathbb{N} \setminus S$ и $T \neq \emptyset$. В силу принципа полной упорядоченности T имеет наименьший элемент, который мы обозначим через a . С помощью (1.1) заключаем, что $a > 1$ и,

таким образом, $0 < a - 1 < a$. Но a — наименьший элемент в T , следовательно, $a - 1 \in S$. Учитывая (1.2), получаем, что $a \in S$. Это противоречие приводит к равенствам $T = \emptyset$ и $S = \mathbb{N}$.

В качестве применения метода математической индукции докажем равенство

$$1^2 + 2^2 + \dots + n^2 = \frac{n(2n+1)(n+1)}{6}, \quad n = 1, 2, 3, \dots \quad (1.3)$$

Пусть S обозначает множество всех положительных целых чисел n , для которых выполняется (1.3). Так как

$$1 = \frac{1(2+1)(1+1)}{6} = 1,$$

то $1 \in S$. Далее предположим, что $k \in S$, т.е.

$$1^2 + 2^2 + \dots + k^2 = \frac{k(2k+1)(k+1)}{6}.$$

Тогда

$$\begin{aligned} 1^2 + 2^2 + \dots + k^2 + (k+1)^2 &= \frac{k(2k+1)(k+1)}{6} + (k+1)^2 = \\ &= (k+1) \left[\frac{k(2k+1)}{6} + (k+1) \right] = (k+1) \left[\frac{k(2k+1) + 6(k+1)}{6} \right] = \\ &= (k+1) \left[\frac{2k^2 + 7k + 6}{6} \right] = \frac{(k+1)(2k+3)(k+2)}{6} = \\ &= \frac{(k+1)[2(k+1)+1][(k+1)+1]}{6} \end{aligned}$$

Таким образом, если $k \in S$, то $k+1 \in S$. По теореме 1.2 заключаем, что $S = \mathbb{N}$ и равенство (1.3) выполняется для $n = 1, 2, 3, \dots$

В то время как математическая индукция дает стандартную технику для доказательства утверждений о натуральных числах, она не помогает в формулировке таких утверждений. С другой стороны, математическая индукция часто позволяет проверить справедливость той или иной гипотезы. Рассмотрим, например, список ра-

$$1 = 1,$$

$$1 + 2 = 3,$$

$$1 + 2 + 2^2 = 7,$$

$$1 + 2 + 2^2 + 2^3 = 15,$$

$$1 + 2 + 2^2 + 2^3 + 2^4 = 31,$$

$$1 + 2 + 2^2 + 2^3 + 2^4 + 2^5 = 63$$

Найдем правило, согласно которому "устроены" правые части этих равенств. После недолгих размышлений читатель может заметить, что

$$\begin{aligned} 1 &= 2 - 1, & 3 &= 2^2 - 1, & 7 &= 2^3 - 1, \\ 15 &= 2^4 - 1, & 31 &= 2^5 - 1, & 63 &= 2^6 - 1. \end{aligned}$$

Как приходит такое заключение, трудно сказать, но помогает эксперимент. Примеры, появляющиеся из этих нескольких случаев, предполагают формулу для получения значения выражения $1 + 2 + 2^2 + \dots + 2^{n-1}$. Именно,

$$1 + 2 + 2^2 + 2^3 + \dots + 2^{n-1} = 2^n - 1 \quad (1.4)$$

для каждого натурального числа n .

Для проверки корректности нашего предположения обозначим через S множество натуральных чисел n , для которых формула (1.4) верна для $n = k$, следовательно,

$$1 + 2 + 2^2 + \dots + 2^{k-1} = 2^k - 1$$

и докажем справедливость этой формулы для $n = k + 1$. Прибавление слагаемого 2^k к обеим частям последнего равенства дает

$$1 + 2 + 2^2 + \dots + 2^{k-1} + 2^k = 2^k - 1 + 2^k = 2 \cdot 2^k - 1 = 2^{k+1} - 1.$$

Это показывает, что $k+1 \in S$, как только $k \in S$. Согласно принципу индукции $S = \mathbb{N}$.

Замечание. При доказательстве методом математической индукции мы будем сокращать наши аргументы, не прибегая к множеству S . Именно, проверив, что соответствующий результат верен для $n = 1$, установим его справедливость для $n = k + 1$, если он верен для $n = k$.

Мы должны здесь отметить, что в теореме 1.2 ни одно из двух предположений нельзя опустить. Доказательство условия (1.1) в теореме 1.2 обычно называется *базисом индукции*, в то время как доказательство условия (1.2) называется *шагом индукции*. Предположение о выполнении шага индукции называется *индуктивной гипотезой*.

Справедливость шага индукции не обязательно зависит от истинности утверждения, которое мы стремимся доказать. Рассмотрим ложную формулу

$$1 + 3 + 5 + \dots + (2n - 1) = n^2 + 3. \quad (1.5)$$

Предположим, что она верна для $n = k$, т.е.

$$1 + 3 + 5 + \dots + (2k - 1) = k^2 + 3.$$

Зная это, мы получаем

$$1 + 3 + 5 + \dots + (2k - 1) + (2k + 1) = k^2 + 3 + 2k + 1 = (k + 1)^2 + 3.$$

Таким образом, если формула (1.5) верна для $n = k$, то она верна и для $n = k + 1$. С другой стороны, формула (1.5) не верна для любого n .

Существует вариант принципа математической индукции, который часто используется, когда теорема 1.2 оказывается неэффективной. Как и в случае с первой версией, второй принцип конечной индукции обеспечивает два условия, которые гарантируют, что определённое подмножество натуральных чисел в действительности совпадает с \mathbb{N} . При этом мы оставляем требование (1.1) теоремы 1.2, а условие (1.2) заменяем на следующее.

Если k — натуральное число, такое, что $1, 2, \dots, k$ принадлежит множеству S , то $k + 1$ должно также принадлежать к S . (1.2)'

Доказательство того, что S совпадает с \mathbb{N} , имеет ту же "изюминку", что и при доказательстве теоремы 1.2. Снова пусть $T = \mathbb{N} \setminus S$. Предполагая, что T — непустое, выбираем n как наименьшее в T . Тогда в силу (1.1) число $n > 1$. Выбор n позволяет заключить, что ни одно из чисел $1, 2, \dots, n - 1$ не лежит в T . Следовательно, все числа $1, 2, \dots, n - 1$ принадлежат к S . В силу (1.2)' отсюда следует, что $n = (n - 1) + 1 \in S$, что приводит к противоречию. Таким образом, $T = \emptyset$ и $S = \mathbb{N}$.

Отметим, что оба варианта конечной индукции могут быть обобщены таким образом, чтобы начинать с любого натурального n . В

этом случае заключение выглядит так: "Тогда множество S совпадает с множеством всех положительных чисел $n \geq n_0$ ".

Математическая индукция часто используется не только как метод доказательства, но и как способ определения. Например, символ $n! = n \cdot (n-1)!$ для $n > 1$. Удобно это определение дополнить до $0! = 1$.

Пример 1. Приведем один пример применения Второго принципа конечной индукции. Рассмотрим последовательность

$$1, 3, 4, 7, 11, 18, 29, 47, 76, \dots$$

Исключая первые два члена, каждый член есть сумма двух предыдущих. Эта последовательность может быть определена индуктивно:

$$a_1 = 1$$

$$a_2 = 3$$

$$a_n = a_{n-1} + a_{n-2} \text{ для } n \geq 3.$$

Мы утверждаем, что для каждого $n \in \mathbb{N}$ выполняется неравенство

$$a_n < \left(\frac{7}{4}\right)^n.$$

Прежде всего заметим, что

$$a_1 < \left(\frac{7}{4}\right)^1, \quad a_2 = 3 < \left(\frac{7}{4}\right)^2 = \frac{49}{16}.$$

Пусть теперь $k \geq 3$ и предположим, что наше неравенство верно для $n = 1, 2, \dots, k-1$. Тогда в частности

$$a_{k-1} < \left(\frac{7}{4}\right)^{k-1} \text{ и } a_{k-2} < \left(\frac{7}{4}\right)^{k-2}, \text{ откуда } a_k = a_{k-1} + a_{k-2} < \left(\frac{7}{4}\right)^{k-1} + \left(\frac{7}{4}\right)^{k-2} = \left(\frac{7}{4}\right)^{k-2} \left(\frac{7}{4} + 1\right) = \left(\frac{7}{4}\right)^{k-2} \left(\frac{11}{4}\right) < \left(\frac{7}{4}\right)^{k-2} \left(\frac{7}{4}\right)^2 = \left(\frac{7}{4}\right)^k.$$

1.2. Задачи

1. С помощью математической индукции доказать справедливость следующих формул:

- (а) $1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$, для всех $n \in \mathbb{N}$;
 (б) $1 + 3 + 5 + \dots + (2n - 1) = n^2$, для всех $n \in \mathbb{N}$;
 (с) $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \dots + n(n+1) = \frac{n(n+1)(n+2)}{3}$, для всех $n \in \mathbb{N}$;
 (д) $1^2 + 3^2 + 5^2 + \dots + (2n - 1)^2 = \frac{n(4n^2 - 1)}{3}$, для всех $n \in \mathbb{N}$;
 (е) $1^3 + 2^3 + 3^3 + \dots + n^3 = \left[\frac{n(n+1)}{2} \right]^2$, для всех $n \in \mathbb{N}$.

2. Доказать, что если $r \neq 1$, то

$$a + ar + ar^2 + \dots + ar^n = \frac{a(r^{n+1} - 1)}{r - 1},$$

если $n \in \mathbb{N}$.

3. С помощью Второго принципа конечной индукции доказать справедливость формулы $a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \dots + a + 1)$ для $n \in \mathbb{N}$.

Указание. Заметим, что

$$a^{n+1} - 1 = (a + 1)(a^n - 1) - a(a^{n-1} - 1)$$

4. Доказать, что куб любого целого можно представить как разность двух квадратов.

Указание. Заметим, что

$$n^3 = (1^3 + 2^3 + \dots + n^3) - (1^3 + 2^3 + \dots + (n-1)^3)$$

5. (а) Найти значения n ($n \leq 7$), для которых $(n! + 1)$ есть точный квадрат.

(б) Пусть $m, n \in \mathbb{N}$. Справедливы или нет формулы $(mn)! = m!n!$ и $(m+n)! = m! + n!$?

6. Доказать, что $n! > n^2$ для $n \geq 4$ и $n! \geq n^3$ для $n \geq 6$.

7. Доказать, что если $n \geq 1$, то

$$1(1!) + 2(2!) + \dots + n(n!) = (n+1)! - 1$$

1.3. Биномиальная теорема

Пусть $n \in \mathbb{N}$ и $0 \leq k \leq n$. Определим биномиальный коэффициент

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Сокращая числитель и знаменатель на $k!$ или $(n-k)!$, получим равенства:

$$\binom{n}{k} = \frac{n(n-1) \cdots (k+1)}{(n-k)!} = \frac{n(n-1) \cdots (n-k+1)}{k!}$$

Приведем здесь одно из тождеств, касающихся биномиальных коэффициентов, известное, как правило Паскаля:

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}, \quad 1 \leq k \leq n$$

Для его доказательства напомним равенство:

$$\frac{1}{k} + \frac{1}{n-k+1} = \frac{n+1}{k(n-k+1)},$$

обе части которого умножим на $\frac{n!}{(k-1)!(n-k)!}$. Тогда получим

$$\begin{aligned} \frac{n!}{k(k-1)!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)(n-k)!} &= \\ &= \frac{(n+1)n!}{k(k-1)!(n-k+1)(n-k)!}, \end{aligned}$$

откуда следует, что

$$\frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-(k-1))!} = \frac{(n+1)!}{k!(n+1-k)!},$$

и правило Паскаля доказано. Это соотношение ведет к конфигурации, известной как *треугольник Паскаля*, в котором $\binom{n}{k}$ появляется как $(k+1)$ -ое число в n -й строке.

$$\begin{array}{ccccccc} 1 & 1 & & & & & \\ 1 & 2 & 1 & & & & \\ 1 & 3 & 3 & 1 & & & \\ 1 & 4 & 6 & 4 & 1 & & \\ 1 & 5 & 10 & 10 & 5 & 1 & \\ 1 & 6 & 15 & 20 & 15 & 6 & 1 \\ \dots & & & & & & \end{array}$$

Стороны этого треугольника состоят из единиц, а число, не находящееся на стороне треугольника, равно сумме двух ближайших чисел, стоящих в верхней строке.

Так называемая *биномиальная теорема* есть формула для представления $(a + b)^n$, $n \geq 1$, в виде суммы произведений степеней a и b . Легко непосредственно проверить, что имеют место равенства:

$$\begin{aligned}(a + b)^1 &= a + b, \\(a + b)^2 &= a^2 + 2ab + b^2, \\(a + b)^3 &= a^3 + 3a^2b + 3ab^2 + b^3, \\(a + b)^4 &= a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4.\end{aligned}$$

Вопрос состоит в том, как угадать коэффициенты. Ключ — в наблюдении, что они появляются в соответствующей строке треугольника Паскаля. Все это приводит к предположению, что имеет место формула

$$(a + b)^n = \binom{n}{0} a^n + \binom{n}{1} a^{n-1}b + \binom{n}{2} a^{n-2}b^2 + \dots + \binom{n}{n-1} ab^{n-1} + \binom{n}{n} b^n,$$

или в более компактной записи:

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k.$$

Математическая индукция является наилучшим способом для подтверждения нашей гипотезы. Для $n = 1$ имеем

$$(a + b)^1 = \sum_{k=0}^1 \binom{1}{k} a^{1-k} b^k = \binom{1}{0} ab^0 + \binom{1}{1} a^0 b = a + b.$$

Предполагая, что формула верна для некоторого фиксированного натурального m , мы должны доказать, что она верна и для $n = m + 1$.

Заметим сначала, что

$$(a + b)^{m+1} = a(a + b)^m + b(a + b)^m.$$

В силу индукционного предположения имеем:

$$a(a + b)^m = \sum_{k=0}^m \binom{m}{k} a^{m-k+1} b^k = a^{m+1} + \sum_{k=1}^m \binom{m}{k} a^{m+1-k} b^k$$

и

$$\begin{aligned} b(a+b)^m &= \sum_{j=0}^m \binom{m}{j} a^{m-j} b^{j+1} = \sum_{k=1}^{m+1} \binom{m}{k-1} a^{m+1-k} b^k = \\ &= \sum_{k=1}^m \binom{m}{k-1} a^{m+1-k} b^k + b^{m+1}. \end{aligned}$$

Таким образом, имеет место равенство:

$$\begin{aligned} (a+b)^{m+1} &= a^{m+1} + \sum_{k=1}^m \left[\binom{m}{k} + \binom{m}{k-1} \right] a^{m+1-k} b^k + b^{m+1} = \\ &= \sum_{k=0}^{m+1} \binom{m+1}{k} a^{m+1-k} b^k. \end{aligned}$$

Следовательно, биномиальная теорема доказана.

Перед тем, как расстаться с этими идеями, мы должны отметить, что первая формулировка метода математической индукции появилась в трактате "Traite du Triangle Arithmétique" французского математика и философа 17-го века Блеза Паскаля. Эта короткая работа была написана в 1653 году, но не публиковалась до 1665 года, так как Паскаль удалился (в возрасте 25 лет) от математики, чтобы посвятить свой талант религии. Его тонкий анализ свойств биномиальных коэффициентов помог заложить основы теории вероятностей.

1.4. Задачи

1. Доказать, что для $n \geq 1$

$$(a) \quad \binom{n}{k} < \binom{n}{k+1} \text{ тогда и только тогда, когда } 0 \leq k < \frac{1}{2}(n-1);$$

$$(b) \quad \binom{n}{k} = \binom{n}{k+1} \text{ тогда и только тогда, когда } n \text{ — нечетное и } k = \frac{1}{2}(n-1).$$

2. Доказать, что если $n \geq 4$, $2 \leq k \leq n-2$, то

$$\binom{n}{k} = \binom{n-2}{k-2} + 2\binom{n-2}{k-1} + \binom{n-2}{k}.$$

3. Доказать, что если $n \geq 1$, то справедливы равенства:

$$(a) \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n;$$

Указание. Применить биномиальную теорему для случая $a = b = 1$.

$$(b) \binom{n}{0} - \binom{n}{1} + \binom{n}{2} + \cdots + (-1)^n \binom{n}{n} = 0;$$

$$(c) \binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \cdots + n\binom{n}{n} = n2^{n-1};$$

Указание. Применить биномиальную теорему для $n(1 + b)^{n-1}$, когда $b = 1$. Учесть также, что $\binom{n-1}{k} = (k+1)\binom{n}{k+1}$.

$$(d) \binom{n}{0} + 2\binom{n}{1} + 2^2\binom{n}{2} + \cdots + 2^n\binom{n}{n} = 3^n;$$

$$(e) \binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \binom{n}{6} + \cdots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots = 2^{n-1}.$$

Указание. Использовать задачи (3a) и (3b).

4. (a) Доказать, что если $n \geq 2$, то

$$\binom{2}{2} + \binom{3}{2} + \cdots + \binom{n}{2} = \binom{n+1}{3}$$

Указание. Использовать индукцию и правило Паскаля.

(b) С помощью задачи (4a) и того факта, что

$$2\binom{m}{2} + m = m^2, \text{ если } m \geq 2$$

вывести формулу

$$1 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

1.5. Ранняя теория чисел

Перед тем как перейти к детальному описанию предмета, мы должны сказать несколько слов о начале теории чисел. Теория чисел

является одной из старейших ветвей математики. В то время как вероятно, что греки в значительной мере обязаны Вавилону и Египту знаниями первоначальной информации о свойствах натуральных чисел, первые зачатки настоящей теории обычно приписывают Пифагору и его ученикам.

Наши знания о жизни Пифагора являются скудными, и мы можем мало сказать об этом с какой-либо уверенностью. Он родился между 580 и 562 годом до рождения Христова на Самосе — острове в Эгейском море. Вероятно, он обучался не только в Египте, но и в Вавилоне. Когда Пифагор вернулся после многих лет странствий, он нашел удобное место для школы и, наконец, устроился на Кротоне, преуспевающей греческой колонии на итальянском "сапоге" (Апеннинский полуостров). Школа сосредоточилась на четырех *mathemata* (предметах обучения): *arithmetica* (арифметика, скорее в смысле теории чисел, а не искусства вычислений), *harmonia* (музыка), *geometra* (геометрия) и *astrologia* (астрономия). Такое деление знаний на четыре части стало известно в средние века как *quadrivium*, к которым добавили логику, грамматику и риторику. Эти семь свободных искусств стали необходимым курсом обучения для образованных лиц. Пифагор разделил тех, кто посещал его лекции, на две группы: испытуемые (или слушатели) и пифагорейцы. После трех лет обучения слушатели могли быть посвящены в пифагорейцы, которым поверяли основные открытия школы. Пифагорейцы образовывали тесно связанное братство, их житейские вещи были общими и всех их связывала клятва не выдавать секреты своего основателя. Существует легенда, что болтливый пифагореец утонул во время кораблекрушения — наказание бога за публичное хвастовство, будто он добавил двенадцатигранник к списку правильных тел, перечисленных Пифагором. Во времена тирании пифагорейцы имели доминирующее влияние в местном руководстве Кротона, но восстание в 501 году до рождения Христова привело к смерти многих их выдающихся представителей. Вскоре был также убит сам Пифагор. Хотя политическое влияние пифагорейцев было таким образом аннулировано, они продолжали существовать как философское и математическое общество по крайней мере еще два столетия.

Пифагорейцы верили, что ключ к постижению Вселенной лежит в числе и форме, их общий тезис — "Всё есть число". Под числом они понимали натуральное число. Пифагорейцы считали, что для

рационального понимания природы достаточно проанализировать свойства определенных чисел. Доктрина Пифагора — удивительная смесь философии и мистицизма, вид супернумерологии, которая связывает с каждым материальным и духовным явлением определенное число. Среди их работ мы находим, что 1 представляет причину, 2 закрепляется для мужчины, 3 — для женщины. Число 4 для пифагорейцев было символом справедливости, будучи первым числом, являющимся произведением равных, число 5 ассоциировалось с браком, так как оно есть сумма чисел 2 и 3 и т.д. Все четные числа, начиная с 4, рассматривались как женское и земное. Будучи преимущественно мужским сообществом, пифагорейцы рассматривали нечетные числа, начиная с 5, как мужское и божественное.

Хотя эти рассуждения о числах, как моделях "вещей", сейчас кажутся легкомысленными, следует иметь в виду, что интеллектуалы классического греческого периода были в значительной мере вовлечены в философию и они занимались установлением основ математики как системы мышления. Для Пифагора и его учеников математика была в значительной мере средством к постижению философии. Только с основанием александрийской школы мы входим в новую фазу, где математикой занимались ради нее самой.

Следует отметить, что мистические размышления о свойствах чисел были свойственны не только пифагорейцам. В средние века одной из абсурдных форм таких размышлений была псевдонаука, известная как *gematria* или *arithmology*. При этом каждой букве алфавита ставилось (некоторым образом) в соответствие число, а слову — сумма чисел, соответствующих буквам, образующим это слово. С точки зрения *gematria* два слова эквивалентны, если соответствующие им числа равны. Все это, вероятно, начиналось в древней Греции, где естественный порядок букв в алфавите давал кодировку с помощью чисел: букве α в алфавите соответствует 1, β число 2 и т.д. Например, слово "аминь" по гречески — $\alpha\mu\eta\eta$ и эти буквы имели значения 1, 40, 8 и 50 соответственно, в сумме — 99. Во многих старых изданиях Библии число 99 появлялось в конце молитвы. Наиболее известным числом было 666, "число зверя", упомянутое в Апокалипсисе. Во времена Реформации любимым развлечением католических богословов была разработка алфавитных схем, в которых число 666 устанавливалось за именем Мартин Лютер, в связи с чем это поддерживало их убеждение, что он был антихристом. Лю-

тер ответил тем же: он нашел систему, в которой число 666 стало именем господствующего папы, Лео X.

В Александрии, а не в Афинах наука о числах начала развиваться в отрыве от мистики и философии. Почти тысячу лет, до разрушения арабами в 641 году нашей эры, Александрия оставалась культурным и торговым центром эллинистического мира. (После падения Александрии большинство ее школ переместилось в Константинополь. В течение следующих 800 лет этот анклав в Константинополе поддерживал математические работы греческих школ.) Так называемый александрийский музей, предшественник современного университета, собрал вместе ведущих поэтов и ученых, а его библиотека насчитывала свыше 700000 томов. Из всех выдающихся имен, связанных с музеем, имя Евклида (350 лет до рождения Христа), основателя математической школы, стоит особо. Последующие поколения стали знать его как автора "Начал", старейшего греческого трактата, дошедшего до нас полностью. "Начала" являются компиляцией многих математических работ, собранных в тринадцать частей или книг, как они теперь называются. Имя Евклида часто связывают только с геометрией, забывая, что три книги (VII, VIII и IX), посвящены теории чисел.

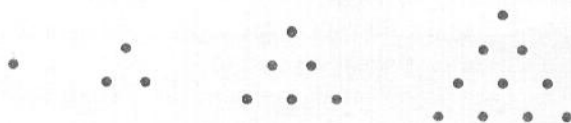
"Начала" Евклида являются выдающимся явлением в мировой литературе. Едва ли какая-либо другая книга, кроме Библии, является более распространенной или читаемой. Со времен первой публикации в 1482 году "Начала" выдержали более тысячи изданий.

1.6. Задачи

1. Каждое из чисел:

$$1 = 1, 3 = 1 + 2, 6 = 1 + 2 + 3, 10 = 1 + 2 + 3 + 4, \dots$$

является числом точек, равномерно распределенных в равносided треугольнике:



Древние греки поэтому называли эти числа *треугольными*. Они являются суммой последовательных чисел, начиная с 1. Дока-

зять следующие свойства треугольных чисел:

- (а) Число является треугольным тогда и только тогда, когда оно имеет вид $\frac{n(n+1)}{2}$ для некоторого $n \geq 1$. (Пифагор, 550 лет до н.э.)
 - (б) Число n является треугольным тогда и только тогда, когда $8n + 1$ является точным квадратом. (Плутарх, 100 лет н.э.)
 - (с) Сумма любых двух последовательных треугольных чисел есть точный квадрат. (Никомаху, 100 лет н.э.)
 - (д) Если n — треугольное число, то таковыми являются и числа $9n + 1$, $25n + 3$ и $49n + 6$. (Эйлер, 1775)
2. Если t_n обозначает n -ое треугольное число, доказать, что

$$t_n = \binom{n+1}{2}, \quad n \geq 1.$$

3. Вывести следующую формулу для суммы треугольных чисел, приписываемую индийскому математику Арьябхата (500 лет н.э.):

$$t_1 + t_2 + t_3 + \dots + t_n = \frac{n(n+1)(n+2)}{6}, \quad n \geq 1.$$

Указание. Сгруппировать слагаемые в левой части парами и учесть, что $t_{k-1} + t_k = k^2$.

4. Доказать, что квадрат любого нечетного числа, кратного числу 3, есть разность двух треугольных чисел, более точно: $9(2n+1)^2 = t_{9n+4} - t_{3n+1}$.
5. В последовательности $t_1, t_2, \dots, t_n, \dots$ треугольных чисел найти:
- (а) два треугольных чисел, сумма и разность которых являются также треугольными числами;
 - (б) три последовательных треугольных числа, произведение которых есть квадрат;
 - (с) три последовательных треугольных числа, сумма которых есть точный квадрат.
6. (а) Если $2n^2 \pm 1$ является точным квадратом, скажем $2n^2 \pm 1 = m^2$, то $(mn)^2$ является треугольным числом. Доказать это утверждение.
- (б) Использовать утверждение (6а), чтобы найти три примера квадратов, являющихся треугольными числами.

Глава 2

Теория делимости целых чисел

Целые числа являются
первоисточником всей матема-
тики.

Г. Минковский

2.1. Алгоритм деления

Мы начинаем этот параграф с утверждения, являющегося основным в теории чисел, с алгоритма деления. Этот результат знаком большинству из вас и приблизительно он утверждает, что целое число a можно "разделить" на натуральное число b таким образом, что остаток меньше, чем b .

Теорема 2.1 (Алгоритм деления). Для заданных целых a, b , где $b > 0$, существует единственная пара целых чисел q и r , удовлетворяющих условию

$$a = bq + r, \quad 0 \leq r < b.$$

Целые числа q и r называются соответственно (неполным) частным и остатком при делении a на b .

Доказательство. Докажем сначала, что множество

$$S = \{a - xb \mid x \in \mathbb{Z}, a - xb \geq 0\}$$

непусто. Для этого достаточно найти целое x , делающее $a - xb$ неотрицательным. Так как $b \geq 1$, то $|a|b \geq |a|$ и, таким образом,

$$a - (-|a|b) = a + |a|b \geq a + |a| \geq 0.$$

Следовательно, если $x = -|a|$, число $a - xb \in S$. Это позволяет применить принцип полной упорядоченности, из которого следует,

что S содержит наименьший элемент. Обозначим его через r . По определению множества S существует целое q такое, что

$$r = a - qb, \quad 0 \leq r.$$

Мы утверждаем, что $a < b$. Если бы это было не так, то $r \geq b$ и

$$a - (q+1)b = (a - qb) - b = r - b \geq 0.$$

Следствием этого факта является принадлежность числа $a - (q+1)b$ к S . Но $a - (q+1)b < r$, что ведет к противоречию (r — наименьшее число в S). Таким образом, $r < b$.

Докажем единственность пары чисел q и r . Предположим, что a имеет два представления:

$$a = qb + r = q'b + r',$$

где $0 \leq r < b$, $0 \leq r' < b$. Тогда $r' - r = (q - q')b$ и

$$|r' - r| = b|q - q'|. \quad (2.1)$$

Теперь, складывая неравенства $-b < -r \leq 0$ и $0 \leq r' < b$, получим, $-b < r' - r < b$, т.е.

$$|r' - r| < b. \quad (2.2)$$

Из (2.1) и (2.2) заключаем, что

$$b|q - q'| < b,$$

откуда следует, что

$$0 \leq |q - q'| < 1.$$

Так как $|q - q'| \in \mathbb{N}$, то $|q - q'| = 0$ и $q = q'$. Но $|r' - r| = b|q - q'| = 0$. Следовательно, и $r = r'$. Теорема полностью доказана.

Более общая версия теоремы 2.1 получается при замене условия в $b \in \mathbb{N}$ на требование $b \neq 0$.

Следствие 1. Если a и b целые, причем $b \neq 0$, то существует единственная пара целых чисел q и r таких, что

$$a = qb + r, \quad 0 \leq r < |b|.$$

Доказательство. Достаточно рассмотреть случай $b < 0$. Тогда $|b| > 0$ и теорема дает единственную пару чисел q' и r , для которых

$$a = q'|b| + r, \quad 0 \leq r < |b|.$$

Учитывая, что $|b| = -b$, мы можем положить $q = -q'$ и получить

$$a = qb + r, \quad 0 \leq r < |b|.$$

Следствие доказано.

Для иллюстрации алгоритма деления в случае $b < 0$ рассмотрим несколько примеров с $b = -7$. Тогда, выбирая $a = 1, -2, 61, -59$, получим:

$$\begin{aligned} 1 &= 0(-7) + 1, \\ -2 &= 1(-7) + 5, \\ 61 &= (-8)(-7) + 5, \\ -59 &= 9(-7) + 4. \end{aligned}$$

Рассмотрим алгоритм деления в случае $b = 2$, при котором возможны два остатка: $r = 0$ и $r = 1$. Если $r = 0$, то целое a имеет вид $a = 2q$ и оно называется *чётным* числом. Когда $r = 1$, то целое a имеет вид $a = 2q + 1$ и оно называется *нечётным* числом. Далее, если $b = 2$, то $a^2 = (2q)^2 = 4k$ или $a^2 = (2q+1)^2 = 4(q^2+q)+1 = 4k+1$. Таким образом, при делении на 4 квадрата целого числа возможны два остатка: 0 или 1.

Покажем теперь, что квадрат любого нечётного числа имеет вид $8k+1$. Согласно алгоритму деления, любое целое число можно представить одним из способов: $4q, 4q+1, 4q+2, 4q+3$. Среди них нечётные имеют вид: $4q+1, 4q+3$. После возведения в квадрат получим $(4q+1)^2 = 8(2q^2+q)+1 = 8k+1$, $(4q+3)^2 = 8(2q^2+3q+1)+1 = 8k+1$. Например, $7^2 = 49 = 8 \cdot 6 + 1$, как $13^2 = 169 = 8 \cdot 21 + 1$.

Заметим, наконец, что требование неотрицательности остатка r является существенным. Без этого ограничения доказать единственность пары (q, r) , удовлетворяющей соотношению

$$a = bq + r, \quad 0 \leq |r| < |b|,$$

уже нельзя, как показывает следующий пример. Пусть $a = 15, b = 4$.

$$\begin{aligned} 15 &= 3 \cdot 4 + 3, \\ 15 &= 4 \cdot 4 + (-1). \end{aligned}$$

В первом случае остаток $r = 3$, а во втором $-r = -1$. В обоих случаях $|r| < |b|$. Эта неоднозначность иногда оказывается полезной.

2.2. Задачи

1. Пусть $a, b \in \mathbb{Z}, b > 0$. Доказать, что существуют единственная пара целых чисел q, r , удовлетворяющих условию $a = qb + r$, где $2b \leq r < 3b$.
2. Доказать, что любое целое вида $6k + 5$ можно представить в форме $3l + 2$. Обратное утверждение неверно.
3. С помощью алгоритма деления доказать:
 - (а) каждое нечётное число имеет вид $4k + 1$ или $4k + 3$;
 - (б) квадрат любого целого можно представить или как $3k$, или $3k + 1$;
 - (в) куб любого целого есть или $9k$, или $9k + 8$;

4. Доказать, что $\frac{n(n+1)(2n+1)}{6}$, где $n \geq 1$, является целым числом.

Указание. Учесть, что любое k можно представить одним из способов: $6k, 6k + 1, 6k + 2, 6k + 3, 6k + 4, 6k + 5$.

5. Доказать, что если целое число является одновременно квадратом и кубом (как в случае $64 = 8^2 = 4^3$), то его можно представить или в виде $7k$, или $7k + 1$.
6. Доказать следующую версию алгоритма деления. Для целых a и $b, b \neq 0$, существуют единственная пара целых чисел q и r таких, что $a = qb + r$, где $-\frac{1}{2}|b| < r \leq \frac{1}{2}|b|$.

Указание. Представить a в виде: $a = q'b + r', 0 \leq r' < |b|$. Если $0 \leq r' \leq \frac{1}{2}|b|$, положить $r = r'$ и $q = q'$. Если $\frac{1}{2} < r' < |b|$, положить $r = r' - |b|$ и $q = q' + 1$, если $b > 0$ и $q = q' - 1$, если $b < 0$.

7. Доказать, что ни одно из целых в последовательности 11, 111, 1111, 11111, ... не является точным квадратом.

Указание. Установить, что каждый член последовательности имеет вид $4k + 3$.

2.3. Наибольший общий делитель

Рассмотрим случай, когда после применения алгоритма деления получаем $r = 0$.

Определение 1. Будем говорить, что целое число b делится на целое число a , $a \neq 0$ (обозначение $a|b$), если существует некоторое целое c такое, что $b = ac$. Будем писать $a \nmid b$, если b не делится на a .

Например, -12 делится на 4 , так как $-12 = 4(-3)$, однако 10 не делится на 3 , так как не существует целого c такого, что $10 = 3c$.

Для выражения делимости b на a применяют также другие слова: " a является делителем числа b ", " a является множителем (фактором) числа b ", " b является числом, кратным числу a ".

Если a является делителем числа b , то b делится также на $(-a)$ (из $b = ac$ следует, что $b = (-a)(-c)$). Таким образом, делители числа всегда появляются парами. Для того, чтобы найти все делители целого числа, достаточно найти положительные делители и затем присоединить соответствующие отрицательные числа. По этой причине мы обычно будем ограничиваться положительными делителями.

Следующее утверждение является простым следствием определения 1

Теорема 2.2. Для целых a, b, c справедливы следующие:

- 1) $a|0$, $1|a$, $a|a$.
- 2) $a|1$ тогда и только тогда, когда $a = \pm 1$.
- 3) Если $a|b$ и $c|d$, то $ac|bd$.
- 4) Если $a|b$ и $b|c$, то $a|c$.
- 5) $a|b$ и $b|a$ тогда и только тогда, когда $a = \pm b$.
- 6) Если $a|b$ и $b \neq 0$, то $|a| \leq |b|$.
- 7) Если $a|b$ и $a|c$, то $a|(bx + cy)$ для произвольных целых чисел x и y .

Доказательство. Докажем утверждения 6) и 7), остальные оставим, как упражнение. Если $a|b$, то $b = ac$ для некоторого целого c . Так как $b \neq 0$, то $c \neq 0$, следовательно, $|c| \geq 1$. Таким образом, $|b| = |ac| = |a||c|$ и $|b| \geq |a|$.

Переходя к доказательству 7), заметим, что из условия $a|b$ и $a|c$ следует существование целых r и s таких, что $b = ar$ и $c = as$. Но

тогда

$$bx + cy = arx + asy = a(rx + sy)$$

при любых целых x и y . Таким образом, $a|(bx + cy)$.

Заметим, что утверждение 7) предыдущей теоремы распространяется по индукции на случай более, чем двух слагаемых. То есть, если $a|b_k$, $k = 1, 2, \dots, n$, то

$$a|(b_1x_1 + b_2x_2 + \dots + b_nx_n)$$

для любых целых x_1, x_2, \dots, x_n . Если a и b — произвольные целые числа, то говорят, что целое число d является *общим делителем* чисел a и b , если $d|a$ и $d|b$. Так как 1 является делителем каждого целого числа, то 1 есть общий делитель чисел a и b , следовательно, множество положительных общих делителей чисел a и b непусто. Заметим теперь, что число 0 делится на любое целое число, следовательно, если $a = b = 0$, то каждое целое является их общим делителем и в этом примере множество положительных общих делителей чисел a и b бесконечно. Если же по крайней мере одно из чисел a и b отлично от 0, то существует только конечное множество положительных общих делителей. Это приводит к следующему определению.

Определение 2. Пусть a и b — целые числа, хотя бы одно из которых отлично от нуля. Наибольшим общим делителем чисел a и b , обозначаемым через $\text{НОД}(a, b)$, называется положительное целое число d , удовлетворяющее условиям:

- 1) $d|a$ и $d|b$,
- 2) если $c|a$ и $c|b$, то $c \leq d$.

Пример 2. Положительными делителями числа -12 являются числа: 1, 2, 3, 4, 6, 12, а положительными делителями числа 30 являются числа 1, 2, 3, 5, 6, 10, 15, 30. Следовательно, общие положительные делители чисел -12 и 30 образуют числа: 1, 2, 3, 6. Так как 6 — наибольшее из этих чисел, то $\text{НОД}(-12, 30) = 6$. Таким же образом можно показать, что $\text{НОД}(-5, 5) = 5$, $\text{НОД}(8, 17) = 1$ и $\text{НОД}(-8, -36) = 4$. Следующая теорема показывает, что $\text{НОД}(a, b)$ может быть представлен в виде линейной комбинации чисел a и b (т.е. в виде $ax + by$, где $x, y \in \mathbb{Z}$).

Теорема 2.3. Для заданных целых чисел a и b , хотя бы одно из которых отлично от нуля, существуют целые числа x и y такие, что

$$\text{НОД}(a, b) = ax + by.$$

Доказательство. Рассмотрим множество S , состоящее из всех положительных линейных комбинаций чисел a и b :

$$S = \{au + bv \mid au + bv > 0 : u, v \in \mathbb{Z}\}.$$

Сначала заметим, что $S \neq \emptyset$. Например, если $a \neq 0$, то целое $|a| = au + b \cdot 0$ принадлежит к S , где мы выбираем $u = 1$, если $a > 0$ и $u = -1$, если $a < 0$. В силу принципа полной упорядоченности множество S содержит наименьший элемент d . Таким образом, по определению множества S существуют целые x и y , для которых $d = ax + by$. Мы утверждаем, что $d = \text{НОД}(a, b)$.

Применив алгоритм деления, имеем $a = qd + r$, $0 \leq r < d$. Тогда

$$r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy).$$

Если бы выполнялось неравенство $r > 0$, то это бы приводило к противоречию, так как $r \in S$ и $r < d$. Поэтому $r = 0$ и $d|a$. Аналогично получим, что $d|b$. Таким образом, d является общим делителем чисел a и b .

Теперь предположим, что c есть произвольный положительный общий делитель чисел a и b . Тогда утверждение 7) теоремы 2.2 позволяет заключить, что $c|(ax + by)$, то есть $c|d$. С помощью утверждения 6) той же теоремы $c = |c| \leq |d| = d$. Таким образом, $d = \text{НОД}(a, b)$. Теорема доказана.

Заметим, что теорема 2.3 не дает практического метода для отыскания x и y (в современной математической литературе они иногда называются коэффициентами Безу). В дальнейшем мы приведем метод нахождения этих коэффициентов.

Следствие 2. Если a и b — целые числа, хотя бы одно из которых не равно нулю, то множество

$$T = \{ax + by \mid x, y \in \mathbb{Z}\}$$

есть множество всех целых чисел, кратных числу $d = \text{НОД}(a, b)$.

Доказательство. Так как $d|a$ и $d|b$, то (см. утверждение 7) теоремы 2.2) $d|(ax + by)$ для всех $x, y \in \mathbb{Z}$. Следовательно, каждый элемент из множества T есть число, кратное d . С другой стороны $d = ax_0 + by_0$ для соответствующих $x_0, y_0 \in \mathbb{Z}$. Таким образом, произвольное кратное nd число d имеет вид

$$nd = n(ax_0 + by_0) = a(nx_0) + b(ny_0).$$

Следовательно, $nd \in T$ и следствие доказано.

Может случиться, что множество общих делителей чисел a и b состоит из 1 и -1 . В этом случае $\text{НОД}(a, b) = 1$, например,

$$\text{НОД}(2, 5) = \text{НОД}(-9, 16) = \text{НОД}(-27, -35) = 1$$

Это приводит к следующему определению

Определение 3. Два целых числа a и b , хотя бы одно из которых отлично от нуля, называются взаимно простыми, если $\text{НОД}(a, b) = 1$.

Следующая теорема характеризует взаимно простые числа в терминах линейных комбинаций.

Теорема 2.4. Пусть a и b — целые числа. Тогда a и b взаимно простые в том и только в том случае, когда существуют целые x и y , для которых

$$1 = ax + by.$$

Доказательство. Если $\text{НОД}(a, b) = 1$, то теорема 2.3 гарантирует существование целых чисел x и y , удовлетворяющих условию $1 = ax + by$ и первая часть теоремы доказана. Предположим теперь, что $1 = ax + by$ для некоторых $x, y \in \mathbb{Z}$ и $d = \text{НОД}(a, b)$. Так как $d|a$ и $d|b$, то теорема 2.2 даст $d|(ax + by)$, т.е. $d|1$. Так как $d > 0$, то, применив теорему 2.2 (утверждение 2), заключаем, что $d = 1$. Теорема доказана.

Следствие 3. Если $\text{НОД}(a, b) = d$, то $\text{НОД}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Доказательство. Если $\text{НОД}(a, b) = d$, то в силу теоремы 2.3 имеем $d = ax + by$, $x, y \in \mathbb{Z}$. Следует, что $1 = \left(\frac{a}{d}\right)x + \left(\frac{b}{d}\right)y$, и осталось только применить теорему 2.4.

В качестве примера применения последнего следствия заметим, что $\text{НОД}(-12, 30) = 6$ и

$$\text{НОД}\left(\frac{-12}{6}, \frac{30}{6}\right) = \text{НОД}(-2, 5) = 1.$$

Из того, что $a|c$ и $b|c$ вообще не следует, что $ab|c$. Например, $6|24$ и $8|24$, но $6 \cdot 8 \nmid 24$. Однако справедливо следующее утверждению.

Следствие 4. Если $a|c$ и $b|c$, а $\text{НОД}(a, b) = 1$, то $ab|c$.

Доказательство. Так как $a|c$ и $b|c$, то существуют целые r и s такие, что $c = ar = bs$. Из условия $\text{НОД}(a, b) = 1$ в силу теоремы 2.4 заключаем, что $1 = ax + by$, $x, y \in \mathbb{Z}$. Умножая последнее равенство на c , получим:

$$c = c \cdot 1 = c(ax + by) = acx + bcy,$$

откуда следует равенство

$$c = a(bs)x + b(ar)y = ab(sx + ry),$$

Таким образом, $ab|c$ и следствие доказано.

Следующий результат имеет фундаментальное значение.

Теорема 2.5 (Лемма Евклида). Если $a|bc$ и $\text{НОД}(a, b) = 1$, то $a|c$.

Доказательство. Начнем с применения теоремы 2.3 и напомним $1 = ax + by$, $x, y \in \mathbb{Z}$. Умножив это равенство на c , получим

$$c = c \cdot 1 = (ax + by)c = acx + bcy.$$

Так как $a|ac$ и $a|bc$, то отсюда заключаем, что $a|(acx + bcy)$, т.е. $a|c$ и теорема доказана.

Если a и b не являются взаимно простыми, то утверждение теоремы 2.5, вообще говоря, неверно, как показывает пример: $12|9 \cdot 8$, но $12 \nmid 9$ и $12 \nmid 8$.

Следующая теорема приводит к другому определению $\text{НОД}(a, b)$. Его преимущество состоит в том, что при этом не используется упорядоченность целых чисел. Такое определение можно использовать в алгебраических системах, не имеющих отношения порядка.

Теорема 2.6. Пусть a и b — два целых числа, хотя бы одно из которых отлично от нуля. Положительное число d является наибольшим общим делителем чисел a и b тогда и только тогда, когда

- 1) $d|a$ и $d|b$,
- 2) если $c|a$ и $c|b$, то $c|d$.

Доказательство. Пусть $d = \text{НОД}(a, b)$. Тогда $d|a$, $d|b$ и выполнено условие 1). В силу теоремы 2.3 число $d = ax + by$ для $x, y, z \in \mathbb{Z}$. Таким образом, если $c|a$ и $c|b$, то $c|(ax + by)$, т.е. $c|d$ и условие 2) выполнено.

Предположим теперь, что выполнены условия 1) и 2). В этом случае d является общим делителем чисел a и b и $c \leq d$ (см. утв. 6) теоремы 2.2). Теорема доказана.

2.4. Задачи

1. Проверить, что если $a|b$, то $(-a)|b$, $a|(-b)$ и $(-a)|(-b)$.
2. Для заданных $a, b, c \in \mathbb{Z}$ проверить, что:
 - (а) если $a|b$, то $a|bc$,
 - (б) если $a|b$ и $a|c$, то $a^2|bc$,
 - (с) $a|b$ тогда и только тогда, когда $ac|bc$, где $c \nmid 0$.
3. Доказать или опровергнуть утверждение: если $a|(b+c)$, то или $a|b$, или $a|c$.
4. Доказать, что для любого $a \in \mathbb{Z}$ одно из чисел $a, a+2, a+4$ делится на 3.

Указание. Согласно алгоритму деления, число a можно представить в виде $3k, 3k+1$ или $3k+2$.
5. (а) Для произвольного целого a установить, что $2|a(a+1)$, а $3|a(a+1)(a+2)$.
(б) Доказать, что ни для какого целого a число a^2+2 не делится на 4.
6. Пользуясь индукцией, доказать, что, если $n \geq 1$, то:
 - (а) $7|2^{3n}-1$ и $8|3^{2n}+7$,
 - (б) $3|2^n+(-1)^{n+1}$.
7. Показать, что если $2 \nmid a$ и $3 \nmid a$, то $24|(a^2-1)$.
8. Доказать, что справедливы следующие утверждения:
 - (а) сумма квадратов двух нечетных чисел не является точным квадратом;
 - (б) произведение четырех последовательных целых чисел на единицу меньше полного квадрата.
9. Доказать, что разность двух последовательных кубов не делится на 2.
10. Пусть $a \neq 0$. Показать, что $\text{НОД}(a, 0) = |a|$ и $\text{НОД}(a, a) = |a|$.
11. Пусть a, b — целые числа, не равные нулю. Показать, что $\text{НОД}(a, b) = \text{НОД}(-a, b) = \text{НОД}(a, -b) = \text{НОД}(-a, -b)$.

12. Доказать, что если $n \in \mathbb{N}$ и $a \in \mathbb{Z}$, то число $\text{НОД}(a, a+n)$ делит n , вывести отсюда, что $\text{НОД}(a, a+1) = 1$.

13. Даны $a, b \in \mathbb{Z}$. Доказать, что:

(а) Существуют целые x и y , для которых $c = ax + by$ тогда и только тогда, когда $\text{НОД}(a, b) | c$;

(б) Если $ax + by = \text{НОД}(a, b)$, то $\text{НОД}(x, y) = 1$.

14. Доказать, что произведение любых трех последовательных целых чисел делится на 6; произведение любых четырех последовательных целых чисел делится на 24; произведение пяти последовательных целых чисел делится на 120.

Указание. Использовать следствие 4 теоремы 2.4

15. Доказать следующие утверждения.

(а) Если a — нечётное целое число, то $24 | a(a^2 - 1)$.

Указание. Воспользоваться тем, что квадрат нечётного числа можно представить в виде $8k + 1$.

(б) Если a и b — нечётные целые числа, то $8 | (a^2 - b^2)$.

(с) Если a — целое, которое не делится ни на 2, ни на 3, то $24 | (a^2 + 23)$.

Указание. Всякое целое число a можно представить одним из способов: $6k, 6k + 1, 6k + 2, 6k + 3, 6k + 4, 6k + 5$.

(d) Если a — целое число, то $360 | a^2(a^2 - 1)(a^2 - 4)$.

16. Доказать следующие свойства наибольшего общего делителя.

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

Указание. Так как $1 = ax + by = au + av$ для некоторых $x, y, u, v \in \mathbb{Z}$, то $1 = (ax + by)(au + cv) = a(x + byu) + bc(yv)$.

(б) Если $\text{НОД}(a, b) = 1$ и $c | a$, то $\text{НОД}(b, c) = 1$.

(с) Если $\text{НОД}(a, b) = 1$, то $\text{НОД}(ac, b) = \text{НОД}(c, b)$.

(d) Если $\text{НОД}(a, b) = 1$ и $c | (a + b)$, то $\text{НОД}(a, c) = \text{НОД}(b, c) = 1$.

Указание. Пусть $d = \text{НОД}(a, c)$. Тогда $d | a, d | c$, отсюда следует, что $d | [(a + b) - a]$, т.е. $d | b$.

2.5. Алгоритм Евклида

Наибольший общий делитель двух целых чисел может быть найден путем перечисления всех положительных чисел, делящих каждое из этих чисел, и выбора наибольшего среди них. Но это слишком неудобно для больших чисел. Более эффективный процесс, включающий повторное применение алгоритма деления, приведен в седьмой книге "Начал". Хотя существуют свидетельства того, что этот метод был известен еще до Евклида, сегодня на него ссылаются как на алгоритм Евклида.

Алгоритм Евклида может быть описан следующим образом. Пусть a и b — два целых числа, для которых требуется найти наибольший общий делитель. Так как $\text{НОД}(|a|, |b|) = \text{НОД}(a, b)$, то будем предполагать, что $a \geq b > 0$. Первый шаг состоит в применении алгоритма деления к a и b . Имеем

$$a = q_1 b + r_1, \quad 0 \leq r_1 < b.$$

Если $r_1 = 0$, то $b|a$ и $\text{НОД}(a, b) = b$. Если $r_1 \neq 0$, то имеем

$$b = q_2 r_1 + r_2, \quad 0 \leq r_2 < r_1.$$

Если $r_2 = 0$, то процесс останавливается, в противном случае получим

$$r_1 = q_3 r_2 + r_3, \quad 0 \leq r_3 < r_2.$$

Процесс деления продолжается до тех пор, пока не появится нулевой остаток на $(n+1)$ шаге, в котором r_{n-1} делится на r_n . Заметим, что рано или поздно появится нулевой остаток, так как убывающая последовательность $b > r_1 > r_2 > \dots \geq 0$ не может содержать больше чем b целых. В результате получим следующую последовательность равенств:

$$\begin{aligned} a &= q_1 b + r_1, & 0 \leq r_1 < b, \\ b &= q_2 r_1 + r_2, & 0 \leq r_2 < r_1, \\ r_1 &= q_3 r_2 + r_3, & 0 \leq r_3 < r_2, \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n, & 0 \leq r_n < r_{n-1} \\ r_{n-1} &= q_{n+1} r_n + 0 \end{aligned}$$

Мы утверждаем, что r_n , последний ненулевой остаток, который появляется в этом процессе, равен $\text{НОД}(a, b)$. Наше доказательство основано на следующей лемме.

Лемма 1. Если $a = qb + r$, то $\text{НОД}(a, b) = \text{НОД}(b, r)$.

Доказательство. Если $\text{НОД}(a, b)$, то из того, что $d|a$ и $d|b$ следует, что $d|(a - qb)$, т.е. $d|r$. Таким образом, d есть общий делитель чисел b и r . С другой стороны, если c — произвольный общий делитель чисел b и r , то $c|(qb + r)$. Следовательно, $c|a$ и c является общим делителем чисел a и b , поэтому $c \leq d$. Лемма доказана.

Применяя необходимое число раз эту лемму, мы устанавливаем, что $\text{НОД}(a, b) = \text{НОД}(b, r_1) = \dots = \text{НОД}(r_{n-1}, r_n) = \text{НОД}(r_n, 0) = r_n$, что и требовалось доказать.

Хотя теорема 2.3 утверждает, что $\text{НОД}(a, b)$ можно представить в виде $ax + by$, ее доказательство не указывает, как найти целые x и y . Этот пробел восполняется алгоритмом Евклида. С помощью предпоследнего шага алгоритма имеем

$$r_n = r_{n-2} - q_n r_{n-1},$$

откуда, учитывая, что согласно алгоритму

$$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1},$$

получим

$$r_n = r_{n-2} - q_n(r_{n-3} - q_{n-1}r_{n-2}) = (1 + q_n q_{n-1})r_{n-2} + (-q_n)r_{n-3}.$$

Это равенство представляет r_n как линейную комбинацию остатков r_{n-2} и r_{n-3} . Продолжая этот процесс, мы последовательно исключим остатки $r_{n-1}, r_{n-2}, \dots, r_2, r_1$ и придем к представлению $r_k = \text{НОД}(a, b)$ в виде линейной комбинации чисел a и b .

Пример 3. Применим алгоритм Евклида для вычисления наибольшего общего делителя чисел 12378 и 3054.

$$12378 = 4 \cdot 3054 + 162,$$

$$3054 = 18 \cdot 162 + 138,$$

$$162 = 1 \cdot 138 + 24,$$

$$138 = 5 \cdot 24 + 18,$$

$$24 = 1 \cdot 18 + 6,$$

$$18 = 3 \cdot 6 + 0.$$

Таким образом, $6 = \text{НОД}(12378, 3054)$.

Представим теперь число 6 в виде линейной комбинации чисел 12378 и 3054. Мы начинаем с предпоследнего равенства и последовательно исключаем остатки 18, 24, 138 и 162:

$$\begin{aligned}
 6 &= 24 - 18 = \\
 &= 24 - (138 - 5 \cdot 24) = \\
 &= 6 \cdot 24 - 138 = \\
 &= 6(162 - 138) - 138 = \\
 &= 6 \cdot 162 - 7 \cdot 138 = \\
 &= 6 \cdot 162 - 7(3054 - 18 \cdot 162) = \\
 &= 132 \cdot 162 - 7 \cdot 3054 = \\
 &= 132 \cdot 12378 + (-535)3054.
 \end{aligned}$$

Таким образом,

$$6 = \text{НОД}(12378, 3054) = 12378x + 3054y,$$

где $x = 132$ и $y = -535$. Нужно отметить, что это не единственный способ представить 6, как линейную комбинацию чисел 12378 и 3054, например, другое представление получится после прибавления вычитания числа $3054 \cdot 12378$. Тогда получим

$$6 = (132+3054)12378 + (-535-12378)3054 = 3186 \cdot 12378 + (-12913)3054$$

Французский математик Ламэ (1795-1870) доказал, что число шагов в алгоритме Евклида не больше чем число цифр в наименьшем из чисел a и b , умноженном на 5. В Примере 3 наименьшее из чисел a и b есть 3054, у которого 4 цифры. Поэтому общее число делений $\leq 5 \cdot 4 = 20$. В действительности нам потребовалось всего 6 делений.

Важным следствием алгоритма Евклида является следующее утверждение.

Теорема 2.7. Если $k > 0$, то $\text{НОД}(ka, kb) = k\text{НОД}(a, b)$.

Доказательство. Если каждое из равенств в алгоритме Евклида для чисел a и b умножить на k , то получим

$$\begin{aligned}
 ak &= q_1(bk) + r_1k, & 0 \leq r_1k < bk, \\
 bk &= q_2(r_1k) + r_2k, & 0 \leq r_2k < r_1k, \\
 &\vdots \\
 r_{n-2}k &= q_n(r_{n-1}k) + r_nk & 0 \leq r_nk < r_{n-1}k \\
 r_{n-1}k &= q_{n+1}(r_nk) + 0
 \end{aligned}$$

Ясно, что эти равенства есть применение алгоритма Евклида к числам ak , bk и наибольший общий делитель этих чисел есть последний ненулевой остаток, т.е. $r_n k$. Следовательно,

$$\text{НОД}(ak, bk) = r_n k = k \text{НОД}(a, b),$$

что и требовалось доказать.

Следствие 5. Для любого целого $k \neq 0$

$$\text{НОД}(ka, kb) = |k| \text{НОД}(a, b).$$

Доказательство. Достаточно рассмотреть случай, в котором $k < 0$. Тогда $-k = |k| > 0$ и по теореме 2.7 имеем

$$\text{НОД}(ak, bk) = \text{НОД}(-ak, -bk) = \text{НОД}(a|k|, b|k|) = |k| \text{НОД}(a, b).$$

В качестве иллюстрации теоремы 2.7 заметим, что

$$\text{НОД}(12, 30) = 3 \text{НОД}(4, 10) = 3 \cdot 2 \text{НОД}(2, 5) = 6 \cdot 1 = 6.$$

Существует понятие, двойственное понятию наибольшего общего делителя двух чисел, известное как наименьшее общее кратное. Говорят, что целое c есть общее кратное двух ненулевых целых a и b , если $a|c$ и $b|c$. Очевидно, что 0 есть общее кратное для любых a и b . Для того, чтобы убедиться в существовании нетривиальных общих кратных, достаточно рассмотреть числа ab и $-(ab)$, которые являются общими кратными a и b . Заметим, что либо ab , либо $-ab$ положительно. С помощью принципа полной упорядоченности заключаем, что множество положительных общих кратных целых a и b должно содержать наименьший элемент. Мы называем его наименьшим общим кратным a и b .

Определение 4. Наименьшее общее кратное двух ненулевых целых a и b , обозначаемое через $\text{НОК}(a, b)$, есть положительное целое m , удовлетворяющее условиям:

- (1) $a|m$ и $b|m$,
- (2) если $a|c$ и $b|c$, $c > 0$, то $m \leq c$.

Например, положительные общие кратные целых -12 и 30 есть $60, 120, 180, \dots$, следовательно, $\text{НОК}(-12, 30) = 60$.

Заметим, что для заданных ненулевых целых чисел a и b $\text{НОК}(a, b)$ всегда существует и $\text{НОК}(a, b) \leq |ab|$.

Какая связь между $\text{НОК}(a, b)$ и $\text{НОД}(a, b)$? Ответом на этот вопрос является следующее утверждение.

Теорема 2.8. Для положительных целых a и b

$$\text{НОД}(a, b) \text{НОК}(a, b) = ab.$$

Доказательство. Пусть $d = \text{НОД}(a, b)$, тогда $a = dr, b = d$, где r и s — целые. Если $m = \frac{ab}{d}$, то $m = as = rb$ и m является общим кратным для a и b .

Теперь пусть c есть произвольное положительное число, являющееся общим кратным чисел a и b , т.е. $c = au = bv$. Как известно, существуют целые x и y такое, что $d = ax + by$. Следовательно,

$$\frac{c}{m} = \frac{cd}{ab} = \frac{c(ax + by)}{ab} = \left(\frac{c}{b}\right)x + \left(\frac{c}{a}\right)y = ux + vy.$$

Отсюда следует, что $m|c$, поэтому $m \leq c$. Таким образом, $m = \text{НОК}(a, b)$, т.е.

$$\text{НОК}(a, b) = m = \frac{ab}{d} = \frac{ab}{\text{НОД}(a, b)}.$$

Теорема доказана.

Следствие 6. Для данных положительных целых a и b $\text{НОК}(a, b) = ab$ тогда и только тогда, когда $\text{НОД}(a, b) = 1$.

Теорема 2.8 позволяет вычислять наименьшее общее кратное двух целых чисел с помощью наибольшего общего делителя этих чисел, что в свою очередь опирается на алгоритм Евклида. Учитывая результаты из Примера 3, имеем:

$$\text{НОК}(3054, 12378) = \frac{3054 \cdot 12378}{6} = 6300402.$$

Заметим, что понятие наибольшего общего делителя двух чисел может быть расширено до понятия наибольшего делителя более, чем двух чисел очевидным образом. В случае трех чисел a, b, c , не все из которых равны нулю $\text{НОД}(a, b, c)$ определяется как положительное целое d , удовлетворяющее следующим свойствам:

- (1) d является делителем каждого из чисел a, b, c .
- (2) если c делит числа a, b, c , то $c \leq d$.

Например, $\text{НОД}(30, 42, 54) = 3$, $\text{НОД}(49, 210, 350) = 7$.

2.6. Задачи

1. Найти $\text{НОД}(143, 227)$, $\text{НОД}(306, 657)$, $\text{НОД}(272, 1479)$.

2. Найти x и y , удовлетворяющие равенству

(a) $\text{НОД}(56, 72) = 56x + 72y$;

(b) $\text{НОД}(24, 138) = 24x + 138y$;

(c) $\text{НОД}(119, 272) = 119x + 272y$;

(d) $\text{НОД}(1769, 2378) = 1769x + 2378y$.

3. Доказать, что если d является общим делителем чисел a и b , то $d = \text{НОД}(a, b)$ тогда и только тогда, когда $\text{НОД}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Указание. Использовать теорему 2.7.

4. Предположим, что $\text{НОД}(a, b) = 1$. Доказать, что:

(a) $\text{НОД}(a + b, a - b) = 1$ или 2.

Указание. Пусть $d = \text{НОД}(a + b, a - b)$. Показать, что $d|2a$, $d|2b$. Таким образом, $d \leq \text{НОД}(2a, 2b) = 2\text{НОД}(a, b)$.

(b) $\text{НОД}(2a + b, a + 2b) = 1$ или 3.

(c) $\text{НОД}(a + b, a^2 + b^2) = 1$ или 2.

Указание. $a^2 + b^2 = (a + b)(a - b) + 2b^2$.

(d) $\text{НОД}(a + b, a^2 - ab + b^2) = 1$ или 3.

Указание. $a^2 - ab + b^2 = (a + b)^2 - 3ab$.

5. Пусть a и b — положительные целые, $n \geq 1$. Доказать, что:

(a) если $\text{НОД}(a, b) = 1$, то $\text{НОД}(a^n, b^n) = 1$.

Указание. Использовать решение задачи 16 а) из параграфа 2.5.

(b) Если $a^n|b^n$, то $a|b$.

Указание. Пусть $d = \text{НОД}(a, b)$, тогда $a = rd$, $b = sd$, где $\text{НОД}(r, s) = 1$. С помощью 5а заключаем, что $\text{НОД}(r^n, s^n) = 1$. Показать, что $r = 1$, откуда $a = d$.

6. Пусть a и b — целые, отличные от нуля. Доказать, что следующие свойства эквивалентны:

7. $a|b$,

8. $\text{НОД}(a, b) = |a|$,

9. $\text{НОК}(a, b) = |b|$.

10. Найти $\text{НОК}(143, 227)$, $\text{НОК}(306, 651)$, $\text{НОК}(272, 1479)$.

11. Доказать, что наибольший общий делитель двух положительных целых всегда делит их наименьшее общее кратное.
12. Пусть a и b — два целых, отличных от нуля. Доказать следующие утверждения.
 - (а) $\text{НОД}(a, b) = \text{НОК}(a, b)$ тогда и только тогда, когда $a = b$.
 - (б) Если $k > 0$, то $\text{НОК}(ka, kb) = k\text{НОК}(a, b)$.
 - (с) Если m — произвольное общее кратное чисел a и b , то $\text{НОК}(a, b) \mid m$.

Указание. Пусть $t = \text{НОК}(a, b)$. Согласно алгоритму деления $m = qt + r$, где $0 \leq r < t$. Показать, что r — общее кратное a и b .
13. Пусть a, b, c — целые, никакие два из которых не равны нулю, и $d = \text{НОД}(a, b, c)$. Доказать, что

$$d = \text{НОД}(\text{НОД}(a, b), c) = \text{НОД}(a, \text{НОД}(b, c)) = \text{НОД}(\text{НОД}(a, c), b)$$
14. Найти целые числа x, y, z , удовлетворяющие следующему условию: $\text{НОД}(198, 288, 512) = 198x + 288y + 512z$.

Указание. Пусть $d = \text{НОД}(198, 288)$. Так как $\text{НОД}(198, 288, 512) = \text{НОД}(d, 512)$, сначала найти целые числа u и v , для которых $\text{НОД}(d, 512) = du + 512v$.

2.7. Диофантово уравнение $ax + by = c$

Перейдем к изучению диофантовых уравнений. Название дано в честь математика Диофанта, который впервые изучал такие уравнения. Практически нам ничего неизвестно о нем, кроме того, что он жил в Александрии приблизительно около 250 года н.э. Хотя работы Диофанта написаны на греческом и он демонстрировал греческий гений в теоретических исследованиях, он больше похож на эллинизированного вавилонца.

Известна знаменитая работа Диофанта под названием "Арифметика", которую можно считать одним из самых ранних трактатов по алгебре. Сохранилось только 6 книг из 13 написанных Диофантом. В "Арифметике" мы впервые находим использование математических обозначений: неизвестная величина в уравнении, степени неизвестного, символ для вычитания и равенства. Обычно термин диофантово уравнение применяется к уравнению с одним или большим чис-

лом неизвестных, решение которого мы ищем в целых числах. Простейший тип диофантова уравнения, который мы будем рассматривать, есть линейное диофантово уравнение с двумя неизвестными:

$$ax + by = c,$$

где a, b, c — данные целые числа, причем a и b не равны нулю одновременно. Решения этого уравнения есть пары целых чисел x_0, y_0 , для которых $ax_0 + by_0 = c$.

Данное линейное диофантово уравнение может иметь несколько решений, например для уравнения $3x + 6y = 18$, имеем

$$\begin{aligned} 3 \cdot 4 + 6 \cdot 1 &= 18, \\ 3 \cdot (-6) + 6 \cdot 6 &= 18, \\ 3 \cdot (10) + 6 \cdot (-2) &= 18. \end{aligned}$$

С другой стороны, уравнение $2x + 10y = 17$ не имеет ни одного решения. В самом деле, левая часть этого уравнения есть чётное число при любом выборе x и y , в то время как правая часть является нечетным числом. Условие для разрешимости состоит в следующем. Диофантово уравнение $ax + by = c$ имеет решение тогда и только тогда, когда $d|c$, где $d = \text{НОД}(a, b)$. Мы знаем, что существуют целые числа r и s , для которых $a = dr$ и $b = ds$. Если решение уравнения $ax + by = c$ существует и $ax_0 + by_0 = c$ для некоторых целых x_0 и y_0 , то

$$c = ax_0 + by_0 = drx_0 + dsy_0 = d(rx_0 + sy_0),$$

откуда следует, что $d|c$. С другой стороны, если $d|c$, то $c = dt$ и, применяя теорему 2.3, найдем целые числа x_0 и y_0 , для которых $d = ax_0 + by_0$. Если последнее равенство умножим на t , то получим

$$c = dt = (ax_0 + by_0)t = a(tx_0) + b(ty_0).$$

Следовательно, диофантово уравнение $ax + by = c$ имеет решение $x = tx_0, y = ty_0$. Это рассуждение доказывает первое утверждение следующей теоремы.

Теорема 2.9. Линейное диофантово уравнение $ax + by + c = 0$ имеет решение тогда и только тогда, когда $d|c$, где $d = \text{НОД}(a, b)$. Если x_0, y_0 есть частное решение этого уравнения, то общее решение задается равенством

$$x = x_0 + \left(\frac{b}{d}\right)t, \quad y = y_0 - \left(\frac{a}{d}\right)t,$$

где t — произвольное число.

Доказательство. Чтобы доказать второе утверждение этой теоремы, предположим, что решение x_0, y_0 данного уравнения известно. Если пара чисел x', y' является произвольным другим решением, то

$$ax_0 + by_0 = c = ax' + by',$$

это эквивалентно равенству

$$a(x' - x_0) = b(y_0 - y').$$

В силу следствия 3 из теоремы 2.4 существуют взаимно простые целые r и s такие, что $a = dr, b = ds$, подставляя эти значения в последнее равенство и сокращая общий множитель d , получим

$$r(x' - x_0) = s(y_0 - y').$$

Из этого равенства следует, что $r|s(y_0 - y')$, причем $\text{НОД}(r, s) = 1$. Используя лемму Евклида, заключаем, что $r|(y_0 - y')$ или $y_0 - y' = rt$ для некоторого целого t . Следовательно, т.к. $r(x' - x_0) = s(y_0 - y')$, $x' - x_0 = st$. Это приводит к формулам

$$\begin{aligned}x' &= x_0 + st = x_0 + \left(\frac{b}{d}\right)t, \\y' &= y_0 - rt = y_0 - \left(\frac{a}{d}\right)t.\end{aligned}$$

Легко видеть, что эти числа удовлетворяют данному диофантову уравнению при любом выборе t . В самом деле,

$$\begin{aligned}ax' + by' &= a\left[x_0 + \frac{b}{d}t\right] + b\left[y_0 - \frac{a}{d}t\right] = \\&= (ax_0 + by_0) + \left(\frac{ab}{d} - \frac{ab}{d}\right)t = c + 0 \cdot t = c.\end{aligned}$$

Таким образом, существует бесконечное число решений данного уравнения.

Пример 4. Рассмотрим линейное диофантово уравнение

$$172x + 20y = 1000.$$

Применяя алгоритм Евклида для вычисления НОД(172, 20), найдем, что

$$172 = 8 \cdot 20 + 12,$$

$$20 = 1 \cdot 12 + 8,$$

$$12 = 1 \cdot 8 + 4,$$

$$8 = 2 \cdot 4,$$

следовательно, НОД(172, 20) = 4. Т.к. $4 \mid 1000$, то данное уравнение разрешимо. Представим теперь 4 как линейную комбинацию чисел 172 и 20. Имеем

$$\begin{aligned} 4 &= 12 - 8 = \\ &= 12 - (20 - 12) = \\ &= 2 \cdot 12 - 20 = \\ &= 2(172 - 8 \cdot 20) - 20 = \\ &= 2 \cdot 172 + (-17)20. \end{aligned}$$

Таким образом,

$$4 = 2 \cdot 172 + (-17)20.$$

Умножая это равенство на 250, получим

$$1000 = 250 \cdot 4 = 250[2 \cdot 172 + (-17)20] = 500 \cdot 172 + (-4250)20.$$

Таким образом, $x_0 = 500$, $y_0 = -4250$ есть частное решение нашего уравнения. Все другие решения имеют вид

$$\begin{aligned} x &= 500 + \left(\frac{20}{4}t\right) = 500 + 5t, \\ y &= -4250 - \left(\frac{172}{4}t\right) = -4250 - 43t. \end{aligned}$$

Следствие 7. Если НОД(a, b) = 1 и x_0, y_0 — частное решение линейного диофантова уравнения $ax + by = c$, то общее решение имеет вид

$$x = x_0 + bt, \quad y = y_0 - at,$$

где t — произвольное целое.

2.8. Алгоритм Берлекэмп

Следует отметить, что алгоритм Евклида, в частности, нахождение коэффициентов Безу, весьма часто необходим в современной вычислительной технике. От скорости вычисления коэффициентов Безу зависит во многом эффективность применяемых остальных алгоритмов. Классический способ вычисления весьма расточителен в этом смысле. Для нахождения коэффициентов Безу требуется помнить результаты промежуточных вычислений, а затем проделывать большую часть вычислений в обратном порядке. До появления вычислительной техники, базирующейся на теоретико-числовых алгоритмах и соответствующих прикладных задач (теория кодирования, дискретное преобразование Фурье, быстрые вычисления), вопросы такого рода даже не возникали. Массовость теоретико-числовых задач, используемых в современной технике, заставила по-новому взглянуть на алгоритм Евклида спустя более чем 2000 лет после его описания и разработать более удобную версию. Приведём пример такого усовершенствования, принадлежащий Э.Берлекэмп (названный им алгоритмом непрерывных дробей).

Рассмотрим последовательность делений алгоритма Евклида, начинающихся с чисел a и b . Тогда $a = q_1b + r_1$ с $0 \leq r_1 < b$, $b = q_2r_1 + r_2$ с $0 \leq r_2 < r_1$. Тогда на $k+2$ -ом шаге имеем равенство

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

Для большего единообразия обозначим $a = r_{-1}$, $b = r_0$. Напомним, что последний шаг имеет вид $r_{n-1} = q_{n+1}r_n$, где r_n и есть искомый наибольший общий делитель чисел a и b .

Каждый шаг алгоритма Евклида представляет собой переход от пары чисел (r_k, r_{k+1}) к паре (r_{k+1}, r_{k+2}) . Учитывая сказанное выше, можно записать этот переход с помощью матричного равенства:

$$(r_{k+1}, r_{k+2}) = (r_k, r_{k+1})A_k,$$

где через A_k обозначена матрица

$$= \begin{pmatrix} 0 & 1 \\ 1 & -q_{k+2} \end{pmatrix}.$$

Таким образом,

$$A_{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix},$$

а из ассоциативности операции умножения матриц легко следует, что

$$(r_{-1}, r_0)(A_{-1}A_0 \cdots A_{n-1}) = (r_n, r_{n+1}),$$

где r_n уже наибольший общий делитель чисел a и b . В этом случае, понятно, $r_{n+1} = 0$, а матрица $M = A_{-1}A_0 \cdots A_{n-1}$ обладает свойством $(r_{-1}, r_0)M = (r_n, r_{n+1})$. Если обозначить через m_{ij} элементы матрицы M , то получим, что

$$r_{-1}m_{11} + r_0m_{21} = r_n = am_{11} + bm_{21},$$

т.е. соотношение Безу. Элементы первого столбца матрицы M как раз и дают искомые коэффициенты. При этом вовсе не обязательно помнить все промежуточные результаты деления. Достаточно иметь текущее на данный момент значение матрицы M и очередное неполное частное q_{k+2} , умножая текущее значение матрицы M на только что полученную матрицу A_k . В качестве начального значения матрицы M естественно выбрать единичную матрицу. Нумеровать промежуточные матрицы в процессе вычислений (что при программировании на вычислительной машине подразумевает выделение соответствующей памяти машины) также не обязательно. Достаточно иметь лишь текущую матрицу $A = A_k$, изменяя её содержимое в соответствии с очередным делением. Структура матрицы A_k , как видно из её описания, позволяет вычислить очередное значение матрицы M , используя всего одну операцию умножения и одну операцию вычитания.

Рассмотрим ещё раз пример 3 с использованием алгоритма Берлекэмпа. Применим алгоритм Евклида для вычисления наибольшего общего делителя чисел $r_{-1} = 12378 = a$ и $r_0 = 3054 = b$.

Пусть $M = I$ — единичная 2×2 -матрица.

Так как $12378 = 4 \cdot 3054 + 162$, то матрица $A = A_{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix} = MA$.

Дальнейшие вычисления дают $3054 = 18 \cdot 162 + 138$, $A = A_0 = \begin{pmatrix} 0 & 1 \\ 1 & -18 \end{pmatrix}$, $M := MA = \begin{pmatrix} 1 & -18 \\ -4 & 73 \end{pmatrix}$.

Здесь запись $M := MA$ означает, что на место коэффициентов матрицы M записываются коэффициенты матрицы MA . Остальные вычисления мы приводим без комментариев.

$$162 = 1 \cdot 138 + 24, A = A_1 = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}, M := MA = \begin{pmatrix} -18 & 19 \\ 73 & -77 \end{pmatrix}.$$

$$138 = 5 \cdot 24 + 18, A = A_1 = \begin{pmatrix} 0 & 1 \\ 1 & -5 \end{pmatrix}, M := MA = \begin{pmatrix} 19 & -113 \\ -77 & 458 \end{pmatrix}.$$

$$24 = 1 \cdot 18 + 6, A = A_2 = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}, M := MA = \begin{pmatrix} -113 & 132 \\ 458 & -535 \end{pmatrix}.$$

$$18 = 3 \cdot 6 + 0, A = A_3 = \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix}, M := MA = \begin{pmatrix} 132 & -509 \\ -535 & 2063 \end{pmatrix}.$$

Теперь мы можем прочитать коэффициенты Безу из первого столбца "накопленной" матрицы M . Получаем

$$6 = 12378 \cdot 132 + 3054 \cdot (-535).$$

Следует заметить, что программирование алгоритма несколько отличается от описанной последовательности вычислений и гораздо больше напоминает процесс построения непрерывной дроби, к чему мы ещё вернёмся впоследствии.

2.9. Задачи

1. Найти все целочисленные решения каждого из следующих уравнений:

(a) $56x + 72y = 40$;

(b) $24x + 138y = 18$;

(c) $221x + 91y = 117$;

(d) $84x - 438y = 156$.

2. Найти все положительные целочисленные решения каждого из следующих уравнений:

(a) $30x + 17y = 300$;

(b) $54x + 21y = 900$;

(c) $123x + 360y = 99$;

(d) $158x - 57y = 7$.

3. Доказать, что если a и b взаимно простые натуральные числа, то диофантово уравнение имеет бесконечно множество положительных и целых решений.

Указание. Существуют целые x_0, y_0 такие, что $ax_0 + by_0 = 1$. Для любого целого t , большего, чем $\frac{|x_0|}{b}$ и $\frac{|y_0|}{a}$, числа $x = x_0 + bt$ и $y = -(y_0 - at)$ дают положительные и целые решения данного уравнения.

- (а) Доказать, что диофантово уравнение $ax + by + cz = d$ разрешимо в целых числах тогда и только тогда, когда $\text{НОД}(a, b, c) \mid d$.
(б) Найти все целочисленные решения уравнения $15x + 12y + 30z = 24$.

Указание. Положить $y = 3s - 5t$, $z = -s + 2t$.

2.10. Дополнение

Относительно операции сложения и умножения множество \mathbb{Z} целых чисел образует структуру, известную как *кольцо*, т.е. обладает следующими свойствами:

- 1) сумма и произведение двух целых чисел есть целое число;
- 2) умножение и сложение коммутативны, т.е. $ab = ba$, $a + b = b + a$;
- 3) $a + 0 = a$, $a \cdot 1 = a$;
- 4) $a + (-a) = 0$;
- 5) дистрибутивный закон: $(a + b)c = ac + bc$;
- 6) ассоциативный закон: $(ab)c = (a b)c$, $(a + b) + c = a + (b + c)$.

Так как умножение здесь коммутативно, то \mathbb{Z} является *коммутативным* кольцом. Кроме того, \mathbb{Z} обладает еще одним свойством:

закон сокращения: если $ab = 0$ и $a \neq 0$, то $b = 0$.

Это свойство обеспечивает для \mathbb{Z} структуру, называемую *областью целостности*.

Рациональные числа, которые мы обозначаем с помощью \mathbb{Q} , также образуют коммутативное кольцо относительно сложения и умножения. Однако в дополнение к условиям 1)–5), перечисленным выше, \mathbb{Q} удовлетворяет мультипликативному аналогу условия 1), именно, если $a \neq 0$, то

$$a \cdot \left(\frac{1}{a}\right) = 1.$$

В результате рациональные числа дают пример структуры, известной как *поле*. Ясно, что кольцо \mathbb{Z} не является полем. Поэтому простое уравнение

$$ax = b, \text{ где } a, b \in \mathbb{Z},$$

вообще говоря, не имеет решения в \mathbb{Z} . Вполне естественным, следовательно, выглядит определение 1 делимости целых чисел.

Многие задачи теории чисел связаны со свойствами подмножеств множества \mathbb{Z} . Простой тип подмножеств может быть определен, рассматривая все числа, кратные данному числу s . Мы будем обозначать это подмножество с помощью M_s . Оно обладает следующими очевидными свойствами:

если $m, n \in M_s$, то $m - n \in M_s$;

если $t \in \mathbb{Z}, n \in M_s$, то $tn \in M_s$.

Это приводит к следующему определению.

Определение 5. *Непустое подмножество T множества \mathbb{Z} называется идеалом кольца \mathbb{Z} , если*

$t_1, t_2 \in T$ влечет $t_1 - t_2 \in T$;

$m \in \mathbb{Z}, t \in T$ влечет $mt \in T$.

Из этого определения следует, что M_s , где s — произвольное неотрицательное целое, является идеалом кольца \mathbb{Z} . Ясно, что M_0 состоит только из числа 0, а $M_1 = \mathbb{Z}$. Естественно спросить, существуют ли идеалы кольца \mathbb{Z} , отличные от M_s ? Ответ — отрицательный, как показывает следующее утверждение.

Теорема 2.10. Пусть \mathcal{I} — идеал кольца \mathbb{Z} . Тогда существует неотрицательное целое s , такое, что $\mathcal{I} = M_s$.

Доказательство. Если \mathcal{I} состоит только из числа 0, то $\mathcal{I} = M_0$. В противном случае \mathcal{I} содержит ненулевое целое число t . Если $t < 0$, то \mathcal{I} содержит $(-1)t = -t > 0$, следовательно, \mathcal{I} содержит положительные целые числа. В силу принципа полной упорядоченности \mathcal{I} содержит наименьшее положительное целое число, которое мы обозначим через s . Мы утверждаем, что $\mathcal{I} = M_s$. Для доказательства достаточно показать, что все элементы из \mathcal{I} делятся на s . Пусть $t \in \mathcal{I}, t \neq 0$, применим алгоритм деления:

$$t = sq + r, \quad 0 \leq r < s.$$

Так как $r = t - sq \in T$; то если бы было $r > 0$, это противоречило бы выбору s , как наименьшего положительного элемента из T . Таким образом, $r = 0$, $t = sq$ и s делит t . Теорема доказана.

Идеалы, состоящие из кратных одного элемента, называются *главными идеалами*. Таким образом, теорема 2.10 утверждает, что все идеалы кольца \mathbb{Z} являются главными.

Отсюда легко следует, что сумма двух главных идеалов кольца \mathbb{Z} — главный идеал. Так как множество всех целых чисел, кратных числу s , есть идеал $T = M_s$, то условие $m|n$ может быть записано в виде отношения включения между идеалами:

$$m|n \text{ равносильно включению } M_n \subseteq M_m.$$

Обратим внимание на "перевёрнутость" отношения включения к отношению делимости.

Из сказанного и теоремы 2.10 немедленно следует, что для любых двух целых чисел a и b найдётся такое натуральное число d , что

$$M_a + M_b = M_d,$$

так что $d = ua + vb$, причём u и v — целые числа и d — наименьшее натуральное число, представимое в виде целочисленной линейной комбинации элементов a и b . Разумеется, d оказывается наибольшим общим делителем чисел a и b , а u и v — коэффициентами Безу.

2.11. Задачи

1. Полином $f(x)$ с целыми коэффициентами есть выражение вида $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$, $a_i \in \mathbb{Z}$. Если $a_n \neq 0$, то говорят, что $f(x)$ есть полином *степени* $\deg f = n$. Обозначая множество всех таких полиномов через $\mathbb{Z}[x]$, доказать, что $\mathbb{Z}[x]$ является коммутативным кольцом, относительно естественного определения сложения и умножения полиномов. Показать также, что $\mathbb{Z}[x]$ есть область целостности. Доказать то же самое для $\mathbb{Q}[x]$ — множества всех полиномов с рациональными коэффициентами.
2. Пусть $f(x), g(x) \in \mathbb{Q}[x]$ такие, что

$$\begin{aligned} f(x) &= a_n x^n + \dots + a_0, \quad a_n \neq 0 \\ g(x) &= b_m x^m + \dots + b_0, \quad b_m \neq 0. \end{aligned}$$

Показать, что если $n \geq m$, то степень полинома $h(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x)$ меньше, чем n .

3. Алгоритм деления имеет аналог в $\mathbb{Q}[x]$, т.е. справедливо следующее утверждение. Для данных двух полиномов $f(x)$ и $g(x)$ из $\mathbb{Q}[x]$, где $g(x)$ не равен нулю, существуют $q(x), r(x) \in \mathbb{Q}[x]$, такие, что

$$f(x) = g(x)q(x) + r(x), \quad (*)$$

где или $r(x) \equiv 0$, или $0 \leq \deg r(x) < \deg g(x)$. Доказать это.

Указание. Сначала рассмотреть случай $f(x) \equiv 0$ или степень полинома $f(x)$ равна 0 ($f(x)$ — константа). Затем применим индукцию по степени полинома $f(x)$ и предположим, что результат верен для всех полиномов $f(x)$ степени $< n$. Пусть $f(x)$ имеет степень n . Рассмотреть сначала случай, когда $\deg g > \deg f$. В случае, когда $\deg f \geq \deg g$, рассмотреть полином h из задачи 1.

4. Доказать единственность представления (*).
5. Доказать, что утверждение задачи 3 можно перенести для случая, когда $f(x), g(x), q(x), r(x)$ принадлежат к $\mathbb{Z}[x]$, при условии, что $b_m = 1$.
6. Для данных двух полиномов $f, g \in \mathbb{Q}[x]$ говорят, что g делит f (или f кратно g), если существует $h \in \mathbb{Q}[x]$, такой, что $f = gh$. Пусть M_f есть подмножество множества $\mathbb{Q}[x]$, состоящее из многочленов, кратных f . Доказать, что M_f является идеалом кольца $\mathbb{Q}[x]$.
7. Доказать, что каждый идеал кольца $\mathbb{Q}[x]$ имеет вид M_f для некоторого многочлена $f \in \mathbb{Q}[x]$.

Глава 3

Простые числа и их распределение

Практическое приложение находят тогда, когда его не ищут, и можно сказать, что вся программа современной цивилизации зиждется на этом принципе.

Ж. Адамар

3.1. Основная теорема арифметики

В этой главе важнейшим является понятие простого числа. Отметим, что произвольное целое число $a > 1$ делится на ± 1 и $\pm a$. Если числа ± 1 и $\pm a$ исчерпывают все делители числа a , то говорят, что a — простое число.

Определение 6. *Целое число $p > 1$ называется простым числом, если положительными делителями его являются только числа 1 и p . Целое число, большее единицы, которое не является простым, называется составным.*

Среди первых десяти натуральных чисел числа 2, 3, 5, 7 являются простыми, в то время как 4, 6, 8, 9, 10 — составные числа. Заметим, что целое число 2 является единственным чётным простым и в соответствии с нашим определением число 1 играет особую роль, так как оно не является ни простым, ни составным.

Предложение 14 из книги IX "Начал" Евклида включает результат, который впоследствии стал известен как фундаментальная теорема арифметики, и состоящий в том, что каждое целое число, боль-

шее единицы, с точностью до порядка сомножителей, представимо как произведение простых одним и только одним способом.

Так как каждое целое число является или простым, или, согласно основной теореме, может быть представлено произведением простых чисел из однозначно определённого набора, то простые числа служат "строительными блоками", из которых все другие целые числа могут быть собраны. Поэтому простые числа привлекали математиков во все времена. Хотя за прошедшее время был доказан ряд замечательных результатов, касающихся распределения простых чисел среди всех положительных, осталось еще много знаменитых нерешенных проблем.

Начнем с простого замечания. Число 3 делит число 36, при этом 36 можно представить как одно из произведений:

$$6 \cdot 6 = 9 \cdot 4 = 12 \cdot 3 = 18 \cdot 2.$$

В каждом из этих примеров число 3 делит по крайней мере один из сомножителей, входящих в произведение. Это является типичным примером более общей ситуации.

Теорема 3.1. Если p — простое и $p|ab$, то $p|a$ или $p|b$.

Доказательство. Если $p|a$, то нечего доказывать. Предположим, что $p \nmid a$. Так как единственными положительными делителями числа a являются 1 и p , то $\text{НОД}(p, a) = 1$. Следовательно, учитывая лемму Евклида, получаем, что $p|b$.

Эта теорема легко распространяется на случай, когда произведение содержит более двух сомножителей.

Следствие 8. Если p — простое и $p|a_1 a_2 \cdots a_n$, то $p|a_k$ для некоторого k , $1 \leq k \leq n$.

Доказательство. Применим индукцию по числу сомножителей. Если $n = 1$, то утверждение теоремы, очевидно, справедливо, а для $n = 2$ результат вытекает из теоремы 3.1. Предположим, что $n > 2$ и что если $p|a_1 \cdots a_m$ ($m < n$), то p делит один из m этих сомножителей. Пусть теперь $p|a_1 \cdots a_n$. По теореме 3.1 или $p|a_1 \cdots a_{n-1}$. Если $p|a_n$, то утверждение доказано. Что касается случая $p|a_1 \cdots a_{n-1}$, то предположение индукции приводит к тому, что $p|a_k$ для некоторого k , $1 \leq k \leq n-1$. В любом случае p делит одно из целых a_1, \dots, a_n .

Следствие 9. Если p, q_1, q_2, \dots, q_n — простые числа и $p|q_1 \cdots q_n$, то $p = q_k$ для некоторого k , $1 \leq k \leq n$.

Доказательство. С помощью следствия 8 заключаем, что $p|q_k$ для некоторого k , $1 \leq k \leq n$. Будучи простым, число q_k делится только на 1 и на самого себя, но так как $p > 1$, то отсюда следует, что $p = q_k$.

Теорема 3.2 (Основная теорема арифметики). Каждое положительное целое $n > 1$ можно представить как произведение простых. Это представление единственно с точностью до порядка сомножителей.

Доказательство. Каждое число n является или простым, или составным. В первом случае доказывать нечего. Если n — составное, то существует целое d , такое, что $d|n$ и $1 < d < n$. Среди всех таких целых d выберем p_1 , как наименьшее (это возможно в силу принципа полной упорядоченности). Тогда p_1 должно быть простым. В самом деле, если p_1 не является простым, то оно имеет делители q , $1 < q < p_1$. Тогда $q|p_1$ и следовательно, т.к. $p_1|n$, получим, что $q|n$, что противоречит выбору p_1 как наименьшего делителя числа n , отличного от 1.

Теперь мы можем предположить, что $n = p_1 n_1$, где p — простое и $1 < n_1 < n$. Если n_1 было бы простым, то мы имели бы требуемое теоремой представление. В противном случае повторим наше рассуждение и получим второе простое число p_2 такое, что $n_1 = p_2 n_2$, т.е.

$$n = p_1 p_2 n_2, \quad 1 < n_2 < n_1.$$

Если n_2 — простое, то нечего доказывать. В противном случае имеем $n_2 = p_3 n_3$, где p_3 — простое. Следовательно,

$$n = p_1 p_2 p_3 n_3, \quad 1 < n_3 < n_2.$$

Убывающая последовательность

$$n > n_1 > n_2 > \dots > 1$$

не может быть бесконечной. Поэтому после конечного числа шагов придем к числу n_k , являющимся простым, которое обозначим через p_k . Это приводит к разложению числа n в произведение простых:

$$n = p_1 p_2 \dots p_k.$$

Чтобы доказать вторую часть теоремы (единственность разложения), предположим, что целое число n может быть представлено в

виде произведения простых другим способом. Тогда получим

$$n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s, \quad r \leq s$$

где p_i и q_j — простые для $i = 1, \dots, r, j = 1, \dots, s$, и

$$p_1 \leq p_2 \leq \dots \leq p_r, \quad q_1 \leq q_2 \leq \dots \leq q_s.$$

Так как $p_1 | q_1 q_2 \dots q_s$, то в силу следствия 9 из теоремы 3.1 заключаем, что $p_1 = q_k$ для некоторого k , $1 \leq k \leq s$. Отсюда следует, что $q_1 \leq p_1$. Подобные рассуждения показывают, что $p_1 \leq q_1$, следовательно, $p_1 = q_1$. Сокращение на общий множитель приводит к равенству

$$p_2 p_3 \dots p_r = q_2 q_3 \dots q_s.$$

Продолжив этот процесс, придем в предположении, что $r < s$, к равенству

$$1 = q_{r+1} q_{r+2} \dots q_s,$$

что невозможно, т.к. $q_i > 1$, $1 \leq i \leq s$. Следовательно, $r = s$ и справедливо равенство

$$p_1 = q_1, p_2 = q_2, \dots, p_r = q_r,$$

что доказывает совпадение двух разложений и теорема полностью доказана.

Совершенно очевидно, что некоторые простые числа, появляющиеся в разложении числа, могут повторяться, как видно из примера с числом 360, которое равно $2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5$. Собирая одинаковые простые и помещая их в один множитель, мы можем перефразировать теорему 3.2 следующим образом.

Следствие 10. Каждое положительное целое $n > 1$ может быть единственным образом представлено в каноническом виде:

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r},$$

где $p_1 < p_2 < \dots < p_r$ — простые числа и k_1, \dots, k_r — положительные целые.

Теорему 3.2 не следует воспринимать как нечто очевидное, так как существуют числовые системы, в которых разложение на "простые" множители не является единственным. Возможно, наиболее элементарным примером является множество E всех положительных четных чисел. Будем называть чётное целое число e -простым

, если оно не является произведением двух других четных чисел. Например, числа 2, 6, 10, 14 являются e -простыми, тогда как числа 4, 8, 12, 16 таковыми не являются. Нетрудно видеть, что число 60 можно факторизовать в e -простые двумя разными способами:

$$60 = 2 \cdot 30 = 6 \cdot 10.$$

Причина состоит в том, что теорема 3.1 не имеет места для множества E . Очевидно, $6 \nmid 2 \cdot 30$, но $6 \nmid 2$ и $6 \nmid 30$.

Два других примера показывают, что существуют весьма естественные обобщения кольца целых чисел, в которых справедлива Основная теорема арифметики, а также нетривиальность вопросов относительно однозначности разложения в этих кольцах.

Пример 5. Пусть $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}, i^2 = -1\}$ — кольцо целых Гауссовых чисел, i — мнимая единица, рассматриваемое как подмножество множества комплексных чисел.

Можно показать, что любой идеал этого кольца является главным и что Основная теорема арифметики справедлива и в этом кольце. "Простыми" элементами здесь уже будут числа вида $a + bi$, для которых $a^2 + b^2$ — простое целое число, а также простые целые числа, не являющиеся суммой двух квадратов целых чисел.

Пример 6. Пусть $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}, \sqrt{-5}^2 = -5\}$ — кольцо чисел вида $a + b\sqrt{-5}$, где $\sqrt{-5}$ — корень квадратный из -5 , рассматриваемое как подмножество множества комплексных чисел.

В этом кольце Основная теорема арифметики уже не имеет места. Более того, нетрудно указать два разложения числа 6, где каждый из сомножителей может рассматриваться как "простой" элемент кольца :

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

В связи с этим более тонкая теория делимости в кольцах различает неприводимые и простые элементы (т.е. такие, для которых из делимости произведения на такой элемент следует, что хотя бы один из сомножителей делится на него).

Приведем теперь доказательство знаменитого результата Пифагора, как следствие основной теоремы арифметики. Математика как наука началась с Пифагора (569-500 до н.э.) и многое из содержания "Начал" Евклида принадлежит Пифагору и его школе. Пифагор впервые ввел понятие чётные и нечётные числа, простые и составные.

Теорема 3.3 (Пифагор). Число $\sqrt{2}$ является иррациональным.

Доказательство. Предположим, что $\sqrt{2}$ является рациональным числом и $\sqrt{2} = \frac{a}{b}$, где a и b — целые, такие что $\text{НОД}(a, b) = 1$. Отсюда следует, что $a^2 = 2b^2$, следовательно, $b|a^2$. Если $b > 1$, то основная теорема арифметики гарантирует существование простого числа p такого, что $p|b$. Тогда $p|a^2$ и из теоремы 3.1 заключаем, что $p|a$, следовательно, $\text{НОД}(a, b) \geq p$, что приводит к противоречию. Остается предположить, что $b = 1$. Но тогда $a^2 = 2$, что невозможно, так как a — целое. Наше предположение о том, что $\sqrt{2}$ — рациональное привело к противоречию, следовательно, $\sqrt{2}$ — иррациональное.

3.2. Задачи

1. Найти пять простых чисел среди чисел вида

$$n^2 - 2$$

2. Привести пример, показывающий, что предположение о том, что каждое натуральное число представимо в виде $p + a^2$, где p — простое или 1, а число $a > 0$, является неверным.

3. Доказать каждое из следующих утверждений.

(a) Каждое простое число, имеющее вид $3n + 1$, можно представить в форме $6m + 1$.

(b) Каждое целое число вида $3n + 2$ имеет множителем простое число такого же вида.

(c) Единственным простым числом, которое можно представить в виде $n^3 - 1$, является число 7.

Указание. Учсть, что $n^3 - 1 = (n - 1)(n^2 + n + 1)$.

(d) Единственным простым числом p , для которого $3p + 1$ является точным квадратом, есть $p = 5$.

4. Доказать, что $p^2 + 2$ является составным числом, если p — простое и $p \geq 5$.

Указание. Число p может иметь одну из форм: $6k + 1$ или $6k + 5$.

5. (a) p — простое и $p|a^n$. Доказать, что $p^n|a^n$.

(b) Пусть $\text{НОД}(a, b) = p$ — простое число. Каковы возможные значения для $\text{НОД}(a^2, b^2)$, $\text{НОД}(a^2, b)$ и $\text{НОД}(a^3, b^2)$?

6. Доказать каждое из следующих утверждений.

- (а) Каждое целое вида $n^4 + 1$, где $n > 1$, является составным.
 - (б) Каждое целое вида $n^4 + 4$, где $n > 1$, является составным (теорема Софи Жермен).
 - (с) Если $n > 4$ и составное, то n делит $(n - 1)!$
 - (д) Каждое целое вида $8^n + 1$, где $n \leq 1$, является составным.
- Указание.** Учесть, что $2^n + 1 | 2^{3n} + 1$.
- (е) Каждое целое $n > 11$ может быть представлено как сумма двух составных чисел.

Указание. Если n — чётное ($n = 2k$), то $n - 6 = 2(k - 3)$; если n — нечётное, рассмотреть целое $n - 9$.

7. Найти все простые числа, которые делят 50!

8. Доказать, что $24 | p^2 - q^2$, если $p \geq q \geq 5$ и p, q — простые числа.

9. (а) Нерешенная проблема состоит в следующем. Существует ли бесконечное множество чисел вида $2^n + 1$, где $n > 1$. Найти несколько простых чисел этого вида.

(б) Еще одна гипотеза: существует ли бесконечное множество простых чисел вида $n^2 + 1$? Найти несколько простых чисел этого вида? Например, $257 = 16^2 + 1$.

10. Доказать, что либо $p^2 - 1$, либо $p^2 + 1$ делится на 10, если p — нечётное простое, отличное от 5.

Указание. Число p имеет одну из форм: $5k + 1, 5k + 2, 5k + 3, 5k + 4$.

11. Другая нерешенная проблема: существует ли бесконечное множество простых чисел вида $2^n - 1$?

12. Найти несколько простых чисел этого вида.

13. Доказать, что если $p = 2^k - 1$ является простым числом, то k — нечётное, кроме $k = 2$.

Указание. Учесть, что $3 | 4^n - 1$ для всех $n \geq 1$.

14. Представить числа 1234, 10140, 36000 в виде произведения простых.

15. Рассмотрим множество S положительных целых чисел вида $3k+1$, т.е. $S = \{1, 4, 7, 10, 13, 16, \dots\}$. Будем говорить, что целое $a > 1$, принадлежащее к S , называется простым, если его нельзя представить произведением двух меньших чисел из S . Например, 10, 25 являются простыми, а числа $16 = 4 \cdot 4$ и $28 = 7 \cdot 4$ — нет.

(а) Доказать, что каждое число из S является либо простым, либо произведением простых.

(б) Привести пример, показывающий, что в S нет единственности для представления через произведение простых.

16. Существует гипотеза, что каждое чётное число может быть представлено разностью двух соседних простых чисел бесконечным числом способов. Например,

$$6 = 29 - 23 = 137 - 131 = 599 - 593 = 1019 - 1013 = \dots$$

Выразить число 10 подобным образом пятнадцатью способами.

17. Доказать, что положительное $a > 1$ является точным квадратом тогда и только тогда, когда в канонической форме числа a все показатели простых чисел являются чётными.

18. Говорят, что целое число свободно от квадратов, если оно не делится на квадрат целого, большего единицы. Доказать, что справедливы следующие утверждения:

(а) целое $n \geq 1$ является свободным от квадратов тогда и только тогда, когда оно представимо произведением разных простых;

(б) каждое целое $n > 1$ является произведением числа, свободного от квадратов, и числа, являющегося точным квадратом.

Указание. Если $n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$ — каноническая форма числа k , представим k_i в виде $k_i = 2q_i + r_i$, где $r_i = 0$ или 1.

19. Проверить, что каждое целое n можно представить в виде $n = 2^k m$, где $k \geq 0$, а m — нечётное целое.

20. Численные эксперименты делают правдоподобным предположение о том, что существует бесконечное множество простых чисел p , таких, что $p+50$ также простые. Приведите 15 таких простых.

3.3. Решето Эратосфена

Как установить для данного целого числа, является ли оно простым или составным? В последнем случае, как найти нетривиальный делитель? Наиболее очевидный подход состоит в последовательном делении данного числа на каждое из чисел, предшествующих ему. Если ни одно из них (кроме 1) не является делителем, то исходное число — простое. Хотя этот метод очень прост, его нельзя признать полезным с практической точки зрения.

Мы можем слегка сократить вычисления, если воспользуемся следующим свойством составных чисел. Если целое $a > 1$ составное, то его можно представить, как $a = bc$, где $1 < b < a$ и $1 < c < a$. Предполагая, что $b \leq c$, получим $b^2 \leq bc = a$ и, таким образом, $b \leq \sqrt{a}$. Так как $b > 1$, то, согласно теореме 3.2, b имеет по крайней мере один простой множитель p . Тогда $p \leq b \leq \sqrt{a}$. Более того, так как $p|b$ и $b|a$, то $p|a$. Отсюда вывод: составное число a всегда обладает простым делителем p , удовлетворяющим неравенству $p \leq \sqrt{a}$.

Таким образом, проверяя простоту данного числа $a > 1$, достаточно делить a на простые, не превосходящие числа \sqrt{a} . Рассмотрим целое $a = 509$. Так как $22 < \sqrt{509} < 23$, то мы должны рассмотреть простые числа 2, 3, 5, 11, 13, 17, 19. Деля 509 на каждое из них, находим, что ни один из них не является делителем чисел 509. Следовательно, 509 — простое.

Пример 7. Приведенная выше техника дает практический метод для нахождения канонической формы целого числа a . Пусть $a = 2093$. Так как $45 < \sqrt{2093} < 46$, достаточно проверить простые 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43. Убеждаемся, что первым из этого списка делит данное число 7. $2093 = 7 \cdot 299$. Применим тот же прием к числу 299. Имеем неравенство $17 < \sqrt{299} < 18$ и рассмотрим простые числа 2, 3, 5, 7, 11, 13, 17. Первым в этом списке числом, делящем число 299, является 13 и $299 = 13 \cdot 23$. Так как 23 — простое, то получим каноническое разложение: $2093 = 7 \cdot 13 \cdot 23$.

Эратосфен из Кирены (276-194 до н.э.) — греческий математик, чьи работы оставили значительный след в теории чисел. В то время как потомство помнит его главным образом как директора знаменитой библиотеки в Александрии, Эратосфен был одарен во всех ветвях знаний и получил имя Бета, т.к., по его словам, стоял по крайней мере на втором месте в каждой из областей. Возможно,

наиболее впечатляющее мастерство Эратосфен проявил при аккуратном вычислении траектории Земли с помощью евклидовой геометрии.

Мы уже убедились в том, что если $a > 1$ не делится на простое $p \leq \sqrt{a}$, то a является простым числом. Эратосфен использовал этот факт как основу искусной техники, называемой "Решето Эратосфена", для нахождения всех простых чисел, не превосходящих данного числа n . Метод состоит в следующем. Напишем числа от 2 до n в естественном порядке и затем удалим из этого списка все составные числа, вычеркивая числа, кратные $p, 2p, 3p, 4p, \dots$, где $p \leq \sqrt{n}$ и простое. Оставшиеся в этом списке числа, т.е. числа, не прошедшие сквозь "сито", являются простыми.

Найдем с помощью приведенного выше метода (решето Эратосфена) все простые числа, не превосходящие числа 100. Рассмотрим список всех чисел 2, 3, 4, ..., 100, поместив их в следующую таблицу.

2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19
21	22	23	24	25	26	27	28	29
31	32	33	34	35	36	37	38	39
41	42	43	44	45	46	47	48	49
51	52	53	54	55	56	57	58	59
61	62	63	64	65	66	67	68	69
71	72	73	74	75	76	77	78	79
81	82	83	84	85	86	87	88	89
91	92	93	94	95	96	97	98	99
100								

Учитывая, что 2 — простое, вычеркиваем все четные числа из этого списка, кроме самого числа 2. Первое из оставшихся чисел в этом списке есть число 3, являющееся простым. Сохраним его, но вычеркнем все числа, кратные ему. Наименьшее число после 3, которое не удалено, есть 5. Оно не делится ни на 2, ни на 3, иначе мы бы его вычеркнули. Следовательно, оно — простое. Оставляем число 5 и вычеркиваем все кратные ему. Первое из оставшихся, кроме 2, 3, 5, есть 7, которое является простым, т.к. оно не делится ни на 2, ни на 3, ни на 5. Остаётся вычеркнуть все числа, кратные 7, кроме самого числа 7. Заметим, что 7 — наибольшее из простых, которое не превышает $\sqrt{100}$. В результате в нашем списке остались числа 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83,

89, 97, т.е. все простые числа, не превышающие 100.

Очевидный вопрос, возникающий при знакомстве с простыми числами таков: "существует ли самое большое простое число?" Ответ был дан в удивительно простом доказательстве, приведенном Евклидом в книге IX его "Начал". Доказательство Евклида общепризнано образцом математической элегантности. Суть состоит в следующем. Если бы простые числа образовывали конечное множество, то можно было бы найти простое, не находящееся в нем, следовательно, число простых чисел бесконечно.

Теорема 3.4 (Евклид). Простые числа образуют бесконечное множество.

Доказательство. Доказательство Евклида — пример метода приведения к абсурду. Пусть $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \dots$ — простые числа, естественно упорядоченные. Предположим, что существует наибольшее из них, и обозначим его через p_n . Рассмотрим положительное целое число

$$P = p_1 p_2 \dots p_n + 1.$$

Так как $p > 1$, согласно теореме 3.2, p делится на некоторое простое p . Так как p_1, p_2, \dots, p_n образуют все простые числа, то P совпадает с одним из них. Следовательно, $p | p_1 p_2 \dots p_n$ и $p | P$ и, таким образом, $p | P - p_1 p_2 \dots p_n$, т.е. $p | 1$. Но единственным положительным делителем числа 1 является 1, и так как $p > 1$, это приводит к противоречию. Теорема доказана.

Интересно отметить, что обозначая число $p_1 p_2 \dots p_k + 1$, через P_k , первые пять чисел этой последовательности:

$$P_1 = 2 + 1 = 3,$$

$$P_2 = 2 \cdot 3 + 1 = 7,$$

$$P_3 = 2 \cdot 3 \cdot 5 + 1 = 31,$$

$$P_4 = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211,$$

$$P_5 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311,$$

являются простыми числами. Однако $P_6 = 59 \cdot 509$, $P_7 = 19 \cdot 97 \cdot 277$, $P_8 = 347 \cdot 27953$ — составные числа. До сих пор неизвестно, существует ли бесконечное множество значений k , для которых P_k — простое?

Пусть p_n — n -ое простое число, при естественном упорядочении всех простых чисел. Доказательство теоремы 3.4 показывает, что

$$p_{n+1} \leq p_1 p_2 \dots p_n + 1 < p_n^n + 1.$$

Например, если $n = 3$, имеем

$$7 = p_4 < p_3^2 + 1 = 5^2 + 1 = 26,$$

что показывает "грубость" этой оценки. Приведем более точную оценку роста p_n ?

Теорема 3.5. Если p_n — простое число, то $p_n \leq 2^{2^n - 1}$.

Доказательство. Проведем индукцию по n . Ясно, что при $n = 1$ утверждение теоремы справедливо. Предположим, что утверждение верно для всех номеров последовательных простых чисел, меньших, чем n . Тогда

$$p_{n+1} \leq p_1 p_2 \dots p_n + 1 \leq 2 \cdot 2^2 \cdot \dots \cdot 2^{2^{n-1}} + 1 = 2^{1+2+2^2+\dots+2^{n-1}} + 1.$$

Если применим равенство

$$1 + 2 + 2^2 + \dots + 2^{n-1} = 2^n - 1,$$

то из последнего неравенства следует, что

$$p_{n+1} \leq 2^{2^n - 1} + 1.$$

Но $1 \leq 2^{2^n - 1}$, $n = 1, 2, \dots$, следовательно,

$$p_{n+1} \leq 2^{2^n - 1} + 2^{2^n - 1} = 2 \cdot 2^{2^n - 1} = 2^{2^n}$$

и теорема доказана.

Следствие 11. Для $n \geq 1$ существует по крайней мере $n + 1$ простых чисел, меньших, чем 2^{2^n} .

Доказательство. Из предыдущей теоремы видно, что каждое из чисел p_1, p_2, \dots, p_{n+1} меньше, чем 2^{2^n} .

Методы, развивающие идею решета Эратосфена, занимают весьма почетное место в современной теории чисел. Основная задача при этом — оценить количество простых чисел с различными свойствами. Наиболее известные — решето Бруна (1920 г.), решето Сельберга (1947 г.) и "большое решето Линника" (1941 г.). Одной из наиболее интригующих задач теории чисел до последнего времени была

задача распознавания простоты числа по его записи в десятичной системе счисления. Если число N записано с использованием n десятичных цифр (т.е. длина его записи равна n), то метод перебора делителей, меньших, чем корень квадратный из N , требует экспоненциального количества операций и потому непригоден для практических задач, когда длина n более сотни знаков. Однако в 1980 году Адлеман, Померанс и Рамели нашли алгоритм существенно меньшей трудоёмкости, основанный на глубоких теоретико - числовых соображениях. Этот алгоритм позволил эффективно решать задачу определения простоты числа для чисел, имеющих 100 — 200 знаков в своей записи. Однако проблема существования алгоритма с полиномиальной от числа n сложностью долгое время оставалась открытой. Лишь в 2002 году индийские математики Агравал, Кайал и Саксена нашли алгоритм, требующий порядка n^{12} арифметических операций для решения этой задачи. Задача же разложения натурального числа на множители и в настоящий момент представляется весьма трудной.

3.4. Задачи

1. Выяснить, является ли число 701 простым, деля его на все простые, не превышающие $\sqrt{701}$.
2. Используя решето Эратосфена, найти все простые p , такие, что $100 < p < 200$.
3. Известно, что $p \neq n$ для всех простых $p \leq \sqrt[3]{n}$. Доказать, что либо n — простое, либо оно является произведением двух простых.

Указание. Предположив противное, установить, что n содержит по крайней мере три простых сомножителя.

4. Выяснить, справедливы или нет следующие утверждения:

- (a) \sqrt{p} — иррациональное для любого простого p ;
- (b) Если $a > 0$ и $\sqrt[3]{a}$ — рациональное, то $\sqrt[3]{a}$ — целое;
- (c) Для $n \geq 2$ число $\sqrt[3]{n}$ — иррационально.

Указание. Использовать неравенство $2^n > n$.

- (d) Доказать, что если $n > 2$, то существует простое число p , удовлетворяющее неравенству $n < p < n!$

Указание. Если $n! - 1$ — не простое, то существует у этого числа простой делитель p . С другой стороны, неравенство $p \leq n$ влечет $p|n!$ (противоречие).

5. Если p_n — простое число с номером n при естественном упорядочении множества простых чисел, показать, что ни одно из чисел $P_n = p_1 p_2 \dots p_n + 1$ не является точным квадратом.

Указание. Каждое p_n имеет вид $4k + 3$.

3.5. Гипотеза Гольдбаха

Хотя известно, что простые числа образуют бесконечное множество, распределение их среди натуральных чисел весьма загадочно. Разность между соседними простыми числами может быть мала, как в случае пар 11 и 13, 17 и 19, или, например, 1000000000061 и 1000000000063. В то же самое время существуют сколь угодно большие интервалы последовательности натуральных чисел, в которых нет ни одного простого числа.

До сих пор неизвестно, существует ли бесконечно много *простых близнецов*, т.е. пар соседних нечетных чисел p и $p + 2$, каждое из которых есть простое число. Численные эксперименты позволяют предположить, что ответ — положительный.

Докажем теперь один факт, упомянутый выше. Для данного натурального n существует n последовательных натуральных чисел, каждое из которых — составное. Для доказательства рассмотрим числа

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

Ясно, что эти натуральные числа отличаются на единицу, т.е. они образуют n последовательных натуральных чисел. С другой стороны, каждое из них является составным числом, так как $(n+1)! + 2$ делится на 2, $(n+1)! + 3$ делится на 3 и т.д.

Например, для $n = 4$ имеем

$$5! + 2 = 122 = 2 \cdot 61,$$

$$5! + 3 = 123 = 3 \cdot 41,$$

$$5! + 4 = 124 = 4 \cdot 31,$$

$$5! + 5 = 125 = 5 \cdot 25.$$

Конечно, можно найти и другую четверку последовательных натуральных чисел 24, 25, 26, 27 или 32, 33, 34, 35.

Перейдем к другой нерешенной проблеме, касающейся простых чисел, — гипотезе Гольдбаха. В письме к Эйлеру (1742) Кристиан Гольдбах рискнул предположить, что каждое чётное целое число есть сумма двух чисел, каждое из которых простое или единица. Несколько более общая формулировка выглядит так: каждое чётное число, большее, чем 4, может быть представлено суммой двух нечётных простых. Гипотеза подтверждается следующими примерами:

$$\begin{aligned}2 &= 1 + 1, \\4 &= 2 + 2, \\6 &= 3 + 3 = 1 + 5, \\8 &= 3 + 5 = 1 + 7, \\10 &= 3 + 7 = 5 + 5, \\12 &= 5 + 7 = 1 + 11, \\14 &= 3 + 11 = 7 + 7 = 1 + 13, \\16 &= 3 + 13 = 5 + 11, \\18 &= 5 + 13 = 7 + 11 = 1 + 17, \\20 &= 3 + 17 = 7 + 13 = 1 + 19, \\22 &= 3 + 19 = 5 + 17 = 11 + 11, \\24 &= 5 + 19 = 7 + 17 = 11 + 13 = 1 + 23, \\26 &= 3 + 23 = 7 + 19 = 13 + 13, \\28 &= 5 + 23 = 11 + 17, \\30 &= 7 + 23 = 11 + 19 = 13 + 17 = 1 + 29.\end{aligned}$$

По-видимому, Эйлер никогда не пытался доказывать эту гипотезу, но в ответном письме Гольдбаху высказал собственную гипотезу: каждое чётное целое (≥ 6) вида $4n+2$ есть сумма двух чисел, каждое из которых или простое вида $4n+1$, или 1.

Большое количество численных экспериментов подтверждает гипотезу Гольдбаха (она проверена для всех четных до 100000 включительно), но общего доказательства её или контрпримера до сих пор нет. Современный подход к гипотезе Гольдбаха демонстрирует знаменитый результат И.М. Виноградова: почти все чётные числа являются суммой двух простых. Техническое значение термина "по-

что все¹¹ состоит в том, что если $A(n)$ обозначает число целых $m \leq n$, которые не представимы суммой двух простых, то

$$\lim_{n \rightarrow \infty} \frac{A(n)}{n} = 0.$$

Заметим, что если гипотеза Гольдбаха верна, то каждое нечётное число, большее, чем 7, должно быть суммой трех нечётных простых. В самом деле, если n — нечётное и $n > 7$, то $n - 3$ чётное и $n - 3 > 4$. Если $n - 3$ представимо суммой двух нечётных простых, то n есть сумма трех нечётных простых. В 1937 году И.М. Виноградов доказал, что это действительно так для достаточно большого нечётного целого, скажем большего, чем N . Таким образом, достаточно ответить на вопрос для каждого нечётного n , $9 \leq n < N$. К сожалению, N столь велико, что это превышает возможности современных компьютеров.

Из результата Виноградова следует, что каждое достаточно большое чётное целое есть сумма не более четырех нечётных простых.

Теперь мы немного отклонимся от этой темы и заметим, что согласно алгоритму деления, каждое натуральное число можно представить одним из способов:

$$4n, 4n + 1, 4n + 2, 4n + 3$$

для некоторого $n \geq 0$. Ясно, что $4n$ и $4n + 2 = 2(2n + 1)$ — оба чётные. Таким образом, все нечетные целые попадают в две прогрессии: одна содержит целые вида $4n + 1$, т.е.

$$1, 5, 9, 13, 17, 21, \dots,$$

а другая содержит целые вида $4n + 3$, т.е.

$$3, 7, 11, 15, 19, 23, \dots$$

Ясно, что каждая из этих прогрессий содержит простые числа и возникает вопрос, содержит ли каждая из этих прогрессий бесконечное число простых. Это дает приятную возможность для повторной демонстрации метода Евклида доказательства бесконечности простых чисел. Небольшая модификация его аргументов обнаруживает, что существует бесконечное число простых вида $4n + 3$. Доказательству этого предположим лемму.

Лемма 2. Произведение двух или большего числа целых вида $4n + 1$ есть число такого же вида.

Доказательство. Достаточно рассмотреть произведение двух чисел. Пусть $k = 4n + 1$ и $k' = 4m + 1$. Умножая их, получим

$$kk' = (4n + 1)(4m + 1) = 16nm + 4n + 4m + 1 = 4(4nm + n + m) + 1.$$

Теорема 3.6. Существует бесконечное число простых среди чисел вида $4n + 3$.

Доказательство. В ожидании противоречия предположим, что числа вида $4n + 3$ образуют конечное множество, которое мы обозначим q_1, q_2, \dots, q_s . Рассмотрим натуральное число

$$N = 4q_1q_2\dots q_s - 1 = 4(q_1q_2\dots q_s - 1) + 3,$$

и пусть $N = r_1r_2\dots r_i$ его каноническое разложение с помощью простых. Так как N — нечётное, то $r_k \neq 2$ для всех k . Поэтому $r_k = 4n + 1$ или $r_k = 4n + 3$. В силу леммы произведение любого числа сомножителей вида $4n + 1$ есть число такого же вида. Так как N имеет вид $4n + 3$, то отсюда ясно, что N должно иметь хотя бы один множитель $r_i = 4n + 3$. Но, с другой стороны, r_i не находится в списке q_1, q_2, \dots, q_s , ибо это привело бы к противоречию: $r_i | 1$. Остается одна возможность — существует бесконечное множество простых вида $4n + 3$.

Остается вопрос, касающийся прогрессии, состоящей из чисел вида $4n + 1$. Ответ здесь также положителен, но доказательство требует специальной техники. Оба эти результата являются специальными случаями замечательной теоремы Дирихле, доказанной в 1837. Доказательства при этом слишком громоздкое, чтобы его здесь приводить. Поэтому ограничимся лишь формулировкой утверждения.

Теорема 3.7 (Дирихле). Если a и b — взаимно простые натуральные числа, то арифметическая прогрессия

$$a, a + b, a + 2b, a + 3b, \dots$$

содержит бесконечное число простых.

Не существует арифметической прогрессии $a, a + b, a + 2b, \dots$ состоящей только из простых чисел. Чтобы в этом убедиться, предположим, что $a + nb = p$, где p — простое. Если положить $n_k = n + kp$, где $k = 1, 2, 3, \dots$, то член с номером n_k данной прогрессии имеет вид:

$$a + n_kb = a + (n + kp)b = a + nb + kpb = p + kpb.$$

Так как каждое слагаемое справа делится на p , то $a + n_k b$ — составное. Таким образом, прогрессия должна содержать бесконечное множество составных чисел.

Имеется гипотеза, что существует арифметическая прогрессия конечной (но произвольной) длины, составленная из последовательных простых чисел. Примером таких прогрессий, состоящих из трех и четырех простых, являются 41, 47, 53 и 251, 257, 263, 269. Не так давно компьютерные исследования обнаружили прогрессии из пяти и шести последовательных простых. Их члены имеют общую разность 30 и они начинаются с простых чисел 9843019 и 121174811. В настоящее время неизвестна арифметическая прогрессия, состоящая из семи последовательных простых. Если ограничение, состоящее в отсутствии между соседними простыми числами прогрессии других простых чисел, устранить, то можно найти бесконечное множество арифметических прогрессий из семи членов, например,

$$7, 157, 307, 457, 607, 757, 907.$$

В целях полноты мы должны упомянуть другую знаменитую проблему, которая до сих пор не поддается никаким усилиям математиков. Веками математики пытались найти простую формулу, которая давала бы каждое простое число или хотя бы бесконечное подмножество простых и никакие другие. На первый взгляд это требование кажется довольно скромным: найти функцию $f(n)$ с областью определения \mathbb{N} и с областью значений — бесконечное подмножество множества всех простых. В средние века очень верили, что квадратичский полином

$$f(n) = n^2 + n + 41$$

допускает только простые значения. Следующая таблица показыва-

ет, что эта вера подкрепляется только для $n = 0, 1, 2, \dots, 39$.

n	$f(n)$	n	$f(n)$	n	$f(n)$
0	41	14	251	28	853
1	43	15	281	29	911
2	47	16	313	30	971
3	53	17	347	31	1033
4	61	18	383	32	1097
5	71	19	421	33	1163
6	81	20	461	34	1231
7	97	21	503	35	1301
8	113	22	547	36	1373
9	131	23	593	37	1447
10	151	24	641	38	1523
11	173	25	691	39	1601
12	197	26	743		
13	223	27	797		

Однако, $f(40) = 40 \cdot 41 + 41 = 41^2$, $f(41) = 41 \cdot 42 + 41 = 41 \cdot 43$.

Следующее значение $f(42) = 1744$ снова простое. До сих пор неизвестно, содержит ли область значений функции f бесконечно много простых.

Неудача, связанная с рассмотрением выше функций f неслучайна, т.к. легко доказать, что не существует полинома (отличного от константы), с целыми коэффициентами, который принимает только простые значения на \mathbb{N} . Предположим, что такой полином существует. Пусть

$$f(n) = a_k n^k + a_{k-1} n^{k-1} + \dots + a_2 n^2 + a_1 n + a_0,$$

где $a_i \in \mathbb{Z}$, $k = 0, 1, \dots, n$. По предположению для фиксированного значения $n = n_0$ число $p = f(n_0)$ — простое. Теперь для любого $t \in \mathbb{Z}$ рассмотрим выражение $f(n_0 + tp)$:

$$\begin{aligned} f(n_0 + tp) &= a_k (n_0 + tp)^k + \dots + a_1 (n_0 + tp) + a_0 = \\ &= (a_k n_0^k + \dots + a_1 n_0 + a_0) + pQ(t) = \\ &= f(n_0) + pQ(t) = \\ &= p + pQ(t) = p(1 + Q(t)), \end{aligned}$$

где $Q(t)$ — полином с целыми коэффициентами. Это показывает, что $f(n_0 + tp)$ — составное число, иначе было бы: $f(n_0 + tp) = \pm p$ или

0, что невозможно, так как f — полином степени k , отличный от константы.

Чуть более общее утверждение касается многочленов многих переменных. А именно множество значений многочлена $f(x_1, x_2, \dots, x_k)$ от k переменных с целыми коэффициентами в точках с целыми координатами не может состоять только из простых чисел. Тем не менее в 1976 году был найден многочлен степени 25 от 26 переменных (число букв английского алфавита), для которого множество всех положительных значений, принимаемых им в целых точках совпадает со множеством всех простых чисел.

Отметим, что в 1947 году Миллс (W.H. Mills) доказал, что существует положительное вещественное число r , такое, что выражение $f(n) = [r^{3^n}]$ является простым числом для $n = 1, 2, 3, \dots$ Это результат типа теоремы существования и ничего неизвестно о значении числа r . В 1951 году Нивен несколько уточнил эту теорему, доказав, что для любого $c > 8/3$ существует такое число r , что $f(n) = [r^n]$ всегда простое.

3.6. Задачи

1. Убедиться, что числа 1949 и 1951 — простые близнецы.
2. (a) Доказать, что, если к произведению любых простых близнецов добавить единицу, то получится точный квадрат.
(b) Доказать, что, если $p > 3$ и простое, то сумма простых близнецов p и $p + 2$ делится на 12.
3. Найти все пары простых p и q , для которых $p - q = 3$.
4. Сильвестр (1896) перефразировал гипотезу Гольдбаха: "Каждое чётное целое $2n$, большее чем 4, есть сумма двух простых. При этом одно — больше, чем $\frac{n}{2}$, а другое — меньше, чем $\frac{3n}{2}$." Проверить эту версию гипотезы Гольдбаха для всех чётных n , $6 < n < 76$.
5. В 1752 г. Гольдбах предложил Эйлеру следующую гипотезу: "Каждое нечётное целое можно представить в виде $p + a$, где p или простое, или 1, целое $a \geq 0$. Проверить, что число 5777 опровергает эту гипотезу.

6. Доказать, что гипотеза Гольдбаха (каждое чётное число, большее, чем 2, есть сумма двух простых) эквивалентна утверждению о том, что каждое целое, большее, чем 5, есть сумма трех простых.

Указание. Если $2n - 2 = p_1 + p_2$, то $2n = p_1 + p_2 + 2$, а $2n + 1 = p_1 + p_2 + 3$.

7. Гипотеза Лагранжа (1775) утверждает, что каждое нечётное целое, большее, чем 5, представимо суммой $p_1 + 2p_2$, где p_1, p_2 — простые. Проверить это для всех нечетных 7, 9, ..., 75.
8. Можно доказать, что для данного $n \in \mathbb{N}$ существует чётное число a , которое представимо суммой двух простых n разными способами. Убедиться, что числа 60, 78 и 84 можно представить суммой двух простых шестью, семью, и восемью способами соответственно.
9. (а) Для $n > 1$ показать, что целые $n, n + 2, n + 4$ не могут быть все простыми.
- (б) Три целых $p, p + 2, p + 6$, каждое из которых простое, называется *простым триплетом*. Найти пять простых триплетов.
10. Найти наименьшее n , для которого $f(n) = n^2 + n + 17$ — составное. Сделать то же самое для функций $g(n) = n^2 + 21n + 1$ и $h(n) = 3n^2 + 3n + 23$.
11. Следующий результат известен как постулат Бертрана (доказан П.Л. Чебышевым в 1850 г.). Для каждого натурального $n > 1$ существует по крайней мере одно простое p , для которого $n < p < 2n$. Использовать этот результат для доказательства неравенства $p_n < 2^n$, где p_n — n -ое простое число.

3.7. Знаменитая теорема о простых числах

Хотя последовательность простых чисел демонстрирует сильную нерегулярность, что касается деталей, она имеет тенденцию к определенной ясности в целом. Знаменитая теорема о простых числах позволяет нам предсказывать, по крайней мере асимптотически, сколько имеется простых чисел, что для данного n имеется

"примерно" $\frac{n}{\log n}$ простых чисел, не превышающих n .

Мерой распределения простых является функция $\pi(x)$, определяющая для $x \in \mathbb{R}$. При этом $\pi(x)$ есть число простых чисел, которые не превышают x , т.е. $\pi(x) = \sum_{p \leq x} 1$. В главе 3 мы доказали, что

$\lim_{x \rightarrow \infty} \pi(x) = +\infty$. С другой стороны, таблица простых чисел показывает, что они распределены с большими промежутками. На неформальном языке можно сказать, что почти все натуральные числа — составные.

Чтобы обосновать последнее утверждение, покажем, что $\lim_{x \rightarrow \infty} \frac{\pi(x)}{x} = 0$. Мы должны доказать, что если $\varepsilon > 0$, то существует натуральное число N , такое, что $\frac{\pi(x)}{x} < \varepsilon$, когда $x \geq N$.

Пусть n — положительное целое. С помощью постулата Бертрана выберем простое p , для которого $2^{n-1} < p \leq 2^n$. Тогда $p \mid (2^n)!$. Но $p \nmid 2^{n-1}$, следовательно, биномиальный коэффициент $\binom{2^n}{2^{n-1}}$ делится на p . Это приводит к неравенствам

$$2^{2^n} \geq \binom{2^n}{2^{n-1}} \geq \prod_{2^{n-1} < p \leq 2^n} p \geq (2^{n-1})^{\pi(2^n) - \pi(2^{n-1})},$$

отсюда следует, что

$$2^{2^n} \geq 2^{(n-1)(\pi(2^n) - \pi(2^{n-1}))}.$$

Поэтому,

$$\pi(2^n) - \pi(2^{n-1}) \leq \frac{2^n}{n-1}. \quad (3.1)$$

Если мы положим $n = 2k, 2k-1, 2k-2, \dots, 3$ в (3.1) и сложим соответствующие неравенства, то получим

$$\pi(2^{2k}) - \pi(2^2) \leq \sum_{r=3}^{2k} \frac{2^r}{r-1}.$$

Так как, очевидно, что $\pi(2^2) < 2^2$, то из последнего неравенства заключаем, что справедливо неравенство

$$\pi(2^{2k}) < \sum_{r=2}^{2k} \frac{2^r}{r-1} = \sum_{r=2}^k \frac{2^r}{r-1} + \sum_{r=k+1}^{2k} \frac{2^r}{r-1}.$$

В последних двух суммах заменим знаменатели $r-1$ на 1 и k соответственно. Тогда получим неравенство

$$\pi(2^{2k}) < \sum_{r=2}^k 2^r + \sum_{r=k+1}^{2k} \frac{2^r}{r} < 2^{k+1} + \frac{2^{2k+1}}{k}.$$

или

$$\frac{\pi(2^{2k})}{4} < \frac{4}{k}. \quad (3.2)$$

Ясно, что для любого вещественного $x \geq 2$ существует единственное натуральное k , для которого $2^{2k-2} < x \leq 2^{2k}$. Поэтому из (3.2) следует, что справедливо неравенство

$$\frac{\pi(x)}{x} \leq \frac{2^{2k}}{x} < \frac{2^{2k}}{2^{2k-2}} = 4 \left(\frac{\pi(2^{2k})}{2^{2k}} \right) < \frac{16}{k}.$$

Если мы теперь возьмем $x \geq N = 2^{2(\lfloor \frac{16}{\varepsilon} \rfloor + 1)}$, то $k \geq \lfloor \frac{16}{\varepsilon} \rfloor + 1$. Следовательно,

$$\frac{\pi(x)}{x} < \frac{16}{\lfloor \frac{16}{\varepsilon} \rfloor + 1} < \varepsilon,$$

что и требовалось доказать.

В 1740 году Эйлер ввел в математический анализ дзета-функцию

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = 1^{-s} + 2^{-s} + 3^{-s} + \dots,$$

функцию, от свойств которой в конечном счете зависит доказательство теоремы о простых числах. При этом основной результат Эйлера, касающийся дзета-функции, состоит в формуле, представляющей $\zeta(s)$ в виде сходящегося бесконечного произведения:

$$\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}}, \quad (s > 1)$$

где p пробегает все простые числа.

Это представление для $\zeta(s)$ следует из разложения каждого сомножителя в ряд:

$$\frac{1}{1 - \frac{1}{p^s}} = 1 + \frac{1}{p^s} + \left(\frac{1}{p^s}\right)^2 + \left(\frac{1}{p^s}\right)^3 + \dots + \dots$$

и наблюдения, что их произведение есть сумма членов вида

$$\frac{1}{(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r})^s},$$

p_1, \dots, p_r — различные простые. Так как каждое натуральное n единственным образом представимо произведением степеней простых чисел, то каждое слагаемое $\frac{1}{n^s}$ появляется один и только один раз в этой сумме, т.е. в $\sum_{n=1}^{\infty} \frac{1}{n^s}$.

Лежандр в его книге *Essai sur la Théorie des Nombres* (1798) высказал предположение, что $\pi(x)$ приближенно равна функции

$$\frac{x}{\log x - 1,08366}.$$

Гаусс предположил, что $\pi(x)$ имеет такую же скорость роста, что и функция $\frac{x}{\log x}$, а

$$Li(x) = \int_2^x \frac{du}{\log u}$$

даст лучшее приближение для $\pi(x)$.

Заметим, что здесь и всюду в этом параграфе \log означает логарифм по основанию e (натуральный логарифм).

Интересно сравнить эти предположения с данными таблицы:

x	$\pi(x)$	$\frac{x}{\log x - 1,08366}$	$\frac{x}{\log x}$	$Li(x)$
1000	168	172	145	178
10000	1229	1231	1086	1246
100000	9592	9588	8686	9630
1000000	78498	78534	72382	78628
10000000	664579	665138	620420	664918
100000000	5761455	5769341	5428681	5762209

Первый значительный прогресс в сравнении $\pi(x)$ с $\frac{x}{\log x}$ был достигнут П.Л. Чебышевым. В 1850 г. он доказал, что существуют положительные константы a и b , $a < 1 < b$, такие, что

$$a \left(\frac{x}{\log x} \right) < \pi(x) < b \left(\frac{x}{\log x} \right)$$

для достаточно больших x . Далее Чебышев доказал, что если функция $\pi(x)/(x/\log x)$ имеет предел при x , стремящемся к бесконечности, то он равен 1. Этот замечательный результат был омрачен

неудачей (отсутствие доказательства существования предела). Пробел был устранен 45 лет спустя.

Мы должны заметить, что из результата Чебышева следует расходимость ряда $\sum_p \frac{1}{p}$, где p пробегает все множество простых чисел.

В самом деле, пусть p_n — n -ое простое число, т.е. $\pi(p_n) = n$. Так как

$$\pi(x) > a \left(\frac{x}{\log x} \right)$$

для достаточно больших x , то отсюда следует справедливость неравенства

$$n = \pi(p_n) > a \frac{p_n}{\log p_n} > \sqrt{p_n}$$

для достаточно больших n .

Но $n^2 > p_n$ и $\log p_n < 2 \log n$. Таким образом,

$$ap_n < n \log p_n < 2n \log n$$

для достаточно больших n . Следовательно, ряд $\sum_{k=1}^{\infty} \frac{1}{p_n}$ расходится,

так как известно, что ряд $\sum_{n=2}^{\infty} \frac{1}{n \log n}$ расходится.

Радикально новые идеи, давшие ключ к доказательству знаменитой теоремы о простых числах, содержатся в эпохальной работе Римана "Über die Anbahnung der Primzahlen unter einer gegebenen Grösse" (1859). В то время как Эйлер ограничивался вещественными значениями для s в функции $\zeta(s)$, Риман установил связь между распределением простых и поведением $\zeta(s)$, как функции комплексной переменной $s = a + bi$. Он установил ряд свойств дзета-функции вместе с замечательным тождеством (явная формула Римана), связывающим $\pi(x)$ с нулями функции $\zeta(s)$, $s \in \mathbb{C}$.

В упомянутой выше работе Римана высказан ряд гипотез, касающихся распределения нулей дзета-функции. Наиболее известная из них — *гипотеза Римана*, которая утверждает, что все не вещественные нули функции $\zeta(s)$ являются некоторыми точками вида $\frac{1}{2} + bi$ комплексной плоскости, т.е. они лежат на "критической прямой" $\Re(s) = \frac{1}{2}$. Эта знаменитая гипотеза до сих пор не доказана и не опровергнута.

Исследования Римана были использованы Адамаром и Валле Пуссен, которые в 1896 году независимо и одновременно доказали, что

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x / \log x} = 1$$

Этот результат стал известен как знаменитая теорема о простых числах. Валле Пуссен пошел дальше в своих исследованиях. Он показал, что для достаточно больших значений x функция $\pi(x)$ более точно приближается с помощью $Li(x)$, чем с помощью функции $\frac{x}{\log x - A}$, как бы ни выбирать A .

До недавнего времени преобладало мнение, что теорема о простых числах не может быть доказана без использования свойств дзета-функции и без сведения к теории функций комплексного переменного. Тем не менее в 1949 г. норвежский математик Селберг нашел чисто арифметическое доказательство. Его работа Alte Selberg "On elementary Proof of the Prime Number Theorem" является "элементарной" в том смысле, что не использует методов современного анализа. Селберг был удостоен Филдсовской медали в 1950 году на Международном математическом конгрессе за работу в этой области.

3.8. Задачи

1. Доказать, что для достаточно большого числа N существует по меньшей мере 3 простых числа, заключённых в промежутке между N и $2N$. Можно ли уточнить величину N ?
2. Используя предыдущую задачу, доказать, что любое достаточно большое натуральное число представимо в виде суммы различных простых чисел.
3. Найти количество простых чисел в промежутке от 1 до 1250.
4. Найти каноническое разложение числа $n!$ в произведение простых чисел. Если простое число $p < n$, то какова наибольшая степень числа p , делящая $n!$?

Список литературы

- [1] *Айерлэнд К., Роузен М.* Классическое введение в современную теорию чисел, М.: Мир, 1987.
- [2] *Боревич З.И., Шафаревич И.Р.* Теория чисел. М.: Наука, 1964.
- [3] *Виноградов И.М.* Основы теории чисел. М.: Наука, 1965
- [4] *Дэвенпорт Г.* Высшая арифметика (Введение в теорию чисел). М.: Наука, 1965.
- [5] *Делоне Б.Н.* Петербургская школа теории чисел. М.: Изд.-во АН СССР, 1947.
- [6] *Хинчин А.Я.* Великая теорема Ферма. М.: Гостехиздат, 1934.
- [7] *Хинчин А.Я.* Три жемчужины теории чисел. М.: Гостехиздат, 1948.

Оглавление

Глава 1	Некоторые предварительные соображения	3
1.1.	Математическая индукция	3
1.2.	Задачи	8
1.3.	Биномиальная теорема	9
1.4.	Задачи	12
1.5.	Ранняя теория чисел	13
1.6.	Задачи	16
Глава 2	Теория делимости целых чисел	19
2.1.	Алгоритм деления	19
2.2.	Задачи	22
2.3.	Наибольший общий делитель	23
2.4.	Задачи	28
2.5.	Алгоритм Евклида	30
2.6.	Задачи	34
2.7.	Диофантово уравнение $ax + by = c$	36
2.8.	Алгоритм Берлекэмпса	40
2.9.	Задачи	42
2.10.	Дополнение	43
2.11.	Задачи	45
Глава 3	Простые числа и их распределение	47
3.1.	Основная теорема арифметики	47
3.2.	Задачи	52
3.3.	Решето Эратосфена	55
3.4.	Задачи	59
3.5.	Гипотеза Гольдбаха	60
3.6.	Задачи	66
3.7.	Знаменитая теорема о простых числах	67
3.8.	Задачи	72
	Список литературы	73

Учебное издание

Казарин Лев Сергеевич
Шалашов Виктор Константинович

Теория чисел
Часть 1

Учебное пособие

Редактор, корректор Аладьева А. А.
Компьютерная вёрстка Янишевский В. В.

Подписано в печать 25.11.03. Формат 60 x 84/16. Бумага
тип. Печать офсетная. Усл. печ. л. 4,65. Уч.-изд.л. 5,0.
Тираж 100 экз. Заказ. 416

Оригинал-макет подготовлен
в редакционно-издательском отделе ЯрГУ,
150000 Ярославль, ул. Советская, 14

Отпечатано
ООО «Ремдер» ЛР ИД № 06151 от 26.10.2001.
г. Ярославль, пр. Октября, 94, оф. 37.
тел. (0852) 73-35-03.