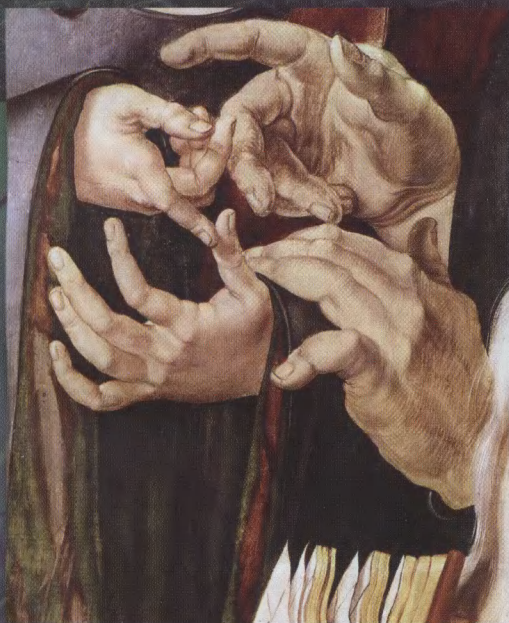


ВЫПУСК

# 109

## Библиотечка КВАНТ



# Арифметика-2

Б Ю Р О



КВАНТУМ



БИБЛИОТЕЧКА  
**КВАНТ**  
ВЫПУСК

**109**

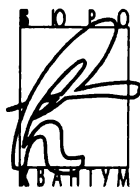
Приложение к журналу  
«Квант» № 5/2008

**А.В.Спивак**

# Арифметика-2



0010635



Москва  
2008

УДК 511.3(082)

ББК 22.130

С72



Серия  
«Библиотечка «Квант»  
основана в 1980 г.

РЕДАКЦИОННАЯ КОЛЛЕГИЯ:

Б.М.Болотовский, А.А.Варламов, В.Л.Гинзбург,  
Г.С.Голицын, Ю.В.Гуляев, М.И.Каганов, С.С.Кротов,  
С.П.Новиков, Ю.А.Осипьян (председатель),  
В.В.Произволов, Н.Х.Розов, А.Л.Стасенко, В.Г.Сурдин,  
В.М.Тихомиров, А.Р.Хохлов,  
А.И.Черноуцан (ученый секретарь)

**С72 Спивак А.В.**

Арифметика-2. – М.: Бюро Квантум, 2008. – 160 с. (Библиотечка «Квант». Вып. 109. Приложение к журналу «Квант» № 5/2008.)

ISBN 5-85843-067-8

Книга посвящена таким вопросам элементарной теории чисел, как суммы квадратов и уравнения Пелля. Эти темы рассмотрены всесторонне и подробно. В обоих случаях изложение развивается от простых соображений, доступных семикласснику, до довольно сложных и неожиданных фактов. В книге множество задач и примеров.

Может служить учебным пособием для математических классов и кружков. Адресована школьникам 7–11 классов, учителям, а также всем любителям математики.

ББК 22.130

ISBN 978-5-85843-080-3

© Бюро Квантум, 2008

## ОГЛАВЛЕНИЕ

---

Предисловие	4
РАЗЛОЖЕНИЕ НА МНОЖИТЕЛИ	5
Решето Эратосфена	5
Алгоритм Ферма	6
Алгоритм Дрэма	7
НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ	10
СУММЫ КВАДРАТОВ	12
Часть I. Первые наблюдения	12
Часть II. Критерий Жирара	21
Часть III. Комплексные числа	37
Часть IV. Целые гауссовы числа	42
Часть V. Количество представлений	48
Часть VI. Суммы четырех квадратов	52
УРАВНЕНИЯ ПЕЛЛЯ	57
Часть I. Примеры	57
Часть II. Структура решений	74
Часть III. Поиск нетривиального решения	91
Часть IV. Уравнение $C_x^{y-1} = C_{x-1}^y$	100
ИЗБРАННЫЕ ЗАДАЧИ	105
ЛЕОНАРД ЭЙЛЕР (1707–1783)	107
КАРЛ ФРИДРИХ ГАУСС (1777–1855)	112
Решения	116

## ПРЕДИСЛОВИЕ

---

В первой части «Арифметики» речь шла об алгоритме Евклида, основной теореме арифметики, рядах Фарея, периодических дробях, малой теореме Ферма, числах Фибоначчи, цепных дробях и квадратичном законе взаимности.

Основное содержание второй части — всестороннее обсуждение сумм квадратов и уравнений Пелля. В обоих случаях мы начинаем с простых соображений, доступных семикласснику, а заканчиваем довольно трудными — даже изысканными — сведениями. Подробно изложены классические рассуждения, в частности, метод бесконечного спуска, которым очень гордился Пьер Ферма.

При написании этой книги произошли два чуда. На клетчатой бумаге, абсолютно наглядно, мне удалось изобразить доказательство теоремы Ферма-Эйлера (см. раздел «Крылатые квадраты» статьи «Суммы квадратов»).

И — когда рукопись уже была отдана в набор — я прочитал статью австралийца Вайлдбергера, которая разительно сокращает и проясняет классическое изложение теории уравнений Пелля. Я успел внести соответствующие изменения, хотя и не все: будь моя воля, в свете новых знаний изменил бы и статью «Цепные дроби» первой части «Арифметики». Но внести поправку в изданную в прошлом году книжку не в моих силах.

Обе части «Арифметики» рассчитаны на вдумчивое неоднократное чтение и могут служить основой для факультативных курсов по математике. Каждый раз вы будете продвигаться дальше и глубже, осваиваясь с новыми идеями. Упражнений очень много; скорее всего, при первом чтении удастся справиться лишь с небольшой их долей.

Книга составлена из статей журнала «Квант», энциклопедии «Числа и фигуры» издательства «Росмэн» и нескольких новых статей. Авторы статей «Суммы квадратов» и «Уравнения Пелля» — В. Сендеров и А. Спивак; остальных статей — А. Спивак. Многие упражнения заимствованы из «Задачника «Кванта»». По традиции, номера таких задач отмечены буквой М.

*То, что с трудом великим измыслили знатоки, раскрывается другими, еще более великими знатоками как призрачное.*

А.И. Солженицын

Простейший способ разложить натуральное число на простые множители – испытать, делится ли оно на 2, на 3, на 5 и так далее, используя ряд простых чисел. Поскольку для всякого собственного (отличного от 1 и от  $n$ ) делителя  $p$  числа  $n$  частное  $n/p$  тоже является собственным делителем, то достаточно проверить только простые числа  $p$ , удовлетворяющие неравенству  $p \leq \frac{n}{p}$ , т.е. неравенству  $p^2 \leq n$ . Это весьма трудоемкий процесс, к тому же требующий предварительного знания ряда простых чисел.

В докомпьютерные времена была составлена таблица для разложения чисел, в которой для каждого числа, меньшего 10000000, был указан его наименьший простой делитель. Сейчас она потеряла практическое значение, поскольку компьютерные программы – например, программа Mathematica – довольно быстро выполняют разложение на множители 55-значных (и даже несколько больших!) чисел. Разумеется, они используют не полный перебор, а малую теорему Ферма и другие, гораздо более сложные идеи.

Тем не менее, полезно не только уметь использовать компьютерные программы, но и понимать хотя бы самые несложные методы, которые можно использовать для поиска простых чисел и для разложения чисел на множители.

### Решето Эратосфена

Пожалуй, самый известный и естественный алгоритм – решето Эратосфена. Начинаем с выписывания ряда натуральных чисел от 2 до некоторого натурального  $n$  (чем больше  $n$ , тем больше простых чисел, но и вычислений придется выполнить больше).

Число 2 – наименьшее простое, обведем его в кружок; все большие двух четные числа составные, поэтому их вычеркиваем

② ~~3~~, ~~4~~, ~~5~~, ~~6~~, ~~7~~, ~~8~~, ~~9~~, ~~10~~, 11, ~~12~~, 13, ~~14~~, 15, ~~16~~, 17, ~~18~~, 19, ~~20~~, 21, ~~22~~, 23, ~~24~~, 25,  
~~26~~, 27, ~~28~~, 29, ~~30~~, 31, ~~32~~, 33, ~~34~~, 35, ~~36~~, 37, ~~38~~, 39, ~~40~~, 41, ~~42~~, 43, ~~44~~, 45, ~~46~~,  
 47, ~~48~~, 49, ~~50~~, 51, ~~52~~, 53, ~~54~~, 55, ~~56~~, 57, ~~58~~, 59, ~~60~~, 61, ~~62~~, 63, ~~64~~, 65, ~~66~~, 67

Рис. 1

(рис.1). Следующий шаг построения решета Эратосфена – обведение в кружок наименьшего невычеркнутого и не обведенного числа 3 и вычеркивание чисел 6, 9, 12, 15, ... (рис. 2).

②③ ~~4~~, ~~5~~, ~~6~~, ~~7~~, ~~8~~, ~~9~~, ~~10~~, 11, ~~12~~, 13, ~~14~~, ~~15~~, ~~16~~, 17, ~~18~~, 19, 20, ~~21~~, ~~22~~, 23, ~~24~~, 25,  
~~26~~, ~~27~~, 28, 29, ~~30~~, 31, ~~32~~, ~~33~~, ~~34~~, 35, ~~36~~, 37, ~~38~~, ~~39~~, ~~40~~, 41, ~~42~~, 43, ~~44~~, ~~45~~, ~~46~~,  
 47, ~~48~~, 49, ~~50~~, ~~51~~, ~~52~~, 53, ~~54~~, 55, ~~56~~, ~~57~~, 58, 59, ~~60~~, 61, ~~62~~, ~~63~~, ~~64~~, 65, ~~66~~, 67

Рис. 2

Заметьте: первое вычеркиваемое при этом и ранее невычеркнутое число –  $9 = 3^2$ . Третий шаг – обведение в кружок числа 5 и вычеркивание чисел 10, 15, 20, 25, ... (наименьшее впервые вычеркиваемое число –  $25 = 5^2$ ); четвертый (и последний для  $n = 100$ ) шаг – вычеркивание чисел 14, 21, 28, 35, ... (разумеется, наименьшее вычеркиваемое ранее невычеркнутое число –  $49 = 7^2$ ). Как только очередное обводимое в кружок простое число удовлетворит неравенству  $p^2 > n$  (например,  $11^2 > 100$ ), работу следует остановить; обведенные в кружок числа – как и числа, оставшиеся невычеркнутыми, – простые.

## Алгоритм Ферма

Пусть  $n$  – нечетное натуральное число,  $n > 1$ ,  $m$  – наименьшее натуральное число, удовлетворяющее неравенству  $m^2 > n$ . Рассмотрим разности

$$m^2 - n, \quad (m+1)^2 - n, \quad (m+2)^2 - n, \quad (m+3)^2 - n, \dots$$

Если какое-то из этих чисел является квадратом, получаем уравнение вида  $x^2 - n = y^2$ , откуда

$$n = x^2 - y^2 = (x - y)(x + y).$$

(Вычисление чисел  $m^2 - n$ ,  $(m+1)^2 - n$ ,  $(m+2)^2 - n$  облегчается тем, что их последовательные разности возрастают с постоянной скоростью: второе больше первого на  $2m+1$ , третье больше второго на  $2m+3$ , четвертое больше третьего на  $2m+5$ , и так далее.)

Метод Ферма удобен, если число  $n$  разлагается на два множителя почти одинаковой величины, ибо тогда  $y$  невелико. Если  $n$  простое, вычисления продолжатся до тех пор, пока не дойдем до системы  $x + y = n$  и  $x - y = 1$ .

В качестве примера рассмотрим  $n = 9271$ . Оно лежит между  $96^2$  и  $97^2$ . Следовательно,  $m = 97$  и  $97^2 - 9271 = 138$ . Следующие разности получаются прибавлением чисел  $2m + 1$ ,  $2m + 3$ , и так далее. Это дает ряд чисел  $138, 333, 530, 729 = 27^2$ . Следовательно,

$$9271 = 100^2 - 27^2 = 127 \cdot 73.$$

### Упражнения

1. Методом Ферма разложите на множители число а) 77; б) 8091; в) 13221.

2 (М437). Нечетное число, являющееся произведением  $n$  различных простых чисел, представимо в виде разности квадратов двух натуральных чисел ровно  $2^n - 1$  способами: например, число 5 13 представимо двумя способами:  $65 = 9^2 - 4^2 = 33^2 - 32^2$ . Докажите это.

### Алгоритм Дрэма

Алгоритм, предложенный капитаном военно-морских сил США Дрэмом, как и алгоритм Ферма, на практике не используют. Но он весьма остроумен и абсолютно элементарен. Поясним действие этого алгоритма при  $n = 4511$ .

Первый шаг – деление на 3:

$$4511 = 3 \cdot 1503 + 2;$$

вычитание удвоенного неполного частного из исходного числа:

$$4511 - 2 \cdot 1503 = 1505;$$

прибавление остатка:

$$1505 + 2 = 1507.$$

Второй шаг – деление полученного числа на 5:

$$1507 = 5 \cdot 301 + 2;$$

вычитание удвоенного неполного частного из числа, полученного на предыдущем шаге при помощи вычитания:

$$1505 - 2 \cdot 301 = 903;$$

прибавление остатка:

$$903 + 2 = 905.$$



Далее действуем аналогичным образом:

$$\begin{aligned}905 &= 7 \cdot 129 + 2, & 903 - 2 \cdot 129 &= 645, & 645 + 2 &= 647; \\647 &= 9 \cdot 71 + 8, & 645 - 2 \cdot 71 &= 503, & 503 + 8 &= 511; \\511 &= 11 \cdot 46 + 5, & 503 - 2 \cdot 46 &= 411, & 411 + 5 &= 416; \\416 &= 13 \cdot 32 + 0, & 411 - 2 \cdot 32 &= 347.\end{aligned}$$

Получили нулевой остаток, и Дрэм утверждает, что 13 – делитель числа 4511, причем  $4511 = 13 \cdot 347$ .

Обоснуем работу алгоритма Дрэма в общем случае. Пусть  $n_1$  – исходное нечетное число. Проследим за работой алгоритма Дрэма: сначала делим  $n_1$  с остатком на 3, получая равенство

$$n_1 = 3q_1 + r_1,$$

затем вычитаем удвоенное неполное частное:

$$m_1 = n_1 - 2q_1$$

и прибавляем остаток:

$$n_2 = m_1 + r_1.$$

Второй шаг алгоритма Дрэма записывается равенствами

$$n_2 = 5q_2 + r_2, \quad m_2 = m_1 - 2q_2, \quad n_3 = m_2 + r_2.$$

Третий шаг – равенствами

$$n_3 = 7q_3 + r_3, \quad m_3 = m_2 - 2q_3, \quad n_4 = m_3 + r_3,$$

и так далее. Из этих равенств следует, что

$$n_2 = m_1 + r_1 = (n_1 - 2q_1) + (n_1 - 3q_1) = 2n_1 - 5q_1,$$

$$m_2 = m_1 - 2q_2 = n_1 - 2q_1 - 2q_2,$$

$$n_3 = m_2 + r_2 = (n_1 - 2q_1 - 2q_2) + (n_2 - 5q_2) =$$

$$= n_1 - 2q_1 + 2n_1 - 5q_1 - 7q_2 = 3n_1 - 7q_1 - 7q_2,$$

$$m_3 = m_2 - 2q_3 = n_1 - 2q_1 - 2q_2 - 2q_3,$$

$$n_4 = m_3 + r_3 = (n_1 - 2q_1 - 2q_2 - 2q_3) + (n_3 - 7q_3) =$$

$$= n_1 - 2q_1 - 2q_2 + 3n_1 - 7q_1 - 7q_2 - 9q_3 = 4n_1 - 9q_1 - 9q_2 - 9q_3.$$

И вообще, для любого натурального  $k$  верны, как легко доказать по индукции, равенства

$$m_k = n_1 - 2(q_1 + q_2 + \dots + q_k),$$

$$n_{k+1} = (k+1)n_1 - (2k+1)(2k+1)(q_1 + q_2 + \dots + q_k).$$

Поскольку любое натуральное число  $k$  взаимно просто с числом  $2k + 1$ , то  $n_1$  делится на  $2k + 1$  тогда и только тогда, когда на  $2k + 1$  делится число

$$kn_1 - (2k + 1)(q_1 + q_2 + \dots + q_{k-1}) = n_k.$$

В случае делимости имеем  $r_k = 0$  и  $n_k = (2k + 1)q_k$ , следовательно, в этом случае

$$kn_1 = (2k + 1)(q_1 + q_2 + \dots + q_k),$$

$$m_{k+1} = n_1 - 2(q_1 + q_2 + \dots + q_k) = n_1 \left( 1 - \frac{2k}{2k + 1} \right) = \frac{n_1}{2k + 1},$$

что и требовалось доказать:  $n_1 = (2k + 1)m_{k+1}$ .

**Упражнение 3.** Методом Дрэма разложите на множители число  
а) 6647; б) 289.

*Бросая в воду камешки, наблюдай круги, ими образуемые.*

Козьма Прутков

В посвященной алгоритму Евклида статье книги «Арифметика»<sup>1</sup> рассказано, как этот замечательный алгоритм позволяет быстро вычислять наибольший общий делитель  $d$  любых двух целых чисел  $a$  и  $b$ , и доказано, что число  $d$  представимо в виде  $d = ax + by$  с целыми числами  $x$  и  $y$ .

Числа  $x$  и  $y$  нетрудно найти, анализируя шаги алгоритма Евклида. Смотрите, как это можно сделать при помощи матриц. Матрица – это прямоугольная таблица из чисел. Например, такая:

$$\begin{pmatrix} 35 & 1 & 0 \\ 15 & 0 & 1 \end{pmatrix}. \quad \begin{matrix} \alpha \\ \beta \end{matrix}$$

(Буквами  $\alpha$  и  $\beta$  обозначены соответственно верхняя и нижняя строки матрицы.) Вычтем из верхней строки удвоенную нижнюю:

$$\begin{pmatrix} 5 & 1 & -2 \\ 15 & 0 & 1 \end{pmatrix}. \quad \begin{matrix} \alpha - 2\beta \\ \beta \end{matrix}$$

А теперь вычтем утроенную верхнюю строку из нижней:

$$\begin{pmatrix} 5 & 1 & -2 \\ 0 & -3 & 7 \end{pmatrix}. \quad \begin{matrix} \alpha - 2\beta \\ -3\alpha + 7\beta \end{matrix}$$

Заметьте:  $1 \cdot 35 - 2 \cdot 15 = 5$ .

Прежде чем формулировать общий закон, рассмотрим другой частный случай:

$$\begin{pmatrix} 1876 & 1 & 0 \\ 365 & 0 & 1 \end{pmatrix}. \quad \begin{matrix} \alpha \\ \beta \end{matrix}$$

Руководствуясь равенством  $1876 = 5 \cdot 365 + 51$ , вычтем упятеренную нижнюю строку из верхней:

$$\begin{pmatrix} 51 & 1 & -5 \\ 365 & 0 & 1 \end{pmatrix}. \quad \begin{matrix} \alpha - 5\beta \\ \beta \end{matrix}$$

---

<sup>1</sup> А. В. Спивак. Арифметика. – М. Бюро Квантум, 2007. – Библиотечка «Квант», вып. 102.

Вычтем теперь усеченную верхнюю строку из нижней:

$$\begin{pmatrix} 51 & 1 & -5 \\ 8 & -7 & 36 \end{pmatrix}. \quad \begin{array}{l} \alpha - 5\beta \\ -7\alpha + 36\beta \end{array}$$

Ушестеренную нижнюю строку вычтем из верхней:

$$\begin{pmatrix} 3 & 43 & -221 \\ 8 & -7 & 36 \end{pmatrix}. \quad \begin{array}{l} 43\alpha - 221\beta \\ -7\alpha + 36\beta \end{array}$$

Как видите, над числами левого столбца выполняются шаги алгоритма Евклида. Рано или поздно одно из чисел этого столбца станет равно нулю. Дождемся же этого момента, осталось всего три шага: вычтем из нижней строки удвоенную верхнюю:

$$\begin{pmatrix} 3 & 43 & -221 \\ 2 & -93 & 478 \end{pmatrix}; \quad \begin{array}{l} 43\alpha - 221\beta \\ -93\alpha + 478\beta \end{array}$$

вычтем из верхней строки полученной таблицы нижнюю ее строку:

$$\begin{pmatrix} 1 & 136 & -699 \\ 2 & -93 & 478 \end{pmatrix}; \quad \begin{array}{l} 136\alpha - 699\beta \\ -93\alpha + 478\beta \end{array}$$

наконец, вычтем из нижней строки удвоенную верхнюю:

$$\begin{pmatrix} 1 & 136 & -699 \\ 0 & -365 & 1876 \end{pmatrix}. \quad \begin{array}{l} 136\alpha - 699\beta \\ -365\alpha + 1876\beta \end{array}$$

Заметьте:  $136 \cdot 1876 - 699 \cdot 365 = 1$ .

Пора формулировать общий закон. Рассмотрим произвольные целые числа  $a$ ,  $b$  и приведем при помощи преобразований над строками (преобразований, аналогичных вышепримененным) матрицу

$$\begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \end{pmatrix} \quad \begin{array}{l} \alpha \\ \beta \end{array}$$

к виду

$$\begin{pmatrix} d & x & y \\ 0 & z & t \end{pmatrix}. \quad \begin{array}{l} x\alpha + y\beta \\ z\alpha + t\beta \end{array}$$

В таком случае

$$ax + by = d = \text{НОД}(a; b)$$

(подумайте, почему).

*«Зачем складывать простые числа? – недоумевал физик Л.Д.Ландау. – Простые числа надо умножать, а не складывать!»*

Зачем складывать квадраты целых чисел? Почему бы не складывать их кубы или 66-е степени? Такие вопросы встают перед каждым, кто начинает изучать математику. Не все задачи достойны пристального внимания. Задача о сумме квадратов – в высшей степени достойна. К сожалению для философа, это трудно объяснить, не рассказав ее решение и не углубившись тем самым в детали.

«Детали» – это критерий того, какие натуральные числа представимы в виде суммы квадратов двух целых чисел. В одном из доказательств этого критерия будут использованы не только «обычные» целые числа, но и числа комплексные – прекрасный пример применения абстрактной теории к конкретной арифметической задаче!

### Часть I. Первые наблюдения

*Если вы внимательно проследите за вычислениями в основном тексте и будете рассматривать упражнения вычислительного характера не только как отнимающие время (неизбежно они обладают этой особенностью), но и как представляющие интерес, доставляющие наслаждение и понимание, то я убежден, что вы сможете оценить как мощь, так и крайнюю простоту теории.*

Г Эдвардс

#### Таблица сумм квадратов

Рассмотрим таблицу, в верхней строке и левом столбце которой – квадраты целых чисел, а в других клетках – суммы квадратов.

Некоторые числа представимы несколькими способами: например,  $25 = 5^2 + 0^2 = 4^2 + 3^2$  и  $65 = 8^2 + 1^2 = 7^2 + 4^2$ . Не вошедшие в таблицу числа первой сотни (3, 6, 7, 11, 12, 14, 15, ...) в виде суммы двух квадратов не представимы.

0	1	4	9	16	25	36	49	64	81	100
1	2	5	10	17	26	37	50	65	82	101
4	5	8	13	20	29	40	53	68	85	104
9	10	13	18	25	34	45	58	73	90	109
16	17	20	25	32	41	52	65	80	97	116
25	26	29	34	41	50	61	74	89	106	125
36	37	40	45	52	61	72	85	100	117	136
49	50	53	58	65	74	85	98	113	130	149
64	65	68	73	80	89	100	113	128	145	164
81	82	85	90	97	106	117	130	145	162	181
100	101	104	109	116	125	136	149	164	181	200

### Остатки от деления на 3

Наименьшее натуральное число, не представимое в виде суммы двух квадратов целых чисел, – это 3. Кратные 3 числа 6, 12, 15, 21 тоже не представимы, а вот числа  $9 = 3^2 + 0^2$  и  $18 = 3^2 + 3^2$  – представимы. Возникает гипотеза: числа, которые кратны 3, но не кратны 9, не представимы в виде суммы двух квадратов. Верно даже более сильное утверждение: *если сумма квадратов двух целых чисел кратна 3, то слагаемые тоже кратны 3.*

Для доказательства выпишем остатки от деления квадратов целых чисел на 3:

$n^2$	0	1	4	9	16	25	36	49	64	81	100	121
$n^2 \bmod 3$	0	1	1	0	1	1	0	1	1	0	1	1

Закономерность очевидна: остатки периодически повторяются, и никаких остатков кроме 0 и 1 не бывает. Точнее говоря, остаток от деления квадрата целого числа  $x$  на 3 равен 0, если  $x$  кратно 3, т.е. представимо в виде  $x = 3k$ , где  $k$  – целое число, и остаток равен 1, если  $x$  не кратно 3, т.е. представимо в виде  $x = 3k \pm 1$ . В самом деле, в первом случае  $x^2 = 9k^2$  делится на 3 без остатка, а во втором случае  $x^2 = 9k^2 \pm 6k + 1$  дает при делении на 3 остаток 1.

Суммы остатков  $0 + 1$  и  $1 + 1$  не кратны 3. Значит, сумма квадратов  $x^2 + y^2$  кратна 3 в том и только том случае, когда  $x$  и  $y$  кратны 3.

**Упражнение 1.** Если сумма квадратов двух целых чисел кратна  $3^{1999}$ , то эта сумма кратна  $3^{2000}$ . Докажите это.

### Остатки от деления на 7

Следующее после 3 и 6 не представимое в виде суммы двух квадратов число – это 7. Кратные 7 числа 14, 21, 28, 35, 42, 56, 63 не представимы в виде суммы квадратов. Опять возникает гипотеза: *если сумма  $x^2 + y^2$  кратна 7, то и сами целые числа  $x, y$  кратны 7.* Составим таблицу остатков:

$n^2$	0	1	4	9	16	25	36	49	64	81	100	121	144	169
$n^2 \bmod 7$	0	1	4	2	2	4	1	0	1	4	2	2	4	1

Поскольку сумма никаких двух из чисел 1, 2, 4 не кратна 7, гипотеза доказана.

### Упражнения

2. Остаток от деления квадрата целого числа  $x$  на 7 равен 0, если  $x = 7k$ , где  $k$  – целое число; равен 1, если  $x = 7k \pm 1$ ; равен 2, если  $x = 7k \pm 3$ ; равен 4, если  $x = 7k \pm 2$ . Докажите это.

3. Если сумма квадратов двух целых чисел кратна 21, то она кратна и 441. Докажите это.

4. а) Какие остатки дают квадраты целых чисел при делении на 11?

б) Если сумма квадратов двух целых чисел кратна 11, то она кратна 121. Докажите это.

в) Если сумма квадратов двух целых чисел кратна 1331, то она кратна и 14641. Докажите это.

### Остатки от деления на 19

*Полезные истины следует говорить и повторять как можно чаще.*

Для  $p = 19$  тоже легко составить таблицу остатков:

$n^2$	0	1	4	9	16	25	36	49	64	81	100	121	144	169	196	225	256	289	324
$n^2 \bmod 19$	0	1	4	9	16	6	17	11	7	5	5	7	11	17	6	16	9	4	1

В верхней строке – квадраты чисел 0, 1, ..., 18: другие квадраты можно не рассматривать, поскольку любое целое число  $x$  представимо в виде  $x = 19q + r$ , где  $q$  – целое,  $0 \leq r \leq 18$ , и при этом число  $x^2 = 19^2 q^2 + 38qr + r^2$  дает при делении на 19 такой же остаток, как и  $r^2$ .

В нижней строке таблицы один раз присутствует число 0 и по два раза – числа 1, 4, 5, 6, 7, 9, 11, 16 и 17. Ненулевые остатки

от деления квадратов целых чисел на простое число  $p > 2$  называют, как известно из статьи «Квадратичный закон взаимности» «Арифметики», *квадратичными вычетами по модулю  $p$* . Другие ненулевые остатки – *квадратичные невычеты* (при  $p = 19$  это 2, 3, 8, 10, 12, 13, 14, 15 и 18).

Поскольку сумма никаких двух из чисел 1, 4, 5, 6, 7, 9, 11, 16 и 17 не кратна 19, приходим к выводу: сумма квадратов двух целых чисел кратна 19 в том и только том случае, когда слагаемые кратны 19.

### Упражнения

5. Если  $p$  – простое число,  $p > 2$ , то существует  $(p - 1)/2$  квадратичных вычетов и столько же квадратичных невычетов по модулю  $p$ . Докажите это.

6. Докажите следующие утверждения.

а) Квадрат нечетного числа дает при делении на 8 остаток 1.

б) Уравнение  $x^2 + y^2 + z^2 = 8n - 1$  не имеет решений в целых числах.

в) Никакое число вида  $4^m(8n + 7)$ , где  $m, n$  – целые неотрицательные числа, не представимо в виде суммы квадратов трех целых чисел.

г) Если число  $8n + 3$ , где  $n$  – целое неотрицательное число, представимо в виде суммы трех квадратов, то число  $n$  представимо в виде суммы трех треугольных чисел, т.е. в виде  $n = \frac{x^2 + x}{2} + \frac{y^2 + y}{2} + \frac{z^2 + z}{2}$ , где  $x, y$  и  $z$  – целые числа.

*Замечание.* К.Ф.Гаусс (1777–1855) доказал, что в виде суммы квадратов трех целых чисел представимы все натуральные числа, кроме чисел вида  $4^m(8n + 7)$ , где  $m, n$  – целые неотрицательные числа. (Современное изложение его доказательства – в «Курсе арифметики» Ж.П.Серра и в «Теории чисел» З.И. Боровича и И.Р.Шафаревича. Оно использует  $p$ -адические числа, символ Гильберта и теорему Минковского–Хассе.)

7. Может ли сумма квадратов двух нечетных чисел быть квадратом или более высокой степенью натурального числа?

8. а) Остаток от деления на 16 четвертой степени нечетного числа равен 1. Докажите это.

б) Решите в целых числах уравнение  $x_1^4 + x_2^4 + x_3^4 + \dots + x_{14}^4 = 1000\,000\,001\,983$ .

в) Если натуральные числа  $x, y, z, u, v$  удовлетворяют равенству

$$x^4 + y^4 + z^4 + u^4 = v^4,$$

то хотя бы три из них четны. Докажите это и убедитесь при помощи калькулятора, что  $30^4 + 120^4 + 272^4 + 315^4 = 353^4$ .

9. Если  $a^2 + b^2 = c^2$ , где  $a, b, c$  – целые числа, то произведение  $abc$  кратно 60. Докажите это.



10. Если  $p$  – простое число, представимое в виде а)  $p = a^2 + 2b^2$ ; б)  $p = a^2 + 3b^2$ ; в)  $p = a^2 + 5b^2$ , где  $a, b$  – целые числа, то, соответственно, а)  $p = 2$  или  $p \equiv 1$  или  $3 \pmod{8}$ ; б)  $p = 3$  или  $p \equiv 1 \pmod{3}$ ; в)  $p = 5$  или  $p \equiv 1$  или  $9 \pmod{20}$ . Докажите это.

11. Каково наибольшее количество подряд идущих натуральных чисел, ни одно из которых не представимо в виде  $ab^2$ , где  $a$  и  $b$  взаимно просты, причем  $b > 1$ ?

### Делимость суммы квадратов на простое число

*Как относиться к трудностям? В области неизвестного надо рассматривать трудности как скрытый клад! Обычно: чем труднее, тем полезнее. Не так ценно, если трудности возникают от твоей борьбы с самим собой. Но когда трудности исходят от увеличившегося сопротивления предмета – это прекрасно!!*

А.И.Солженицын

Чем больше по величине простое число  $p$ , тем больше квадратичных вычетов по модулю  $p$ . Поэтому пора менять метод исследования: если мы не желаем погрязнуть в нескончаемых вычислениях, то должны каким-то одним общим рассуждением охватить числа 3, 7, 11, 19 и многие другие простые числа.

Обратите внимание: числа 3, 7, 11 и 19 при делении на 4 дают остаток 3, а именно,  $3 = 4 \cdot 0 + 3$ ,  $7 = 4 \cdot 1 + 3$ ,  $11 = 4 \cdot 2 + 3$  и  $19 = 4 \cdot 4 + 3$ .

**Теорема 1.** Если сумма квадратов  $a^2 + b^2$  целых чисел  $a$  и  $b$  делится на простое число  $p$  вида  $p = 4n + 3$ , где  $n$  – целое неотрицательное число, то числа  $a$  и  $b$  делятся на  $p$ .

**Доказательство. I способ – с использованием малой теоремы Ферма.** Пусть  $a$  не делится на  $p$ . Тогда и  $b$  не делится на  $p$ . Возведем обе части сравнения  $a^2 \equiv -b^2 \pmod{p}$  в  $(2n + 1)$ -ю степень:

$$a^{4n+2} \equiv -b^{4n+2} \pmod{p}.$$

В силу малой теоремы Ферма  $a^{4n+2} \equiv 1 \equiv b^{4n+2} \pmod{p}$ , поэтому  $1 \equiv -1 \pmod{p}$ , что невозможно при  $p > 2$ .

**II способ.** Рассмотрим числа 1, 2, ...,  $p - 1$ . Пусть  $x$  – любое из них. Числа  $x, 2x, \dots, (p - 1)x$ , как легко убедиться, не делятся на  $p$  и дают разные остатки при делении на  $p$ ; поэтому в точности одно из них дает остаток 1 при делении на  $p$ , так что существует такое число  $y$ , что  $xy \equiv 1 \pmod{p}$  и  $1 \leq y < p$ .

Рассмотрим множество  $M_x = \{x, p - x, y, p - y\}$  остатков от деления чисел  $x, -x, y$  и  $-y$  на  $p$ . Нетрудно проверить, что

$M_y = \{y, p - y, x, p - x\}$ ,  $M_{p-y} = \{p - y, y, p - x, x\}$  и  $M_{p-x} = \{p - x, x, p - y, y\}$ ; следовательно,  $M_x = M_{p-x} = M_y = M_{p-y}$ .

Хотя это и не нужно для доказательства, разберем ясности ради три примера. При  $p = 3$  имеем  $M_1 = \{1, 2\}$  (рис. 1). При  $p = 7$  множество ненулевых остатков является объединением множеств  $M_1 = \{1, 6\}$  и  $M_2 = \{2, 5, 4, 3\}$  (рис. 2). При  $p = 19$  — объединением множеств  $M_1 = \{1, 18\}$ ,  $M_2 = \{2, 17, 10, 9\}$ ,  $M_3 = \{3, 16, 13, 6\}$ ,  $M_4 = \{4, 15, 5, 14\}$  и  $M_7 = \{7, 12, 11, 8\}$  (рис. 3). Заметьте: во всех трех рассмотренных случаях множество  $M_1$  двухэлементное, а остальные множества состоят из четырех элементов каждое. Сплошной линией соединены остатки, сумма которых равна  $p$ , а пунктиром — те, произведение которых сравнимо с 1 по модулю  $p$ .

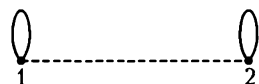


Рис. 1

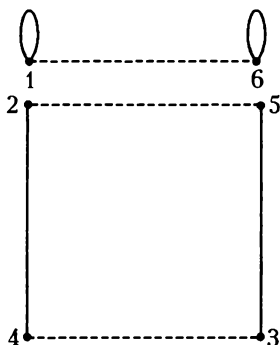


Рис. 2

Множество  $M_x$  не всегда состоит из четырех разных остатков. Например, если  $x \equiv 1$  или  $x \equiv p - 1$ , то  $y \equiv x$  и  $-y \equiv -x \pmod{p}$ . И обратно: если  $x \equiv y$ , то  $x^2 \equiv 1$ , так что  $(x - 1)(x + 1) = x^2 - 1$  делится на  $p$ , т.е.  $x \equiv \pm 1 \pmod{p}$ .

Априори вообразима ситуация, когда  $x \equiv -y$ , т.е.  $x^2 \equiv -1 \pmod{p}$ . А вот сравнение  $x \equiv -x \pmod{p}$  невозможно: вы помните, что  $0 < x < p$ , а  $p$  нечетно. Мы пришли к основной мысли этого доказательства: кроме двухэлементного множества  $M_1 = M_{p-1}$  двухэлементным может быть лишь такое множество  $M_x$ , что  $x^2 \equiv -1 \pmod{p}$ . Поскольку сравнению второй степени удовлетворяют не более чем два остатка, то отличное от  $M_1$  двухэлементное множество  $M_x$  не более чем одно.

При удалении двухэлементного множества  $M_1$  из  $(4n + 2)$ -элементного множества всех ненулевых остатков получаем  $4n$ -элементное множество  $\{2, 3, \dots, 4n + 1\}$ . Следовательно, при  $p = 4n + 3$  множество  $M_1$  — единственное двухэлементное множество, и ни для какого целого  $x$  сумма  $x^2 + 1$  не делится на простое число  $p = 4n + 3$ . Перечитав первый абзац этого доказательства, вы легко завершите доказательство теоремы 1.

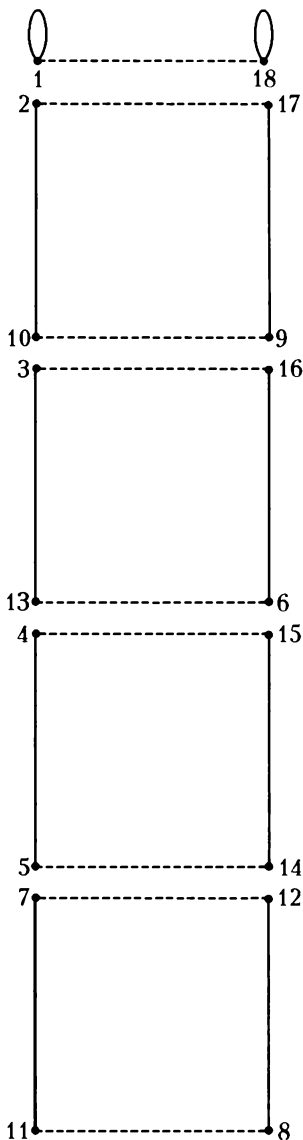


Рис. 3

### Упражнения

12. Если сумма квадратов  $x^2 + y^2$  целых чисел кратна  $p^{2m-1}$ , где  $m$  – натуральное число,  $p$  – простое число, которое при делении на 4 дает остаток 3, то числа  $x$  и  $y$  кратны  $p^m$ . Докажите это.

13. Существует бесконечно много натуральных чисел, которые дают остаток 1 при делении на 4, но не представимы в виде суммы квадратов двух целых чисел. Докажите это.

14. Существует бесконечно много простых чисел, дающих при делении на 4 остаток а) 3; б) 1. Докажите это.

При  $p = 5$  имеем  $M_1 = \{1, 4\}$  и  $M_2 = \{2, 3\}$  (рис. 4). При  $p = 17$  – пять множеств:  $M_1 = \{1, 16\}$ ,  $M_2 = \{2, 15, 9, 8\}$ ,  $M_3 = \{3, 14, 6, 11\}$ ,  $M_4 = \{4, 13\}$ ,  $M_5 = \{5, 12, 7, 10\}$  (рис. 5).

**Теорема 2.** Если остаток от деления простого числа  $p$  на 4 равен 1, то существует такое целое число  $m$ , что  $m^2 + 1$  делится на  $p$ .

**Доказательство.** Первый способ. При удалении множества  $M_1$  из  $(p - 1)$ -элементного множества ненулевых остатков остается множество  $\{2, 3, \dots, p - 2\}$ , количество элементов которого не делится на 4.

Мария Ивановна: «Пусть  $p$  – простое число. Тогда теорема Вильсона утверждает, что  $(p - 1)! + 1$  делится на  $p$ .»

Вовочка: «Я уже доказал! Надо всего лишь раскрыть скобки:

$$(p - 1)! + 1 = p! - 1! + 1 = p!.$$

Очевидно,  $p!$  делится на  $p$ .»

Второй способ основан на теореме изучавшего математику в Кэмбридже юриста Дж. Вильсона (1741–1793), доказательство которой впервые опубликовал в 1770 году англичанин Э. Варинг (1734–1798).

**Теорема Вильсона.** Для любого простого числа  $p$  сумма  $(p - 1)! + 1$  кратна  $p$ .

**Доказательство Гаусса** теоремы Вильсона продемонстрируем на примере числа  $p = 17$ . Смотрите:

$$6! = 1 \cdot (2 \cdot 9) \cdot (3 \cdot 6) \cdot (4 \cdot 13) \cdot (5 \cdot 7) \cdot$$

$$\cdot (8 \cdot 15) \cdot (10 \cdot 12) \cdot (11 \cdot 14) \cdot 16 \equiv$$

$$\equiv 16 \equiv -1 \pmod{17}.$$

И вообще, для любого простого числа  $p > 3$  числа  $2, 3, \dots, p - 2$ , как вы помните, можно разбить на такие пары  $(x; y)$ , что  $xy \equiv 1 \pmod{p}$ . Теорема Вильсона доказана.

Завершим доказательство теоремы 2, рассмотрев  $p = 4n + 1$  и  $m = (2n)!$ . Очевидно,

$$(p - 1)! = 1 \cdot 2 \cdot \dots \cdot (2n - 1) \cdot (2n) \cdot$$

$$\cdot (2n + 1) \cdot (2n + 2) \cdot \dots \cdot (4n - 1) \cdot (4n) =$$

$$= 1 \cdot 2 \cdot \dots \cdot (2n - 1) \cdot (2n) \cdot (p - 2n) \cdot$$

$$\cdot (p - (2n - 1)) \cdot \dots \cdot (p - 2) \cdot (p - 1)$$

дает при делении на  $p$  такой же остаток, как и число

$$1 \cdot 2 \cdot \dots \cdot (2n - 1) \cdot (2n) \cdot (-1)^{2n} \cdot$$

$$\cdot (2n) \cdot (2n - 1) \cdot \dots \cdot 2 \cdot 1 = m^2.$$

Следовательно,

$$m^2 + 1 \equiv (p - 1)! + 1 \equiv 0 \pmod{p}.$$

Теоремы 1 и 2, вместе взятые, известны как первое дополнение к квадратичному закону взаимности. Другое доказательство этих теорем изложено в статье «Квадратичный закон взаимности» (см. «Арифметичу»).

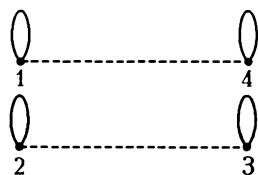


Рис. 4

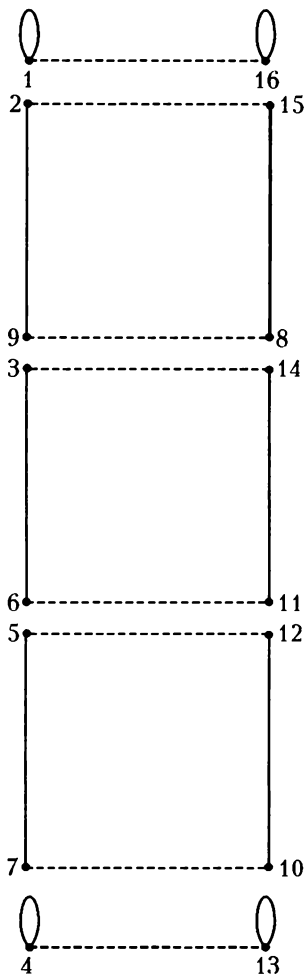


Рис. 5

## Упражнения

**15 (M1357).** Числа а)  $97! \cdot 1901! - 1$ ; б)  $98! \cdot 1900! + 1$  кратны 1999. Докажите это. (Указание. Число 1999 простое.)

**16.** Если  $p$  – простое число,  $p > 2$ ,  $m = ((p-1)/2)!$ , то  $m^2 \equiv (-1)^{(p+1)/2} \pmod{p}$ , так что остаток от деления числа  $m^2$  на  $p$  равен 1, если  $p = 4n + 3$ , и равен  $p - 1$ , если  $p = 4n + 1$ . Докажите это.

**17.** Если  $n$  – составное число,  $n > 4$ , то  $(n-1)!$  кратно  $n$ . Докажите это.

**18.** Если  $(n-1)! + 1$  делится на  $n$ , где  $n > 1$ , то  $n$  – простое. Докажите это. (Замечание. К сожалению, никакой пользы для вычислений это не дает: при сколь-нибудь значительном  $n$  число  $(n-1)!$  слишком велико.)

**19.** Число  $4(1 + (n-1)!) + n$  делится на произведение  $n(n+2)$  тогда и только тогда, когда числа  $n$  и  $n+2$  простые или  $n = 1$ . Докажите это.

**20.** а) Для любого делителя  $d$  числа  $n^2 + 1$ , где  $n$  – натуральное, существует бесконечно много таких натуральных  $m$ , что  $m^2 + 1$  кратно  $d$ . Докажите это.

б) Сколько существует натуральных чисел  $n < 1000$ , для которых  $n^2 + 1$  кратно 65?

**21.** Никакое число вида  $n^2 + 1$ , где  $n$  – целое, не имеет ни одного делителя вида  $4k - 1$ , где  $k$  – натуральное число. Докажите это.

**22.** Если  $x, y, z$  – целые числа и  $4xy - x - y = z^2$ , то  $x \leq 0$  и  $y \leq 0$ . Докажите это. (Это упражнение придумал Л.Эйлер.)

**23.** а) Никакое число вида  $m^2 + 1$  не кратно никакому числу вида  $n^2 - 1$ , где  $m, n$  – целые числа,  $n > 1$ . Докажите это.

б) Решите в целых числах уравнение  $x^2 y^2 = x^2 + y^2 + z^2$ .

## Часть II. Критерий Жирара

Мария Ивановна: «Тожество – это равенство двух выражений, справедливое для любых значений входящих в него переменных, при которых все эти выражения имеют смысл».

Вовочка: «Понял! Например,  $\sqrt{x} = \sqrt{-x}$ . Или  $\sqrt{x} + \sqrt{-1-x} = 0$ ».

Мария Ивановна: «Зачем же так? Это, конечно, тождества, но уж очень маленькие области определения: в первом случае одна точка, а во втором – пустое множество!»

Вовочка: «Ну ладно, Мария Ивановна. Тогда вот тождество:  $\sqrt{x + \sqrt{2x-1}} + \sqrt{x - \sqrt{2x-1}} + \sqrt{1-x} = \sqrt{2} + \sqrt{1-x}$ . Его область определения – отрезок  $[1/2; 1]$ ».

Мария Ивановна: «А упростить нельзя? Вычеркнуть  $\sqrt{1-x}$  из обеих частей?»

Вовочка: «Нет, нельзя! Тожество испортится!»

Если  $n = x^2 + y^2$ , то

$$\begin{aligned}(x+y)^2 + (x-y)^2 &= \\ &= x^2 + 2xy + y^2 + x^2 - 2xy + y^2 = 2(x^2 + y^2) = 2n.\end{aligned}$$

Значит, если  $n$  представимо в виде суммы двух квадратов, то представимо и  $2n$ . Далее,

$$\begin{aligned}(2x+y)^2 + (x-2y)^2 &= \\ &= 4x^2 + 4xy + y^2 + x^2 - 4xy + 4y^2 = 5(x^2 + y^2) = 5n.\end{aligned}$$

Легко проверить и формулы

$$\begin{aligned}(2x+3y)^2 + (3x-2y)^2 &= 13n, \\ (4x+y)^2 + (x-4y)^2 &= 17n.\end{aligned}$$

Все они являются частными случаями тождества, которое представляет произведение сумм двух квадратов в виде суммы двух квадратов. Чтобы получить его, раскроем скобки, прибавим и отнимем  $2abxy$  и изменим порядок слагаемых:

$$\begin{aligned}(a^2 + b^2)(x^2 + y^2) &= a^2x^2 + b^2x^2 + a^2y^2 + b^2y^2 = \\ &= a^2x^2 - 2axby + b^2y^2 + b^2x^2 + 2bxa y + a^2y^2 = \\ &= (ax - by)^2 + (bx + ay)^2.\end{aligned}$$

**Упражнение 24.** Докажите, что

а) если четное число  $n$  есть сумма квадратов двух целых чисел, то и число  $n/2$  представимо в виде суммы квадратов двух целых чисел;

б) если кратное 5 число  $n$  есть сумма квадратов двух целых чисел, то число  $n/5$  тоже представимо в таком виде;

в) если  $13k = x^2 + y^2$ , где  $k, x, y$  – целые числа, то хотя бы одна из формул  $k = \left(\frac{3x+2y}{13}\right)^2 + \left(\frac{2x-3y}{13}\right)^2$  и  $k = \left(\frac{3x-2y}{13}\right)^2 + \left(\frac{2x+3y}{13}\right)^2$  представляет  $k$  в виде суммы квадратов целых чисел.

**Какие числа – суммы двух квадратов?**

*Первое увлечение А.Н.Колмогорова историей относится к 1920 году, когда он был участником семинара С.В.Бахрушина. На основе изучения писцовых книг Колмогоров подготовил обширную работу «Новгородское землевладение XV века».*

*Окончательное решение в пользу математики, возможно, пришло к нему, когда на вопрос «Можно ли публиковать полученный результат?» Бахрушин ответил: «Ну что вы, публиковать еще рано. Дано лишь одно доказательство, а в истории нужно много подтверждений. Ищите дополнительные подтверждения».*

Выясним, какие простые числа представимы в виде суммы двух квадратов целых чисел. Как вы помните, числа вида  $4n + 3$  в виде суммы двух квадратов не представимы. Все другие простые числа, как мы сейчас докажем, представимы:  $2 = 1^2 + 1^2$ ,  $5 = 2^2 + 1^2$ ,  $13 = 3^2 + 2^2$ ,  $17 = 4^2 + 1^2$ ,  $29 = 5^2 + 2^2$ ,  $37 = 6^2 + 1^2$ ,  $41 = 5^2 + 4^2$ ,  $53 = 7^2 + 2^2$ , ...

**Теорема Ферма–Эйлера.** Любое простое число  $p = 4n + 1$ , где  $n$  – натуральное число, представимо в виде суммы квадратов двух натуральных чисел.

Эту теорему сформулировал Пьер Ферма (1601–1665), а доказал ее (при помощи любимого Ферма метода бесконечного спуска) Леонард Эйлер (1707–1783). Перед тем как ее доказывать, сформулируем критерий того, какие числа представимы в виде суммы двух квадратов.

Как вы помните, произведение суммы двух квадратов на сумму двух квадратов – сумма двух квадратов; квадрат любого простого числа – тоже сумма двух квадратов (один из них равен 0). Теорема 1, упражнение 12 и теорема Ферма–Эйлера приводят к следующему выводу: натуральное число представимо в виде суммы квадратов двух целых чисел тогда и только тогда, когда в его разложение на простые множители любой

простой множитель, дающий остаток 3 при делении на 4, входит в четной степени.

Этот критерий впервые был сформулирован голландцем Альбером Жираром (1595–1632) в следующем виде: *натуральное число представимо в виде суммы двух квадратов тогда и только тогда, когда оно является или квадратом, или числом 2, или простым числом, которое на 1 больше, чем некоторое кратное 4, или произведением нескольких вышеперечисленных чисел*. Скорее всего, Жирар опирался лишь на изучение таблиц и не умел доказывать необходимость и достаточность своих условий.

Мы докажем теорему Ферма–Эйлера пятью способами: четырьмя в этой части статьи и пятым – в следующей части.

### Упражнения

**25.** Число 15 не представимо в виде суммы квадратов двух рациональных чисел. Докажите это. (Этот факт упомянут в «Арифметике» древнегреческого математика Диофанта.)

**26.** Решите в целых числах уравнения: а)  $x^2 + y^2 = 1999(z^2 + t^2)$ ; б)  $x^3 + 7 = y^2$ ; в)  $x^3 + x^2 - 2x - 1 = y^2$ .

**27 (M814\* и M1556).** Отметим в натуральном ряду числа, которые можно представить в виде суммы двух квадратов натуральных чисел. Среди отмеченных чисел встречаются тройки последовательных чисел, например,  $72 = 6^2 + 6^2$ ,  $73 = 8^2 + 3^2$ ,  $74 = 7^2 + 5^2$ . Докажите следующие утверждения.

а) Не существуют четыре последовательных отмеченных числа.

б) Существует бесконечно много троек отмеченных последовательных чисел.

в) Существует бесконечно много таких отмеченных чисел  $n$ , что ни число  $n - 1$ , ни  $n + 1$  не является отмеченным.

г) Существует бесконечно много таких пар отмеченных чисел  $n$  и  $n + 1$ , что ни число  $n - 1$ , ни  $n + 2$  не является отмеченным.

д) Существуют сколь угодно длинные отрезки натурального ряда, состоящие сплошь из неотмеченных чисел.

### I способ. Крылатые квадраты

*«То, что мне удалось что-то сделать в математике, – однажды сказал великий немецкий математик Давид Гильберт (1862–1943), – объясняется тем, что я всегда находил все очень сложным. Когда я читаю или когда мне что-то рассказывают, мне почти всегда это кажется очень трудным и практически невозможным понять. Тогда я не могу не задать себе вопрос, а не может ли это быть проще. И в некоторых случаях, – добавил он с*



*простодушной улыбкой, — оказывалось, что это действительно намного проще.»*

Для любых трех натуральных чисел  $a$ ,  $b$  и  $c$  нарисует на клетчатой бумаге квадрат со стороной  $a$ ; от его левой верхней вершины отложим вверх отрезок длины  $b$ ; от верхнего конца только что построенного отрезка вправо отложим отрезок длины  $c$ ; построим прямоугольник, двумя сторонами которого являются только что построенные отрезки; вращая этот прямоугольник вокруг центра исходного квадрата на  $90^\circ$ ,  $180^\circ$  и  $270^\circ$ , получим еще три прямоугольника размером  $b \times c$  каждый. Возникла фигура площади  $a^2 + 4bc$ .

На рисунках 6, 7, 8 и 9 показаны 5 из 7 существующих способов представить число 37 в виде  $a^2 + 4bc$ , где  $a$ ,  $b$  и  $c$  — натуральные числа. Найдите два недостающих и убедитесь, что все семь представлений естественным образом разбиваются на представление  $37 = 1^2 + 4 \cdot 9 \cdot 1$  и три пары представлений.

В общем виде конструкция такова: поскольку

Рис. 6

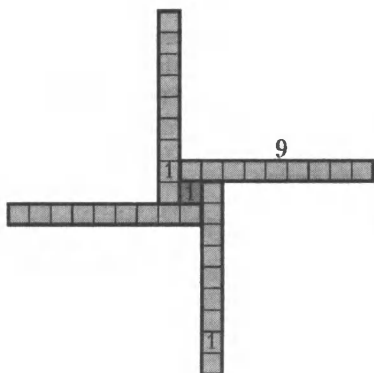
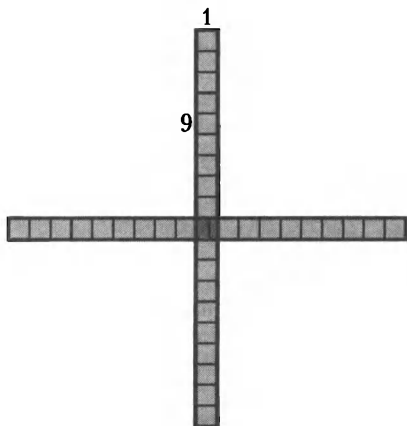


Рис. 7

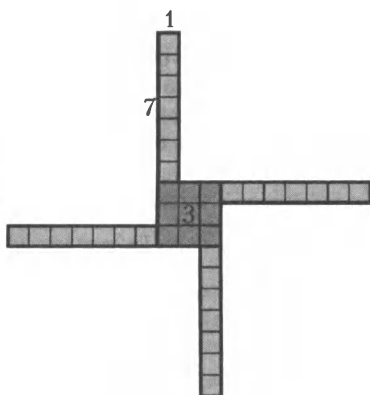


Рис. 8

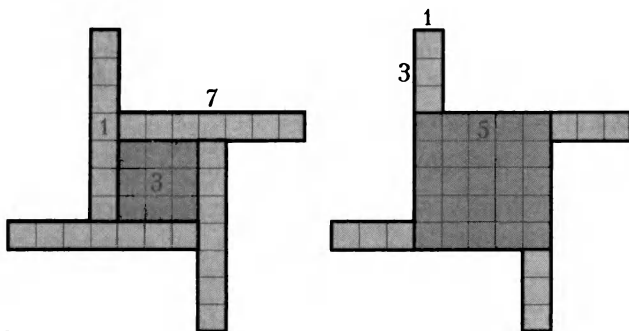


Рис. 9

имеется одно представление в виде «креста»  $p = 1^2 + 4 \cdot n \cdot 1$  и еще несколько пар (это слово – главное!), то количество решений уравнения  $p = a^2 + 4bc$  в натуральных числах  $a, b$  и  $c$  нечетно. Поскольку можно каждому решению  $(a, b, c)$  сопоставить решение  $(a, c, b)$ , а количество решений нечетно, то хотя бы в одном решении  $b = c$  (иначе множество, состоящее из нечетного числа элементов, удалось бы разбить на пары элементов). Теорема Ферма–Эйлера доказана. Удивительно красиво, не правда ли?

**Упражнение 28.** Где была использована простота числа  $p$ ?

*Мудрено пишут только о том, чего не понимают.*

В.О.Ключевский

Дон Цагир в 1990 году излагал то же самое доказательство, не используя клетчатую бумагу. Каждому решению в натуральных числах  $(a, b, c)$  уравнения  $a^2 + 4bc = p$  он сопоставил решение  $f(a, b, c)$  следующим образом:

$$f(a, b, c) = \begin{cases} (a + 2b, c - a - b, b), & \text{если } a + b < c; \\ (a - 2c, c, a + b - c), & \text{если } c < a + b \text{ и } 2c < a; \\ (2c - a, a + b - c, c) & \text{если } c < a + b \text{ и } a < 2c. \end{cases}$$

Поскольку

$$(a + 2b)^2 + 4(c - a - b)b = a^2 + 4bc$$

и

$$(a - 2c)^2 + 4c(a + b - c) = (2c - a)^2 + 4(a + b - c)c = a^2 + 4bc,$$

то отображение  $f$  переводит решение уравнения  $a^2 + 4bc = p$  в другое его решение.

Докажем, что  $f$  – инволюция, т.е.  $f(f(a, b, c)) = (a, b, c)$  для любых натуральных чисел  $a, b$  и  $c$ . В случае, когда  $a + b < c$ , имеем  $b < (a + 2b) + (c - a - b)$  и  $2b < a + 2b$ , поэтому

$$\begin{aligned} f(f(a, b, c)) &= f(a + 2b, c - a - b, b) = \\ &= ((a + 2b) - 2b, b, (a + 2b) + (c - a - b) - b) = (a, b, c). \end{aligned}$$

Если  $c < a + b$  и  $2c < a$ , то вследствие неравенства  $(a - 2c) + c < a + b - c$  имеем

$$\begin{aligned} f(f(a, b, c)) &= f(a - 2c, c, a + b - c) = \\ &= ((a - 2c) + 2c, (a + b - c) - (a - 2c) - c, c) = (a, b, c). \end{aligned}$$

Наконец, если  $c < a + b$  и  $a < 2c$ , то вследствие неравенств  $c < (2c - a) + (a + b - c)$  и  $2c - a < 2c$  имеем

$$\begin{aligned} f(f(a, b, c)) &= f(2c - a, a + b - c, c) = \\ &= (2c - (2c - a), (2c - a) + (a + b - c) - c, c) = (a, b, c). \end{aligned}$$

Неподвижные точки отображения  $f$  – решения, которые переходят сами в себя, – находим из системы

$$\begin{cases} 2c - a = a, \\ a + b - c = b, \\ a^2 + 4bc = p. \end{cases}$$

Очевидно, она равносильна системе

$$\begin{cases} a = c, \\ a(a + 4b) = p, \end{cases}$$

которая благодаря простоте числа  $p$  имеет единственное решение:  $a = c = 1$  и  $b = (p - 1)/4$ .

Следовательно, количество решений уравнения  $a^2 + 4bc = p$  в натуральных числах *нечетно*. Сопоставляя каждому решению  $(a, b, c)$  решение  $(a, c, b)$ , видим, что хотя бы одно решение удовлетворяет равенству  $b = c$ . А это и есть теорема Ферма–Эйлера.

Согласитесь, доказательство Дона Цагира с клетчатой бумагой гораздо понятнее, чем без нее. Хотя использованы те же самые инволюции. Иногда лучше рисовать, чем говорить!

### Упражнения

**29.** Роджер Хит-Броун в придуманном в 1971 и опубликованном в 1984 году доказательстве теоремы Ферма–Эйлера рассмотрел множества

$$F = \{(a, b, c) \mid a^2 + 4bc = p, \quad a \in \mathbf{Z}, \quad b, c \in \mathbf{N}\}$$

$$G = \{(a, b, c) \in F \mid a + c > b\} \quad H = \{(a, b, c) \in F \mid a > 0\},$$

и отображения  $f: F \rightarrow F, g: G \rightarrow G, h: H \rightarrow H$ , определенные формулами

$$f(a, b, c) = (-a, c, b),$$

$$g(a, b, c) = (2b - a, b, a + c - b),$$

$$h(a, b, c) = (a, c, b).$$

Проследите за его рассуждениями:

а)  $f$  – инволюция, т.е.  $f(f(a, b, c)) = f(-a, c, b) = (a, b, c)$ ; отображение  $f$  устанавливает биекцию (взаимно однозначное соответствие) как между множествами  $G$  и  $F \setminus G$ , так и между множествами  $H$  и  $F \setminus H$ ; следовательно,  $|G| = |F|/2 = |H|$ .

б)  $g$  – инволюция, поскольку  $(2b - a) + (c + a - b) > b$  и

$$g(g(a, b, c)) = g(2b - a, b, c + a - b) =$$

$$= (2b - (2b - a), b, (c + a - b) + (2b - a) - b) = (a, b, c).$$

в)  $g$  имеет единственную неподвижную точку, поскольку равенства  $a = 2b - a$  и  $c + a - b = c$  означают, что  $a = b$ ; уравнение  $p = a(a + 4c)$  имеет лишь одно решение в натуральных числах:  $a = 1$  и  $c = (p - 1)/4$ . Таким образом, множество  $G$  состоит из одной неподвижной точки и нескольких пар. Следовательно, количество элементов множества  $G$  нечетно – значит, нечетно и равное ему количество элементов множества  $H$ .

г)  $h$  – тоже инволюция:  $h(h(a, b, c)) = h(a, c, b) = (a, b, c)$ .

д) Поскольку множество  $H$  состоит из нечетного множества элементов, то его невозможно разбить на пары элементов и, следовательно, существует элемент  $(a, b, c)$  множества  $H$ , который под действием  $h$  переходит сам в себя, т.е. удовлетворяет равенству  $b = c$ .

## II способ. Доказательство Лагранжа

*Если бы не изобрели электричество, то мы по сей день смотрели бы телевизор при свечах.*

В силу теоремы 2 достаточно доказать, что любой простой делитель  $p$  числа  $m^2 + 1$ , где  $m$  – целое, представим в виде суммы квадратов двух натуральных чисел.

Рассмотрим все такие пары  $(r; s)$  целых чисел, что  $0 \leq r, s < \sqrt{p}$ , и для каждой пары рассмотрим остаток от деления числа  $r + ms$  на  $p$ . Поскольку количество таких пар равно  $([\sqrt{p}] + 1)^2 > p$ , среди них есть такие две пары  $(r_1; s_1)$  и  $(r_2; s_2)$ , что остатки от деления на  $p$  чисел  $r_1 + ms_1$  и  $r_2 + ms_2$  равны.

Сумма  $r + ms$ , где  $r = r_1 - r_2$  и  $s = s_1 - s_2$ , кратна  $p$ , поэтому

кратна  $p$  и сумма квадратов

$$r^2 + s^2 = r^2 - m^2 s^2 + (m^2 + 1)s^2 = (r + ms)(r - ms) + (m^2 + 1)s^2.$$

Очевидно,  $0 < r^2 + s^2 < p + p = 2p$ . Единственное кратное  $p$  число, которое расположено между 0 и  $2p$ , — само число  $p$ . Значит,  $r^2 + s^2 = p$ .

**Упражнение 30.** Как доказано в главе «Уравнения Пелля», для любого вещественного числа  $\xi$  и любого натурального числа  $n$  существуют такие целое число  $t$  и натуральное число  $s$ , что  $s \leq n$  и  $|s\xi - t| \leq \frac{1}{n+1}$ . Рассмотрев  $n = [\sqrt{p}]$  и  $\xi = m/p$ , докажите равенство  $p = (ms - tp)^2 + s^2$ .

### III способ. Доказательство Эйлера

*Чтобы попасть в цель, часто нужна не меткость, а смелость.*

Ферма писал: «Если бы выбранное простое число, которое на единицу больше некоторого числа, делящегося на 4, не было суммой квадратов, то существовало бы простое число такой же природы, меньшее заданного, а затем еще и третье, и так далее, бесконечно убывая до тех пор, пока не будет достигнуто простое число 5, которое является наименьшим из всех чисел такой природы; отсюда следовало бы, что 5 не является суммой двух квадратов, что не соответствует действительности. Отсюда сведением к абсурду следует заключить, что все числа такой природы являются суммами двух квадратов».

Л.Эйлер в 1747–1749 годах превратил этот проект бесконечного спуска в общепонятное доказательство.

**Лемма 1.** Если сумма квадратов кратна простому числу, являющемуся суммой квадратов, то частное — тоже сумма квадратов.

**Доказательство.** Пусть  $a^2 + b^2$  делится на простое число  $p = r^2 + s^2$ . Тогда

$$(ar - bs)(ar + bs) = a^2 r^2 - b^2 s^2 = (a^2 + b^2)r^2 - b^2(r^2 + s^2) : p.$$

Значит,  $ar - bs$  или  $ar + bs$  кратно  $p$ . Если  $ar - bs : p$ , то

$$\frac{a^2 + b^2}{p} = \frac{(a^2 + b^2)(r^2 + s^2)}{p^2} = \left( \frac{ar - bs}{p} \right)^2 + \left( \frac{as + br}{p} \right)^2$$

— представление числа  $(a^2 + b^2)/p$  в виде суммы квадратов двух

целых чисел. (Поймите, почему второе слагаемое правой части не может быть нецелым!) Случай, когда  $ar + bs$  делится на  $p$ , аналогичен:

$$\frac{a^2 + b^2}{p} = \left( \frac{ar + bs}{p} \right)^2 + \left( \frac{as - br}{p} \right)^2.$$

**Лемма 2.** *Всякое натуральное число, являющееся делителем суммы квадратов двух взаимно простых чисел, является суммой двух квадратов.*

**Доказательство.** Пусть сумма  $a^2 + b^2$  кратна натуральному числу  $m$ , причем  $\text{НОД}(a; b) = 1$ . Представим числа  $a$  и  $b$  в виде  $a = mx + c$  и  $b = my + d$ , где  $c$  и  $d$  по абсолютной величине не превосходят  $m/2$ . Тогда

$$\begin{aligned} c^2 + d^2 &= (a - mx)^2 + (b - my)^2 = \\ &= (a^2 + b^2) - 2amx + m^2x^2 - 2bmy + m^2y^2 : m, \end{aligned}$$

следовательно,  $c^2 + d^2 = mn$ , где  $n$  – целое, причем

$$n = \frac{c^2 + d^2}{m} \leq \frac{(m/2)^2 + (m/2)^2}{m} = \frac{m}{2}.$$

Если  $n = 0$ , то  $m$  – общий делитель (взаимно простых!) чисел  $a$  и  $b$ , так что  $m = 1 = 1^2 + 0^2$ .

Пусть  $n > 0$ . Очевидно,  $m$  взаимно просто с наибольшим общим делителем чисел  $c$  и  $d$ . Разделив числа  $c$  и  $d$  на  $\text{НОД}(c; d)$ , видим, что  $n$  – делитель суммы квадратов взаимно простых чисел. Если все простые делители числа  $n$  – суммы квадратов, то в силу леммы 1 число  $m$  – сумма квадратов. Если же хотя бы один из них – не сумма квадратов, получаем меньшее число, являющееся делителем суммы квадратов взаимно простых чисел и не представимое в виде суммы квадратов, и так далее. Поскольку бесконечной убывающей последовательности натуральных чисел не существует, лемма 2 доказана.

Осталось сослаться на теорему 2 – и теорема Ферма–Эйлера доказана! Впрочем, Эйлер в 1749 году рассуждал не так: он использовал следующую лемму.

**Лемма 3.** *Если  $p = 4n + 1$  – простое число, то существует сумма квадратов двух взаимно простых целых чисел, делящаяся на  $p$ .*

**Доказательство.** В силу малой теоремы Ферма каждое из чисел  $1^{4n}$ ,  $2^{4n}$ ,  $3^{4n}$ , ...,  $(4n-1)^{4n}$ ,  $(4n)^{4n}$  дает при делении на  $p$  остаток 1. Следовательно, все разности  $(a+1)^{4n} - a^{4n} =$

$= ((a+1)^{2n} - a^{2n})((a+1)^{2n} + a^{2n})$ , где  $1 \leq a < 4n$ , кратны  $p$ . Если ни одна из сумм  $(a+1)^{2n} + a^{2n}$  не кратна  $p$ , то все разности  $(a+1)^{2n} - a^{2n}$  кратны  $p$  и поэтому  $a^{2n} \equiv 1 \pmod{p}$  при  $a = 1, 2, \dots, p-1$ ; но многочлен степени  $2n$  не может иметь  $4n$  корней.

### Упражнения

**31.** Никакое простое число не может двумя существенно разными способами быть представлено в виде суммы двух квадратов натуральных чисел. Докажите это.

**32 (M1288\*).** Число  $1000\,009 = 235^2 + 972^2$  составное. а) Докажите это. б) Представьте его в виде произведения двух отличных от 1 натуральных чисел.

**33.** Проверьте тождество  $(a^2 + nb^2)(r^2 + ns^2) = (ar - nbs)^2 + n(as + br)^2$ .

**34.** Если  $p$  – простое число,  $m$  – натуральное число, причем  $pm = a^2 + nb^2$  и  $p = r^2 + ns^2$ , где  $a, b, r, s, n$  – целые числа, то и число  $m$  представимо в виде  $m = x^2 + ny^2$ , где  $x$  и  $y$  – целые числа. Докажите это.

**35.** а) Пусть  $q$  – нечетное простое число,  $m$  – натуральное число, причем  $q^2m = a^2 + nb^2$  и  $q^2 = r^2 + ns^2$ , где  $a, b$  – целые числа,  $r, s, n$  – натуральные числа. Докажите следующие утверждения.

а)  $m$  представимо в виде  $m = x^2 + ny^2$ , где  $x$  и  $y$  – целые числа.

б) Если числа  $a$  и  $b$  взаимно простые, то и число  $m$  представимо в виде  $m = x^2 + ny^2$ , где  $x$  и  $y$  – взаимно простые числа.

**36\*.** Докажите следующие утверждения.

а) Никакой квадрат не может дать остаток 2 при делении на простое число, дающее остаток 3 или 5 при делении на 8.

б) Никакой квадрат, сложенный с числом 2, не делится ни на какое простое число, дающее остаток 5 или 7 при делении на 8.

**37\*.** Для любого простого числа  $p$ , дающего остаток а) 3; б) 7 при делении на 8, существует квадрат, дающий при делении на  $p$  остаток, соответственно, а)  $p-2$ ; б) 2. Докажите это.

**38\*.** Для любого простого числа  $p$ , дающего остаток 1 при делении на 8, существует квадрат, дающий остаток а) 2; б)  $p-2$  при делении на  $p$ . Докажите это.

**39.** Докажите следующие утверждения.

а) Число 2 является квадратичным вычетом по модулю простого числа  $p$  тогда и только тогда, когда  $p \equiv \pm 1 \pmod{8}$ .

б) Число  $p-2$  является квадратичным вычетом по модулю простого числа  $p$  тогда и только тогда, когда  $p \equiv 1$  или  $3 \pmod{8}$ .

## Неоткрытие Эйлера

Вполне возможно, что Ферма действительно знал вышеизложенное доказательство, как и доказательства двух аналогичных гипотез:

- всякое простое число  $p$ , дающее остаток 1 или 3 при делении на 8, представимо в виде  $p = x^2 + 2y^2$ , где  $x$  и  $y$  – целые числа;
- всякое простое число  $p$ , дающее остаток 1 при делении на 3, представимо в виде  $p = x^2 + 3y^2$ , где  $x$  и  $y$  – целые.

Ферма предположил, что верно следующее утверждение (но не претендовал на то, что умеет его доказывать):

- произведение любых двух простых чисел, каждое из которых при делении на 20 дает остаток 3 или 7, представимо в виде  $p = x^2 + 5y^2$ , где  $x$  и  $y$  – целые. (Например, число 21 представимо в виде суммы квадрата и упятеренного квадрата, и даже двумя способами:  $21 = 4^2 + 5 \cdot 1^2 = 1^2 + 5 \cdot 2^2$ . А числа 3 и 7 – не представимы.)

Леонард Эйлер предположил, но не смог доказать, что

- всякое простое число  $p$ , дающее остаток 1 или 9 при делении на 20, представимо в виде  $p = x^2 + 5y^2$ , где  $x$  и  $y$  – целые;
- для всякого простого числа  $p$ , дающего остаток 3 или 7 при делении на 20, число  $2p$  представимо в виде  $2p = x^2 + 5y^2$ , где  $x$  и  $y$  – целые;
- простое число  $p$  представимо в виде  $p = x^2 + 27y^2$ , где  $x$  и  $y$  – целые, тогда и только тогда, когда  $p \equiv 1 \pmod{3}$  и число 2 является остатком от деления куба некоторого целого числа на  $p$ ;<sup>1</sup>

- простое число  $p$  представимо в виде  $p = x^2 + 64y^2$ , где  $x$  и  $y$  – целые, тогда и только тогда, когда  $p \equiv 1 \pmod{4}$  и число 2 является остатком от деления четвертой степени некоторого целого числа на  $p$ .<sup>2</sup>

Жозеф Луи Лагранж (1736–1813) и Адриен Мари Лежандр (1752–1833) доказали первую из вышеуказанных гипотез Эйлера и доказали, что всякое простое число  $p$ , дающее остаток 3 или 7 при делении на 20, представимо в виде

---

<sup>1</sup> Об этой гипотезе мы ничего не расскажем. Заинтересованному читателю советуем «Классическое введение в современную теорию чисел» К.Айерлэнда и М.Роузена.

<sup>2</sup> Доказательство Петера Густава Лежена Дирихле (1805–1859) этой гипотезы Эйлера – в упражнении 47.



$p = 2x^2 + 2xy + 3y^2$ , где  $x$  и  $y$  – целые. Поскольку

$$2(2x^2 + 2xy + 3y^2) = (2x + y)^2 + 5y^2,$$

тем самым они доказали и вторую из гипотез Эйлера. А тождество

$$\begin{aligned} (2a^2 + 2ab + 3b^2)(2x^2 + 2xy + 3y^2) = \\ = (2ax + bx + ay + 3by)^2 + 5(bx - ay)^2 \end{aligned}$$

показывает, что верна и гипотеза Ферма о том, что произведение любых двух простых чисел, каждое из которых при делении на 20 дает остаток 3 или 7, представимо в виде  $p = x^2 + 5y^2$ , где  $x$  и  $y$  – целые. (Впрочем, вскоре мы докажем эту гипотезу Ферма без этого ужасного «взятого с потолка» тождества.)

В 2006 году Йинг Жанг придумал доказательство теоремы о числах, представимых в виде  $x^2 + 5y^2$ , основанное на тех же идеях, что и доказательство Эйлера теоремы Ферма–Эйлера. При первом чтении советуем пропустить этот раздел статьи, сначала полностью освоившись с суммой двух квадратов: теорема 3 доступна только тем, кто знает – например, из статьи «Квадратичный закон взаимности» «Арифметики», – что для всякого нечетного простого числа  $p$

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{5}{p}\right) = (-1)^{(p-1)/2} (-1)^{(5-1)(p-1)/4} \left(\frac{p}{5}\right)$$

и, следовательно,  $\left(\frac{-5}{p}\right) = 1$  для тех и только тех нечетных простых чисел  $p$ , которые удовлетворяют одному из сравнений

$$\left(\frac{-5}{p}\right) = 1, 3, 7 \text{ или } 9 \pmod{20}.$$

**Теорема 3.** Если остаток от деления простого числа  $p$  на 20 равен 1 или 9, то существуют такие натуральные числа  $x$  и  $y$ , что  $p = x^2 + 5y^2$ . Если  $q$  и  $Q$  – простые числа, причем  $q \equiv 3$  или  $7 \pmod{20}$  и  $Q = 2$  или  $Q \equiv 3$  или  $7 \pmod{20}$ , то произведение  $qQ$  представимо в виде  $qQ = x^2 + 5y^2$ , где  $x$  и  $y$  – натуральные числа.

**Доказательство** – индукция. База:  $3 \cdot 2 = 1^2 + 5 \cdot 1^2$  и  $3 \cdot 3 = 2^2 + 5 \cdot 1^2$ .

**Переход:** предположим, что для некоторого простого числа  $P$ , дающего остаток 1, 3, 7 или 9 при делении на 20, все простые

числа  $p < P$ , для которых  $p \equiv 1$  или  $9 \pmod{20}$ , представимы в виде суммы квадрата и упятеренного квадрата натуральных чисел, а все простые числа  $q < P$ , удовлетворяющие сравнению  $q \equiv 3 \pmod{20}$  или сравнению  $q \equiv 7 \pmod{20}$ , обладают тем свойством, что для любого простого числа  $Q < P$ , где  $Q = 2$  или  $Q \equiv 3$  или  $7 \pmod{20}$ , произведение  $qQ$  представимо в виде суммы квадрата и упятеренного квадрата; докажем, что аналогичное утверждение верно и при замене строгих неравенств  $p < P$ ,  $q < P$  и  $Q < P$  на нестрогие.

Для рассматриваемого простого числа  $P$  существует такое целое число  $a$ , что  $a^2 + 5$  делится на  $P$ . Заменяя число  $a$  на наименьшее по абсолютной величине число, сравнимое с  $a$  по модулю  $P$ , мы видим, что можно считать выполненным неравенство  $|a| \leq (P-1)/2$ , а вместе с ним и неравенства

$$a^2 + 5 \cdot 1^2 \leq \frac{(P-1)^2}{4} + 5 < P^2.$$

Следовательно, существуют такие натуральные числа  $x$ ,  $y$  и  $m$ , что

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

причем  $m < P$ . При рассматриваемом  $P$  выберем из всех таких равенств то, где  $m$  — наименьшее возможное. Очевидно, для такого  $m$  числа  $x$  и  $y$  взаимно простые (иначе  $m$  можно было бы разделить на квадрат их наибольшего общего делителя).

Как вы помните, перед формулировкой теоремы 3 мы вывели из квадратичного закона взаимности, что любой нечетный простой делитель числа  $m$  при делении на 20 дает один из остатков 1, 3, 7 и 9.

Если  $m$  делится на простое число  $p$ , сравнимое с 1 или 9 по модулю 20, то в силу предположения индукции  $p$  представимо в виде суммы квадрата и упятеренного квадрата. Вспоминая упражнение 34, получаем противоречие: в роли  $m$  может выступить и  $m/p$ , следовательно,  $m$  — не наименьшее возможное.

Итак, на роль простого делителя числа  $m$  претендуют только число 2 и простые нечетные числа  $q$ , дающие остаток 3 или 7 при делении на 20. Рассмотрим два случая.

Если  $m$  делится на  $q^2$ , то достаточно вспомнить упражнение 35. Если  $m$  делится на  $qQ$ , где  $q \neq Q$ , причем число  $Q$  простое,  $Q = 2$  или же  $Q \equiv 3$  или  $7 \pmod{20}$ , то по предположению индукции  $qQ$  представимо в виде суммы квадрата и упятеренного квадрата. В силу формулы упражнения 33, представимо в таком виде и произведение  $qQ \cdot Pm$ . Поскольку  $qQ Pm =$

$= q^2 Q^2 \cdot P \frac{m}{qQ}$ , то, дважды применив утверждение упражнения 35, видим, что в виде суммы квадрата и упятеренного квадрата представимо и число  $P \cdot \frac{m}{qQ}$ ; однако  $\frac{m}{qQ} < m$ .

Итак, число  $m$  имеет не более одного простого делителя: проще говоря,  $m = 1$  или  $m$  – простое число. Случай  $m = 1$  соответствует тому, что  $P \equiv 1$  или  $9 \pmod{20}$ . Осталось разобрать случай, когда  $m$  и  $P$  – простые числа, которые при делении на 20 дают остаток 3 или 7. Рассмотрим простое число  $Q$ , которое равно 2 или дает при делении на 20 остаток 3 или 7. По предположению индукции, число  $mQ$  представимо в виде суммы квадрата и упятеренного квадрата. В силу упражнения 33, произведение  $mP \cdot mQ = m^2 \cdot PQ$  тоже представимо. Осталось вспомнить упражнение 35 – и теорема 3 доказана.

### Упражнения

**40\*.** Всякое простое число  $p$ , которое дает остаток 1 или 3 при делении на 8, представимо в виде  $p = x^2 + 2y^2$ , где  $x$  и  $y$  – целые числа. Докажите это.

**41.** Если  $4n = a^2 + 3b^2$ , где  $a, b, n$  – целые числа, то и число  $n$  представимо в виде  $x^2 + 3y^2$ , где  $x$  и  $y$  – целые числа. Докажите это.

**42\*.** Всякое простое число  $p$ , которое дает остаток 1 при делении на 3, представимо в виде  $p = x^2 + 3y^2$ , где  $x$  и  $y$  – целые числа. Докажите это.

**43.** Докажите следующие утверждения.

а) Натуральное число представимо в виде суммы квадрата и удвоенного квадрата тогда и только тогда, когда оно является или квадратом, или числом 2, или простым числом, дающим остаток 1 или 3 при делении на 8, или произведением таких чисел.

б) Натуральное число представимо в виде суммы квадрата и утроенного квадрата тогда и только тогда, когда оно является или квадратом, или числом 3, или простым числом, дающим остаток 1 при делении на 6, или произведением таких чисел.

**44.** Для любых целых чисел  $a$  и  $b$  уравнение  $x^2 + xy + y^2 = a^2 + 3b^2$  имеет решение в целых числах  $x$  и  $y$ . Докажите это.

**45.** Существует ли число, представимое в виде  $a^2 + ab + b^2$ , где  $a, b$  – целые неотрицательные числа, но не представимое в виде  $c^2 - cd + d^2$ , где  $c, d$  – тоже целые неотрицательные числа?

**46.** Всякое простое число  $p$ , которое дает остаток 3 или 7 при делении на 20, представимо в виде  $p = 2a^2 + 2ab + 3b^2$ , где  $a$  и  $b$  – целые числа. Докажите это.

**47.** Пусть  $p$  – простое число, дающее остаток 1 при делении на 4. В силу теоремы Ферма–Эйлера, для некоторых целых чисел  $a$  и  $b$  имеем  $p = a^2 + b^2$ .

Поскольку числа  $a$  и  $b$  разной четности, можно считать, что  $a$  нечетно, а  $b$  четно. Пусть  $f$  – такое целое число, что  $b \equiv af \pmod{p}$ . Применяя свойства символа Якоби и критерий Эйлера, убедитесь в следующем:

$$а) \left(\frac{a}{b}\right) = (-1)^{\frac{(p-1)(a-1)}{4}} \left(\frac{p}{a}\right) = \left(\frac{a^2 + b^2}{a}\right) = \left(\frac{b^2}{a}\right) = 1;$$

$$\begin{aligned} б) \left(\frac{a+b}{p}\right) &= (-1)^{\frac{(p-1)(a+b-1)}{4}} \left(\frac{p}{a+b}\right) = \\ &= \left(\frac{2p}{a+b}\right) \left(\frac{2}{a+b}\right) = \left(\frac{(a+b)^2 + (a-b)^2}{a+b}\right) \left(\frac{2}{a+b}\right) = \\ &= \left(\frac{(a-b)^2}{a+b}\right) \left(\frac{2}{a+b}\right) = (-1)^{((a+b)^2-1)/8}; \end{aligned}$$

$$в) f^2 \equiv -1 \pmod{p};$$

$$\begin{aligned} г) 2^{(p-1)/4} &= \frac{(2ab)^{(p-1)/4}}{(ab)^{(p-1)/4}} \equiv \frac{((a+b)^2)^{(p-1)/4}}{(a^2f)^{(p-1)/4}} = \frac{(a+b)^{(p-1)/2}}{a^{(p-1)/2} f^{(p-1)/4}} \equiv \\ &= (-1)^{((a+b)^2-1)/8} f^{(1-p)/4} \equiv f^{\frac{a^2+2ab+b^2}{4} + \frac{1-p}{4}} = f^{ab/2} \pmod{p}. \end{aligned}$$

д) Поскольку порядок числа  $f$  по модулю  $p$  равен 4, то сравнение  $2^{(p-1)/4} \equiv 1 \pmod{p}$  выполнено тогда и только тогда, когда  $ab/2$  делится на 4, т.е. когда  $b$  делится на 8. Таким образом, простое число  $p$  представимо в виде  $p = x^2 + 64y^2$ , где  $x$  и  $y$  целые, тогда и только тогда, когда  $p \equiv 1 \pmod{4}$  и число 2 является остатком от деления четвертой степени некоторого целого числа на  $p$ .

#### IV способ. Доказательство Минковского

Доказательство Германа Минковского (1864–1909) основано на рассмотрении решеток. Каждая такая решетка получена проведением двух систем параллельных прямых, которые делят плоскость на равные параллелограммы. На рисунке 10 показана одна из решеток. Из рисунка 11 очевидно, что в качестве порождающего параллелограмма можно было взять и параллелограмм, закрашенный на рисунке 10. Параллелограмм, закрашенный на рисунке 11, приводит нас к системе прямых, изображенной на рисунке 12. А закрашенный на рисунке 12 параллелограмм возвращает к системе прямых рисунка 10.

**Лемма 4.** Для любого параллелограмма  $OABC$  площади  $S$  хотя бы одна из вершин порожжденной им решетки удалена от точки  $O$  не более чем на  $\sqrt{2S/\sqrt{3}}$ .

**Доказательство.** Выбрав находящиеся на наименьшем расстоянии  $\rho$  точки решетки  $A_0$  и  $A_1$  (рис.13), видим, что

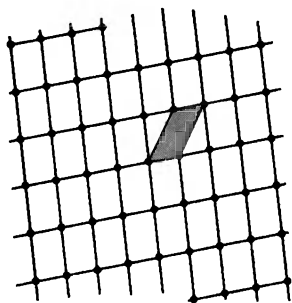


Рис. 10

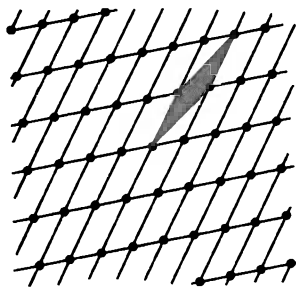


Рис. 11

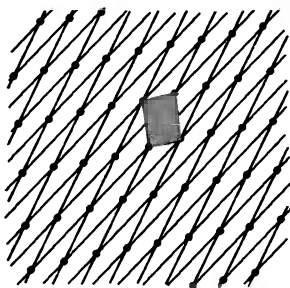


Рис. 12

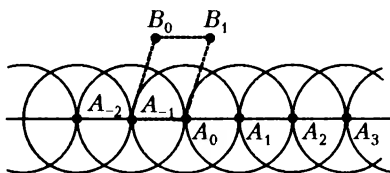


Рис. 13

решетка содержит все точки  $A_k$ , где  $k \in \mathbb{Z}$  и  $\overline{A_0 A_k} = k \overline{A_0 A_1}$ , и не содержит ни одной точки внутри кругов радиуса  $\rho$  с центрами в этих точках; поэтому высота основного параллелограмма  $A_0 A_1 B_1 B_0$  решетки, опущенная на сторону  $A_0 A_1$ , не меньше  $\rho \sin 60^\circ$ , откуда  $S \geq \rho^2 \sqrt{3}/2$ .

**Лемма 5.** Если  $a, b, c$  — целые числа,  $a > 0$  и  $ac - b^2 = 1$ , то существуют такие целые числа  $x$  и  $y$ , что  $ax^2 + 2bxy + cy^2 = 1$ .

**Доказательство.** Рассмотрим векторы  $\overline{OA}$  и  $\overline{OC}$  длин  $\sqrt{a}$  и  $\sqrt{c}$  соответственно, угол  $\varphi$  между которыми выберем так, чтобы скалярное произведение равнялось  $b$ , т.е.  $\cos \varphi = b/\sqrt{ac}$ . Площадь  $S$  параллелограмма  $OABC$  равна

$$S = OA \cdot OC \cdot \sin \varphi = \sqrt{a} \sqrt{c} \sqrt{1 - \cos^2 \varphi} = \sqrt{a} \sqrt{c} \sqrt{\frac{ac - b^2}{ac}} = 1.$$

В силу леммы 4 существуют такие целые числа  $x$  и  $y$ , хотя бы одно из которых отлично от нуля, что  $|x\overline{OA} + y\overline{OC}| \leq \sqrt{2/\sqrt{3}}$ .

Следовательно,

$$ax^2 + 2bxy + cy^2 = (x\overline{OA} + y\overline{OC})^2 \leq 2/\sqrt{3} < 2.$$

Поскольку скалярный квадрат любого ненулевого вектора положителен, то  $ax^2 + 2bxy + cy^2 > 0$ . А поскольку между нулем и двойкой есть только одно целое число – единица, то  $ax^2 + 2bxy + cy^2 = 1$ . Лемма 5 доказана.

Применяя ее к числам  $a = p$ ,  $b = m$  и  $c = \frac{m^2 + 1}{p}$ , получаем для некоторых целых чисел  $x$  и  $y$  равенство  $1 = px^2 + 2mxy + cy^2$ . Домножая обе его части на  $p$ , получаем

$$p = p^2x^2 + 2pmtx + (m^2 + 1)y^2 = (px + my)^2 + y^2.$$

Теорема Ферма–Эйлера доказана при помощи решеток!

### Упражнения

**48** (лемма Минковского о выпуклом теле). Всякая выпуклая и симметричная относительно начала координат фигура, площадь которой больше 4, содержит кроме начала координат еще хотя бы одну точку с целыми координатами. Докажите это.

**49.** Применяя лемму Минковского о выпуклом теле к эллипсу, заданному уравнением  $ax^2 + 2bxy + cy^2 = 2$ , докажите лемму 5.

## Часть III. Комплексные числа

Изложенные во второй части статьи доказательства теоремы Ферма–Эйлера производят впечатление то ли чудес, то ли фокусов. Суть дела помогает понять арифметика целых гауссовых чисел. Она дает не только еще одно доказательство теоремы Ферма–Эйлера, но и позволяет получить формулы для количества представлений числа в виде суммы двух квадратов. Перед тем, как в третьей части статьи мы будем изучать целые гауссовы числа, познакомимся с комплексными числами.

### Что такое комплексное число?

*Что нам стоит дом построить?  
Нарисуем – будем жить!*

Первопричиной появления комплексных чисел послужило то обстоятельство, что некоторые квадратные уравнения с вещественными коэффициентами имеют вещественные решения, а некоторые (дискриминанты которых отрицательны) не имеют. Математику трудно смириться с тем, что какая-то

задача не имеет решения. Поэтому в таких случаях стараются так расширить основные понятия, чтобы эту невозможность устранить. Так приходят к расширению поля  $\mathbb{R}$  вещественных чисел (числовой прямой) до поля  $\mathbb{C}$  комплексных чисел («числовой плоскости»).

Одной из привлекательных черт теории комплексных чисел является ее подлинная комплексность: в ней сочетаются алгебраические, аналитические, геометрические и топологические методы. Понятия и методы комплексного анализа используют во многих разделах математики.

### Что такое $i$ ?

Изобретение целых чисел, т.е. расширение множества  $\mathbb{N} = \{1, 2, 3, \dots\}$  натуральных чисел до множества  $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ , дает возможность решить, например, уравнение  $x + 7 = 5$ . Построив более широкое множество  $\mathbb{Q} = \left\{ \frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{N} \right\}$  рациональных чисел, получаем возможность решать уравнения вроде  $3x = 8$ . Желание измерить диагональ единичного квадрата (или, что то же, решить уравнение  $x^2 = 2$ ) приводит к очередному расширению множества чисел до множества  $\mathbb{Q}[\sqrt{2}]$  чисел вида  $a + b\sqrt{2}$ , где  $a, b \in \mathbb{Q}$ . Очевидно, сумма, разность и произведение чисел вида  $a + b\sqrt{2}$  — число такого же вида. С делением тоже все в порядке, например,

$$\frac{1 + \sqrt{2}}{3 - 2\sqrt{2}} = \frac{(1 + \sqrt{2})(3 + 2\sqrt{2})}{(3 - 2\sqrt{2})(3 + 2\sqrt{2})} = 7 + 5\sqrt{2},$$

$$\frac{2 - 5\sqrt{2}}{3 + \sqrt{2}} = \frac{(2 - 5\sqrt{2})(3 - \sqrt{2})}{(3 + \sqrt{2})(3 - \sqrt{2})} = \frac{16 - 17\sqrt{2}}{7}.$$

Видите, как просто? В общем виде это выглядит так:

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{(c + d\sqrt{2})(c - d\sqrt{2})} = \frac{ac - 2bd + (bc - ad)\sqrt{2}}{c^2 - 2d^2}.$$

Для алгебраических вычислений важно, что квадрат числа  $\sqrt{2}$  равен 2. Комплексные числа мы получим, введя в рассмотрение число  $i$ , квадрат которого равен  $-1$ . Может показаться, что

«такого не бывает», ведь уравнение  $x^2 + 1 = 0$  не имеет решений не только в рациональных, но и в вещественных числах. Однако число  $\sqrt{2}$ , заметьте, тоже «не существовало» до тех пор, пока мы рассматривали только рациональные числа.

Итак, рассмотрим выражения вида  $a + bi$ , где  $a, b$  – вещественные числа. Эти выражения мы и будем называть *комплексными числами*. Сумму и произведение определим естественными формулами

$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$

$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i.$$

Последняя формула, быть может, нуждается в комментарии:

$$(a + bi) \cdot (c + di) = ac + adi + bci + bdi^2 = ac + adi + bci - bd.$$

Это именно комментарий, а не доказательство, поскольку пользоваться обычными правилами раскрытия скобок можно только после того, как даны определения сложения и умножения комплексных чисел и проверены эти «обычные правила», т.е. формулы  $z_1 + z_2 = z_2 + z_1$  (переместительный закон, или коммутативность сложения),  $z_1 z_2 = z_2 z_1$  (коммутативность умножения),  $(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$  (сочетательный закон, или ассоциативность сложения),  $(z_1 z_2) z_3 = z_1 (z_2 z_3)$  (ассоциативность умножения),  $(z_1 + z_2) z_3 = z_1 z_3 + z_2 z_3$  (распределительный закон, или дистрибутивность).

### Упражнения

**50.** Выполните эту проверку.

**51.** Докажите, что

а) для любого комплексного числа  $z$  существует и определено единственным образом такое число  $w$ , что  $z + w = 0 + 0i$ ;

б) для любого отличного от числа  $0 + 0i$  комплексного числа  $z$  существует и определено единственным образом такое число  $w$ , что  $zw = 1 + 0i$ .

в) Научитесь делить комплексные числа, т.е. для вещественных чисел  $a, b, c, d$  найдите, при условии  $c^2 + d^2 \neq 0$ , такие вещественные числа  $x$  и  $y$ , что  $a + bi = (c + di)(x + yi)$ . (Не удивляйтесь, что последняя формула записана без знака деления: если бы он был, то все равно пришлось бы дать определение частного  $(a + bi)/(c + di)$  комплексных чисел. А самый разумный способ сделать это – назвать частным  $u/v$ , где  $v \neq 0$ , такое число  $w$ , что  $u = vw$ .)

**52.** Вычислите: а)  $i^3$ ; б)  $i^4$ ; в)  $i^{1999}$ ; г)  $1 + i + i^2 + \dots + i^{10} + i^{11}$ ; д)  $(1 + i)^{12}$ ; е)  $(i^{34} + i^{39}) / (i^{41} + i^{44})$ .



## Геометрическая интерпретация

Формулы сложения и умножения комплексных чисел позволяют отождествить комплексное число  $a + 0i$  с вещественным числом  $a$ . Поэтому в дальнейшем мы будем писать не  $a + 0i$ , а попросту  $a$ .

Расширение множества  $\mathbb{R}$  вещественных чисел до множества  $\mathbb{C}$  комплексных чисел можно пояснить геометрически. Это сделал в 1799 году датчанин Каспар Вессель (1745–1818), но его сочинение «Об аналитическом представлении направлений» долгое время оставалось неизвестным. В 1806 году геометрическую интерпретацию комплексных чисел независимо от Весселя открыл швейцарец Жан Робер Арган (1768–1822). Впрочем, немец Карл Фридрих Гаусс (1777–1855),

скорее всего, пользовался этими наглядными представлениями раньше Весселя и Аргана.

Отождествим ось абсцисс координатной плоскости с вещественной осью (т.е. с множеством всех вещественных чисел); единичный вектор  $(1; 0)$  оси абсцисс обозначим просто 1, а единичный вектор  $(0; 1)$  оси ординат обозначим через  $i$  (рис.14). Произвольный вектор  $z =$

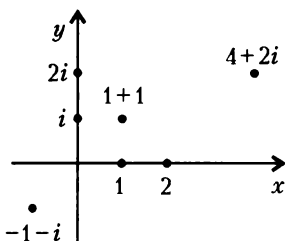


Рис. 14

$= (x; y)$  плоскости можно теперь записать в виде  $z = x(1; 0) + y(0; 1) = x + yi$ . Принято вещественные числа  $x$  и  $y$  называть *вещественной и мнимой частями* комплексного числа  $z$ . Обозначения:  $x = \operatorname{Re} z$ ,  $y = \operatorname{Im} z$ . Сложение комплексных чисел – это обычное сложение векторов. А умножение определяется, как мы уже видели, более «хитрой» формулой.

### Модуль комплексного числа

Модулем (абсолютной величиной) числа  $z = a + bi$  называют расстояние  $|z| = \sqrt{a^2 + b^2}$  от начала координат до точки  $(a; b)$ .

**Теорема 4.** *Модуль произведения комплексных чисел равен произведению их модулей:  $|(a + bi)(x + yi)| = |a + bi| \cdot |x + yi|$ .*

**Доказательство:**

$$\begin{aligned} |(a + bi)(x + yi)| &= |(ax - by) + (ay + bx)i| = \\ &= \sqrt{(ax - by)^2 + (ay + bx)^2} = \sqrt{(a^2 + b^2)(x^2 + y^2)} = |a + bi| \cdot |x + yi|. \end{aligned}$$

## Упражнения

53. Научитесь извлекать квадратный корень из комплексного числа: для вещественных чисел  $a, b$  найдите такие пары  $(x; y)$  вещественных чисел, что  $(x + iy)^2 = a + bi$ .

54. Решите в комплексных числах уравнения: а)  $z^2 - 2z + 1 = i$ ; б)  $z^2 - 5z + 7 = i$ ; в)  $z^2 + 10 + 2i = (4 + i)z$ .

## Сопряженные числа

Уравнение  $z^2 = -1$  имеет два корня:  $i$  и  $-i$ . Поскольку при вычислениях используется именно равенство  $i^2 = -1$ , возникает идея заменить  $i$  на  $-i$ . Верное равенство при одновременной замене всех входящих в него символов  $i$  на  $-i$  останется верным!

Точная реализация этой идеи такова: два комплексных числа, действительные части которых равны, а мнимые части равны по абсолютной величине и противоположны по знаку, называют *сопряженными*. Число, сопряженное с  $z = x + yi$ , обозначают  $\bar{z} = x - yi$  (рис.15). Геометрический смысл перехода от числа к сопряженному – симметрия относительно оси абсцисс. Легко проверить тождества

$$\overline{u + v} = \bar{u} + \bar{v},$$

$$\overline{u \cdot v} = \bar{u} \cdot \bar{v},$$

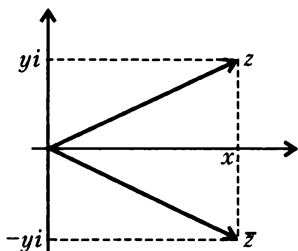


Рис. 15

которые как раз и позволяют заменять в формулах все числа на сопряженные.

Между прочим,  $|z|^2 = x^2 + y^2 = (x + iy)(x - iy) = z\bar{z}$ . Это позволяет очень изящно доказать теорему 4:

$$|uv|^2 = (uv)\overline{uv} = uv\bar{u}\bar{v} = (u\bar{u})(v\bar{v}) = |u|^2 \cdot |v|^2.$$

Формула  $|u|^2 \cdot |v|^2 = |uv|^2$  ранее встречалось нам в следующем виде: произведение сумм квадратов является суммой квадратов.

## Какие числа «настоящие»?

Переход к комплексным числам является очередным шагом в последовательности: натуральные числа – целые числа – рациональные числа – действительные числа – комп-

лексные числа. Может сложиться впечатление, что до действительных чисел это на самом деле числа, а комплексные числа – это уже не числа, а объекты более сложной природы. Конечно, терминология может быть принята любая, однако в действительности комплексные числа вполне заслуживают, чтобы их называли числами.

Первое возражение против этого может состоять в том, что это не числа, а пары чисел. Вспомним, однако, что подобным же образом вводятся рациональные числа. Рациональное число – это класс эквивалентных дробей, где дроби – это пары целых чисел, записываемые в виде  $\frac{m}{n}$  (где  $n \neq 0$ ); дроби  $\frac{m_1}{n_1}$  и  $\frac{m_2}{n_2}$  эквивалентны, если  $m_1 n_2 = m_2 n_1$ .

Действия над рациональными числами – это просто действия над парами целых чисел. Поэтому первое возражение несостоятельно. Другое возражение может состоять в том, что числа – это то, чем можно что-то измерять. Если понимать под этим, что числа – это то, чем можно измерять все, что угодно, то тогда надо запретить, например, отрицательные числа, так как не бывает отрезков длиной  $-3$  см, а поезд не может ехать  $-4$  дня. Придется запретить и слишком большие: температура манной каши не бывает  $1000^\circ\text{C}$ . Если же считать, что числа – это то, чем можно (или удобно) измерять хоть что-нибудь, то тогда комплексные числа оказываются ничем не хуже других чисел – ими очень удобно описывать, например, ток, напряжение и сопротивление в электрических цепях переменного тока, и это широко используют в электротехнике.

Таким образом, переход от действительных чисел к комплексным является таким же естественным, как, например, переход от целых чисел к рациональным.

## Часть IV. Целые гауссовы числа

### Определения

Комплексное число  $a + bi$  называют *целым гауссовым*, если  $a$  и  $b$  – целые числа. Сумма, разность и произведение целых гауссовых чисел – целые гауссовы, так что множество  $\mathbb{Z}[i]$  целых гауссовых чисел является, как говорят алгебраисты, кольцом. По определению, целое гауссово число  $u$  кратно целому гауссову числу  $v$ , если существует такое целое гауссово число  $w$ , что  $u = vw$ .

Отметив на плоскости целые гауссовы числа, мы получим

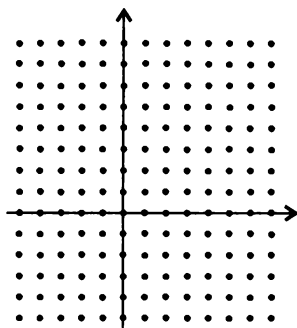


Рис. 16

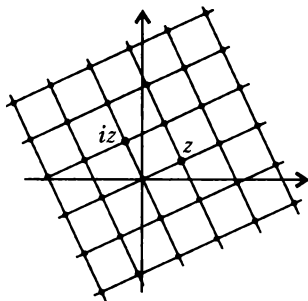


Рис. 17

решетку (рис.16). Числа, кратные данному числу  $z$ , тоже образуют решетку (рис.17).

На рисунке 18 кружочком выделены кратные числа  $2 + i$ , звездочками – кратные числа  $2 - i$ . Спросим себя, какие целые гауссовы числа кратны и числу  $2 + i$ , и числу  $2 - i$ . Ответ очевиден: пересечение состоит из чисел, кратных 5. Другими словами, наименьшее общее кратное чисел  $2 + i$  и  $2 - i$  равно 5.

Произведение  $(a + bi)(a - bi) = a^2 + b^2$  комплексного числа  $z = a + bi$  и сопряженного к нему числа  $\bar{z} = a - bi$  является числом вещественным. Поэтому для любого ненулевого целого гауссова числа  $z$  существует кратное ему натуральное число  $z\bar{z} = a^2 + b^2$ .

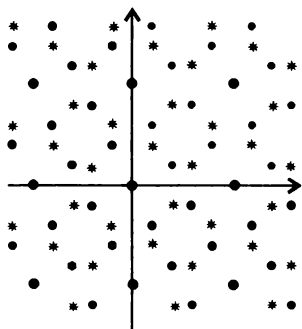


Рис. 18

**Теорема 5.** Если числа  $a$  и  $b$  взаимно просты, то наименьшим натуральным числом  $n$ , которое кратно числу  $a + bi$ , является именно число  $a^2 + b^2$ .

**Доказательство.** Поскольку  $\frac{n}{a + bi} = \frac{n(a - bi)}{(a + bi)(a - bi)} = \frac{na}{a^2 + b^2} - \frac{nb}{a^2 + b^2}i$ , натуральное число  $n$  кратно числу  $a + bi$  только в тех случаях, когда числа  $na$  и  $nb$  кратны  $a^2 + b^2$ . Поскольку числа  $a$  и  $b$  взаимно просты, это бывает только когда  $n$  кратно  $a^2 + b^2$ .

## Упражнения

55. При каком условии на целые числа  $a$  и  $b$  частное  $(a + bi)/(1 + i)$  является целым гауссовым числом?

56. Изобразите на плоскости числа, кратные числу а)  $1 + 3i$ ; б)  $1 - 3i$ . в) Какие целые гауссовы числа являются кратными и числа  $1 + 3i$ , и числа  $1 - 3i$  одновременно?

57. Если целое вещественное число  $n$  кратно ненулевому целому гауссову числу  $a + bi$ , то  $n$  кратно числу  $(a^2 + b^2)/\text{НОД}(a, b)$ . Докажите это.

## Делители единицы

Очевидно,  $1 = 1 \cdot 1 = i \cdot (-1) \cdot (-1) = (-i) \cdot i$ . Других способов разложить 1 в произведение двух целых гауссовых чисел нет: мы сейчас докажем, что целое гауссово число  $a + bi$  является делителем единицы в том и только том случае, когда  $a^2 + b^2 = 1$ .

**Теорема 6.** В  $\mathbb{Z}[i]$  нет делителей единицы, кроме чисел 1,  $i$ ,  $-1$  и  $-i$ .

**Доказательство.** Если  $1 = uv$ , где  $u, v \in \mathbb{Z}[i]$ , то  $1 = |u| \cdot |v|$ . Поскольку модуль ненулевого целого гауссова числа не меньше 1, имеем  $|u| = |v| = 1$ , откуда и следует утверждение теоремы.

## Ассоциированные числа

Числа  $u$  и  $v$  называют *ассоциированными*, если они кратны друг другу, т.е.  $u$  кратно  $v$  и  $v$  кратно  $u$ . Всякое целое гауссово число  $z$  можно представить в виде произведения

$$z = 1 \cdot z = i(-iz) = (-1)(-z) = (-i)(iz),$$

первый множитель которого – делитель единицы, а второй – ассоциирован с числом  $z$ . Столь же очевидно, что если целое гауссово число  $w$  кратно числу  $z$ , то делителями числа  $w$  являются также и числа  $-z$ ,  $iz$ ,  $-iz$ . Поэтому, рассматривая разложения на множители, можно «не различать» ассоциированные числа.

## Упражнения

58. Для комплексного числа  $z = 2 + i$  отметьте на комплексной плоскости числа  $iz$ ,  $-z$ ,  $-iz$ .

59. Ассоциированные с числом  $z$  числа – это в точности числа вида  $\varepsilon z$ , где  $\varepsilon$  – делитель единицы. Докажите это.

60. Докажите, что

а) числа  $1 + i$  и  $1 - i$  ассоциированы;

б) числа  $a + bi$  и  $a - bi$  ассоциированы в том и только том случае, когда выполнено хотя бы одно из условий:  $a = 0$ ,  $b = 0$ ,  $a = b$ ,  $a = -b$ .

### Основная теорема арифметики $\mathbb{Z}[i]$

В силу теоремы 2 для простого числа  $p \equiv 1 \pmod{4}$  существует такое целое число  $m$ , что  $(m^2 + 1) : p$ . Числу  $p$  не кратен ни один из множителей  $m + i$  и  $m - i$ , но кратно произведение  $m^2 + 1 = (m + i)(m - i)$ . Что это значит? Как может произведение быть кратно  $p$ , если ни один из множителей не кратен  $p$ ? Неужели арифметика гауссовых чисел настолько своеобразна, что в ней не действуют привычные нам законы, например, основная теорема арифметики?

Нет, действуют! В статье «Основная теорема арифметики» «Арифметики» тремя разными способами – в том числе при помощи деления с остатком – доказано, что разложение на простые множители в множестве натуральных чисел единственно. Делить с остатком можно и целые гауссовы числа: мы сейчас докажем, что для любого целого гауссова числа  $w$  и любого ненулевого целого гауссова числа  $z$  расстояние от точки  $w$  до ближайшей к ней точки решетки, состоящей из кратных числа  $z$ , меньше  $z$  (и даже не превышает  $|z|/\sqrt{2}$ ). Поэтому разложение целых гауссовых чисел на простые гауссовы множители единственно в том же смысле, в каком оно единственно для обычных целых чисел – с точностью до перестановки множителей и до ассоциированности.

**Теорема 7.** *Разложение на простые множители в  $\mathbb{Z}[i]$  единственно (с точностью до перестановки множителей и ассоциированности).*

**Доказательство.** Тот факт, что любое ненулевое целое гауссово число можно представить в виде произведения простых гауссовых чисел, очевиден: разлагаем, пока можно, а когда перестанет разлагаться, то все уже разложилось! (Любитель «абсолютной» строгости то же самое оформит следующим образом. Предположим, что не все целые гауссовы числа имеют разложения на простые гауссовы множители. Рассмотрим такое число  $z$  с наименьшим модулем. Если  $z$  – делитель единицы или простое число, то оно в разложении не нуждалось. А если  $z$  представимо в виде произведения  $z = uv$  целых гауссовых чисел, где  $|u| < |z|$  и  $|v| < |z|$ , то числа  $u$  и  $v$  имеют разложения на простые множители. Объединив их, мы как раз получаем разложение числа  $z$ .)

Намного труднее и интереснее доказательство единственности разложения. Предположим, что некоторое целое гауссово число  $z$  двумя существенно разными способами представлено в виде произведения простых гауссовых чисел:

$$z = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s.$$

Можно считать, что  $z$  — *наименьшее* по абсолютной величине из чисел, обладающих разными разложениями на простые гауссовы множители. Тогда ни одно из чисел  $p_1, \dots, p_r$  не ассоциировано ни с одним из чисел  $q_1, q_2, \dots, q_s$  (в противном случае мы сократили бы обе части равенства на общий множитель, получив меньшее по модулю число).

Обозначим  $P = p_2 \dots p_r$  и  $Q = q_2 \dots q_s$ . Тогда  $z = p_1 P = q_1 Q$ . Не ограничивая общности, можно считать, что  $|p_1| \leq |q_1|$ . При этом  $|P| \geq |Q|$  и, значит,  $|p_1 Q| \leq |z|$ . Рассмотрим число  $w = \varepsilon z - p_1 Q$ , где  $\varepsilon$  — такой делитель единицы, что  $|w| < |z|$ .

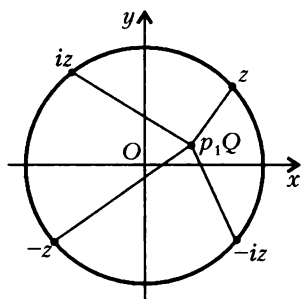


Рис. 19

(Почему такой делитель единицы  $\varepsilon$  можно выбрать, ясно из рисунка 19: числа  $z, iz, -z$  и  $-iz$  — вершины квадрата; точка  $p_1 Q$  расположена внутри описанного круга этого квадрата. Весь описанный круг можно покрыть четырьмя кругами с центрами в вершинах квадрата, радиусы которых равны половине диагонали квадрата. Значит, хотя бы одна из вершин квадрата расположена к точке  $p_1 Q$  ближе, чем на расстояние  $|z|$ .) Число  $w$  может быть разложено на множители двумя способами:

$$w = \varepsilon z - p_1 Q = p_1 (\varepsilon P - Q) = (\varepsilon q_1 - p_1) q_2 \dots q_s.$$

Поскольку  $|w| < |z|$ , для числа  $w$  должна иметь место единственность разложения на простые гауссовы множители. Значит, хотя бы один из множителей  $\varepsilon q_1 - p_1, q_2, \dots, q_s$  должен быть кратен простому числу  $p_1$ . Если число  $\varepsilon q_1 - p_1$  кратно  $p_1$ , то  $q_1$  кратно  $p_1$ , откуда следует, поскольку  $q_1$  — простое гауссово число, что числа  $p_1$  и  $q_1$  ассоциированы, что невозможно. Еще очевиднее противоречие в случае, когда кратен числу  $p_1$  один из множителей  $q_2, \dots, q_s$ .

## Простые и составные целые гауссовы числа

Некоторые простые числа  $p$  перестают быть простыми при расширении  $\mathbb{Z}$  до  $\mathbb{Z}[i]$ . Например,  $2 = (1+i)(1-i) = -i(1+i)^2$  и  $5 = (1+2i)(1-2i)$ . Какие же простые натуральные числа остаются простыми во множестве целых гауссовых чисел, а какие становятся составными? И как устроены разложения «новых составных» чисел? Как доказать при помощи целых гауссовых чисел теорему Ферма–Эйлера и, главное, как найти количество способов представить данное натуральное в виде суммы двух квадратов?

Пусть  $p$  – простой делитель суммы  $m^2 + 1$ , где  $m \in \mathbb{N}$ . Делитель  $p$  числа  $(m+i)(m-i)$  не может быть простым гауссовым числом. Значит,  $p = (a+bi)(c+di)$ , где целые гауссовы числа  $(a+bi)$  и  $(c+di)$  – не делители единицы. Поскольку модуль произведения равен произведению модулей, имеем

$$p = \sqrt{a^2 + b^2} \sqrt{c^2 + d^2},$$

т.е.  $p^2 = (a^2 + b^2)(c^2 + d^2)$ , откуда  $p = a^2 + b^2 = c^2 + d^2$ .

**Лемма 6.** Никакое простое натуральное число не представимо в виде произведения более чем двух целых гауссовых чисел, не являющихся делителями единицы.

**Доказательство.** Если  $p = (a+bi)(c+di)(e+fi)$ , то  $|p| = |a+bi| \cdot |c+di| \cdot |e+fi|$ , откуда  $p^2 = (a^2 + b^2)(c^2 + d^2)(e^2 + f^2)$ . Квадрат простого числа никак не может быть произведением трех отличных от 1 натуральных чисел.

**Следствие.** Если простое натуральное число  $p$  ассоциировано с произведением двух не являющихся делителями единицы целых гауссовых чисел, то эти числа – простые гауссовы.

**Теорема 8.** Всякое простое натуральное число вида  $p = 4n + 3$  простое и в  $\mathbb{Z}[i]$ ; всякое простое натуральное число вида  $p = 4n + 1$  разлагается на два сопряженных множителя:  $p = (a+bi)(a-bi)$ , причем множители  $a+bi$  и  $a-bi$  – простые гауссовы числа; наконец, число 2 ассоциировано с квадратом простого гауссова числа  $1+i$ .

**Доказательство.** Если число  $p = 4n + 3$  представлено в виде произведения двух целых гауссовых чисел  $p = (a+bi)(c+di)$ , то

$$|p| = |a+bi| \cdot |c+di|,$$

откуда  $p^2 = (a^2 + b^2)(c^2 + d^2)$ . Значит, либо один из множителей



$a^2 + b^2$  и  $c^2 + d^2$  равен 1, а другой равен  $p^2$ , либо  $p = a^2 + b^2 = c^2 + d^2$ . В первом случае ясно, что число  $p$  было представлено в виде произведения делителя единицы и ассоциированного с  $p$  числа. Второй случай невозможен, поскольку  $p$  при делении на 4 дает остаток 3, а не 1.

Простое число  $p = 4n + 1$  в силу теоремы Ферма–Эйлера разложимо в сумму квадратов  $p = a^2 + b^2$ , так что  $p = (a + bi)(a - bi)$ . Множители, в силу следствия леммы 6, являются простыми гауссовыми числами. Число 2 тоже представимо в виде суммы двух квадратов:  $2 = 1^2 + 1^2 = -i(1 + i)^2$ ; число  $1 + i$  простое в силу этого же следствия. Теорема доказана.

## Часть V. Количество представлений

*Начнешь читать с начала и дочитаешь до того места, где совсем ничего не будешь понимать. Потом снова начнешь с начала и будешь так работать с книгой до тех пор, пока не разберешься со всем.*

Совет Ричарда Фейнмана его сестре Джоан

По теореме Ферма–Эйлера любое простое число  $p$ , которое при делении на 4 дает остаток 1, представимо в виде суммы двух квадратов. Давайте докажем, что такое представление единственно с точностью до порядка слагаемых.

**Теорема 9.** *Никакое простое число не может быть представлено в виде суммы квадратов двух целых чисел существенно разными (не получающимися один из другого перестановкой слагаемых) способами.*

**Доказательство.** Если бы простое число  $p$  имело два существенно разных представления,  $p = a^2 + b^2 = c^2 + d^2$ , то разложения  $p = (a + bi)(a - bi) = (c + di)(c - di)$  противоречили бы теореме 7.

В седьмом замечании Пьера Ферма (1601–1665) на полях «Арифметики» Диофанта сказано<sup>1</sup>: «Простое число, которое на единицу превосходит кратное четырех, только один раз является гипотенузой прямоугольного треугольника, его квадрат – два раза, куб – три раза, биквадрат<sup>2</sup> – четыре и т. д. до бесконечности.

<sup>1</sup> См. «Исследования по теории чисел и диофантову анализу», под ред. И. Г. Башмаковой, М., «Наука», 1992 год.

<sup>2</sup> Биквадрат – четвертая степень, квадрато-куб – пятая, кубо-куб – шестая.

Это же простое число и его квадрат только одним способом разлагаются на два квадрата<sup>3</sup>, его куб и биквадрат – двумя, квадрато-куб и кубо-куб – тремя и т. д. до бесконечности.

Если простое число, представимое суммой двух квадратов, умножено на другое простое число, тоже представимое суммой двух квадратов, то произведение дважды представимо суммой двух квадратов; если умножено на квадрат второго простого числа, то произведение трижды представимо суммой двух квадратов; если умножено на куб второго простого числа, то произведение представимо суммой двух квадратов четырежды способами; и так до бесконечности.

...

Пусть надо найти число, которое было бы гипотенузой семью различными способами. Данное число 7 удваиваем, будет 14. Прибавляем единицу, будет 15. Берем все простые делители числа 15: это 3 и 5. Вычитаем из каждого единицу и берем половины остатков; получаем 1 и 2. Возьмем теперь столько различных простых множителей, сколько здесь чисел, а именно два, и перемножим их между собой с показателями 1 и 2, а именно один на квадрат другого; так получаем число, удовлетворяющее условиям задачи, только бы взятые простые множители превосходили кратные четырех на единицу.

...

*А вот метод узнать, сколькими способами данное число может быть составлено из двух квадратов:*

Пусть данное число 325. Его простыми делителями, которые превосходят на единицу кратное четырех, – это 5 и 13; последнее – один раз, а первое – в квадрате. Возьмем показатели 2 и 1. Сложим их произведение и сумму, получится 5; прибавим к нему единицу, получится 6, половина которого – 3. Значит, столькими способами данное число составляется из двух квадратов.

Если бы было три показателя, например, 2, 2, 1, то действовать надо было бы так. Произведение двух первых, сложенное с их суммой, даст 8. Умножаем на третий и прибавляем их сумму, что дает 17. Прибавляем к нему единицу, будет 18; половина есть 9. Столькими способами предложенное число составляется из двух квадратов.

---

<sup>3</sup> Натуральных чисел. Во времена Ферма к отрицательным числам и нулю все еще относились настороженно.

Если последнее число, которое нужно разделить пополам, нечетно, тогда от него следует отнять единицу и взять половину остатка<sup>4</sup>.»

В III веке нашей эры греческий математик Диофант не только знал, что число 65 представимо двумя способами, но и объяснял это тем, что 65 является произведением чисел 13 и 5, каждое из которых – сумма двух квадратов. Комплексных чисел Диофант не знал, иначе он непременно выписал бы разложения  $5 = (2 + i)(2 - i)$ ,  $13 = (3 + 2i)(3 - 2i)$  и продолжил бы свои объяснения следующим образом:

$$\begin{aligned} 65 &= (2 + i)(3 + 2i) \cdot (2 - i)(3 - 2i) = (4 + 7i) \cdot (4 - 7i) = 4^2 + 7^2 = \\ &= (2 + i)(3 - 2i) \cdot (2 - i)(3 + 2i) = (8 - i) \cdot (8 + i) = 8^2 + 1^2. \end{aligned}$$

Понимаете? По-разному группируя множители, получили два разных разложения!

Далее, 25 – наименьшее число, двумя способами представимое в виде суммы квадратов двух целых чисел. Оба эти разложения легко получить, по-разному группируя множители:

$$\begin{aligned} 25 &= (2 + i)^2 \cdot (2 - i)^2 = (3 + 4i) \cdot (3 - 4i) = 3^2 + 4^2 = \\ &= (2 + i)(2 - i) \cdot (2 + i)(2 - i) = 5 \cdot 5 = 5^2 + 0^2. \end{aligned}$$

Последний пример – число 5746. Как мы хорошо знаем, всякому представлению  $5746 = a^2 + b^2$  соответствует разложение  $5746 = (a + bi)(a - bi)$  на сопряженные множители. Поэтому разложим рассматриваемое число сначала на простые натуральные, а затем и на простые гауссовы множители:

$$5746 = 2 \cdot 13^2 \cdot 17 = (1 + i)(1 - i)(3 + 2i)^2 (3 - 2i)^2 (4 + i)(4 - i).$$

Теперь мы должны из нескольких этих множителей составить  $a + bi$ , да так, чтобы произведение остальных множителей равнялось  $a - bi$ . Это нетрудно сделать:

$$a + bi = (1 + i)(3 + 2i)^2 (4 + i) = -45 + 61i,$$

$$a - bi = (1 - i)(3 - 2i)^2 (4 - i) = -45 - 61i.$$

При этом, разумеется,  $45^2 + 61^2 = 2025 + 3721 = 5746$ . Легко найти и еще два варианта:

$$a + bi = (1 + i)(3 + 2i)(3 - 2i)(4 + i) = 39 + 65i$$

или

$$a + bi = (1 + i)(3 - 2i)^2 (4 + i) = 75 - 11i.$$

---

<sup>4</sup> Не удивляйтесь тому, что Ферма не вычитает, а прибавляет единицу: дело в том, что Ферма не признает разложений вида  $n^2 + 0^2$ .

Они приводят к представлениям  $39^2 + 65^2 = 1521 + 4225 = 5746$  и  $75^2 + 11^2 = 5625 + 121 = 5746$ . Никаких других представлений нет (попытайтесь их придумать – и довольно скоро поймете причину этого).

Аналогично можно найти число представлений в виде суммы двух квадратов любого натурального числа  $M = 2^\mu p_1^{a_1} \dots p_r^{a_r} Q$ , где  $p_1, \dots, p_r$  – попарно различные простые числа, каждое из которых дает остаток 1 при делении на 4,  $S$  – число, не имеющее простых делителей кроме тех, которые дают остаток 3 при делении на 4. А именно, если  $S$  не является точным квадратом, то  $n$  не представимо в виде суммы двух квадратов; если же  $S$  – точный квадрат, то, применив необходимое число раз теорему 2, получаем: количество представлений числа  $M$  в виде суммы двух квадратов равно количеству представлений числа  $m = 2^a p_1^{a_1} \dots p_r^{a_r}$  в виде суммы двух квадратов.

На странице 200 русского перевода изданных в 1801 году «Арифметических исследований» К.Ф.Гаусса в подстрочном примечании читаем: «Если  $M = 2^\mu S a^\alpha b^\beta c^\gamma \dots$ , где  $a, b, c, \dots$  обозначают различные простые числа вида  $4n + 1$ , и  $S$  – произведение всех простых сомножителей числа  $M$  вида  $4n + 3$  (в таком виде можно представить любое положительное число, если положить  $\mu = 0$ , когда  $M$  – нечетно, и  $S = 1$ , когда  $M$  не содержит сомножителей вида  $4n + 3$ ), то  $M$  не может быть разложено на два квадрата, если  $S$  не является квадратом. Если же  $S$  есть квадрат, то имеется  $\frac{1}{2}(\alpha + 1)(\beta + 1)(\gamma + 1) \dots$  разложений числа  $M$ , когда хотя бы одно из чисел  $\alpha, \beta, \gamma, \dots$  нечетно, и  $\frac{1}{2}(\alpha + 1)(\beta + 1)(\gamma + 1) \dots + \frac{1}{2}$  разложений, когда  $\alpha, \beta, \gamma, \dots$  все четны.»

Короче, мы можем сформулировать следующую теорему:

**Теорема 10.** *Количество представлений числа  $m$  в виде суммы квадратов двух целых чисел равно  $\left[ \frac{((a_1 + 1) \cdot \dots \cdot (a_r + 1) + 1)}{2} \right]$ . (Если число сомножителей равно 0, то произведение считаем равным 1. Представления, отличающиеся порядком слагаемых, не различаем.)*

Надеемся, доказательство не представит непреодолимой трудности. Если трудности возникли – не огорчайтесь, а перечитайте статью заново (и так много раз – до тех пор, пока не поймете, почему эта формула верна).

## Упражнения

61. При каком наименьшем радиусе окружности с центром в начале координат на ней лежат ровно а) 4 целочисленные точки; б) 8 точек; в) 12; г) 16?

62. а) Число, единственным образом представимое в виде суммы квадратов двух натуральных чисел, не всегда является простым:  $10 = 1^2 + 3^2$  и  $25 = 3^2 + 4^2$ . Каким должен быть радиус окружности с центром в начале координат для того, чтобы на ней лежали ровно четыре точки с натуральными координатами?

б) Сколько решений в натуральных числах  $x < y$  имеет уравнение  $x^2 + y^2 = 5^n$ , где  $n$  – данное натуральное число?

б) Для любого натурального  $n$  существует бесконечно много окружностей с центрами в начале координат, на каждой из которых лежат ровно  $4n$  точек с целыми координатами. Докажите это.

63. Рассмотрим окружность с центром в начале координат радиуса  $\sqrt{2^a p_1^{a_1} \dots p_r^{a_r}}$ , где  $p_1, \dots, p_r$  – попарно различные простые числа, каждое из которых дает остаток 1 при делении на 4. Сколько на этой окружности точек с целыми координатами?

64\*. Может ли так быть, что натуральное число  $n$  не представимо в виде суммы двух квадратов а) целых; б) натуральных, в) взаимно простых чисел, а число  $n^{1999}$  представимо в таком виде?

65\*. Какие числа единственным с точностью до перестановки слагаемых образом представимы в виде суммы квадратов двух а) целых неотрицательных; б) натуральных; в) взаимно простых чисел?

66. Если число  $n > 2$  представимо в виде суммы квадратов двух взаимно простых чисел, то число таких представлений равно  $2^{s-1}$ , где  $s$  – количество простых делителей  $n$ , имеющих вид  $4k + 1$ . Докажите это.

67\*. Количество точек с целыми координатами на окружности радиуса  $\sqrt{n}$  с центром в начале координат (т.е. количество решений в целых числах уравнения  $x^2 + y^2 = n$ ) равно учетверенной разности между количеством натуральных делителей числа  $n$ , которые имеют вид  $4k + 1$ , и количеством натуральных делителей вида  $4k + 3$ . Докажите это.

## Часть VI. Суммы четырех квадратов

**Теорема 11** (Ж.Л.Лагранж). *Любое натуральное число представимо в виде суммы четырех квадратов целых чисел.*

**Доказательство** основано на формуле Эйлера

$$\begin{aligned} & (a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + t^2) = \\ & = (ax + by + cz + dt)^2 + (ay - bx + ct - dz)^2 + (az - bt - cx + dy)^2 + \\ & \quad + (at + bz - cy - dx)^2. \end{aligned}$$

В силу этой формулы произведение сумм четырех квадратов – тоже сумма четырех квадратов. Поэтому достаточно доказать теорему Лагранжа для простых чисел. Очевидно,  $2 = 1^2 + 1^2 + 0^2 + 0^2$ . Пусть  $p$  – нечетное простое число.

**Лемма 7.** *Существуют такие целые числа  $x$  и  $y$ , что  $x^2 + y^2 + 1$  кратно  $p$ .*

**Доказательство.** Рассмотрим числа  $0^2, 1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$ . Если какие-то два из них дают один и тот же остаток при делении на  $p$ , т.е. если  $x^2 \equiv y^2 \pmod{p}$ , где  $0 \leq x < y \leq (p-1)/2$ , то число  $(x-y)(x+y) = x^2 - y^2$  кратно  $p$ . Но ни разность  $x - y$ , ни сумма  $x + y$  не кратна  $p$ .

Следовательно, рассматриваемые числа дают разные остатки при делении на  $p$ . Рассмотрим теперь еще  $(p+1)/2$  чисел:  $-1 - 0^2, -1 - 1^2, -1 - 2^2, \dots, -1 - \left(\frac{p-1}{2}\right)^2$ . Они тоже дают разные остатки. Поскольку всего возможных остатков от деления на  $p$  существует  $p$  штук, а в каждом из рассматриваемых нами множеств  $(p+1)/2$  элементов, то хотя бы одно из чисел вида  $x^2$  дает при делении на  $p$  такой же остаток, как и некоторое число вида  $-1 - y^2$ . Значит,

$$x^2 \equiv -1 - y^2 \pmod{p},$$

что и требовалось доказать:  $x^2 + y^2 + 1 \equiv 0 \pmod{p}$ .

Числа  $x$  и  $y$ , как мы помним, не превосходят  $(p-1)/2$ , поэтому

$$x^2 + y^2 + 1 < \left(\frac{p}{2}\right)^2 + \left(\frac{p}{2}\right)^2 + 1 < p^2.$$

При этом  $x^2 + y^2 + 1^2 + 0^2 = pm$ , где  $m < p$ .

Мы хотим доказать, что число  $p$  представимо в виде суммы четырех квадратов целых чисел. Рассмотрим наименьшее натуральное число  $m$ , для которого существуют такие целые числа  $x, y, z, t$ , что

$$x^2 + y^2 + z^2 + t^2 = pm.$$

Как мы уже знаем,  $m < p$ . Докажем равенство  $m = 1$  методом бесконечного спуска: предположим, что  $m > 1$ , и докажем, что в таком случае  $m$  – не наименьшее.

Пусть  $m$  четно. Тогда числа  $x, y, z, t$  либо все четны, либо все нечетны, либо два из них (для определенности, пусть это  $x$

и  $y$ ) четны, а два ( $z$  и  $t$ ) – нечетны. В любом случае формула

$$\left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+t}{2}\right)^2 + \left(\frac{z-t}{2}\right)^2 = \\ = \frac{x^2 + y^2 + z^2 + t^2}{2} = \frac{pm}{2}$$

показывает, что  $m$  – не наименьшее возможное.

Пусть  $m$  нечетно. Рассмотрим остатки  $a, b, c, d$  от деления чисел  $x, y, z, t$  на  $m$ . Хотя бы один из них отличен от 0: в противном случае сумма квадратов  $pm = x^2 + y^2 + z^2 + t^2$  делилась бы на  $m^2$  и (простое!) число  $p$  делилось бы на  $m$ , хотя  $1 < m < p$ .

Можно считать, что числа  $a, b, c, d$  не превосходят  $(m-1)/2$ . (Если, например, величина  $a$  окажется равна  $(m+1)/2$  или больше, то можно заменить  $x$  на противоположное ему число  $-x$ . При этом вместо  $a$  получим остаток

$$m - a \leq m - \frac{m+1}{2} = \frac{m-1}{2}.)$$

Обозначим  $n = a^2 + b^2 + c^2 + d^2$ . Поскольку

$$a^2 + b^2 + c^2 + d^2 \equiv x^2 + y^2 + z^2 + t^2 = pm \equiv 0 \pmod{m},$$

то  $n \equiv 0 \pmod{m}$ , так что  $n = mk$ , где  $k$  – натуральное число. Поскольку все числа  $a, b, c, d$  меньше  $m/2$ , имеем:

$$mk = a^2 + b^2 + c^2 + d^2 < 4 \cdot \left(\frac{m}{2}\right)^2 = m^2.$$

Следовательно,  $k < m$ . Применим формулу Эйлера:

$$(ax + by + cz + dt)^2 + \\ + (ay - bx + ct - dz)^2 + (az - bt - cx + dy)^2 + (at + bz - cy - dx)^2 = \\ = (a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + t^2) = npt = m^2pk.$$

Как мы помним,  $x \equiv a$ ,  $y \equiv b$ ,  $z \equiv c$  и  $t \equiv d \pmod{m}$ . Поэтому по модулю  $m$  имеем:

$$ax + by + cz + dt \equiv x^2 + y^2 + z^2 + t^2 = pm \equiv 0,$$

$$ay - bx + ct - dz \equiv xy - yx + zt - tz = 0,$$

$$az - bt - cx + dy \equiv xz - yt - zx + ty = 0,$$

$$at + bz - cy - dx \equiv xt + yz - zy - tx = 0.$$

Итак, все числа  $ax + by + cz + dt$ ,  $ay - bx + ct - dz$ ,  $az -$

$-bt - cx + dy$  и  $at + bz - cy - dx$  кратны  $m$ ; формула

$$pk = \left( \frac{ax + by + cz + dt}{m} \right)^2 + \left( \frac{ay - bx + ct - dz}{m} \right)^2 + \left( \frac{az - bt - cx + dy}{m} \right)^2 + \left( \frac{at + bz - cy - dx}{m} \right)^2$$

представляет число  $pk$  в виде суммы четырех квадратов целых чисел. Таким образом, число  $m$  не является наименьшим возможным. Теорема Лагранжа доказана.

Карл Густав Якоб Якоби (1804–1851) при помощи теории эллиптических функций доказал, что для любого натурального  $n$  количество решений уравнения  $x^2 + y^2 + z^2 + t^2 = n$  в целых числах равно сумме всех нечетных делителей числа  $n$ , умноженной на 24 для четного  $n$  и на 8 – для нечетного.

### Кватернионы

Формула Эйлера, представляющая произведение двух сумм четырех квадратов в виде суммы четырех квадратов, выглядит весьма устрашающе. Однако мы помним, что формула, представляющая произведение двух сумм двух квадратов в виде суммы двух квадратов, по сути означает, что произведение модулей комплексных чисел равно модулю их произведения. Ровно такова ситуация и для формулы Эйлера: произведение модулей кватернионов равно модулю их произведения!

Что такое кватернионы? Комплексные числа получают, присоединяя к множеству вещественных чисел мнимую единицу  $i$ , квадрат которой равен  $-1$ . Кватернионы можно получить аналогично, присоединив к множеству  $\mathbb{C}$  комплексных чисел мнимую единицу  $j$ , обладающую свойствами  $j^2 = -1$  и  $zj = j\bar{z}$  для любого комплексного числа  $z$ . Сумму кватернионов  $z_1 + w_1j$  и  $z_2 + w_2j$  определяем формулой  $(z_1 + z_2) + (w_1 + w_2)j$ , а произведение – формулой  $(z_1z_2 - w_1\bar{w}_2) + (z_1w_2 + w_1\bar{z}_2)j$ .

Нетрудно убедиться, что алгебра кватернионов является телом, т.е. ассоциативна и не имеет делителей нуля (произведение любых двух ее ненулевых элементов не равно нулю). Обозначив  $ij = k$  и представив комплексные числа  $z$  и  $w$  в виде  $z = a + bi$  и  $w = c + di$ , где  $a, b, c$  и  $d \in \mathbb{R}$ , приходим к формуле  $z + wj = a + bi + cj + dk$ .



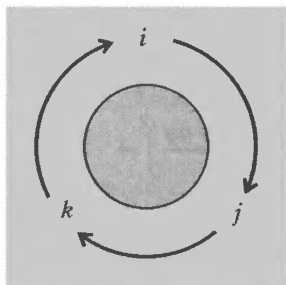


Рис. 20

Правила умножения запомнить легко (рис.20):  $i^2 = j^2 = k^2 = -1$ ,  $ij = k$ ,  $jk = i$ ,  $ki = j$  и, если идти не по часовой стрелке, а против нее,  $ji = -k$ ,  $kj = -i$  и  $ik = -j$ .

Обозначим векторы  $(1; 0; 0)$ ,  $(0; 1; 0)$  и  $(0; 0; 1)$  буквами  $i$ ,  $j$  и  $k$  соответственно. Тогда кватернион  $a + bi + cj + dk$  является суммой числа  $a$  и вектора  $\vec{v} = bi + cj + dk$ . А произведение кватернионов  $a_1 + \vec{v}_1$  и  $a_2 + \vec{v}_2$  равно  $a_1 a_2 - \vec{v}_1 \vec{v}_2 + a_1 \vec{v}_2 + [\vec{v}_1, \vec{v}_2] + a_2 \vec{v}_1$ , где  $\vec{v}_1 \vec{v}_2$  – скалярное произведение векторов  $\vec{v}_1$  и  $\vec{v}_2$ , а  $[\vec{v}_1, \vec{v}_2]$  – их векторное произведение, т.е. вектор, перпендикулярный векторам  $\vec{v}_1$  и  $\vec{v}_2$

и обладающий следующими свойствами: его длина равна площади параллелограмма, натянутого на векторы  $\vec{v}_1$  и  $\vec{v}_2$ , а направлен он так, что тройка векторов  $\vec{v}_1$ ,  $\vec{v}_2$  и  $[\vec{v}_1, \vec{v}_2]$  ориентирована так же, как тройка  $i, j, k$  (рис.21).

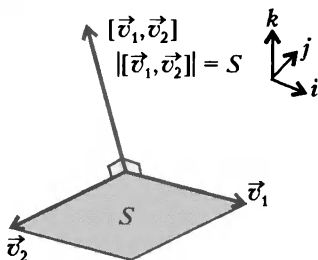


Рис. 21

Сопряженным кватерниона  $u = a + bi + cj + dk$  называют кватернион  $\bar{u} = a - bi - cj - dk$ .

Модуль кватерниона – это число

$|u| = \sqrt{u\bar{u}} = \sqrt{a^2 + b^2 + c^2 + d^2}$ . Для любых двух кватернионов  $u$  и  $v$  имеем

$$|uv| = \sqrt{uv\bar{u}\bar{v}} = \sqrt{uv\bar{v}\bar{u}} = \sqrt{u|v|^2\bar{u}} = |v|\sqrt{u\bar{u}} = |u| \cdot |v|.$$

Модуль произведения двух кватернионов равен произведению их модулей; это по сути и есть формула Эйлера.

## Часть I. Примеры

*Всякое уравнение, имеющее несколько переменных, подлежит исследованию теории чисел. Но не все они одинаково доступны исследованию и не все имеют одинаковую важность по приложениям своим. Теория чисел до сих пор ограничивается только рассмотрением уравнений, наиболее простых и в то же время имеющих наиболее важные приложения.*

П.Л.Чебышёв

Напишем уравнение и спросим, имеет ли оно решение в целых числах, – получится задача. Скорее всего, если уравнение взято «просто так», эта задача будет очень трудной или вообще не поддастся решению, а главное, не будет никому интересна. Но есть уравнения, знакомство с которыми неизбежно и в высшей степени полезно для всякого, кто интересуется математикой. Именно таковы уравнения Пелля:

$$x^2 - dy^2 = 1,$$

где  $d$  – натуральное число, не являющееся точным квадратом.

Почему «не являющееся точным квадратом»? Потому что левую часть уравнения  $x^2 - a^2y^2 = 1$ , где  $a$  – натуральное число, можно разложить на множители:

$$(x - ay)(x + ay) = 1.$$

Число 1 представимо в виде произведения двух целых чисел двумя способами:  $1 \cdot 1$  и  $-1 \cdot (-1)$ . В первом случае  $x - ay = 1$  и  $x + ay = 1$ , откуда  $x = 1$  и  $y = 0$ . Во втором случае  $x - ay = -1$  и  $x + ay = -1$ , откуда  $x = -1$  и  $y = 0$ .

Итак, решить уравнение  $x^2 - a^2y^2 = 1$  очень легко: достаточно разложить на множители разность квадратов. Действительно поразительные эффекты обнаружатся, когда  $d$  – натуральное число, не являющееся квадратом.

Уравнениями Пелля можно заниматься по-разному. Что-то может понять даже семиклассник, только что изучивший формулы сокращенного умножения. Интересны эти уравнения и для студента мехмата МГУ – например, очень важная для математики 10-я проблема Гильберта, поставленная в августе 1900-го года

в докладе на Международном математическом конгрессе в Париже, была решена в 1970 году Ю.В.Матиясевичем при помощи уравнений типа уравнений Пелля.

Мы расскажем как о самых простых свойствах решений уравнений Пелля, так и о серьезных и трудных теоремах и задачах, связанных с этими замечательными уравнениями. История их изучения длится несколько сотен лет. Тем интереснее заметить, что в 2008 году австралиец Вайлдбергер придумал удивительно прозрачное доказательство важнейшего свойства уравнений Пелля: для любого не являющегося квадратом натурального числа  $d$  уравнение  $x^2 - dy^2 = 1$  имеет решение в натуральных числах  $x$  и  $y$ . Доказательство Вайлдбергера настолько естественное, что теперь многие удивляются, почему они сами это не придумали!

### Упражнения

1. Квадрат разрезан на 35 квадратов размером  $1 \times 1$  и один квадрат большего размера. Какого именно?

2. Несколько кошек съели 999919 мышек, причем все кошки съели по одинаковому числу мышек. Сколько было кошек, если каждая кошка съела больше мышек, чем было кошек?

3. Решите в целых числах уравнения а)  $x^2 + 2xy - 3y^2 = 20$  ;  
б)  $6x^2 - xy - 12y^2 = 14$  .

4. Какие числа представимы в виде а)  $x^2 - y^2$  ; б)  $x^2 + 2xy$  ;  
в)  $x^2 + 4xy$  . где  $x, y$  – целые числа?

5. Сколько решений в целых числах имеет уравнение а)  $x^2 - y^2 = 2^{100}$  ;  
б)  $x^2 - y^2 = p^{100}$  , где  $p$  – простое число,  $p > 2$  ; в)  $x^2 - 9y^2 = 1000000$  ?

6. Числа  $144 = 12^2$  и  $441 = 21^2$  после зачеркивания двух последних цифр превращаются в  $1 = 1^2$  и  $4 = 2^2$  . Найдите наибольший из таких квадратов натуральных чисел, которые не делятся на 10 и остаются квадратами после вычеркивания а) двух; б) четырех; в)  $2n$  последних цифр.

7. Существуют ли такие натуральные числа  $x$  и  $y$ , что  $x^2 + y$  и  $y^2 + x$  – квадраты целых чисел?

8. Сумма квадратов 25 последовательных целых чисел может быть квадратом целого числа, а сумма 25 квадратов натуральных чисел – не может. Докажите это.

9. Найдите наибольшее целое число  $x$ , для которого  $4^{27} + 4^{1000} + 4^x$  является квадратом целого числа.

10. Решите в целых числах уравнения а)  $x(x + 1) = 4y(y + 1)$  ;  
б)  $x(x + 1)(x + 7)(x + 8) = y^2$  ; в)  $x^2 + x = y^4 + y^3 + y^2 + y$  ;  
г)  $1 + x + x^2 + x^3 + x^4 = y^2$  ; д)  $x^2 + xy + y^2 = x^2y^2$  ; е)  $(x + 2)^4 - x^4 = y^3$  .

11. Если натуральные числа  $m$  и  $n$  удовлетворяют равенству

$2m^2 + m = 3n^2 + n$ , то числа а)  $m - n$ ; б)  $2m + 2n + 1$ ; в)  $3m + 3n + 1$  являются квадратами целых чисел. Докажите это.

12. Пусть  $p$  – простое число и  $x^2 - py^2 = 1$ , где  $x, y$  – натуральные числа. Докажите, что если  $x$  (не)четно, то одно из чисел  $x - 1$  или  $x + 1$  является (удвоенным) квадратом.

**Уравнение  $x^2 - 2y^2 = \pm 1$**

Рассмотрим уравнение  $x^2 - 2y^2 = \pm 1$  (рис.1). Не удивляйтесь тому, что в правой части не 1, а  $\pm 1$ : так легко догадаться до закономерности, о которой вскоре пойдет речь.

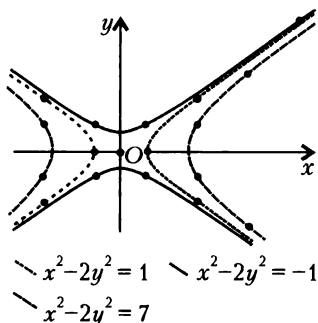


Рис. 1

Подбором найдем несколько решений:  $(x; y) = (1; 0)$ ,  $(1; 1)$  или  $(3; 2)$ . Продолжая вычисления, составим таблицу:

$x$	1	1	3	7	17	41	99	239
$y$	0	1	2	5	12	29	70	169
$x^2 - 2y^2$	1	-1	1	-1	1	-1	1	-1

Если присмотреться, то можно заметить, что каждый следующий столбец получается из предыдущего по простому правилу: «новое» значение  $Y$  есть сумма «старых»  $x$  и  $y$ , а «новое» значение  $X$  есть сумма «старого» и «нового» значений  $y$ . Точнее,

$$\begin{cases} X = x + 2y, \\ Y = x + y. \end{cases}$$

Конечно, таблицы с несколькими первыми решениями недостаточны для того, чтобы быть уверенным в справедливости этих формул для всего множества решений уравнения; мы должны доказать следующие утверждения.

**Теорема 1.** Если  $x^2 - 2y^2 = \pm 1$ , то пара чисел  $(X; Y) = (x + 2y; x + y)$  удовлетворяет равенству  $X^2 - 2Y^2 = \mp 1$ .

**Следствие.** Уравнение  $x^2 - 2y^2 = \pm 1$  имеет бесконечно много решений в натуральных числах.

**Теорема 2.** Уравнение  $x^2 - 2y^2 = \pm 1$  не имеет решений в целых неотрицательных числах кроме тех, что получаются из «тривиального» решения  $(1; 0)$  при помощи (возможно, многократного примененного) правила  $(x; y) \rightarrow (x + 2y; x + y)$ .

Доказать теорему 1 очень легко: достаточно подставить значения  $X$  и  $Y$  вместо  $x$  и  $y$ . А именно,

$$\begin{aligned}(x + 2y)^2 - 2(x + y)^2 &= x^2 + 4xy + 4y^2 - 2(x^2 + 2xy + y^2) = \\ &= 2y^2 - x^2 = -(x^2 - 2y^2).\end{aligned}$$

Как видите, если  $x^2 - 2y^2 = \pm 1$ , то  $X^2 - 2Y^2 = \mp 1$ . Теорема 1 доказана, мы научились строить «новое» решение из «старого».

А вот доказательство теоремы 2 хотя и не очень сложно, но требует привлечения идеи, которая слишком важна, чтобы говорить о ней мимоходом. Поэтому мы займемся этим позже, а пока разберем еще несколько примеров.

### Упражнения

**13.** Рассмотрим последовательности  $x_0 = 1$ ,  $x_1 = 1$ ,  $x_2 = 3$ ,  $x_3 = 7$ ,  $x_4 = 17$ , ... и  $y_0 = 0$ ,  $y_1 = 1$ ,  $y_2 = 2$ ,  $y_3 = 5$ ,  $y_4 = 12$ , ..., заданные своими первыми членами  $x_0 = 1$ ,  $y_0 = 1$  и рекуррентными соотношениями  $x_{n+1} = x_n + 2y_n$  и  $y_{n+1} = x_n + y_n$ . Докажите равенства  $x_{n+2} = 2x_{n+1} + x_n$  и  $y_{n+2} = 2y_{n+1} + y_n$ .

**14.** По правилам новомодного танца надо делать либо шаг вперед, либо два шага вперед, либо два шага вперед и сразу же — шаг назад. Сколькими способами танцор может за несколько таких па сдвинуться на 7 шагов от исходного рубежа?

$$\text{Уравнение } x^2 + (x + 1)^2 = y^2$$

Прямоугольный треугольник со сторонами 3, 4 и 5 обладает тем свойством, что один из его катетов на 1 длиннее другого. Много ли еще таких треугольников, точнее, много ли решений в натуральных числах имеет уравнение  $x^2 + (x + 1)^2 = y^2$ ? Чтобы ответить на этот вопрос, раскроем скобки и приведем подобные:

$$2x^2 + 2x + 1 = y^2.$$

Теперь, домножив обе части на 2, выделим полный квадрат:

$$(2x + 1)^2 + 1 = 2y^2.$$

Обозначая  $z = 2x + 1$ , получаем уравнение

$$z^2 - 2y^2 = -1.$$

Любое удовлетворяющее ему число  $z$  нечетно. Таким образом, мы свели задачу к уравнению  $z^2 - 2y^2 = -1$ , где  $y, z$  — натуральные числа, причем  $z > 1$ .

Как вы помните, если  $z^2 - 2y^2 = -1$ , то

$$(z + 2y)^2 - 2(z + y)^2 = 1.$$

В правой части теперь 1, а не  $-1$ . Мы умеем переходить от 1 к  $-1$ : для любого решения  $(a; b)$  уравнения  $a^2 - 2b^2 = 1$  выполнено равенство

$$(a + 2b)^2 - 2(a + b)^2 = -1.$$

Следовательно, из любой пары натуральных чисел  $(z; y)$ , удовлетворяющей равенству  $z^2 - 2y^2 = -1$ , мы можем получить новую пару:

$$Z = (z + 2y) + 2(z + y) = 3z + 4y,$$

$$Y = (z + 2y) + (z + y) = 2z + 3y,$$

удовлетворяющую равенству  $Z^2 - 2Y^2 = -1$ . Давайте проверим это:

$$(3z + 4y)^2 - 2(2z + 3y)^2 =$$

$$= 9z^2 + 24zy + 16y^2 - 2(4z^2 + 12zy + 9y^2) = z^2 - 2y^2.$$

(Логической необходимости в последней проверке нет. Но, согласитесь, приятно убедиться, что мы не ошиблись в вычислениях.)

### Упражнения

15. а) Найдите некоторые три решения в натуральных числах уравнения  $x^2 + (x + 1)^2 = y^2$ . б) Придумайте такие натуральные числа  $a, b, c, d, e, f$ , что для всякого решения  $x, y$  уравнения  $x^2 + (x + 1)^2 = y^2$  верно равенство  $(ax + by + c)^2 + (ax + by + c + 1)^2 = (dx + ey + f)^2$ .

16. Существует бесконечно много различных прямоугольных треугольников, каждый из которых обладает следующими свойствами: длины сторон — целые числа, длина гипотенузы — квадрат целого числа, а один из катетов на единицу короче гипотенузы. Докажите это.

$$\text{Уравнение } x^2 - 2y^2 = 1$$

При помощи многократно примененного перехода  $(x; y) \rightarrow (3x + 4y; 2x + 3y)$  из решения  $(1; 0)$  получаются решения  $(3; 2), (17; 12), (99; 70), \dots$  уравнения  $x^2 - 2y^2 = 1$ .

Например,

$$99 = 3 \cdot 17 + 4 \cdot 12,$$

$$70 = 2 \cdot 17 + 3 \cdot 12.$$

Таким образом, уравнение  $x^2 - 2y^2 = 1$ , как и уравнение  $x^2 - 2y^2 = -1$ , имеет бесконечно много решений в натуральных числах. Если бы мы уже доказали теорему 2, то могли бы утверждать, что эти уравнения не имеют никаких других решений в целых неотрицательных числах, кроме получаемых из «начального» решения  $(x; y) = (1; 0)$  или  $(1; 1)$  при помощи правила  $(x; y) \rightarrow (3x + 4y; 2x + 3y)$ . Но пока теорема 2 не доказана, торопиться с этим не будем.

### Упражнения

17. Существует ли такой многочлен  $f$  второй степени, что среди его значений  $f(n)$ , где  $n$  – натуральное число, имеется бесконечно много квадратов натуральных чисел, а сам многочлен  $f$  не является квадратом никакого другого многочлена?

18. Рассмотрим последовательности  $x_0 = 1$ ,  $x_1 = 3$ ,  $x_2 = 17$ ,  $x_3 = 99$ , ... и  $y_0 = 0$ ,  $y_1 = 2$ ,  $y_2 = 12$ ,  $y_3 = 70$ , ..., заданные своими начальными членами  $x_0 = 1$ ,  $y_0 = 0$  и рекуррентными соотношениями  $x_{n+1} = 3x_n + 4y_n$ ,  $y_{n+1} = 2x_n + 3y_n$ . Найдите такие числа  $a$  и  $b$ , что для любого натурального  $n$  верны равенства  $x_{n+1} = ax_n + bx_{n-1}$  и  $y_{n+1} = ay_n + by_{n-1}$ .

### Уравнение $x^2 - 2y^2 = 7$

Правило  $(x; y) \rightarrow (3x + 4y; 2x + 3y)$  позволяет из одного решения уравнения  $x^2 - 2y^2 = 7$  получить другое решение. Так, из решения  $(x; y) = (3; 1)$  получаем  $(3 \cdot 3 + 4 \cdot 1; 2 \cdot 3 + 3 \cdot 1) = (13; 9)$ , из которого получаем  $(3 \cdot 13 + 4 \cdot 9; 2 \cdot 13 + 3 \cdot 9) = (75; 53)$ , из которого можно получить еще одно решение, и так далее.

Привычная ситуация, скажете вы? Решения уравнения  $x^2 - 2y^2 = 1$  получались из «начального» решения  $(1; 0)$  при помощи этого же правила  $(x; y) \rightarrow (3x + 4y; 2x + 3y)$ , так что ничего нового нет? Не торопитесь:

$$5^2 - 2 \cdot 3^2 = 7.$$

Решение  $(5; 3)$  не входит в цепочку

$$(3; 1) \rightarrow (13; 9) \rightarrow (75; 53) \rightarrow \dots,$$

а порождает свою цепочку:

$$(5; 3) \rightarrow (3 \cdot 5 + 4 \cdot 3; 2 \cdot 5 + 3 \cdot 3) = \\ = (27; 19) \rightarrow (3 \cdot 27 + 4 \cdot 19; 2 \cdot 27 + 3 \cdot 19) = (157; 111) \rightarrow \dots$$

Других цепочек нет. Точнее говоря, верна следующая теорема.

**Теорема 3.** Уравнение  $x^2 - 2y^2 = 7$  не имеет решений в целых неотрицательных числах, кроме тех, что получаются из одного из двух «начальных» решений  $(3; 1)$  и  $(5; 3)$  при помощи правила  $(x; y) \rightarrow (3x + 4y; 2x + 3y)$ .

Доказательство примерно такое же, как и доказательство теоремы 2. Отложив его на будущее, продолжим рассмотрение примеров.

$$\text{Уравнение } x^2 - 3y^2 = \pm 1$$

Пара  $(x; y) = (1; 0)$  удовлетворяет любому уравнению  $x^2 - dy^2 = 1$ . Подбором легко найти решение  $x = 2$  и  $y = 1$  уравнения

$$x^2 - 3y^2 = 1.$$

Можно найти и решение  $(x; y) = (7; 4)$ , а затем и  $(26; 15)$ . Возможны и дальнейшие вычисления (особенно если есть калькулятор или компьютер). Они приводят к решению  $(97; 56)$ .

Здесь явно пора остановиться и подумать. Мы не нашли ни одного решения уравнения

$$x^2 - 3y^2 = -1.$$

И не потому, что плохо искали, а потому, что их нет. В самом деле, рассмотрим остаток от деления на 3 левой части уравнения  $x^2 - 3y^2 = -1$ . Поскольку  $3y^2$  делится на 3, искомым остатком совпадает с остатком от деления числа  $x^2$  на 3. Число  $x$  можно представить одной из трех формул:  $x = 3k$  (если  $x$  делится на 3),  $x = 3k + 1$  (если  $x$  при делении на 3 дает остаток 1) или, наконец,  $x = 3k + 2$  (если остаток равен 2). При этом  $x^2 = 9k^2$ ,  $9k^2 + 6k + 1$  или  $9k^2 + 12k + 4$ . Остаток от деления на 3 в первом случае равен 0, а в двух других случаях остаток равен 1.

Итак, левая часть уравнения  $x^2 - 3y^2 = -1$  при делении на 3 дает остаток 0 или 1, а правая — остаток 2. Мы доказали, что уравнение  $x^2 - 3y^2 = -1$  не имеет решений в целых числах.

**Упражнение 19.** Может ли сумма квадратов а) трех; б) четырех; в) пяти; г) шести; д) семи; е) восьми; ж) девяти; з) десяти; и) двенадцати последовательных целых чисел быть квадратом целого числа?



### Уравнение $x^2 - 3y^2 = 1$

Уравнение  $x^2 - 3y^2 = 1$  имеет бесконечно много решений в натуральных числах. Чтобы доказать это, мы, как и в теореме 1, укажем формулы, которые из решения  $(x; y)$  строят новое решение  $(X; Y)$ . А именно, пару  $(1; 0)$  эти формулы преобразуют в  $(2; 1)$ , пару  $(2; 1)$  – в  $(7; 4)$ , которую, в свою очередь, они преобразуют в  $(26; 15)$ . Следующая пара, как помните,  $(97; 56)$ .

Что же это за формулы? Немного терпения и удачи, и вы заметите, что  $97 = 2 \cdot 26 + 3 \cdot 15$  и  $6 = 26 + 2 \cdot 15$ .

**Теорема 4.** Если  $x^2 - 3y^2 = 1$ , то пара чисел  $(X; Y) = (2x + 3y; x + 2y)$  удовлетворяет равенству  $X^2 - 3Y^2 = 1$ .

**Теорема 5.** Уравнение  $x^2 - 3y^2 = 1$  не имеет решений в целых неотрицательных числах, кроме тех, что получаются из «тривиального» решения  $(1; 0)$  при помощи правила  $(x; y) \rightarrow (2x + 3y; x + 2y)$ .

Доказательство теоремы 5 отложим на будущее, а теорему 4 докажем:

$$(2x + 3y)^2 - 3(x + 2y)^2 = \\ = 4x^2 + 12xy + 9y^2 - 3(x^2 + 4xy + 4y^2) = x^2 - 3y^2 = 1.$$

Интересно, что мы будем делать, когда  $d$  будет не таким маленьким и догадаться до правила, которое «размножает» решения, будет сложно? Да и всегда ли такое правило существует?

Ответ: всегда, но простое доказательство этого придумано только в 2008 году. Вы ознакомьтесь с ним, когда дочитаете эту главу до доказательства Вайлдбергера теоремы 10. А пока посмотрим, как при решении уравнений Пелля можно использовать иррациональные числа.

### Степени числа $1 + \sqrt{2}$

Если  $d$  не является квадратом натурального числа, то в разложении

$$x^2 - dy^2 = (x - y\sqrt{d})(x + y\sqrt{d})$$

участвует иррациональное число  $\sqrt{d}$ . Казалось бы, мы решаем уравнения в целых числах; зачем нам иррациональности? Но заметьте:

$$(1 + \sqrt{2})^2 = 1 + 2\sqrt{2} + 2 = 3 + 2\sqrt{2}; \\ (1 + \sqrt{2})^3 = 1 + 3\sqrt{2} + 3 \cdot 2 + 2\sqrt{2} = 7 + 5\sqrt{2}.$$

Узнали? Это же решения (3; 2) и (7; 5) уравнения  $x^2 - 2y^2 = \pm 1$  ! Если не убедили два примера, вот еще один:

$$(1 + \sqrt{2})^4 = (1 + \sqrt{2})^3 (1 + \sqrt{2}) = (7 + 5\sqrt{2})(1 + \sqrt{2}) = 17 + 12\sqrt{2}.$$

Впрочем, это всего лишь примеры. Чтобы получить доказательство, посмотрим, что происходит при переходе от  $n$ -й степени числа  $1 + \sqrt{2}$  к  $(n + 1)$ -й. Пусть  $(1 + \sqrt{2})^n = x_n + y_n \sqrt{2}$ , где  $x_n$  и  $y_n$  — натуральные числа. Тогда

$$\begin{aligned}(1 + \sqrt{2})^{n+1} &= (1 + \sqrt{2})^n (1 + \sqrt{2}) = (x_n + y_n \sqrt{2})(1 + \sqrt{2}) = \\ &= x_n + y_n \sqrt{2} + x_n \sqrt{2} + 2y_n = (x_n + 2y_n) + (x_n + y_n) \sqrt{2},\end{aligned}$$

так что  $x_{n+1} = x_n + 2y_n$  и  $y_{n+1} = x_n + y_n$ . Знакомые формулы, не правда ли?

Выясним, что будет, если возводить в степень не  $1 + \sqrt{2}$ , а  $1 - \sqrt{2}$ . Смотрите:

$$(1 - \sqrt{2})^2 = 3 - 2\sqrt{2},$$

$$(1 - \sqrt{2})^3 = 7 - 5\sqrt{2},$$

$$(1 - \sqrt{2})^4 = 17 - 12\sqrt{2},$$

и вообще,  $(1 - \sqrt{2})^n = x_n - y_n \sqrt{2}$ . Это легко доказать по индукции:

$$\begin{aligned}(1 - \sqrt{2})^{n+1} &= (1 - \sqrt{2})^n (1 - \sqrt{2}) = (x_n - y_n \sqrt{2})(1 - \sqrt{2}) = \\ &= x_n - y_n \sqrt{2} - x_n \sqrt{2} + 2y_n = (x_n + 2y_n) - (x_n + y_n) \sqrt{2}.\end{aligned}$$

А можно обойтись и без индукции, заметив, что при возведении числа  $1 + \sqrt{2}$  в степень мы используем равенство  $(\sqrt{2})^2 = 2$ ; но число  $(-\sqrt{2})^2$  тоже равно 2.

Подобные соображения в алгебре используют часто, есть даже термин: *сопряженные числа*. В полной общности это важное понятие нам не понадобится. Поэтому пока просто скажем, что для каждого числа вида  $a + b\sqrt{2}$ , где  $a, b$  — рациональные числа, сопряженным числом называют  $a - b\sqrt{2}$ . Если вы знаете, что такое комплексные числа, и помните, что для любого комплексного числа  $a + bi$  сопряженное — это  $a - bi$ , не удивляйтесь использованию одного и того же слова для разных целей: если бы мы подробно рассказали о сопряженных числах, то все стало бы абсолютно ясно. Но это, к сожалению, слишком отвлекло бы нас от основной темы.

Тем не менее, для нас важно следующее свойство: *сопряженное к сумме (разности, произведению, частному) двух чисел равно сумме (разности, произведению, частному) сопряженных к ним*. Например, вот как выглядит это для сложения:

$$(a + c) - (b + d)\sqrt{2} = (a - b\sqrt{2}) + (c - d\sqrt{2}).$$

Чуть больших усилий потребует от нас проверка этого свойства для умножения. (Строго говоря, надо бы еще разобраться с разностью и частным, но не будем тратить на это силы: вы легко сделаете это самостоятельно.) Прежде всего вычислим произведение

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}.$$

Значит, сопряженное к произведению равно  $(ac + 2bd) - (ad + bc)\sqrt{2}$ . А произведение сопряженных равно  $(a - b\sqrt{2})(c - d\sqrt{2}) = (ac + 2bd) - (ad + bc)\sqrt{2}$ ; как и следовало ожидать.

Отображение  $a + b\sqrt{2} \mapsto a - b\sqrt{2}$  называют *автоморфизмом* поля  $\mathbb{Q}[\sqrt{2}]$ . А произведение

$$(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$$

называют *нормой* числа  $a + b\sqrt{2}$ . Многое из того, что мы расскажем об уравнениях Пелля, можно перенести на случай так называемого норменного уравнения в полях алгебраических чисел. Но мы слишком увлеклись. Порекомендовав заинтересованному читателю когда-нибудь изучить «Теорию чисел» З.И.Боревича и И.Р.Шафаревича и ей подобные книги, вернемся к нашим делам.

**Упражнение 20.** Пусть  $a, b$  – целые числа,  $d$  – натуральное число, не являющееся квадратом,  $x + y\sqrt{d} = \frac{1}{a + b\sqrt{d}}$ , причем  $x, y$  – рациональные числа. Докажите, что числа  $x$  и  $y$  целые в тех и только тех случаях, когда  $a^2 - db^2 = \pm 1$ .

Сложив равенства

$$(1 + \sqrt{2})^n = x_n + y_n\sqrt{2}, \quad (1 - \sqrt{2})^n = x_n - y_n\sqrt{2}$$

и поделив на 2, находим

$$x_n = \frac{(1 + \sqrt{2})^n + (1 - \sqrt{2})^n}{2}.$$

А если не сложить, а вычесть, то получим

$$y_n = \frac{(1 + \sqrt{2})^n - (1 - \sqrt{2})^n}{2\sqrt{2}}.$$

Это и есть не рекуррентные (когда каждую следующую пару получаем из предыдущей), а явные формулы решений уравнения  $x^2 - 2y^2 = \pm 1$  в натуральных числах. Заметьте: натураль-

ные  $x_n$  и  $y_n$  получаются из формул, в которые входит иррациональное число  $\sqrt{2}$  !

### Упражнения

21. а) Докажите равенства  $x_{2n} = 2x_n^2 - (-1)^n$  и  $y_{2n} = 2x_n y_n$ .

б) Если  $d$  – натуральное число, не являющееся квадратом, а  $z$  и  $t$  – натуральные числа, удовлетворяющие равенству  $z^2 - dt^2 = 1$ , то натуральные числа  $a_n$  и  $b_n$ , определенные формулой  $a_n + b_n \sqrt{d} = (z + t\sqrt{d})^n$ , обладают тем свойством, что  $a_{2n} = 2a_n^2 - 1$  и  $b_{2n} = 2a_n b_n$ . Докажите это.

22. а) Для любого натурального  $n$  число  $(1 + \sqrt{2})^n$  представимо в виде  $\sqrt{k} + \sqrt{k+1}$ , где  $k$  – натуральное число. Докажите это.

б) (М1522) Для любых натуральных  $m, d, n$  существует такое натуральное  $k$ , что  $(\sqrt{m} + \sqrt{m+d})^n = \sqrt{k} + \sqrt{k+d^n}$ . Докажите это.

в) Пусть  $m$  и  $n$  – натуральные числа,  $n > 1$ . Докажите, что для некоторого натурального числа  $k$  верно равенство 
$$\left( \frac{n + \sqrt{n^2 - 4}}{2} \right)^m = \frac{k + \sqrt{k^2 - 4}}{2}.$$

23. Существуют ли такие рациональные числа  $a, b, c, d$ , что  $(a + b\sqrt{2})^2 + (c + d\sqrt{2})^2 = 7 + 5\sqrt{2}$  ?

24 (М874). Пусть  $m$  и  $n$  – натуральные числа. Докажите, что а)  $(5 + 3\sqrt{2})^m \neq (3 + 5\sqrt{2})^n$ ; б)\*  $(a + b\sqrt{d})^m \neq (b + a\sqrt{d})^n$ , где  $a, b$  и  $d$  – натуральные числа,  $a \neq b$  и число  $d$  не является точным квадратом.

25. Докажите следующие утверждения.

а) (М352) Число  $\left[ (45 + \sqrt{1975})^{30} \right]$  нечетно.

б) Первые 1000 цифр после запятой десятичной записи числа  $(6 + \sqrt{35})^{1979}$  – девятки.

в) Первые 999 цифр после запятой десятичной записи числа  $(6 + \sqrt{37})^{999}$  – нули.

г)  $\lim_{n \rightarrow \infty} \left\{ (2 + \sqrt{3})^n \right\} = 1$ .

д) Перед запятой в десятичной записи числа  $(\sqrt{2} + \sqrt{3})^{2000}$  стоит цифра 1, а после запятой – не менее 666 девяток. (Указание. Для любого целого неотрицательного  $n$  обозначьте  $a_n = (\sqrt{3} + \sqrt{2})^{2n} + (\sqrt{3} - \sqrt{2})^{2n}$  и докажите равенство  $a_{n+2} = 10a_{n+1} - a_n$ .)

26\* (М520). Рассмотрим последовательность чисел  $x_n = (1 + \sqrt{2} + \sqrt{3})^n$ . Каждое из них можно привести к виду  $x_n = q_n + r_n \sqrt{2} +$

$+ s_n\sqrt{3} + t_n\sqrt{6}$ , где  $q_n, r_n, s_n, t_n$  — целые числа. Найдите пределы  $\lim_{n \rightarrow \infty} \frac{r_n}{q_n}$ ,  $\lim_{n \rightarrow \infty} \frac{s_n}{q_n}$  и  $\lim_{n \rightarrow \infty} \frac{t_n}{q_n}$ .

### Степени числа $2 + \sqrt{3}$

Не каждому читателю, по себе знаем, легко привыкнуть пользоваться иррациональными числами для решения уравнений в целых числах. Поэтому рассмотрим еще один пример.

$$(2 + \sqrt{3})^2 = 4 + 4\sqrt{3} + 3 = 7 + 4\sqrt{3},$$

$$(2 + \sqrt{3})^3 = 8 + 12\sqrt{3} + 18 + 3\sqrt{3} = 26 + 15\sqrt{3}.$$

Мы получили решения (7; 4) и (26; 15) уравнения  $x^2 - 3y^2 = 1$ .

Если

$$(2 + \sqrt{3})^n = x + y\sqrt{3},$$

то

$$(2 + \sqrt{3})^{n+1} = (x + y\sqrt{3})(2 + \sqrt{3}) = (2x + 3y) + (x + 2y)\sqrt{3},$$

что и дает нужную нам формулу.

Вообще, давайте равенство  $2^2 - 3 = 1$  запишем в виде

$$(2 + \sqrt{3})(2 - \sqrt{3}) = 1,$$

а затем возведем обе части в  $n$ -ю степень:

$$(2 + \sqrt{3})^n (2 - \sqrt{3}) = 1.$$

Обозначив через  $x_n$  и  $y_n$  такие натуральные числа, что

$$(2 + \sqrt{3})^n = x_n + y_n\sqrt{3},$$

получим, заменив знаки перед  $\sqrt{3}$ , равенство

$$(2 - \sqrt{3})^n = x_n - y_n\sqrt{3}.$$

(Переход к сопряженным числам законен по той же причине, что и для  $\sqrt{2}$ .) Следовательно,

$$1 = (2 + \sqrt{3})^n (2 - \sqrt{3}) = (x_n + y_n\sqrt{3})(x_n - y_n\sqrt{3}) = x_n^2 - 3y_n^2.$$

Значит, пара

$$(x_n; y_n) = \left( \frac{(2 + \sqrt{3})^n + (2 - \sqrt{3})^n}{2}; \frac{(2 + \sqrt{3})^n - (2 - \sqrt{3})^n}{2\sqrt{3}} \right)$$

– решение уравнения  $x^2 - 3y^2 = 1$ . Других решений в натуральных числах, как следует из (пока не доказанной нами) теоремы 5, у этого уравнения нет.

### Упражнения

27. Докажите следующие утверждения.

а) Уравнение  $(x+1)^3 - x^3 = y^2$  имеет бесконечно много решений в натуральных числах.

б) (М960) Если квадрат некоторого натурального числа  $n$  представим в виде разности кубов последовательных целых чисел, то число  $n$  есть сумма квадратов двух последовательных целых чисел.

в) Уравнение  $(x+2)^3 - x^3 = y^2$  не имеет решений в целых числах.

28. Если натуральные числа  $k$ ,  $m$  и  $n$  удовлетворяют равенству  $m + n\sqrt{3} = (2 + \sqrt{3})^k$ , где  $k$  а) нечетно; б) четно, то число а)  $\sqrt{m-1}$ ; б)  $\sqrt{(m+1)/2}$  целое. Докажите это.

29. Существуют ли такие натуральные числа  $x$ ,  $y$ ,  $d$ , что  $x^2 - dy^2 = 1$  и ни одно из чисел  $x-1$  и  $x+1$  не является ни квадратом, ни удвоенным квадратом?

30. Если  $n$  – целое неотрицательное число, то число  $\left[ (1 + \sqrt{3})^{2n+1} \right]$  делится на  $2^{n+1}$  и не делится на  $2^{n+2}$ . Докажите это.

### Гиперболы и решетки

*...небережливое многословье кажется доступным, потому что оно бессодержательно.*

*...развращенные пустотой шаблонов, мы именно неслыханную содержательность, являющуюся к нам после долгой отвычки, принимаем за претензии формы.*

Б.Л.Пастернак

Устроим привал: разберем красивую геометрическую задачу. Она весьма симпатична и тесно связана с уравнениями Пелля и числами Фибоначчи.

**Задача М1775.** а) Существует ли квадрат, все вершины и все середины сторон которого лежат на гиперболах  $xy = \pm 1$ ?

б) Докажите, что существует бесконечно много параллелограммов, одна из вершин каждого из которых – начало координат, две другие лежат на гиперболе  $xy = 1$ , а четвертая – на гиперболе  $xy = -1$ .

в) Докажите, что площадь любого такого параллелограмма равна  $\sqrt{5}$ .

г) Рассмотрим для некоторого такого параллелограмма  $OABC$  порожденную им решетку, т.е. множество таких точек  $P$ , что

$\overline{OP} = m\overline{OA} + n\overline{OC}$ , где  $m, n$  – целые числа. Докажите, что внутренность «креста», ограниченного гиперболами  $xy = \pm 1$ , содержит лишь одну точку этой решетки – начало координат. (Н.Осипов)

В авторском варианте задача имела продолжение: а на самих гиперболах  $xy = \pm 1$  лежит бесконечно много точек такой решетки! Эту часть редакция вычеркнула, предположив, что задача покажется читателям слишком сложной. Но мы, разумеется, решим и неопубликованный пункт задачи М1775.

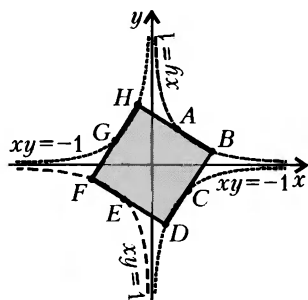


Рис. 2

Начнем с пункта а). Проанализируем ситуацию. Пусть искомый квадрат существует и выглядит так, как показано на рисунке 2. Обозначим координаты точки  $A$  – середины стороны квадрата – через  $\left(a; \frac{1}{a}\right)$ . Тогда, как легко видеть,

$\overline{AB} = \left(\frac{1}{a}; -a\right)$ , так что точка  $B$  имеет координаты  $\left(a + \frac{1}{a}; \frac{1}{a} - a\right)$ . Условие принадлежности точки  $B$  гиперболе  $xy = 1$  дает уравнение

$$\left(a + \frac{1}{a}\right) \cdot \left(\frac{1}{a} - a\right) = 1,$$

откуда  $\frac{1}{a^2} - a^2 = 1$ . Этому уравнению удовлетворяет число

$a = \sqrt{(\sqrt{5} - 1)/2}$ . Анализ окончен. При найденном значении  $a$  все

четыре точки  $B\left(a + \frac{1}{a}; \frac{1}{a} - a\right)$ ,  $D\left(-a + \frac{1}{a}; -\frac{1}{a} - a\right)$ ,

$F\left(-a - \frac{1}{a}; -\frac{1}{a} + a\right)$ ,  $H\left(a - \frac{1}{a}; \frac{1}{a} + a\right)$  (вершины квадрата) и

точки  $A\left(a; \frac{1}{a}\right)$ ,  $C\left(\frac{1}{a}; -a\right)$ ,  $E\left(-a; -\frac{1}{a}\right)$ ,  $G\left(-\frac{1}{a}; a\right)$  (середины сторон) лежат на гиперболах  $xy = \pm 1$ .

**Упражнение 31.** Если все вершины и все середины сторон квадрата лежат на гиперболах  $xy = \pm 1$ , то центр этого квадрата – начало координат. Докажите это.

б) Рассмотрим точки  $A(a; 1/a)$  и  $C(c; -1/c)$ , а также начало координат  $O(0; 0)$  (рис.3). Вершина  $B$  параллелограмма  $OABC$  имеет координаты  $\left(a+c; \frac{1}{a}-\frac{1}{c}\right)$ . Она лежит на гиперболе  $xy = 1$  при условии

$$(a+c) \cdot \left(\frac{1}{a}-\frac{1}{c}\right) = 1,$$

которое можно записать в виде *Рис. 3*

$$\frac{c}{a} - \frac{a}{c} = 1, \text{ т.е. } \frac{c}{a} = \frac{1+\sqrt{5}}{2}.$$

Очевидно, последнему условию удовлетворяют бесконечно многие пары чисел  $a$  и  $c$ .

в) Легко доказать, что площадь  $S$  параллелограмма  $OABC$ , где  $O$  – начало координат,  $\overrightarrow{OA} = (a; b)$  и  $\overrightarrow{OC} = (c; d)$ , равна  $S = |ad - bc|$ . Подставляя  $b = 1/a$  и  $d = -1/c$ , находим

$$S = \left| \frac{a}{c} + \frac{c}{a} \right| = \left| \frac{2}{1 \pm \sqrt{5}} + \frac{1 \pm \sqrt{5}}{2} \right| = \sqrt{5}.$$

Но решение еще не закончено: параллелограмм может выглядеть так, как показано на рисунке 4.

Его вершины  $A(a; 1/a)$  и  $C(c; 1/c)$  лежат на гиперболе  $xy = 1$ .

Точка  $B\left(a+c; \frac{1}{a}+\frac{1}{c}\right)$  лежит на гиперболе  $xy = -1$ , если

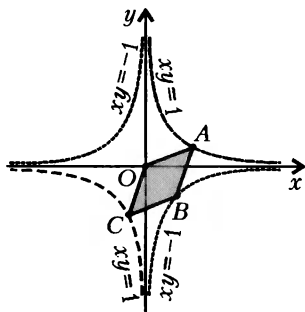
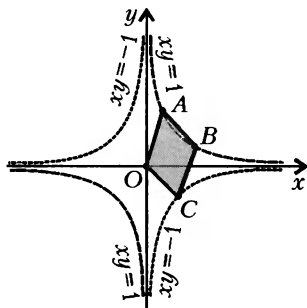
$$(a+c) \left(\frac{1}{a}+\frac{1}{c}\right) = -1,$$

т.е.  $\frac{a}{c} + \frac{c}{a} = -3$ . При этом

$$S = \left| \frac{a}{c} - \frac{c}{a} \right| = \sqrt{\left(\frac{a}{c}\right)^2 - 2 + \left(\frac{c}{a}\right)^2} =$$

$$= \sqrt{\left(\frac{a}{c}\right)^2 + 2 + \left(\frac{c}{a}\right)^2} - 4 = \sqrt{\left(\frac{a}{c} + \frac{c}{a}\right)^2} - 4 = \sqrt{(-3)^2} - 4 = \sqrt{5}.$$

г) Рассмотрим порожденную параллелограммом рисунка 3 решетку (рис.5). Для произвольной точки  $P(x; y)$  этой



*Рис. 4*



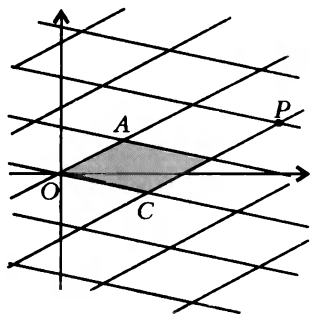


Рис. 5

решетки

$$\begin{aligned}\overline{OP} &= m\overline{OA} + n\overline{OC} = \\ &= \left( ma + nc; \frac{m}{a} - \frac{n}{c} \right),\end{aligned}$$

где  $m, n$  — целые числа, имеем

$$\begin{aligned}|xy| &= \left| (ma + nc) \left( \frac{m}{a} - \frac{n}{c} \right) \right| = \\ &= \left| m^2 + mn \left( \frac{c}{a} - \frac{a}{c} \right) - n^2 \right| = \\ &= \left| m^2 + mn - n^2 \right|.\end{aligned}$$

Внутренность «креста» из гипербол  $xy = \pm 1$  задается неравенствами  $|xy| < 1$ . Но при целых  $m$  и  $n$  величина  $|m^2 + mn - n^2|$  тоже целая. Единственным целым числом, которое по модулю меньше 1, является нуль. Значит, для лежащей внутри креста точки имеем

$$\left| (ma + nc) \left( \frac{m}{a} - \frac{n}{c} \right) \right| = 0,$$

откуда  $ma + nc = 0$  или  $mc - na = 0$ . Ввиду иррациональности отношения  $a/c$  это возможно лишь при  $m = n = 0$ . Следовательно, внутри «креста» из гипербол расположена единственная точка решетки — начало координат.

Для решетки, порожденной параллелограммом рисунка 4, решение аналогично, поэтому выпишем только формулы:

$$\overline{OP} = m\overline{OA} + n\overline{OC} = \left( ma + nc; \frac{m}{a} + \frac{n}{c} \right),$$

$$\begin{aligned}|xy| &= \left| (ma + nc) \left( \frac{m}{a} + \frac{n}{c} \right) \right| = \\ &= \left| m^2 + mn \left( \frac{c}{a} + \frac{a}{c} \right) + n^2 \right| = \left| m^2 - 3mn + n^2 \right| = \\ &= \left| (m - n)^2 - (m - n)n - n^2 \right| = \left| n^2 + kn - k^2 \right|,\end{aligned}$$

где обозначено  $k = m - n$ .

Итак, внутри «креста из гипербол» расположена единственная точка решетки — начало координат. Однако на самой гиперболе лежит бесконечно много таких точек. Чтобы дока-

зять это, достаточно убедиться, что уравнение

$$x^2 + xy - y^2 = \pm 1$$

имеет бесконечно много решений в целых числах.

$$\text{Уравнение } x^2 - xy - y^2 = \pm 1$$

Это уравнение не имеет вида  $x^2 - dy^2 = 1$ . Но умножение на 4 приводит его к виду

$$4x^2 - 4xy - 4y^2 = \pm 4,$$

т.е.

$$(2x - y)^2 - 5y^2 = \pm 4,$$

что уже похоже на уравнение Пелля. Впрочем, мы воспользуемся этим преобразованием позже, а здесь решим уравнение в его первоначальном виде.

Немного посчитав, можно составить таблицу:

$x$	0	1	1	2	3	5	8	13	21
$y$	1	0	1	1	2	3	5	8	13
$x^2 - xy - y^2$	-1	1	-1	1	-1	1	-1	1	-1

Всякий, кто знаком с числами Фибоначчи, уже узнал их. А остальным скажем, что последовательность Фибоначчи задана своими двумя членами  $\varphi_0 = 0$ ,  $\varphi_1 = 1$  и рекуррентной формулой  $\varphi_{n+2} = \varphi_n + \varphi_{n+1}$ . Несколько следующих членов этой замечательной последовательности таковы:  $\varphi_2 = 0 + 1 = 1$ ,  $\varphi_3 = 1 + 1 = 2$ ,  $\varphi_4 = 1 + 2 = 3$ ,  $\varphi_5 = 2 + 3 = 5$ ,  $\varphi_6 = 3 + 5 = 8$ ,  $\varphi_7 = 5 + 8 = 13$ .

**Теорема 6.** Если  $x^2 - xy - y^2 = \pm 1$ , то пара чисел  $(X; Y) = (x + y; x)$  удовлетворяет равенству  $X^2 - XY - Y^2 = \mp 1$ .

**Доказательство.**  $(x + y)^2 - (x + y)x - x^2 = x^2 + 2xy + y^2 - x^2 - xy - x^2 = -(x^2 - xy - y^2) = \mp 1$ .

Доказав теорему 6, мы наконец-то решили задачу М1775.

**Теорема 7.** Уравнение  $x^2 - xy - y^2 = \pm 1$  не имеет решений в целых неотрицательных числах, кроме тех, что получаются из «тривиального» решения  $(0; 1)$  при помощи правила  $(x; y) \rightarrow (x + y; x)$ .

**Следствие.** Все решения уравнения  $z^2 - 5y^2 = \pm 4$  в натуральных числах даются формулой  $(y; z) = (\varphi_n; \varphi_{n+1} + \varphi_{n-1})$ .

**Доказательство следствия.** Каждой паре целых чисел  $(x; y)$ , удовлетворяющей равенству  $x^2 - xy - y^2 = \pm 1$ , соот-

ветствует пара целых чисел  $(z; y) = (2x - y; y)$ , удовлетворяющая равенству  $z^2 - 5y^2 = \pm 4$ , и наоборот (поскольку числа  $y$  и  $z$  одной четности). Осталось заметить, что если  $x = \varphi_{n+1}$  и  $y = \varphi_n$ , то

$$z = 2x - y = 2\varphi_{n+1} - \varphi_n = \varphi_{n+1} + \varphi_{n-1}.$$

Таким образом, следствие выведено из теоремы 7. Ее мы докажем во второй части статьи.

**Упражнение 32.** Докажите а) тождество Кассини  $\varphi_n^2 = \varphi_{n-1}\varphi_{n+1} - (-1)^n$ ; б) тождество  $\varphi_n^2 = \varphi_{n-2}\varphi_{n+2} + (-1)^n$ .

## Часть II. Структура решений

### Формула

$$(x^2 - dy^2)(z^2 - dt^2) = (xz + dyt)^2 - d(xt + yz)^2$$

Можно было бы рассмотреть еще несколько примеров, в которых возникают уравнения Пелля или аналогичные им, но у нас остались недоказанными теоремы 2, 3, 5 и 7. Пора переходить к общим рассмотрениям.

Следующее вычисление – пожалуй, самое главное в теории уравнений Пелля:

$$\begin{aligned}(x^2 - dy^2)(z^2 - dt^2) &= x^2z^2 - dy^2z^2 - dx^2t^2 + d^2y^2t^2 = \\ &= x^2z^2 + 2xzd yt + d^2y^2t^2 - dy^2z^2 - 2dyzxt - dx^2t^2 = \\ &= (xz + dyt)^2 - d(xt + yz)^2.\end{aligned}$$

Вот как можно получить ту же формулу, если разложить разность квадратов на (иррациональные!) множители и переставить их разумным образом:

$$\begin{aligned}(x^2 - dy^2)(z^2 - dt^2) &= (x + y\sqrt{d})(x - y\sqrt{d})(z + t\sqrt{d})(z - t\sqrt{d}) = \\ &= (x + y\sqrt{d})(z + t\sqrt{d}) \cdot (x - y\sqrt{d})(z - t\sqrt{d}) = \\ &= (xz + dyt + (xt + yz)\sqrt{d}) \cdot (xz + dyt - (xt + yz)\sqrt{d}) = \\ &= (x + dyt)^2 - d(xt + yz)^2.\end{aligned}$$

Хотя эта выкладка даже длиннее предыдущей, она проясняет связь между уравнением Пелля и числами вида  $x + y\sqrt{d}$ .

Зачем нам нужна только что доказанная формула? Чтобы строить из одних решений другие! Точнее говоря, формула доказывает следующую важную теорему.

**Теорема 8.** Если  $x^2 - dy^2 = a$  и  $z^2 - dt^2 = b$ , то пара чисел  $(X; Y) = (xz + dyt; xt + yz)$  удовлетворяет равенству  $X^2 - dY^2 = ab$ .

Сформулируем и (опять!) не докажем теорему о том, как устроено множество решений уравнения Пелля.

**Теорема 9.** Если  $a$  – наименьшее натуральное число, для которого существует такое натуральное число  $b$ , что  $a^2 - db^2 = 1$ , то уравнение  $x^2 - dy^2 = 1$  не имеет решений в целых неотрицательных числах, кроме цепочки решений, получаемых из «тривиального» решения  $(1; 0)$  при помощи правила  $(x; y) \rightarrow (ax + dby; bx + ay)$ .

### Упражнения

**33.** Уравнение а)  $x^2 - 2y^2 = 14$ ; б)  $x^2 - 2y^2 = 23^{23}$  имеет бесконечно много решений в целых числах, а уравнение в)  $|x^2 - 2y^2 - 1004| = 1001$  не имеет ни одного. Докажите это.

**34.** Найдите наименьшее натуральное число, квадрат которого представим в виде суммы квадратов 11 последовательных а) целых; б) натуральных чисел. в) Существует бесконечно много натуральных чисел, квадрат каждого из которых представим в виде суммы квадратов 11 последовательных натуральных чисел. Докажите это.

**35.** Пусть  $a, b, x, y, z, t$  – рациональные числа,  $x^2 + ay^2 + bz^2 + abt^2 = 0$  и хотя бы одно из чисел  $x, y, z$  и  $t$  отлично от нуля. Докажите, что существуют такие рациональные числа  $u, v$  и  $w$ , хотя бы одно из которых отлично от нуля, что  $u^2 + av^2 + bw^2 = 0$ .

### Существование решения

*Кажется, что можно придумать кривее и извилистее великорусского проселка? Точно змея проползла. А попробуйте пройти прямее: только проплутаете и выйдете на ту же извилистую тропу.*

В О.Ключевский

**Теорема 10.** Для любого натурального числа  $d$ , не являющегося квадратом, существуют такие натуральные числа  $x$  и  $y$ , что  $x^2 - dy^2 = 1$ .

Вместе взятые, теоремы 8, 9 и 10 позволяют довольно ясно представить себе структуру множества решений уравнения Пелля. Красивое и мудрое доказательство теоремы 10 опубликовал в 2008 году Н.Вайлдбергер (Сидней, Австралия). Оно использует квадратичные формы – выражения вида  $ax^2 + bxy + cy^2$ , где  $a, b$  и  $c$  – числа,  $x$  и  $y$  – переменные. В третьей части статьи мы докажем теорему 10 вторым способом; в статье «Цепные

дроби» «Арифметики» разъяснена связь разложения числа  $\sqrt{d}$  в цепную дробь с уравнением Пелля.

Вот несколько квадратичных форм:

$$\begin{aligned} x^2 - 2y^2, \\ (x+y)^2 - 2y^2 &= x^2 + 2xy - y^2, \\ x^2 + 2x(x+y) - (x+y)^2 &= (2x+y)^2 - 2(x+y)^2 = 2x^2 - y^2 \\ 2x^2 - (x+y)^2 &= (3x+y)^2 - 2(2x+y)^2 = x^2 - 2xy - y^2, \\ (x+y)^2 - 2(x+y)y - y^2 &= (3x+4y)^2 - 2(2x+3y)^2 = x^2 - 2y^2 \end{aligned}$$

Вот еще несколько:

$$\begin{aligned} x^2 - 7y^2, \\ (x+y)^2 - 7y^2 &= x^2 + 2xy - 6y^2, \\ (x+y)^2 + 2(x+y)y - 6y^2 &= (x+2y)^2 - 7y^2 = x^2 + 4xy - 3y^2, \\ x^2 + 4x(x+y) - 3(x+y)^2 &= (3x+2y)^2 - 7(x+y)^2 = 2x^2 - 2xy - 3y^2, \\ 2(x+y)^2 - 2(x+y)y - 3y^2 &= (3x+5y)^2 - 7(x+2y)^2 = 2x^2 + 2xy - 3y^2, \\ 2x^2 + 2x(x+y) - 3(x+y)^2 &= (8x+5y)^2 - 7(3x+2y)^2 = x^2 - 4xy - 3y^2, \\ (x+y)^2 - 4(x+y)y - 3y^2 &= (8x+13y)^2 - 7(3x+5y)^2 = x^2 - 2xy - 6y^2, \\ (x+y)^2 - 2(x+y)y - 6y^2 &= (8x+21y)^2 - 7(3x+8y)^2 = x^2 - 7y^2. \end{aligned}$$

Это не случайные списки, а последовательности форм, рассматриваемые при  $d = 2$  и  $d = 7$  соответственно. Обозначим  $L(x, y) = (x + y, y)$  и  $R(x, y) = (x, x + y)$ . Суть в том, что мы, начиная с  $x^2 - dy^2$ , из очередной квадратичной формы  $g(x, y) = ax^2 + bxy + cy^2$  получаем либо

$$\begin{aligned} gL(x, y) = g(x + y, y) &= a(x + y)^2 + b(x + y)y + cy^2 = \\ &= ax^2 + (2a + b)xy + (a + b + c)y^2, \end{aligned}$$

либо

$$\begin{aligned} gR(x, y) = g(x, x + y) &= ax^2 + bx(x + y) + c(x + y)^2 = \\ &= (a + b + c)x^2 + (b + 2c)xy + cy^2. \end{aligned}$$

Правило, по которому выбираем, какую именно из переменных  $x$  и  $y$  заменять на  $x + y$ , таково: коэффициенты при  $x^2$  и  $y^2$  должны быть разных знаков, точнее,  $a > 0$  и  $c < 0$ . Это значит, что если  $a + b + c < 0$ , то применяем  $L$ , а если  $a + b + c > 0$ , то  $R$ .

**Теорема 10.** *Рано или поздно будет получено тождество вида*

$$(\alpha x + \beta y)^2 - d(\gamma x + \delta y)^2 = x^2 - dy^2,$$

где  $\alpha$ ,  $\beta$ ,  $\gamma$  и  $\delta$  — натуральные числа. (Это тождество позволяет из одного решения уравнения  $x^2 - dy^2 = 1$  получать другое, например, из решения  $(x; y) = (1; 0)$  — решение  $(\alpha; \gamma)$ .)

**Доказательство.** Каждый, кто учился решать квадратные уравнения, вычислял дискриминант

$$D = b^2 - 4ac.$$

Поскольку

$$(2a + b)^2 - 4a(a + b + c) = b^2 - 4ac = (b + 2c)^2 - 4(a + b + c)c,$$

то дискриминанты всех форм последовательности Вайлдберге-ра одинаковы и равны дискриминанту формы  $x^2 - dy^2$ , т.е. числу  $4d$ .

Поскольку  $4d$  не является квадратом целого числа, то ни в одной из форм последовательности ни коэффициент при  $x^2$ , ни коэффициент при  $y^2$  не равны 0; следовательно, сформулированное выше правило однозначно определяет бесконечную последовательность форм.

Коэффициенты  $a$ ,  $b$ ,  $c$  любой из форм  $ax^2 + bx + cx^2$  последовательности Вайлдберге-ра удовлетворяют равенству

$$b^2 - 4ac = 4d.$$

Таким образом,

$$0 < -4ac = 4d - b^2 \leq 4d.$$

Количество решений этой системы неравенств в целых числах конечно. Поскольку число  $b$  с точностью до знака определяется из равенства  $b^2 = d + 4ac$ , то множество форм, которые при данном  $d$  могут встретиться в последовательности Вайлдберге-ра, конечно. Следовательно, рано или поздно некоторая форма повторится. Мы доказали, что последовательность периодическая.

Может ли она иметь предпериод? Нет, в силу следующей леммы.

**Лемма 1.** *Каждая форма  $f(x, y) = Ax^2 + Bxy + Cy^2$  последовательности Вайлдберге-ра однозначно определяет не только следующую за ней, но и предыдущую.*

**Доказательство.** Форма  $f$  может быть получена из некоторой формы  $g$  либо при помощи преобразования  $L$ , либо при помощи

*R.* В первом случае

$$f(1, -1) = g(1 - 1, 1) = g(0, 1) < 0,$$

**а во втором**

$$f(1, -1) = g(1, 1 - 1) = g(1, 0) > 0.$$

Знак величины  $f(1, -1)$  однозначно определяет, какое преобразование применялось!

Теоремы 10 и 10' доказаны. Но цепочки букв  $L$  и  $R$  интересны не только этим. Для  $d = 2$  и  $7$  мы их уже посчитали:  $LRRL$  и  $LLRLRLL$ . Для  $d = 61$ , если не поленитесь, получите такой ответ:

$$L^7 R L^4 R^3 L R^2 L^2 R L^3 R^4 L R^{14} L R^4 L^3 R L^2 R^2 L R^3 L^4 R L^7,$$

где, само собой разумеется,  $L^7 = LLLLLLL$ .

Вы заметили, что цепочки – палиндромы: слева направо они читаются так же, как справа налево? Подумайте, как это можно доказать! А если читали статью «Цепные дроби» «Арифметики», то вы знаете, что  $\sqrt{2} = [1; 2, 2, 2, 2, \dots]$ ,  $\sqrt{7} = [2; 1, 1, 1, 4, 1, 1, 1, 4, \dots]$ .

Подумайте, как связаны эти разложения с последовательностями  $LRLLRLLRLLRLLRLLRLLRLLRLLRRL\dots$  и

*LLRLRLLLRLRLLLRLRLLLRLRLLLRLRLL...*

соответственно. При разложении числа  $\sqrt{61}$  в цепную дробь – если не ошибетесь! – получите такой ответ:

$$\sqrt{61} = [7; \mathbf{1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14}, 1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14, \dots]$$

Вы уже догадались, как обстоит дело в общем случае? Если нет, разберите самостоятельно еще пару примеров. А после этого – изучайте цепные дроби и установите связь между разложением числа  $\sqrt{d}$  в цепную дробь и алгоритмом Вайлбергера! Хотите подсказку? Пожалуй-ста: палиндромность следует из того, что коэффициент при  $xy$  в квадратичной форме  $x^2 - dy^2$  равен 0. А для установления связи с цепными дробями полезно изучить алгоритм вытягивания носов! И еще совет: прочитайте в «Калейдоскопе» второго номера «Кванта» за 2008 г. о дереве Штерна–Броко–Калкина–Вилфа.

## Упражнения

**36.** Вычислите без использования компьютера последовательность преобразований  $L$  и  $R$  для а)  $d = 5$ ; б)  $d = 10$ ; в)  $d = 11$ .

г) Напишите программу, вычисляющую последовательность  $L$  и  $R$ , и сравните результаты ее работы с таблицей, приведенной на странице 125 «Арифметики».

**37.** Если  $d$  – натуральное число, не являющееся квадратом,  $c \neq 0$  и уравнение  $x^2 - dy^2 = c$  имеет хотя бы одно решение в целых числах, то

это уравнение имеет бесконечно много решений в натуральных числах. Выведите это из утверждения теоремы 10.

**38.** а) Пользуясь утверждением теоремы 10, выясните, при каких целых  $a$  уравнение  $a(x^2 - 1) = y^2$  имеет бесконечно много решений в целых числах. б) Пусть  $a$  – целое число. Пользуясь утверждением теоремы 10, выясните, при каких натуральных  $d$  уравнение  $x^2 - dy^2 = a^2$  имеет бесконечно много решений в натуральных числах.

**39.** Если  $n$  – натуральное число,  $n > 1$ , то уравнение а)  $x^2 - (n^2 - 1)y^2 = 1$ ; б)  $x^2 - (n^2 + 1)y^2 = 1$ ; в)  $x^2 - (n^2 + 2)y^2 = 1$ ; г)  $x^2 - (n^2 - 2)y^2 = 1$  имеет бесконечно много решений в натуральных числах. Докажите это.

**40.** Для любого натурального  $a$  уравнение а)  $(a^2 + 1)(x^2 + 1) = y^2$ ; б)  $(a^2 - 1)(x^2 - 1) = y^2$ ; в)  $(a^2 + 1)(x^2 + 1) = y^2 + 1$ ; г)  $(a^2 - 1)(x^2 - 1) = y^2 - 1$ ; д)  $(a^2 + 1)(x^2 - 1) = y^2 - 1$ ; е)  $(a^2 - 1)(x^2 + 1) = y^2 - 1$  имеет бесконечно много решений в целых числах. Докажите это.

**41.** Ни при каком натуральном  $a$  уравнение а)  $(a^2 + 1)(x^2 + 1) = y^2 - 1$ ; б)  $x^2 = (4a - 1)(y^2 + 1)$ ; в)  $a(x^2 - 1) = y^2 + 1$  не имеет решений в целых числах. Докажите это. (Указание к пунктам б) и в). Воспользуйтесь тем, что число вида  $y^2 + 1$  не может делиться на натуральное число вида  $4n - 1$ .)

**42.** Докажите следующие утверждения. а) Существует бесконечно много четверок целых чисел, в каждой из которых числа попарно различны и таковы, что  $x + y + z + t = x^3 + y^3 + z^3 + t^3 = 2$ .

б) Уравнение  $xy(x + 2)(y + 2) = z(z + 2)$  имеет бесконечно много решений в натуральных числах.

в) Существует бесконечно много таких троек натуральных чисел, что произведение любых двух из этих чисел на единицу больше квадрата натурального числа

г) Для любого натурального числа  $a$  система уравнений

$$\begin{cases} xy - 1 = a^2, \\ yz - 1 = u^2, \\ zx - 1 = v^2 \end{cases}$$

имеет бесконечно много решений в натуральных числах  $x, y, z, u$  и  $v$ .

д) Для любого натурального  $n$  существует бесконечно много таких наборов из  $k = 3n^2 - 1$  последовательных натуральных чисел, что сумма их квадратов сама является квадратом натурального числа. (Указание. Воспользуйтесь теоремой 10.)

е) Аналогичное предыдущему пункту утверждение – для натуральных чисел вида  $k = \frac{3a^2 - 1}{3b^2 + 1}$ , где  $a, b$  – натуральные. (В частности, для

$$k = \frac{3 \cdot (13n + 3)^2}{3 \cdot 2^2 + 1} = 39n^2 + 18n + 2 \text{ или для } k = 1293n^2 + 102n + 2.)$$



**43° (M618).** Докажите следующие утверждения.

а) Существует бесконечно много таких натуральных  $n$ , что  $n!$  делится на  $n^2 + 1$ .

б) Для любого числа  $\alpha > 0$  существует бесконечно много таких натуральных  $n$ , что  $[\alpha n]!$  делится на  $n^2 + 1$ .

**44.** Для любого простого числа  $p$ , дающего остаток 1 при делении на 4, существуют такие натуральные числа  $x$  и  $y$ , что  $x^2 - py^2 = -1$ . Докажите это.

### Доказательства теорем 2, 3, 5, 7, 9

Пора заняться теоремами 2, 3, 5, 7 и 9. Мы докажем их двумя способами: сначала обойдемся без помощи иррациональностей, но доказательства будут несколько скучноваты, а затем воспользуемся иррациональностями, чтобы сделать (по сути те же) доказательства более прозрачным, что поможет нам разобраться в структуре решений в целых числах не только уравнений Пелля, но и так называемых норменных уравнений  $x^2 - dy^2 = c$ .

#### Теорема 2 (уравнение $x^2 - 2y^2 = \pm 1$ )

Пусть  $X, Y$  – натуральные числа, удовлетворяющие равенству  $X^2 - 2Y^2 = \pm 1$ . Рассмотрим систему уравнений

$$\begin{cases} x + 2y = X, \\ x + y = Y \end{cases}$$

и решим ее:

$$\begin{cases} x = 2Y - X, \\ y = X - Y. \end{cases}$$

Легко проверить, что

$$\begin{aligned} x^2 - 2y^2 &= (2Y - X)^2 - 2(X - Y)^2 = \\ &= 4Y^2 - 4XY + X^2 - 2(X^2 - 2XY + Y^2) = -(X^2 - 2Y^2). \end{aligned}$$

Понимаете, в чем идея? Каждой паре  $(X; Y)$ , являющейся решением уравнения  $X^2 - 2Y^2 = \pm 1$ , мы сопоставляем ее «предшественницу» – пару  $(x; y) = (2Y - X; X - Y)$ , удовлетворяющую равенству  $x^2 - 2y^2 = \mp 1$ .

**Лемма 2.** Если  $X, Y$  – натуральные числа и  $X^2 - 2Y^2 = \pm 1$ , то  $2Y - X$  и  $X - Y$  – неотрицательные числа, причем  $X - Y < Y$ .

**Доказательство.** Будем рассуждать «от противного». Если

$2Y - X < 0$ , то  $X > 2Y$  и  $X^2 - 2Y^2 > 4Y^2 - 2Y^2 = 2Y^2 \geq 2 > 1$ , что противоречит равенству  $X^2 - 2Y^2 = \pm 1$ .

Если  $X - Y < 0$ , то  $X < Y$  и  $X^2 - 2Y^2 < Y^2 - 2Y^2 = -Y^2 \leq -1$ .

Наконец, если  $X - Y \geq Y$ , то  $X \geq 2Y$  и  $X^2 - 2Y^2 \geq 4Y^2 - 2Y^2 = 2Y^2 \geq 2 > 1$ , что вновь дает противоречие.

Лемма доказана. Эта лемма – основа доказательства теоремы 2. А именно, взяв любую пару  $(X; Y)$  натуральных чисел, удовлетворяющую равенству  $X^2 - 2Y^2 = \pm 1$ , мы можем рассмотреть ее предшественницу – пару  $(x; y)$ . При этом  $y < Y$ . Если  $x$  и  $y$  – натуральные числа, то у пары  $(x; y)$  есть своя предшественница, у которой – своя, и так далее. Бесконечно этот процесс продолжаться не может: неравенство  $y < Y$  гарантирует, что начатый с пары  $(X; Y)$  процесс образования предшественниц оборвется не более чем через  $Y$  шагов. (Любитель строгости сказал бы, что здесь мы воспользовались отсутствием бесконечно убывающей последовательности натуральных чисел.)

В какой момент обрывается процесс образования пар-предшественниц? Очевидно, когда очередная пара  $(x; y)$  состоит не только из натуральных чисел, проще говоря, когда одно из чисел  $x$  и  $y$  равно нулю. Число  $x$  равняться нулю не может, а вот равенство  $x^2 - 2 \cdot 0^2 = \pm 1$  возможно. И возможно оно лишь при  $x = 1$  (напоминаем:  $x \geq 0$ ).

Итак, для любого решения  $(X; Y)$  уравнения  $X^2 - 2Y^2 = \pm 1$  процесс образования пар-предшественниц остановится, дойдя до пары  $(1; 0)$ . Проследив этот процесс в обратном направлении, т.е. не от пары  $(X; Y)$  к паре  $(1; 0)$ , а от пары  $(1; 0)$  к паре  $(X; Y)$ , мы видим, что он происходит по формуле  $(x; y) \rightarrow (x + 2y; x + y)$ . Доказательство теоремы 2 завершено.

### Упражнения

**45.** На листе клетчатой бумаги размером  $32 \times 40$  клеток нарисован прямоугольный треугольник, вершины которого расположены в узлах клеток. На его катетах как на гипотенузах во внешнюю сторону нарисованы равнобедренные прямоугольные треугольники. Оказалось, что разность площадей этих двух треугольников отличается от площади исходного треугольника менее чем на  $1/2$ . Найдите наибольшую возможную площадь такого треугольника.

**46.** Как известно,  $1 + 2 = 3$ . Легко проверить также, что  $1 + 2 + 3 + \dots + 13 + 14 = 105 = 15 + 16 + 17 + 18 + 19 + 20$ . Найдите все такие  $n$ , что сумма первых  $n$  натуральных чисел равна сумме нескольких последующих.

### Теорема 3 (уравнение $x^2 - 2y^2 = 7$ )

Доказательство теоремы 3 похоже на доказательство теоремы 2. Мы рассматриваем систему

$$\begin{cases} 3x + 4y = X, \\ 2x + 3y = Y, \end{cases}$$

находим из нее  $x = 3X - 4Y$  и  $y = 3Y - 2X$ , замечаем, что

$$x^2 - 2y^2 = (3X - 4Y)^2 - 2(3Y - 2X)^2 = X^2 - 2Y^2,$$

а затем формулируем и доказываем следующую лемму.

**Лемма 3.** Если  $X, Y$  – натуральные числа, удовлетворяющие равенству  $X^2 - 2Y^2 = 7$ , и выполнено неравенство  $Y \geq 6$ , то  $3X - 4Y$  и  $3Y - 2X$  – тоже натуральные числа, причем  $3X - 4Y < X$ .

**Доказательство.** Рассуждаем «от противного». Если  $3X - 4Y \leq 0$ , то  $X \leq \frac{4}{3}Y$  и  $7 = X^2 - 2Y^2 \leq \frac{16}{9}Y^2 - 2Y^2 < 0$ .

Если  $3Y - 2X \leq 0$ , то  $X \geq \frac{3}{2}Y$  и  $X^2 - 2Y^2 \geq \frac{9}{4}Y^2 - 2Y^2 = \frac{Y^2}{4} > 7$ .

Наконец, если  $3X - 4Y \geq X$ , то  $X \geq 2Y$  и  $X^2 - 2Y^2 \geq 4Y^2 - 2Y^2 = 2Y^2 > 7$ , что вновь дает противоречие.

Лемма доказана. Дальнейшее доказательство проводится почти так же, как и доказательство теоремы 2. Чтобы понять, где может остановиться процесс образования пар-предшественниц, достаточно разобрать случаи  $Y = 1, 2, 3, 4, 5$ . Сделав это, вы найдете, как и следовало ожидать, два решения: (3; 1) и (5; 3).

### Теорема 5 (уравнение $x^2 - 3y^2 = 1$ )

Доказательство теоремы 5 похоже на доказательство теоремы 2 и 3. Мы рассматриваем систему

$$\begin{cases} 2x + 3y = X, \\ x + 2y = Y, \end{cases}$$

находим из нее  $x = 2X - 3Y$  и  $y = 2Y - X$ , замечаем, что

$$x^2 - 3y^2 = (2X - 3Y)^2 - 3(2Y - X)^2 = X^2 - 3Y^2,$$

а затем формулируем и не доказываем (надеясь на читателя) следующую лемму.

**Лемма 4.** Если  $X, Y$  – натуральные числа, причем  $X^2 - 3Y^2 = 1$ , то  $2X - 3Y$  и  $2Y - X$  – неотрицательные числа, причем  $2Y - X < Y$ .

Окончание доказательства – такое же, как в теореме 2.

**Теорема 7 (уравнение  $x^2 - xy - y^2 = \pm 1$ )**

Из системы

$$\begin{cases} x + y = X, \\ x = Y \end{cases}$$

находим  $x = Y$  и  $y = X - Y$ . Очевидно,

$$\begin{aligned} x^2 - xy - y^2 &= Y^2 - Y(X - Y) - (X - Y)^2 = \\ &= Y^2 - XY + Y^2 - X^2 + 2XY - Y^2 = -(X^2 - XY - Y^2). \end{aligned}$$

**Лемма 5.** Если  $X, Y$  – натуральные числа, удовлетворяющие равенству  $X^2 - XY - Y^2 = \pm 1$ , то  $X \geq Y$ , причем равенство выполнено лишь в случае  $X = Y = 1$ .

**Доказательство.** Как всегда, рассуждаем «от противного». Если  $X < Y$ , то  $X^2 - XY - Y^2 < -Y^2 \leq -1$ , что несовместимо с условием  $X^2 - XY - Y^2 = \pm 1$ .

Если же  $X = Y$ , то  $X^2 - XY - Y^2 = -X^2$ . Очевидно,  $-X^2$  не равняется 1, а  $-X^2 = -1$  лишь при  $X = 1$ . Лемма доказана. Теперь читатель, надеемся, самостоятельно завершит доказательство теоремы 7.

### Упражнения

**47 (М39).** а) Целые неотрицательные числа  $x, y$  удовлетворяют уравнению  $x^2 - mxy + y^2 = 1$  (где  $m$  – данное натуральное число,  $m > 1$ ) тогда и только тогда, когда  $x$  и  $y$  – соседние члены последовательности  $a_0 = 0, a_1 = 1, a_2 = m, a_3 = m^2 - 1, a_4 = m^3 - 2m, a_5 = m^4 - 3m^2 + 1, \dots$ , в которой  $a_{k+2} = ma_{k+1} - a_k$  для всех  $k \geq 0$ . Докажите это.

б) Рассмотрим случай  $m = 3$ . Очевидно,  $a_0 = 0, a_1 = 1, a_2 = 3, a_3 = 3 \cdot 3 - 1 = 8, a_4 = 3 \cdot 8 - 3 = 21$ . Возникает гипотеза, что для любого  $n$  число  $q_n$  – это  $2n$ -й член последовательности Фибоначчи. Докажите эту гипотезу.

**Теорема 9 (уравнение  $x^2 - dy^2 = 1$ )**

Идея доказательства уже была применена нами четырежды. Применим же ее в пятый раз. Рассмотрим систему уравнений:

$$\begin{cases} xz + dyt = X, \\ xt + yz = Y. \end{cases}$$

Чтобы найти  $x$ , домножим первое уравнение на  $z$ , второе — на  $dt$  и вычтем затем второе уравнение из первого:

$$zX - dtY = xz^2 - dxt^2 = x,$$

поскольку  $z^2 - dt^2 = 1$ . Аналогично, чтобы найти  $y$ , домножим первое уравнение на  $t$ , второе на  $z$ , и вычтем второе уравнение из первого:

$$Xt - Yz = dyt^2 - yz^2,$$

откуда  $y = Yz - Xt$ .

**Лемма 6.** Если  $X, Y$  — натуральные числа, удовлетворяющие равенству  $X^2 - dY^2 = 1$ , а  $z$  — наименьшее натуральное число, для которого существует такое натуральное число  $t$ , что  $z^2 - dt^2 = 1$ , то  $zX - dtY \geq 0$  и  $Yz - Xt \geq 0$ , причем  $Yz - Xt < Y$ .

**Доказательство.** Рассуждаем «от противного». Если  $zX - dtY < 0$ , то  $X < \frac{dtY}{z}$  и, следовательно,

$$1 = X^2 - dY^2 < \left(\frac{dtY}{z}\right)^2 - dY^2 = dY^2 \frac{dt^2 - z^2}{z^2} < 0.$$

Если  $Yz - Xt < 0$ , то

$$X^2 - dY^2 > \frac{Y^2 z^2}{t^2} - dY^2 = \frac{Y^2 z^2 - dY^2 t^2}{t^2} = \frac{Y^2}{t^2} \geq 1.$$

(Последнее неравенство следует из того, что наименьшему  $z$  отвечает и наименьшее  $t$ .)

Если же  $Yz - Xt \geq Y$ , то  $X \leq (Yz - Y)/t$  и

$$\begin{aligned} X^2 - dY^2 &\leq \frac{Y^2(z-1)^2}{t^2} - dY^2 = \\ &= Y^2 \frac{z^2 - 2z + 1 - dt^2}{t^2} = Y^2 \frac{2 - 2z}{t^2} \leq 0. \end{aligned}$$

Лемма доказана. Дальнейшее доказательство проводится в точности так, как доказательство теоремы 2.

### Упражнения

**48\*.** Докажите следующие утверждения.

а) Для любого простого числа  $p$  существуют такие целые числа  $x$  и  $y$ , что  $x^2 - 34y^2 \equiv -1 \pmod{p}$ .

б) Если  $p$  — нечетное простое число,  $n$  — натуральное,  $x$  и  $y$  — такие целые числа, что  $x^2 - 34y^2 + 1$  делится на  $p^n$ , то существуют такие целые числа  $z$  и  $t$ , что  $(x + p^n z)^2 - 34(y + p^n t)^2 + 1$  делится на  $p^{n+1}$ .

в) Если  $n > 2$  – натуральное число,  $x$  и  $y$  – такие целые числа, что  $x^2 - 34y^2 + 1$  делится на  $2^n$  и не делится на  $2^{n+1}$ , то число  $(x + 2^{n-1})^2 - 34y^2 + 1$  делится на  $2^{n+1}$ .

г) Если  $m_1$  и  $m_2$  – взаимно простые натуральные числа, для которых существуют такие целые числа  $x_1$ ,  $y_1$ ,  $x_2$  и  $y_2$ , что  $x_1^2 - 34y_1^2 \equiv -1 \pmod{m_1}$  и  $x_2^2 - 34y_2^2 \equiv -1 \pmod{m_2}$ , то существуют такие целые числа  $x$  и  $y$ , что  $x^2 - 34y^2 \equiv -1 \pmod{m_1 m_2}$ .

д) Для любого натурального  $m$  сравнение  $x^2 - 34y^2 \equiv -1 \pmod{m}$  имеет решения в целых числах  $x$  и  $y$ .

е) Уравнение  $x^2 - 34y^2 = -1$  не имеет решений в целых числах.

*Замечание.* Ситуация, когда сравнения имеют решения, а уравнение не имеет, не столь уж редка. Например, для любого натурального числа  $m$  сравнение  $(3x + 1)(2x + 1) \equiv 0 \pmod{m}$  имеет решения в целых числах, а уравнение  $(3x + 1)(2x + 1) = 0$  не имеет целых решений. Тем интереснее знать, что 34 – наименьшее не являющееся точным квадратом натуральное число  $d$ , для которого все сравнения вида  $x^2 - dy^2 \equiv -1 \pmod{m}$  имеют решения, а уравнение  $x^2 - dy^2 = -1$  целочисленных решений не имеет. (Проверьте это!)

**49.** Докажите следующие утверждения.

а) Если  $a, b$  – такие натуральные числа, что  $(\sqrt{3} + \sqrt{2})^{2001} = a\sqrt{3} + b\sqrt{2}$ , то  $3a^2 - 2b^2 = 1$ .

б) Если  $a$  и  $b$  – такие натуральные числа, что  $3a^2 - 2b^2 = 1$ , то для некоторого нечетного натурального числа  $n$  имеем:  $a\sqrt{3} + b\sqrt{2} = (\sqrt{3} + \sqrt{2})^n$ .

**50.** Докажите следующие утверждения.

а) Существует бесконечно много таких пар натуральных чисел  $a$  и  $b$ , что  $a^2 + 1$  делится на  $b$ , а  $b^2 + 1$  делится на  $a$ .

б) Если  $x < y$  – натуральные числа и  $x^2 + y^2 + 1 = 3xy$ , то  $x = \varphi_{2n-1}$  и  $y = \varphi_{2n+1}$ , где  $n$  – некоторое натуральное число.

в) Если  $a, b$  и  $c = \frac{a^2 + b^2 + 1}{ab}$  – натуральные числа, то  $c = 3$ .

г) Если два натуральных числа таковы, что увеличенный на единицу квадрат любого из них делится на другое, то произведение этих чисел на единицу больше квадрата их разности.

д)\* Уравнение  $x^2 - (n^2 - 4)y^2 = -4$  не имеет решений в целых числах при натуральном  $n \neq 3$ .

е) Уравнение  $x^2 - (n^2 - 4)y^2 = -1$  не имеет решений в целых числах при натуральном  $n \neq 3$ .

**51 (M1225\*).** Докажите, что

а\*) если для натуральных чисел  $a$  и  $b$  число  $(a^2 + b^2)/(ab - 1)$  натуральное, то оно равно 5;

б) уравнение  $x^2 - 5xy + y^2 + 5 = 0$  имеет бесконечно много решений в натуральных числах.

**52.** Для любого натурального  $n$  число  $\left[ (3 + \sqrt{11})^{2n-1} \right]$  делится на  $2^n$  и не делится на  $2^{n+1}$ . Докажите это.

**53.** Для любого четного натурального  $n$  число

$$\left[ \left( \frac{3 + \sqrt{5}}{2} \right)^n \right] - 1 = \left( \frac{3 + \sqrt{5}}{2} \right)^n + \left( \frac{3 - \sqrt{5}}{2} \right)^n - 2$$

является квадратом натурального числа, а для любого нечетного — упятеренным квадратом натурального числа. Докажите это.

**54\*.** а) Существуют такие иррациональные числа  $\alpha > 1$  и  $\beta > 1$ , что ни при каких натуральных  $m$  и  $n$  целые части чисел  $\alpha^m$  и  $\beta^n$  не совпадают. Докажите это.

б) Придумайте такую последовательность иррациональных чисел  $\alpha_1, \alpha_2, \alpha_3, \dots$ , что равенство  $[\alpha_r^m] = [\alpha_s^n]$ , где  $r, s, m$  и  $n$  — натуральные числа, верно лишь при  $r = s$  и  $m = n$ .

Использование иррациональностей

Неравенства, неравенства, неравенства... Есть ощущение какого-то фокуса, когда все сходится, но причина удачи спрятана и не видна наивному зрителю. Сейчас мы докажем теорему 9 заново. Надеемся, этим мы поможем вам вполне уяснить ее смысл.

**Лемма 7.** Если  $x^2 - dy^2 > 0$  и  $x + y\sqrt{d} > 0$ , то  $x > 0$ .

**Доказательство.**  $2x = x + y\sqrt{d} + \frac{x^2 - dy^2}{x + y\sqrt{d}} > 0$ .

Есть и другой способ — «от противного». Предположим, что  $x \leq 0$ . Тогда обе части неравенства  $y\sqrt{d} > -x$  можно возвести в квадрат:  $dy^2 > x^2$ , что противоречит неравенству  $x^2 - dy^2 > 0$ .

**Лемма 8.** Если  $x^2 - dy^2 = 1$  и  $x + y\sqrt{d} > 1$ , то  $y > 0$ .

**Доказательство.** Пусть  $y \leq 0$ . Тогда

$$x - y\sqrt{d} \geq x + y\sqrt{d} > 1.$$

Произведение чисел  $x - y\sqrt{d}$  и  $x + y\sqrt{d}$ , каждое из которых больше 1, не может равняться 1.

**Лемма 9.** Если  $a^2 - db^2 = x^2 - dy^2$  и  $x + y\sqrt{d} < a + b\sqrt{d}$ , причем числа  $a, b, x$  и  $y$  неотрицательные, то  $x < a$  и  $y < b$ .

**Доказательство.**

$$a - b\sqrt{d} = \frac{a^2 - db^2}{a + b\sqrt{d}} < \frac{x^2 - dy^2}{x + y\sqrt{d}} = x - y\sqrt{d}.$$

Сложив неравенства

$$-x + y\sqrt{d} < -a + b\sqrt{d}$$

и

$$x + y\sqrt{d} < a + b\sqrt{d},$$

получаем:  $2y\sqrt{d} < 2b\sqrt{d}$ . Дальнейшее очевидно.

**Лемма 10.** Пусть  $a$  – наименьшее натуральное число, для которого существует такое натуральное число  $b$ , что  $a^2 - db^2 = 1$ . Если  $x, y$  – целые числа и  $1 < x + y\sqrt{d} < a + b\sqrt{d}$ , то  $x^2 - dy^2 \neq 1$ .

**Доказательство.** Предположим противное:  $x^2 - dy^2 = 1$ . Тогда в силу лемм 7 и 8 числа  $x$  и  $y$  положительны. В силу леммы 9 имеем  $x < a$ . Получили противоречие.

Следующая теорема – это другая формулировка теоремы 9.

**Теорема 11.** Пусть  $a$  – наименьшее натуральное число, для которого существует такое натуральное число  $b$ , что  $a^2 - db^2 = 1$ . Если  $x, y$  – целые числа,  $x^2 - dy^2 = 1$  и  $x + y\sqrt{d} > 0$ , то для некоторого целого числа  $n$  верно равенство  $x + y\sqrt{d} = (a + b\sqrt{d})^n$ .

**Доказательство.** Обозначим  $q = a + b\sqrt{d}$ . Поскольку числа  $a$  и  $b$  натуральные, то  $q > 1$ . Рассмотрим возрастающую геометрическую прогрессию:

$$1 < q < q^2 < q^3 < q^4 < q^5 < \dots$$

Она стремится к бесконечности. А убывающая геометрическая прогрессия

$$1 < \frac{1}{q} < \frac{1}{q^2} < \frac{1}{q^3} < \frac{1}{q^4} < \frac{1}{q^5} < \dots$$

стремится к нулю.

Поэтому существует такое целое  $n$ , что

$$q^{n-1} < x + y\sqrt{d} \leq q^n.$$

Рассмотрим число

$$E = (x + y\sqrt{d}) : q^{n-1}.$$

Очевидно,  $1 < E \leq q$ . Поскольку

$$\frac{1}{q} = \frac{1}{a + b\sqrt{d}} = \frac{a - b\sqrt{d}}{(a - b\sqrt{d})(a + b\sqrt{d})} = \frac{a - b\sqrt{d}}{a^2 - db^2} = a - b\sqrt{d},$$



$$E = (x + y\sqrt{d})(a - b\sqrt{d})^{n-1}.$$

Воспользовавшись формулой

$$(r + s\sqrt{d})(u + v\sqrt{d}) = (ru + dsu) + (rv + su)\sqrt{d},$$

мы заключаем, что число  $E$  представимо в виде  $E = z + t\sqrt{d}$ , где  $z, t$  — целые числа. Переходя к сопряженным числам, получаем:

$$z - t\sqrt{d} = (x - y\sqrt{d})(a + b\sqrt{d})^{n-1}.$$

Следовательно,

$$\begin{aligned} z^2 - dt^2 &= (z + t\sqrt{d})(z - t\sqrt{d}) = \\ &= (x + y\sqrt{d})(x - y\sqrt{d})(a - b\sqrt{d})^{n-1}(a + b\sqrt{d})^{n-1} = \\ &= (x^2 - dy^2)(a^2 - db^2)^{n-1} = 1. \end{aligned}$$

Итак, числа  $z$  и  $t$  целые,  $1 < z + t\sqrt{d} \leq a + b\sqrt{d}$  и  $z^2 - dt^2 = 1$ . В силу леммы 10 это возможно лишь в случае равенства  $z + t\sqrt{d} = a + b\sqrt{d}$ , т.е. в случае

$$x + y\sqrt{d} = q^n,$$

что и требовалось доказать.

**Упражнение 55.** Пусть  $a$  — наименьшее натуральное число, для которого существует такое натуральное число  $b$ , что  $a^2 - db^2 = 1$ . Если  $x, y$  — целые числа и  $x^2 - dy^2 = 1$ , то для некоторого целого числа  $n$  имеем:  $x + y\sqrt{d} = \pm(a + b\sqrt{d})^n$ . Докажите это.

$$\text{Уравнение } x^2 - dy^2 = c$$

Доказательство теоремы 12 могло показаться довольно длинным. Не вполне ясно, что проще: жонглировать неравенствами или иррациональностями. Оказывается, однако, что использованное при доказательстве теоремы 12 рассуждение позволяет выяснить, как устроены решения в целых числах уравнения  $x^2 - dy^2 = c$ .

Напомним обозначения. Как и прежде,  $d$  — натуральное

число, не являющееся квадратом;  $a$  – наименьшее натуральное число, для которого существует такое натуральное число  $b$ , что  $a^2 - db^2 = 1$ ;  $q = a + b\sqrt{d}$ ; наконец,  $c$  – некоторое целое число,  $c \neq 0$ .

Пусть  $x$  и  $y$  – целые числа,  $x^2 - dy^2 = c$  и  $x + y\sqrt{d} > 0$ . Рассмотрим числа вида  $q^n$ , где  $n$  пробегает множество всех целых чисел. Поскольку  $\lim_{n \rightarrow -\infty} q^n = 0$  и  $\lim_{n \rightarrow +\infty} q^n = +\infty$ , то существует такое целое число  $n$ , что

$$q^{n-1} < x + y\sqrt{d} \leq q^n.$$

Рассмотрим число

$$E = (x + y\sqrt{d}) : q^{n-1}.$$

Легко понять, что  $E$  представимо в виде

$$E = z + t\sqrt{d},$$

где  $z$  и  $t$  – целые числа. При этом

$$z^2 - dt^2 = c \quad (*)$$

и

$$1 < z + t\sqrt{d} \leq q. \quad (**)$$

**Теорема 12.** *Рассмотрим всевозможные пары целых чисел  $(z; t)$ , удовлетворяющие условиям  $(*)$  и  $(**)$ . Верны следующие утверждения.*

1) Если множество  $M$  таких пар пусто, то уравнение  $x^2 - dy^2 = c$  не имеет решений в целых числах  $x$  и  $y$ .

2) Множество  $M$  конечно.

3) Все целочисленные решения уравнения  $x^2 - dy^2 = c$  можно получить из формул  $x + y\sqrt{d} = \pm(z + t\sqrt{d})q^n$ , где  $(z; t) \in M$ , а  $n$  – целое число.

**Доказательство.** Первое и третье утверждения очевидны. Докажем второе. Пусть  $(z; t) \in M$ . Тогда

$$z - t\sqrt{d} = \frac{c}{z + t\sqrt{d}},$$

так что

$$|z - t\sqrt{d}| < |c|$$

и, следовательно,

$$|z| = \left| \frac{(z + t\sqrt{d}) + (z - t\sqrt{d})}{2} \right| < \frac{q + |c|}{2},$$

$$|t| = \left| \frac{(z + t\sqrt{d}) - (z - t\sqrt{d})}{2} \right| < \frac{q + |c|}{2\sqrt{d}}.$$

Теорема 12 доказана. А второму способу доказательства теоремы 10 посвящена следующая часть статьи.

### Упражнения

**56.** Уравнение  $x^2 - 11y^2 = 17$  не имеет решений в целых числах. Докажите это.

**57.** Найдите все наборы а) 11; б) 23 последовательных целых чисел, сумма квадратов которых является квадратом целого числа.

**58.** Найдите все такие натуральные числа  $x$ , что число, получаемое зачеркиванием последней цифры числа  $x^2$ , тоже является квадратом натурального числа.

**59.** Решите в целых числах уравнение а)  $x^2 - 17y^2 = -16$ ; б)  $x^2 - (n^2 + 1)y^2 = -1$ , где  $n$  – натуральное число.

**60.** Если уравнение  $x^2 - dy^2 = -1$  имеет решение в натуральных числах  $x$  и  $y$ , то, выбрав из таких решений то, где  $x$  – наименьшее возможное, получим: а)  $q = (x + y\sqrt{d})^2$ ; б)  $|M| = 1$ . Докажите это.

**61.** Пусть  $p$  – простое число,  $p \equiv 1 \pmod{4}$ ,  $a$  – наименьшее (существующее в силу теоремы 10) натуральное число, для которого существует такое натуральное число  $b$ , что  $a^2 - pb^2 = 1$ . Докажите, что а)  $a$  нечетно; б) для некоторых натуральных чисел  $u$  и  $v$  верны равенства  $a \pm 1 = 2u^2$ ,  $a \mp 1 = 2pv^2$  и  $b = 2uv$ ; в)  $u^2 - pv^2 = -1$ .

**62.** Докажите, что если  $(z; t) \in M$ , то для всех достаточно больших натуральных  $n$  целые числа  $x$  и  $y$ , определяемые равенством  $x + y\sqrt{d} = (z + t\sqrt{d})q^n$ , положительны.

**63.** При  $a \geq 2$  уравнение  $x^2 - (a^2 + 1)y^2 = -a^2$  имеет не менее трех серий решений, т.е. множество  $M$  для него состоит не менее чем из трех элементов. Докажите это.

**64\*.** Решите в натуральных числах уравнение а)  $3^s = 2^r + 1$ ; б)  $x^2 + 2^y = 3^z$ .

**65\*.** Решите в целых числах уравнение а)  $x^2 + 8xy + y^2 + 2x - 4y + 1 = 0$ ; б)  $3u^2 + 11uv + 9v^2 + u + v = 0$ .

### Часть III. Поиск нетривиального решения

#### Вызов Ферма

*Начало есть более, чем половина всего.*

Аристотель

В 1657 году – в довольно поздний период своей деятельности – Пьер Ферма в качестве вызова разослал другим математикам, в частности английским, следующую задачу.

«Сейчас едва ли найдется кто-нибудь, кто предлагает арифметические вопросы, и кто-нибудь, кто их понимает. Не потому ли это происходит, что до сих пор арифметику рассматривали скорее с геометрической, чем с арифметической точки зрения? Так было всегда – и в древних, и в современных работах; примером тому является даже Диофант. Ибо хотя он и более чем другие освободился от геометрии в том отношении, что ограничивает свой анализ рассмотрением рациональных чисел, однако даже у него геометрия не полностью отсутствует...

Теперь арифметика имеет, так сказать, собственную область изучения – теорию целых чисел. Евклид лишь слегка затронул ее в своих «Началах», а его последователи недостаточно занимались этой теорией (если только она не содержалась в тех книгах Диофанта, которых мы лишились вследствие разрушительного действия времени); следовательно, арифметикам предстоит развивать или восстанавливать ее.

Поэтому арифметикам, дабы осветить тот путь, по которому надо следовать, предлагаю я эту теорему, чтобы они доказали ее, или эту задачу, чтобы они решили ее. Если же преуспеют они в ее доказательстве или решении, то им придется признать, что вопросы такого рода ничем не уступают в отношении красоты, трудности или метода доказательства самым знаменитым вопросам геометрии.

*Если дано произвольное число, которое не является квадратом, то найдется бесконечное множество таких квадратов, что если этот квадрат умножить на данное число и к произведению прибавить единицу, то результат будет квадратом.*

Пример. Пусть 3, которое не является квадратом, будет данным числом. Если умножить его на квадрат, равный 1, и к произведению добавить 1, то в результате получится 4, что является квадратом. Если то же самое число 3 умножить на квадрат 16, то получится произведение, которое при увеличении на 1 превращается в 49, тоже квадрат. И кроме 1 и 16 можно найти бесконечное множество квадратов с тем же свойством.

Но я спрашиваю об общем правиле решения – когда дано произвольное число, не являющееся квадратом. Например, найдите такой квадрат, что если произведение этого квадрата и числа 149, 109 или 433 увеличить на 1, то получится квадрат.»

Вступление Ферма к этой задаче ясно показывает, что он желает не традиционного диофантова решения в рациональных числах, а решения в *целых* числах. (По иронии судьбы ныне слово «диофантово» употребляют, желая получить решения в целых числах, тогда как сам Диофант ни в одной из дошедших до нас работ не занимался решениями в целых числах, а только в рациональных.) Как это ни странно, вступление было опущено одним из посредников в том экземпляре письма, который был передан английским математикам; в результате они сочли задачу совершенно глупой. А именно, можно ввести обозначение

$$x = 1 + \frac{m}{n} y$$

и подставить в уравнение:

$$\left(1 + \frac{m}{n} y\right)^2 - dy^2 = 1,$$

$$\frac{2m}{n} y + \frac{m^2}{n^2} y^2 - dy^2 = 0,$$

$$2mn = (dn^2 - m^2) y,$$

откуда

$$y = \frac{2mn}{dn^2 - m^2}, \quad x = \frac{dn^2 + m^2}{dn^2 - m^2}.$$

Полученные формулы, как легко убедиться, дают бесконечно много решений в рациональных числах.

**Упражнение 66.** а) Убедитесь, что эти формулы дают все решения. б) Найдите аналогичные формулы для уравнения  $x^2 + y^2 = 1$ .

Когда же дополнительное требование, что  $x$  и  $y$  должны быть целыми числами, дошло до английских математиков, то они пожаловались, что условие задачи изменили. Конечно, их жалобу можно понять в свете сильной диофантовой традиции, но, как указал Ферма, было наивно надеяться, что он предложил тривиальную задачу. Как видно из таблицы, задача Ферма весьма сложная: для  $d = 61$  наименьшее решение – это пара  $y = 226153980$  и  $x = 1766319049$ . (Впрочем, впервые посчитал это не Ферма, а родившийся в 1114 году индеец Бхаскара Акхария.) А для  $d = 109$  (и этот случай был выделен Ферма!) вообще  $y = 15140424455100$ .

Для каждого числа  $d \leq 150$ , не являющегося квадратом, указано наименьшее натуральное  $y$ , для которого  $dy^2 + 1$  – квадрат.

2) 2	42) 2	79) 9	116) 910
3) 1	43) 531	80) 1	117) 60
5) 4	44) 30	82) 18	118) 28254
6) 2	45) 24	83) 9	119) 11
7) 3	46) 3588	84) 6	120) 1
8) 1	47) 7	85) 30996	122) 22
10) 6	48) 1	86) 1122	123) 11
11) 3	50) 14	87) 3	124) 414960
12) 2	51) 7	88) 21	125) 83204
13) 180	52) 90	89) 53000	126) 40
14) 4	53) 9100	90) 2	127) 419775
15) 1	54) 66	91) 165	128) 51
17) 8	55) 12	92) 120	129) 1484
18) 4	56) 2	93) 1260	130) 570
19) 39	57) 20	94) 221064	131) 927
20) 2	58) 2574	95) 4	132) 2
21) 12	59) 69	96) 5	133) 224460
22) 42	60) 4	97) 6377352	134) 12606
23) 5	61) 226153980	98) 10	135) 21
24) 1	62) 8	99) 1	136) 3
26) 10	63) 1	101) 20	137) 519712
27) 5	65) 16	102) 10	138) 4
28) 24	66) 8	103) 22419	139) 6578829
29) 1820	67) 5967	104) 5	140) 6
30) 2	68) 4	105) 4	141) 8
31) 273	69) 936	106) 3115890	142) 12
32) 3	70) 30	107) 93	143) 1
33) 4	71) 413	108) 130	145) 24
34) 6	72) 2	109) 15140424455100	146) 12
35) 1	73) 267000	110) 2	147) 8
37) 12	74) 430	111) 28	148) 6
38) 6	75) 3	112) 12	149) 2113761020
39) 4	76) 6630	113) 113296	150) 4
40) 3	77) 40	114) 96	
41) 120	78) 6	115) 105	

## Что сделали англичане?

*...все уже сочинено в далекие средние века – и современными авторами только воруются. А средневековые авторы, в свою очередь, покрали эти мысли у античных, и если что-то новое у них мелькнуло – это, значит, из источников не сохранившихся и до нас не дошедших.*

И.Губерман

Англичанам удалось не только найти частные решения при  $d = 149, 109$  или  $433$ , но и разработать общую процедуру получения решений для любого значения  $d$ . Кто это сделал – неизвестно. Хотя Джон Валлис первым дал описание процедуры и получил решения в трех частных случаях, он приписывает авторство виконту Уильяму Броункеру. В опубликованной переписке Валлиса нет никаких указаний на то, что Броункер когда-либо сообщал ему что-либо об этом методе, кроме нескольких простых замечаний, которые, быть может, послужили зародышем идеи, развитой впоследствии Валлисом. Возможно, Валлису было важно добиться расположения Броункера и добиться его покровительства, поэтому он и назвал этот метод методом Броункера (ибо Броункер не только принадлежал к знати, но и был первым президентом Королевского общества). Впрочем, некоторые историки считают самого Броункера весьма способным математиком и утверждают, что по своим личным качествам Валлис скорее мог приписать себе чужие заслуги, чем отказаться от своих.

Строго говоря, англичане не решили задачу Ферма, которая заключалась в том, что при данном (не являющемся квадратом) натуральном  $d$  существует бесконечно много натуральных  $x$  таких, что  $dx^2 + 1$  является квадратом. Они не доказали, что процедура всегда завершится, и, кажется, даже не понимали, что это нужно доказывать.<sup>1</sup>

Ферма написал письмо, в котором признал, что англичанам удалось решить его задачу, не проявив ни малейшей неудовлетворенности их методом. Однако главным для Ферма в этом письме было убедить англичан, что перед ними была поставлена достойная задача, так что он мог сознательно закрыть глаза на недостатки.

---

<sup>1</sup> Даже Эйлеру не удалось доказать, что английский метод всегда приводит к успеху. Удалось – Лагранжу через 110 лет после того, как Валлис отослал ответ на вызов Ферма.

Несколько лет спустя, подводя в письме к Каркави итоги некоторых своих открытий, Ферма указал, что англичане получили решение его задачи только в отдельных частных случаях и им не удалось дать общее доказательство. Очевидная интерпретация этого замечания заключается в том, что Ферма заметил отсутствие доказательства того, что предложенный ими процесс всегда приводит к решению; с другой стороны, в нем можно увидеть и менее глубокую критику того, что процесс был описан в недостаточно общих терминах. Ферма утверждает, что он мог бы дать доказательство, «надлежащим образом» применив метод бесконечного спуска. Эти слова, разумеется, нельзя считать достаточным свидетельством в пользу того, что он умел решать свою задачу.

Термин «уравнение Пелля» возник в результате ошибки Леонарда Эйлера. Почему-то – возможно, по причине смутных воспоминаний, оставшихся от чтения «Алгебры» Валлиса, – у Эйлера создалось впечатление, будто Валлис приписывает метод решения этой задачи не Броункеру, а Пеллю – современнику Валлиса, который много раз упомянут в его работах, но не имел никакого отношения к уравнению  $x^2 - dy^2 = 1$ . Эйлер впервые сделал эту ошибку в 1730 году, когда ему было 23 года, но она попала и в окончательное издание «Введения в алгебру» (примерно 1770 год). Эйлер был самым популярным математическим автором своего времени и поэтому ошибка вошла в историю...

### Индийский и английский методы

*Индия – родина циклического метода.*

Легенды гласят, что за несколько веков до нашей эры в Индии было известно равенство  $2 \cdot 408^2 + 1 = 577^2$ . Равенство  $92 \cdot 120^2 + 1 = 1151^2$  вместе с изощренной техникой его вывода было получено Брахмагуптой (родился в 598 году). Общий способ решения уравнения Пелля дал Бхаскара Акхария. Этот метод называют циклическим или индийским.

Познакомимся с ним на примере  $d = 67$ . Наша цель – найти такие натуральные  $x$  и  $y$ , чтобы разность  $y^2 - 67x^2$  равнялась 1. В качестве первого приближения рассмотрим равенство

$$8^2 - 67 \cdot 1^2 = -3.$$

Вспомнив формулу

$$(a^2 - 67b^2)(c^2 - 67d^2) = (ac + 67bd)^2 - 67(bc + ad)^2$$



и применив ее к равенствам  $8^2 - 67 \cdot 1^2 = -3$  и  $r^2 - 67 \cdot 1^2 = s$ , где  $r$  (а тем самым и  $s$ ) будут определены позже, получим:

$$(8r + 67)^2 - 67(r + 8)^2 = -3s.$$

Пытаясь сделать правую часть (по модулю) как можно меньшей только за счет выбора наименьшего по модулю значения  $s$ , мы выбрали бы  $r = 8$ , при котором  $s = -3$ , и получили бы равенство

$$131^2 - 67 \cdot 16^2 = 9,$$

с которым непонятно что делать дальше.

*Идея циклического метода* – выбор такого  $r$ , чтобы  $r + 8$  делилось на 3 и  $s$  при этом было как можно меньше по модулю. (Когда это сделано, обе части уравнения разделятся нацело на  $3^2$ .)

*Идея английского метода* – выбор такого как можно большего  $r$ , что  $r^2 < d$  и  $r + 8$  делится на 3. Как видите, методы очень похожи. Оба можно применять для поиска решений при данном  $d$ , не будучи заранее уверенным, что это приведет к успеху. (Между прочим, априори нет никакой уверенности в том, что в общем случае в английском методе после каждого шага  $r$  будет существовать. Это – одна из теорем, которые надо доказывать, обосновывая английский метод.)

Проведем подробно вычисления для циклического метода. Чтобы  $r + 8$  делилось на 3, число  $r$  должно равняться одному из чисел бесконечной в обе стороны арифметической прогрессии  $\dots, -2, 1, 4, 7, 10, 13, 16\dots$ . Выбор  $r = 7$  дает наименьшее по модулю значение  $s = -18$ . Этим  $r$  и  $s$  соответствует равенство

$$123^2 - 67 \cdot 15^2 = 54,$$

которое после сокращения на 9 превращается в

$$41^2 - 67 \cdot 5^2 = 6.$$

Теперь – следующий шаг циклического метода:

$$(41r + 67 \cdot 5)^2 - 67(5r + 41)^2 = 6s.$$

Число  $5r + 41$  делится на 6 при  $r = 5, 11, 17, 23, \dots$ . Выбор  $r = 5$  дает наименьшее по модулю  $s = -42$ , и мы получаем равенство  $540^2 - 67 \cdot 66^2 = 6 \cdot (-42)$ , которое после сокращения на  $6^2$  превращается в

$$90^2 - 67 \cdot 11^2 = -7.$$

Дальше надо выполнить следующий шаг циклического метода, потом еще один, и так до тех пор, пока не получим равенство, в правой части которого будет 1.

### Упражнения

**67.** Выполнив еще пять шагов циклического метода, найдите решение  $48842^2 - 67 \cdot 5967^2 = 1$ .

**68.** а) Выполните вычисления для  $d = 67$ , применяя английский метод. б) Сравнив английский и циклический методы для  $d = 67$  и для нескольких других значений  $d$ , сформулируйте гипотезу о взаимосвязи этих двух методов.

Если вы решили эти два упражнения, то убедились, что индийский и английский методы позволяют найти решение для  $d = 67$ . Однако ни для английского, ни для индийского метода нет никаких очевидных причин, по которым равенство с правой частью 1 должно обязательно получиться в общем случае. Есть и много других вопросов. Например, если эти методы дадут нам какое-то решение уравнения Пелля, можно ли утверждать, что это решение – наименьшее из возможных? Ответ на эти вопросы вы найдете в статье «Цепные дроби», если сравните алгоритм разложения числа  $\sqrt{d}$  в цепную дробь с работой английского метода. А еще лучше – поймите, как связаны между собой индийский, английский методы и алгоритм Вайлсбергера.

А мы ограничимся неконструктивным доказательством существования решения уравнения Пелля.

### Приближения иррациональных чисел рациональными

**Лемма 11.** Для любого вещественного числа  $\xi$  и любого натурального числа  $N$  существуют такие целое число  $a$  и натуральное число  $b$ , что  $b \leq N$  и

$$|b\xi - a| \leq \frac{1}{N+1}.$$

**Доказательство.** Рассмотрим числа 0 и 1, а также дробные части чисел  $\xi$ ,  $2\xi$ , ...,  $N\xi$ . Если бы все расстояния между этими  $(N+2)$ -мя числами были больше  $1/(N+1)$ , то получилось бы противоречие. Значит, какое-то из расстояний не превосходит  $1/(N+1)$ . Если, например,

$$|\{b_2\xi\} - \{b_1\xi\}| \leq \frac{1}{N+1},$$

где  $-1 \leq b_1 < b_2 \leq N$ , то

$$\left| (b_2\xi - [b_2\xi]) - (b_1\xi - [b_1\xi]) \right| \leq \frac{1}{N+1},$$

так что достаточно взять  $b = b_2 - b_1$  и  $a = [b_2\xi] - [b_1\xi]$ . Остальные два случая столь же очевидны: если

$$\{b\xi\} - 0 \leq \frac{1}{N+1},$$

то годится  $a = [b\xi]$ ; если же

$$1 - \{b\xi\} \leq \frac{1}{N+1},$$

то можно взять  $a = [b\xi] + 1$ . Лемма доказана.

### Упражнения

**69.** Для любых чисел  $\xi_1, \xi_2, \dots, \xi_k$  и любого натурального числа  $N$  существуют такие целые числа  $b_1, b_2, \dots, b_k$  и  $a$ , что абсолютные величины чисел  $b_1, b_2, \dots, b_k$  не превосходят  $N$  и

$$|b_1\xi_1 + b_2\xi_2 + \dots + b_k\xi_k - a| \leq \frac{1}{N^k + 1}.$$

Докажите это.

**70.** Для любых чисел  $\xi_1, \xi_2, \dots, \xi_k$  и любого натурального числа  $N$  существует такое натуральное число  $b$ , что  $b \leq N^k$  и дробные части чисел  $b\xi_1, b\xi_2, \dots, b\xi_k$  не превосходят  $1/(N+1)$ . Докажите это.

**71.** Какой бы многоугольник мы ни нарисовали на плоскости и какое бы маленькое положительное число  $\epsilon$  ни взяли, можно подвергнуть многоугольник такой гомотетии с натуральным коэффициентом, что все координаты вершин полученного многоугольника будут отличаться от целых чисел не более чем на  $\epsilon$ . Докажите это.

### Доказательство теоремы 10

Положим  $\xi = \sqrt{d}$ . Для любого натурального  $n > 1$  в силу леммы существуют такие натуральные числа  $a_n$  и  $b_n$ , что  $b_n < n$  и

$$|a_n - b_n\sqrt{d}| \leq \frac{1}{n}.$$

Очевидно,

$$\begin{aligned} |a_n^2 - db_n^2| &= |a_n - b_n\sqrt{d}| \cdot |a_n + b_n\sqrt{d}| \leq \frac{1}{n} \cdot |a_n - b_n\sqrt{d} + 2b_n\sqrt{d}| \leq \\ &\leq \frac{1}{n} \cdot \left( \frac{1}{n} + 2n\sqrt{d} \right) < 1 + 2\sqrt{d}. \end{aligned}$$

Итак, величина  $a_n^2 - db_n^2$  может принимать лишь конечное число

значений. Но  $n$  можно брать сколь угодно большим! И при этом в силу неравенства  $\left| a_n - b_n \sqrt{d} \right| \leq \frac{1}{n}$  при  $n \rightarrow \infty$  имеем  $b_n \rightarrow \infty$ . Значит, хотя бы для одного целого числа  $c$ , по модулю меньшего  $1 + 2\sqrt{d}$ , существует бесконечно много пар натуральных чисел  $(a_n; b_n)$ , для которых

$$a_n^2 - db_n^2 = c.$$

Зафиксируем одно из таких чисел  $c$ . Рассмотрим остатки от деления чисел  $a_n$  и  $b_n$  на  $|c|$ . Поскольку количество остатков конечно, то существуют такие две<sup>2</sup> разные пары натуральных чисел  $(a; b)$  и  $(A; B)$ , что

$$a^2 - db^2 = c = A^2 - dB^2$$

и

$$a \equiv A \pmod{|c|},$$

$$b \equiv B \pmod{|c|}.$$

(Продумайте это!) Рассмотрим частное

$$\frac{A + B\sqrt{d}}{a + b\sqrt{d}} = \frac{(a - b\sqrt{d})(A + B\sqrt{d})}{a^2 - db^2} = \frac{aA - bBd + (aB - Ab)\sqrt{d}}{c}.$$

Поскольку

$$aA - bBd \equiv a^2 - b^2d = c \equiv 0 \pmod{|c|}$$

и

$$aB - Ab \equiv ab - ab = 0 \pmod{|c|},$$

то числа  $x = (aA - bBd)/c$  и  $y = (aB - Ab)/c$  целые. Поскольку

$$\begin{aligned} x^2 - dy^2 &= (x - y\sqrt{d})(x + y\sqrt{d}) = \\ &= \frac{A - B\sqrt{d}}{a - b\sqrt{d}} \cdot \frac{A + B\sqrt{d}}{a + b\sqrt{d}} = \frac{A^2 - dB^2}{a^2 - db^2} = \frac{c}{c} = 1 \end{aligned}$$

и  $y \neq 0$ , то  $(x; y)$  – искомое нетривиальное решение уравнения Пелля!

### Упражнения

**72.** Докажите, что  $y \neq 0$ .

**73.** Докажите, что а) для любого натурального числа  $n$  существуют такие натуральные  $x$  и  $y$ , что  $x^2 - 3y^2 = 1$  и  $y$  делится на  $3^n$ ; б) однако степенью тройки  $y$  быть не может.

---

<sup>2</sup> На самом деле даже не две, а бесконечно много, но нам это не нужно.

## Часть IV. Уравнение $C_x^{y-1} = C_{x-1}^y$

*Все авторы стремятся довести читателя до точки, но каждый – по-своему.*

С.Лузан

Напоследок разберем еще один пример. К уравнению  $C_x^{y-1} = C_{x-1}^y$  можно прийти, рассматривая 14-ю строку треугольника Паскаля: 1, 14, 91, 364, **1001**, **2002**, **3003**, 3432, 3003, 2002, 1001, 364, 91, 14, 1.

Коротко расскажем о числах сочетаний  $C_n^m$  тем, кто с ними еще не знаком.  $C_n^m$  – это количество способов из данных  $n$  предметов выбрать какие-нибудь  $m$ . Из чисел  $C_n^m$  можно составить треугольник Паскаля (рис.6): в его  $n$ -й строке на  $m$ -м месте стоит число

$$C_n^m = \frac{n!}{m!(n-m)!},$$

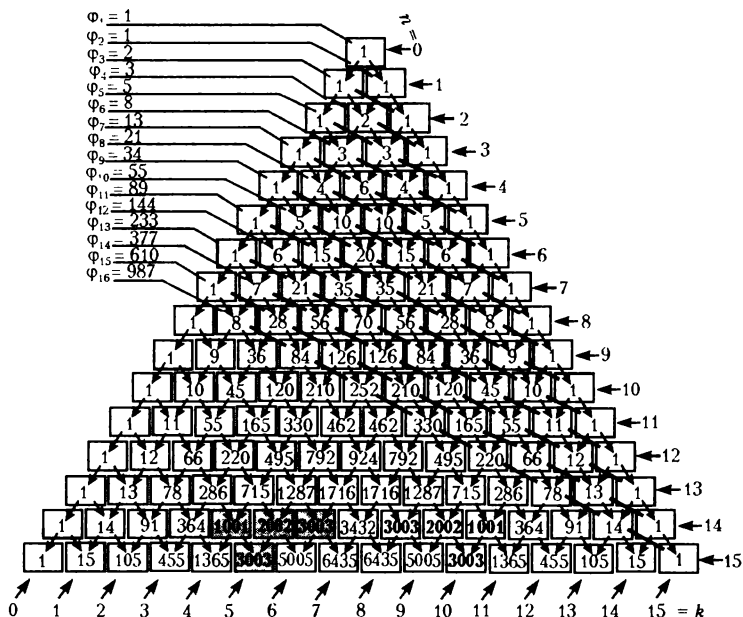


Рис. 6

причем как нумерация чисел в строках, как и нумерация строк начинается с нуля. Основное свойство образования треугольника Паскаля таково: *сумма любых двух соседних чисел некоторой строки равна числу следующей строки, которое расположено «ниже них и между ними»;*

другими словами, для любых натуральных чисел  $m$  и  $n$ , где  $m \leq n$ , верно равенство

$$C_n^{m-1} + C_n^m = C_{n+1}^m.$$

Очевидно,  $1001 + 2002 = 3003$ . Это означает, что  $C_{14}^4 + C_{14}^5 = C_{15}^6$ . Последнее равенство можно записать в виде

$$C_{15}^5 = C_{14}^6.$$

И вообще, любое равенство вида  $C_n^{m-2} + C_n^{m-1} = C_n^m$  можно записать в виде  $C_{n+1}^{m-1} = C_n^m$ .

**Теорема 13.** Равенство  $C_x^{y-1} = C_{x-1}^y$  выполнено тогда и только тогда, когда  $x = \varphi_{2k}\varphi_{2k+1}$  и  $y = \varphi_{2k-1}\varphi_{2k}$ , где  $k$  – некоторое натуральное число.

**Доказательство. I способ.** Выразим числа сочетаний через факториалы:

$$\frac{x!}{(y-1)!(x-y+1)!} = \frac{(x-1)!}{y!(x-1-y)!}.$$

После очевидных преобразований получаем:

$$xy = (x - y + 1)(x - y).$$

Обозначим буквой  $d$  наибольший общий делитель чисел  $x$  и  $y$ . Тогда  $x = ad$  и  $y = bd$ , где числа  $a$  и  $b$  взаимно просты. Подставив выражения для  $x$  и  $y$  в уравнение, после сокращения на  $d$  получаем равенство

$$abd = (ad - bd + 1)(a - b).$$

Поскольку числа  $a - b$  и  $ab$  взаимно просты и поскольку числа  $d$  и  $ad - bd + 1$  тоже взаимно просты, то

$$\begin{cases} ab = ad - bd + 1, \\ d = a - b, \end{cases}$$

т.е.

$$\begin{cases} a = b + d, \\ (b + d)b = (b + d)d - bd + 1. \end{cases}$$

Последнее уравнение после упрощений приобретает вид

$$b^2 + bd - d^2 = 1.$$

Его решения в натуральных числах нам известны:  $b = \varphi_{2k-1}$  и

$d = \varphi_{2k}$ , где  $k$  – натуральное число. Таким образом,

$$\begin{cases} x = ad = (\varphi_{2k-1} + \varphi_{2k}) \varphi_{2k} = \varphi_{2k} \varphi_{2k+1}, \\ y = bd = \varphi_{2k-1} \varphi_{2k}, \end{cases}$$

как и было обещано. Например, при  $k = 1, 2, 3$  имеем, соответственно,  $(x; y) = (2; 1), (15; 6), (104; 40)$ .

*Замечание.* Строго говоря, надо бы проверить, что всякая пара чисел  $(x; y) = (\varphi_{2k} \varphi_{2k+1}; \varphi_{2k-1} \varphi_{2k})$  удовлетворяет равенству  $(x - y + 1)(x - y) = xy$ . Немного подумав, можно понять, что это очевидно: двигаться «снизу вверх» по только что изложенному решению даже легче, чем «сверху вниз». Впрочем, годится и прямая проверка:

$$x - y = \varphi_{2k+1} \varphi_{2k} - \varphi_{2k-1} \varphi_{2k} = (\varphi_{2k+1} - \varphi_{2k-1}) \varphi_{2k} = \varphi_{2k}^2$$

и

$$x - y + 1 = \varphi_{2k}^2 + 1,$$

так что

$$(x - y + 1)(x - y) = (\varphi_{2k}^2 + 1) \varphi_{2k}^2 = \varphi_{2k} \varphi_{2k+1} \varphi_{2k-1} \varphi_{2k} = xy,$$

где мы воспользовались тождеством  $\varphi_{2k}^2 + 1 = \varphi_{2k+1} \cdot \varphi_{2k-1}$

**II способ.** Мы решили уравнение  $(x - y + 1)(x - y) = xy$ , применив довольно неожиданный трюк. Но есть и другой – стандартный – способ. А именно, есть стандартная схема, по которой решают в целых числах уравнения второй степени. Давайте посмотрим, как эта схема работает. Первым делом раскроем скобки и приведем подобные:

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

Теперь освободимся от членов первой степени. Для этого выполним замену  $x = X + a$ ,  $y = Y + b$ , получив уравнение

$$X^2 + 2aX + a^2 - 3XY - 3aY - 3bX - 3ab + Y^2 + 2bY + b^2 + X + a - Y - b = 0,$$

и приравняем коэффициенты при  $X$  и  $Y$  к нулю:

$$\begin{cases} 2a - 3b + 1 = 0, \\ -3a + 2b - 1 = 0. \end{cases}$$

Решив эту систему, находим  $a = -1/5$  и  $b = 1/5$ . При этих значениях  $a$  и  $b$  уравнение принимает вид

$$X^2 - 3XY + Y^2 = \frac{1}{5},$$

где  $X = x + \frac{1}{5}$  и  $Y = y - \frac{1}{5}$ . Домножив обе части уравнения на 20, получаем:

$$20X^2 - 60XY + 20Y^2 = 4,$$

$$5(4X^2 - 12XY + 9Y^2) - 25Y^2 = 4,$$

$$(5Y)^2 - 5(2X - 3Y)^2 = -4,$$

$$z^2 - 5t^2 = -4,$$

где  $z = 5Y = 5y - 1$  и  $t = 2X - 3Y = 2x - 3y + 1$ .

Как вы помните, все решения уравнения  $z^2 - 5t^2 = \pm 4$  в натуральных числах даются формулой  $(z; t) = (\varphi_{n+1} + \varphi_{n-1}; \varphi_n)$ . При этом знаку «+» соответствуют четные  $n$ , а знаку «-» – нечетные. Осталось понять, при каких нечетных  $n$  число  $z = \varphi_{n+1} + \varphi_{n-1}$  дает остаток 4 при делении на 5. Выпишем остатки от деления нескольких первых чисел Фибоначчи на 5:

$n$	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\varphi_n$	1	1	2	3	5	8	13	21	34	55	89	144	233	377
$\varphi_n \bmod 5$	1	1	2	3	0	3	3	1	4	0	4	4	3	2
$\varphi_{n-1} + \varphi_{n+1} \bmod 5$	1	3	4	2	1	3	4	2	1	3	4	2	1	

Закономерность очевидна:

$$n \equiv 3 \pmod{4}.$$

Итак,

$$y = \frac{z+1}{5} = \frac{\varphi_{n-1} + \varphi_{n+1} + 1}{5}$$

и

$$\begin{aligned} x = \frac{t+3y-1}{2} &= \frac{\varphi_n + 3 \frac{\varphi_{n-1} + \varphi_{n+1} + 1}{5} - 1}{2} = \frac{3\varphi_{n-1} + 5\varphi_n + 3\varphi_{n+1} - 2}{10} = \\ &= \frac{\varphi_n + 3\varphi_{n+1} - 1}{5} = \frac{\varphi_{n+1} + \varphi_{n+3} - 1}{5}, \end{aligned}$$

где  $n \equiv 3 \pmod{4}$ . Обозначив  $n = 4k - 1$ , запишем эти формулы в виде

$$x = \frac{\varphi_{4k} + \varphi_{4k+2} - 1}{5} = \varphi_{2k} \varphi_{2k+1}$$

и

$$y = \frac{\varphi_{4k-2} + \varphi_{4k} + 1}{5} = \varphi_{2k-1} \varphi_{2k},$$

где мы воспользовались тождеством

$$\varphi_{2m} + \varphi_{2m+2} - (-1)^m = 5\varphi_m \varphi_{m+1},$$

которое можно доказать по индукции, завершив тем самым второе доказательство теоремы.



### Упражнения

**74.** Докажите, что если  $x, y$  – натуральные числа, удовлетворяющие равенству  $x^2 - 3xy + y^2 + x - y = 0$  и неравенству  $x \geq y$ , то  $2x \geq 3y$ .

**75.** Докажите а) сравнение  $\varphi_{n+3} + \varphi_{n+5} \equiv \varphi_{n-1} + \varphi_{n+1} \pmod{5}$ ; б) тождества  $\varphi_{2m} = \varphi_{m+1}^2 - \varphi_{m-1}^2$  и  $\varphi_{2m+1} = \varphi_m^2 - \varphi_{m+1}^2$ ; в) тождество  $\varphi_{2m} + \varphi_{2m+2} = 5\varphi_m\varphi_{m+1} + (-1)^m$ .

**76 (М905).** Уравнение  $4x^n + (x+1)^2 = y^2$  относительно натуральных чисел  $x$  и  $y$  а) имеет бесконечно много решений при  $n = 2$ ; б) не имеет решений, если  $n \neq 2$  и  $n$  – натуральное число. Докажите это.

Один из важнейших разделов «Кванта» – «Задачник». Часть его задач – по арифметике. Многие из них вошли в качестве упражнений к статьям этой и предыдущей частей книги, однако некоторые другие задачи таким образом естественно включить в книгу не удалось, хотя они весьма достойны вашего внимания. Задачи довольно трудные, однако постарайтесь удержаться от соблазна сразу читать решение: пусть хотя бы неделя отделяет знакомство с условием от чтения решения! Это очень важно: если вы уделите размышлениям несколько минут каждый день, то даже в случаях, когда вы не решите задачу, а таких случаев скорее всего будет абсолютное большинство, вы очень многому научитесь! Без самостоятельных попыток пользы будет гораздо меньше... Наслаждайтесь!

---

**1. (M524)** Ни при каком натуральном  $m$  число  $1978^m - 1$  не делится на  $1000^m - 1$ . Докажите это.

(С.Конягин)

**2. (M1610)** Переаттестация Совета Мудрецов происходит так: король выстраивает их в колонну по одному и надевает на голову каждому колпак а) белого или черного; б) белого, синего или красного цвета. Каждый мудрец видит цвета колпаков всех других мудрецов, но не видит цвет своего колпака. Затем мудрецы по одному называют какой-нибудь цвет (каждому разрешено говорить только один раз). После этого король исключает из Совета всех, не угадавших цвет своего колпака. Могут ли мудрецы накануне переаттестации договориться, чтобы все, кроме быть может одного, избежали исключения?

(П.Кноп)

**3. (M2000)** Есть  $n$  мудрецов и неограниченный запас колпаков каждого из  $n$  различных цветов. Мудрецы одновременно закрывают глаза, и каждому из них надевают на голову колпак (например, все надетые колпаки могут оказаться одного цвета). Затем мудрецы открывают глаза. Каждый видит, какие

колпаки надеты на остальных, но не видит своего. После этого каждый мудрец пытается угадать, какого цвета его колпак, записав свою гипотезу на бумажке втайне от остальных. Докажите, что мудрецы могут заранее договориться таким образом, чтобы в любом случае хотя бы один угадал цвет своего колпака.

*(IX кубок памяти А.Н. Колмогорова)*

4. (M274) Найдите наименьшее число вида а)  $|11^m - 5^n|$ ;  
б)  $|36^m - 5^n|$ ; в)  $|53^m - 37^n|$ , где  $m$  и  $n$  – натуральные числа.

*(Ф.Шлейфер)*

5. (M1863\*) Рассмотрим последовательность, первые два члена которой равны 1 и 2 соответственно, а каждый следующий член – наименьшее натуральное число, которое еще не встретилось в последовательности и которое не взаимно просто с предыдущим членом последовательности. Докажите, что каждое натуральное число входит в эту последовательность.

*Замечание.* Эту последовательность называют ЕКГ-последовательностью (от слова “электрокардиограмма»). Вот первые 25 ее членов: 1, 2, 4, 6, 3, 9, 12, 8, 10, 5, 15, 18, 14, 7, 21, 24, 16, 20, 22, 11, 33, 27, 30, 25, 35, 28, 26, 13, 39, 36.

6. (M1480\*) Назовем ежом тело, составленное из куба и шести приклеенных к нему (в точности по граням) кубов того же размера. Кнопкой назовем тело, полученное из ежа отбрасыванием одного из кубиков (не центрального). Назовем 2-ежом состоящее из 13 кубиков тело, полученное приклеиванием к одному (центральному) кубу по 2 куба в каждом из 6 направлений. Разбейте пространство на а) ежи; б) кнопки; в) 2-ежи. г) Придумайте еще несколько фигур из кубов, на которые можно разбить пространство.

*(А.Спивак)*

Леонард Эйлер – математик, механик, физик и астроном. Родился в швейцарском городе Базеле. Отец его был пастором и хотел, чтобы сын тоже стал священником. В Базельском университете Эйлер изучал богословие и древние языки, но слушал и лекции И. Бернулли (1667–1748), который занимался с одним Эйлером дополнительно.

В 1727 году по рекомендации братьев Бернулли переехал в Санкт-Петербург, где нашел весьма благоприятные условия для научной деятельности. За 14 лет своего первого петербургского периода жизни Эйлер подготовил к печати около 80 трудов и опубликовал свыше 50. В Петербурге он изучил русский язык. Читал лекции студентам. Работал над усовершенствованием карт России. Создал двухтомный труд по теории кораблестроения, книгу по теории музыки и общедоступное «Руководство к арифметике».

В 1733 г. Эйлер женился на Екатерине Гзель – дочери академического живописца родом из Швейцарии, вывезенного Петром I из Голландии. Из тринадцати их детей выжили три сына и две дочери. Никакие научные занятия не были для него поводом пренебречь семейными обязанностями: ему приписывают слова «Где больше дадут, туда и служить пойду».

Неустойчивое положение времен регентства Анны Леопольдовны заставило Эйлера принять в 1741 году предложение прусского короля Фридриха II переехать в Берлин, где предстояла реорганизация почти бездействовавшего Общества наук в новую академию. За 25 лет жизни в Берлине он полностью или вчерне подготовил около 300 работ, среди них ряд больших монографий. Сохранил связи с Россией: печатал



в изданиях Петербургской академии примерно половину своих статей, редактировал математический отдел ее ученых записок, приобретал для академии научную литературу и оборудование, сообщал в частных письмах научные новости. Годами в берлинском доме Эйлера жили русские ученые, с которыми он вел занятия.

В 1766 г. вернулся в Петербург по приглашению Екатерины II. Он всерьез принял ее предложение участвовать в реорганизации Академии, причем стремился не к автономии науки, а к переплетению деятельности Академии и правительственных учреждений. Однако директором Академии Екатерина назначила младшего брата своего фаворита – графа В.Г.Орлова, а президентом тогда был К.Г.Разумовский, который, как командир Измайловского полка, помог Екатерине во время дворцового переворота, приведшего ее к власти.

Эйлеру она отказала в чине с обычным своим дипломатическим мастерством: «Я дала бы, когда он хочет, чин, если бы не опасалась, что этот чин сравняет его с множеством людей, которые не стоят г. Эйлера. Поистине его известность лучше чина для оказания ему должного уважения».

Правый глаз Эйлера ослеп в 1738 году, а левый почти не видел с осени 1766 года. Но это не лишило его работоспособности. Благодаря сохранившейся силе ума и памяти, при помощи учеников за 17 лет второго Санкт-Петербургского периода подготовил около 400 работ, среди них несколько больших книг. Последние годы жизни академические издания не справлялись с потоком его рукописей, и он шутливо обещал Орлову, что его работы будут печатать в «Комментариях» Академии 20 лет после смерти. А на самом деле это длилось полвека!

Эйлер легко вступал в научные дискуссии, давал консультации, охотно думал над случайными задачами и вопросами. Может показаться, что он разбрасывался, проявляя всеядность, но это только на первый взгляд. Он умел своевременно останавливаться, если не видел реальной возможности двигаться вперед; умел организовать жизнь так, чтобы текущие дела не сильно отражались на основном направлении его работы.

По сути всю жизнь он занимался математикой: его успехи в других науках (механике, астрономии) связаны именно с применением математических методов. В своей швейцарской диссертации 19-летний Эйлер писал: «Я не считаю необходимым подтвердить эту новую теорию опытом, потому что она

полностью выведена из самых надежных и неопровержимых принципов механики и, таким образом, сомнение в том, верна ли она и имеет ли место в практике, просто не может возникнуть». Даже законы Ньютона Эйлер пытался вывести из более общих принципов, а в небесной механике он стремился не получать эмпирические формулы из обработки результатов наблюдений, а делать выводы непосредственно из закона всемирного тяготения. Всюду Эйлер стремился двигаться от теории к практике.

Эйлер дал определение логарифмической функции, согласно которому функция  $\ln z$  определена для любого комплексного числа  $z \neq 0$  и принимает в каждой точке бесконечно много значений:

$$\ln z = \ln |z| + i \arg z, \text{ где } \ln |z| = \int_1^{|z|} \frac{dt}{t}.$$

Именем Эйлера называют и формулу  $e^{iz} = \cos z + i \sin z$ , связывающую между собой показательную и тригонометрические функции.

Эйлер заметил, что ортоцентр (точка пересечения высот), центр описанной окружности и центр тяжести (точка пересечения медиан) лежат на одной прямой – прямой Эйлера. Кажется, и теорему о пересечении высот в одной точке, пропущенную в «Началах» Евклида, до Эйлера никто не формулировал. Эйлеру принадлежит и открытие окружности девяти точек (на ней лежат основания высот треугольника, середины его сторон и середины отрезков, соединяющих вершины с ортоцентром).

В марте 1736 года Эйлер писал: «Некогда мне была предложена задача об острове, расположенном в Кенигсберге и окруженным рекой, через которую перекинуто 7 мостов. Спрашивается, может ли кто-нибудь обойти их, переходя только однажды через каждый мост. И тут же мне было сообщено, что никто до сих пор не смог это сделать, но никто и не доказал, что это невозможно. Вопрос этот, хотя и банальный, показался мне, однако, достойным внимания тем, что для его решения недостаточны ни геометрия, ни алгебра, ни комбинаторное искусство».

Ответ получился весьма простой: связный граф можно обойти, пройдя по всем его ребрам по одному разу, если либо степени всех вершин четны – и тогда обход закончится в той же вершине, где он начался, либо же степени двух его вершин

нечетны — и тогда обход надо начать в одной из них, а закончить в другой. Эйлер чувствовал, что задача о мостах — лишь начало нового раздела математики (топологии).

Он открыл многочлен  $n^2 - n + 41$ , значения которого — простые числа при  $n = 0, 1, 2, \dots, 40$ . Заметил, что число  $2^{2^5} + 1$  делится на 641 и тем самым опроверг предположение Ферма о том, что все числа вида  $2^{2^n} + 1$  простые. (Непосредственная проверка всех простых чисел от 3 до 641 была бы непосильна даже для такого виртуозного вычислителя, как Эйлер. Он обнаружил, занимаясь малой теоремой Ферма, что любой делитель числа  $2^{2^n} + 1$  дает остаток 1 при делении на  $2^{n+2}$ .)

Занимался он и задачей об обходе шахматной доски конем, который ни на какой клетке не бывает дважды, и конечными аффинными плоскостями, и многими другими отдельными задачами.

Рассмотрев разность  $1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n} - \ln n$  частичной суммы гармонического ряда и логарифма, заметил, что она стремится при  $n \rightarrow \infty$  к величине 0,577216..., ныне носящей имя Эйлера. Рассматривая функцию  $\sin x$ , Эйлер из того, что она обращается в нуль при  $x = 0, \pm\pi, \pm2\pi, \dots$ , сделал вывод:

$$\sin x = x \left(1 - \frac{x^2}{\pi^2}\right) \left(1 - \frac{x^2}{4\pi^2}\right) \left(1 - \frac{x^2}{9\pi^2}\right) \left(1 - \frac{x^2}{16\pi^2}\right) \dots$$

Если перемножить бесконечное множество скобок, то при  $x^3$  получим коэффициент

$$\frac{1}{\pi^2} + \frac{1}{4\pi^2} + \frac{1}{9\pi^2} + \frac{1}{16\pi^2} + \dots$$

Вспоминая ряд

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \frac{x^9}{9!} - \dots,$$

коэффициент при  $x^3$  в котором равен  $-1/6$ , получаем равенство

$$\zeta(2) = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \dots = \frac{\pi^2}{6}.$$

Аналогично, рассматривая коэффициенты при дальнейших степенях  $x$ , получаем равенства

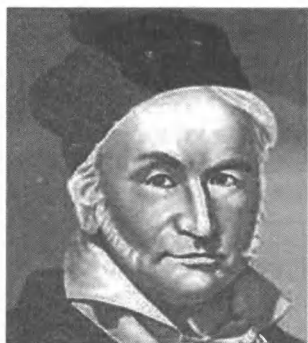
$$\zeta(4) = \sum_{k=1}^{\infty} \frac{1}{k^4} = \frac{\pi^4}{90},$$

$$\zeta(6) = \sum_{k=1}^{\infty} \frac{1}{k^6} = \frac{\pi^6}{42 \cdot 6!}$$

и так далее.



Ему было 12 лет, когда разразилась Французская революция; 29, когда была распущена казавшаяся вечной Римская империя; 38, когда был разгромлен Наполеон; и за 70, когда в Германии произошла революция 1848 года. Его родственники, мелкие фермеры, переехали в Брауншвейг около 1740 года. Средневековые гильдии старались не допустить в город пришельцев из деревни, поэтому даже 30 лет спустя известный в городе своими способностями к счету отец Гаусса работал то садовником, то водопроводчиком, то уличным мясником, то бухгалтером похоронного общества. Главной заботой семьи было приобретение собственного дома: только владелец дома, расположенного в пределах города, мог стать полноправным горожанином.



Гаусс любил рассказывать, что научился считать раньше, чем говорить. По его словам, когда ему было 3 года, отец вычислял, сколько следует заплатить каменщикам, учитывая, что некоторые из них работали и в обеденные часы. Он собирался уже выплачивать деньги, когда сын заявил, что расчет неверен и должно быть столько-то: мальчик в уме повторял выкладки отца; велико же было удивление, когда вторичный расчет подтвердил правоту сына!

В 1784 г. Гаусс пошел в школу. Учитель Бюттнер среди 50 с лишним учеников разного возраста, сидевших одновременно в одной комнате, выделил его и уделил особое внимание. Ассистентом учителя был М.Бартельс (1769–1836), позже профессор математики Казанского университета, который учил математике и Н.И.Лобачевского (1792–1856). Возможно, именно Бартельс зародил в Гауссе идеи неевклидовой геометрии.

В 1791 г. Гаусс был представлен герцогу Брауншвейг-Вольфенбюттельскому и получил ежегодную стипендию. Награды такого рода не были чем-то необычным в то время и

являются прообразом современной системы финансирования образования и науки.

Благодаря покровительству герцога в 1795 году Гаусс поступил в Геттингенский университет. Ф.Клейн (1849–1825) в «Лекциях о развитии математики в XIX столетии» писал: «Естественный интерес, какое-то, я сказал бы, детское любопытство приводит впервые мальчика независимо от каких-либо внешних влияний к математическим вопросам. Первое, что его привлекает, это чистое искусство счета. Он беспрестанно считает с прямо-таки непреодолимым упорством и неутомимым прилежанием. Благодаря этим постоянным упражнениям в действиях над числами, например, над десятичными дробями с невероятным числом знаков, он не только достигает изумительной виртуозности в технике счета, которой отличался всю жизнь, но его память овладевает таким колоссальным числовым материалом, он приобретает такой богатый опыт и такую широту кругозора в области чисел, какими навряд ли обладал кто-либо до или после него. Путем наблюдений над своими числами, стало быть, индуктивным, экспериментальным путем он рано постигает общие соотношения и законы. Этот метод, стоящий в резком противоречии с современными навыками математического исследования, был довольно распространен в XVIII столетии и встречается, например, также у Эйлера... Все эти ранние, придуманные только для своего удовольствия забавы ума являются подходами к значительной, лишь позже осознанной цели. В том-то именно и заключается подсознательная мудрость гения, что он уже при первых пробах сил, полуиграя, еще не сознавая всего значения своих действий, попадает, так сказать, своей киркой как раз в ту породу, которая в глубине своей таит золотоносную жилу». (Сам Гаусс утверждал, что отличается от других людей лишь прилежанием. Известны его слова «*Nil actum reputans si quid superesset agendum*» – «Что не сделано до конца, вообще не сделано».)

В 1799 году Гаусс защитил диссертацию на тему «Новое доказательство теоремы о том, что каждая целая рациональная алгебраическая функция одной переменной может быть разложена на действительные множители первой или второй степени». Коротко говоря, тема – основная теорема алгебры: каждый непостоянный многочлен имеет хотя бы один комплексный корень. Заметьте: хотя Гаусс несомненно владеет идеей комплексного числа, он в названии диссертации остается в вещественной области! В этом проявляется желание

выяснять суть дела, а не искать эффектные переформулировки уже известных результатов.

1 января 1801 года Дж. Пиацци (1746–1826) открыл Цереру – один из сотен астероидов, рассеянных между Марсом и Юпитером. Наблюдение за Церерой было выполнено на интервале величиной  $9^\circ$ . Воспользоваться прежними методами определения орбит было невозможно: они требовали значительного по объему и подтвержденного повторными наблюдениями материала, который для больших планет, известных с древности, и в самом деле имелся. Гаусс составил уравнение восьмой степени и, проведя подробнейшие приближенные вычисления, нашел орбиту. Затем он учел результаты других наблюдений и уточнил ответ с помощью метода наименьших квадратов, известного ему с 1795 года. Планету нашли в указанном месте! Этот результат, оценить который могла и широкая публика, принес Гауссу первую славу: с 1807 года и до конца жизни он был директором обсерватории Геттингена.

С 1820 года он руководил геодезической съемкой Ганноверского королевства, много работал в полевых условиях, измеряя длину дуги меридиана Геттинген-Альтона. Изобрел и многократно использовал гелиотроп – прибор, позволяющий при помощи концентрации солнечных лучей получать хорошо видимые точки визирования. Изучение формы земной поверхности потребовало общего геометрического метода исследования поверхностей («Общие исследования о кривых поверхностях», 1827 года.). Гаусс дал определение кривизны как

величины  $\frac{1}{r_1 r_2}$ , где  $r_1$  и  $r_2$  – главные радиусы кривизны в рассматриваемой точке; доказал теорему о постоянстве кривизны при изгибаниях поверхности (без растяжений).

Он надеялся выяснить, не отклоняется ли сумма углов большого треугольника от  $180^\circ$ : его интересовал не философский вопрос о независимости аксиомы о параллельных, а свойства физического пространства. Полученное отклонение укладывалось в пределы ошибки эксперимента, а ответ на вопрос Гаусса по существу не получен и по сей день.

Первое математически бессмысленное изложение неевклидовой геометрии опубликовал в 1832 году Я.Бойаи (1802–1860), сын друга Гаусса Ф.Бойаи (1775–1856). Гаусс признал храбрость Яноша и его математические достижения, но не захотел обсуждать вопрос, какова геометрия физического пространства. Поддержал Гаусс и публикации Н.И. Лобачевского, отметив, что давно знает все это.

В 1850 году он писал: «... Вы совершенно неправы, если думаете, что я имею в виду лишь окончательную отделку языка и элегантность изложения. На это уходит сравнительно незначительная доля времени; но то, что я имею в виду, — это внутреннее совершенство. В иных из моих работ есть такие особые точки, которые стоили мне нескольких лет размышлений и где на маленьком пространстве сконцентрировано представление, про которое никто не замечает, какие трудности мне пришлось преодолеть!». А успеть придать всем своим мыслям законченную форму он не мог! Например, он планировал труд, который должен был содержать (выполненное в 1812 году) исследование гипергеометрического ряда

$$F(\alpha, \beta, \gamma, x) = \sum_{k=0}^{\infty} \frac{\alpha^{\bar{k}} \beta^{\bar{k}}}{k! \cdot \gamma^{\bar{k}}} \cdot x^k = 1 + \frac{\alpha\beta}{1 \cdot \gamma} x + \frac{\alpha(\alpha+1)\beta(\beta+1)}{1 \cdot 2 \cdot \gamma(\gamma+1)} x^2 + \dots;$$

теорию дифференциальных уравнений с рационально зависящими от  $x$  коэффициентами и теорию эллиптических функций. Но поскольку он так и не разобрался толком с многозначностью аналитических функций (и не мудрено, римановы поверхности открыты значительно позже!), то об эллиптических функциях Гаусс так никогда ничего и не опубликовал, и только после смерти из его бумаг выяснилось, что Якоби и Абель переоткрывали факты, известные ему с 1800 года. В 1811 году (задолго до работ Коши!) он рассмотрел интеграл  $\int \frac{dz}{z}$  по контуру,  $n$  раз обходящему вокруг начала координат, и сказал, что этот интеграл равен  $2\pi i$ .

Исследования Гаусса по теоретической физике (1830–1840) являются результатом совместной работы с В.Э.Вебером (1804–1891). Они вдвоем создали абсолютную систему электромагнитных единиц (CGS) и сконструировали первый электромагнитный телеграф (1833). Гауссу принадлежит понятие потенциала электрического поля. В его честь названа единица измерения магнитной индукции.

В возрасте 62 лет Гаусс изучил русский язык. Кроме научной литературы, просил, например, прислать ему «Капитанскую дочку» А.С.Пушкина.

В 1855 году была выпущена медаль с надписью «*Mathematicorum princeps*» («Король математиков»). Памятник Гауссу в Брауншвейге, согласно его завещанию, стоит на постаменте в виде правильного 17-угольника.

## Разложение на множители

1. а)  $81 - 77 = 4 = 2^2$  и  $77 = 81 - 4 = (9 - 2)(9 + 2) = 7 \cdot 11$ .

б)  $89^2 = 7921 < 8091 < 8100 = 90^2$ . Первая же разность  $90^2 - 8091 = 9$  является квадратом:  $9 = 3^2$ . Следовательно,  $8091 = 90^2 - 3^2 = (90 - 3)(90 + 3) = 83 \cdot 93 = 83 \cdot 3 \cdot 31$ .

2. Представлению нечетного числа  $m$  в виде разности двух квадратов  $m = a^2 - b^2$  соответствует его разложение в произведение двух множителей:  $m = (a - b)(a + b)$ . Это соответствие взаимно однозначное: по каждому разложению  $m = xy$ , где  $x < y$ , из системы уравнений  $x = a - b$  и  $y = a + b$  однозначно определяем  $a = (x + y)/2$  и  $b = (y - x)/2$  (числа  $a$  и  $b$  целые, поскольку  $x$  и  $y$  — нечетные).

Выясним, сколькими способами можно разложить произведение  $m = p_1 p_2 \dots p_n$  различных простых чисел в произведение  $m = xy$ , где  $x$  и  $y$  — натуральные числа, не обязательно удовлетворяющие неравенству  $x < y$ . Из  $n$  множителей  $p_1, p_2, \dots, p_n$  можно  $2^n$  способами выбрать некоторое — возможно, пустое или совпадающее со всем множеством  $\{p_1, p_2, \dots, p_n\}$  — подмножество; произведение элементов выбранного подмножества дает число  $x$  (единицу — если подмножество пустое), а произведение остальных —  $y$ . Таким образом, разложений  $m = xy$  существует  $2^n$  штук, а разложений, удовлетворяющих неравенству  $x < y$ , вдвое меньше:  $2^{n-1}$ .

3. а)  $6647 = 17^2$ ; б)  $289 = 17^2$  — ход вычислений ясен из следующей таблицы:

$k$	1	2	3	4	5	6	7	8
$n_k$	289	98	62	49	37	31	28	34
$2k + 1$	3	5	7	9	11	13	15	17
$q_k$	96	19	8	5	3	2	1	2
$r_k$	1	3	6	4	4	5	13	0
$m_k$	97	59	43	33	27	23	21	17

Обратите внимание:  $n_7 = 28 < 34 = n_8$ . Таким образом, последо-

вательность  $n_1, n_2, n_3, \dots$  не обязательно монотонна. Впрочем, в начале работы алгоритм довольно быстро уменьшает исходное число и «шалит» только тогда, когда рассматриваемое число  $n_k$  уже стало гораздо меньше исходного числа  $n_1$ .

### Сумма квадратов

3. Указание.  $21 = 3 \cdot 7$ .

4. а) 0, 1, 3, 4, 5 или 9.

6. а) *Первый способ.* Нечетное число при делении на 8 может дать один из остатков 1, 3, 5 и 7. Квадраты этих чисел (1, 9, 25 и 49) при делении на 8 дают остаток 1.

*Второй способ.*  $(2n+1)^2 = 4n(n+1)+1$ , где  $n$  или  $n+1$  четно.

*Третий способ.*  $x^2 = (x-1)(x+1)+1$ , где при нечетном  $x$  один множитель четен, а другой кратен 4.

в) Если все три числа  $x, y, z$  четны, то разделим обе части уравнения  $x^2 + y^2 + z^2 = 4^m(8n+7)$  на 4. Так будем делать до тех пор, пока хотя бы одно из чисел  $x, y, z$  не станет нечетным. Поскольку квадрат нечетного числа при делении на 8 дает остаток 1, а квадрат любого целого числа – остаток 0, 1 или 4, и поскольку ни одна из сумм  $1+0+0, 1+0+1, 1+0+4, \dots, 1+4+4$  не дает при делении на 8 в остатке ни 7, ни 4, ни 0, получаем желанное противоречие.

г) Чтобы сумма трех квадратов давала остаток 3 при делении на 8, слагаемые должны быть нечетны. Поэтому

$$8n+3 = (2x+1)^2 + (2y+1)^2 + (2z+1)^2,$$

что равносильно искомому равенству.

7. Нет: она делится на 2, но не делится на 4.

8. а)  $x^4 - 1 = (x-1)(x+1)(x^2+1)$ . Множители четны. Одно из чисел  $x-1$  и  $x+1$  делится не только на 2, но даже на 4.

б) Остаток деления на 16 левой части равен количеству нечетных чисел среди  $x_1, x_2, \dots, x_{14}$ , поэтому не превосходит 14. Остаток правой части – 15.

9.  $60 = 3 \cdot 5 \cdot 4$ . Если ни одно из чисел  $a, b$  и  $c$  не делится на 3, то числа  $a^2, b^2$  и  $c^2$  дают остаток 1 при делении на 3; но  $1+1 \not\equiv 1 \pmod{3}$ .

Если ни одно из чисел  $a, b$  и  $c$  не делится на 5, то числа  $a^2, b^2$  и  $c^2$  дают при делении на 5 остаток 1 или 4; но ни  $1+1$ , ни  $1+4$ , ни  $4+4$  не сравнимо ни с 1, ни с 4 по модулю 5.

Наконец, докажем делимость произведения  $abc$  на 4. Случай, когда числа  $a$  и  $b$  оба четные, очевиден. Если числа  $a$  и  $b$  оба нечетны, то  $a^2 \equiv 1 \equiv b^2 \pmod{4}$  и, следовательно,  $c^2 = a^2 + b^2 \equiv 2 \pmod{4}$ , что невозможно: квадрат целого числа не может давать при делении на 4 остаток 2. Осталось рассмотреть случай, когда

числа  $a$  и  $b$  разной четности. Для определенности, пусть  $a$  нечетно, а  $b$  четно. Поскольку квадрат любого нечетного числа сравним с 1 по модулю 8, то  $b^2 = c^2 - a^2 \equiv 1 - 1 \equiv 0 \pmod{8}$ , откуда  $b \vdots 4$ , что и требовалось доказать.

11. Число  $8n + 4$ , где  $n$  – целое, представимо в виде  $(2n + 1) \cdot 2^2$ . Ряд из 7 чисел существует: например, 29, 30, 31, 32, 33, 34 и 35.

13. Рассмотрите числа вида  $21 \cdot 5^n$  или  $3^{2n-1} \cdot 7$ , где  $n$  – натуральное.

14. а) Предположим, что множество  $M$  простых чисел, сравнимых с 3 по модулю 4, конечно:  $M = \{3, 7, 11, 19, 23, \dots, p\}$ . Перемножим их все, умножим произведение на 4 и вычтем из произведения единицу:  $n = 4 \cdot 3 \cdot 7 \cdot 11 \cdot 19 \cdot 23 \cdot \dots \cdot p - 1$ . Число  $n$  нечетно и удовлетворяет сравнению  $n \equiv 3 \pmod{4}$ . Если все простые делители числа  $n$  дают остаток 1 при делении на 4, то и само число дает при делении на 4 остаток 1. Следовательно, хотя бы один простой делитель  $q$  числа  $n$  удовлетворяет сравнению  $q \equiv 3 \pmod{4}$ , хотя  $n$  не делится ни на один из элементов множества  $M$ .

б) Предположим, что множество  $M$  простых чисел, сравнимых с 1 по модулю 4, конечно:  $M = \{5, 13, 17, 29, 37, \dots, p\}$ . Перемножим их квадраты, умножим произведение на 4 и прибавим к произведению единицу:

$$n = (2 \cdot 5 \cdot 13 \cdot 17 \cdot 29 \cdot 37 \cdot \dots \cdot p)^2 + 1.$$

В силу теоремы 1, ни один простой делитель числа  $n$  не дает остаток 3 при делении на 4. Осталось заметить, что  $n$  нечетно и не делится ни на один из элементов множества  $M$ .

19. Пусть числа  $n$  и  $n + 2$  простые. По теореме Вильсона,  $1 + (n - 1)!$  делится на  $n$ , поэтому на  $n$  делится и  $4(1 + (n - 1)!) + n$ . Далее,

$$-1 \equiv (n + 1)! = (n + 1)n \cdot (n - 1)! \equiv (-1)(-2) \cdot (n - 1)! = 2(n - 1)! \pmod{n + 2},$$

следовательно,  $4(n - 1)! \equiv -2 \pmod{n + 2}$  и

$$4 + 4(n - 1)! + n \equiv 4 - 2 + n \equiv 0 \pmod{n + 2}.$$

Поскольку числа  $n$  и  $n + 2$  простые, то они взаимно простые; из делимости числа на каждое из них по основной теореме арифметики следует делимость этого числа и на их произведение.

Обратно, если  $4(1 + (n - 1)!) + n$  делится на  $n(n + 2)$ , то, как легко проверить,  $n \neq 2$  и  $n \neq 4$ . Предполагая, что  $n = 2k$ , где  $k \geq 3$ , получаем противоречие:  $(n - 1)!$  делится на  $k(k + 1)$ , но  $0 < 4 + n = 4 + 2k < k(k + 1)$  и поэтому  $4 + n$  на  $k(k + 1)$  не делится. Если же  $n$  нечетно, то из делимости числа  $4(1 + (n - 1)!) + n$  на  $n$  следует, что на  $n$  делится сумма  $1 + (n - 1)!$ , а поэтому, в силу предыдущего упражнения,  $n$  – простое; аналогично, из делимости числа  $4(1 + (n - 1)!) + n = 2(1 + 2(n - 1)!) + n + 2$  на  $n + 2$  следует, что на  $n + 2$

делится число

$$\begin{aligned} 1 + 2 \cdot (n-1)! &= 1 + (n+2-n)(n+2-n-1) \cdot (n-1)! \equiv \\ &= 1 + (-n)(-n-1) \cdot (n-1)! = 1 + (n+1)! \end{aligned}$$

и, опять в силу предыдущего упражнения,  $n+2$  — простое.

**20. а)** Если  $n^2 + 1$  кратно  $d$ , то кратно  $d$  и каждое из чисел вида  $(n + dk)^2 + 1$ , где  $k$  — целое.

**б)** Число  $n^2 + 1$  кратно 65 тогда и только тогда, когда оно кратно 5 и 13. Поскольку  $n^2 + 1 = n^2 - 4 + 5 = (n-2)(n+2) + 5$  и  $n^2 + 1 = n^2 - 25 + 26 = (n-5)(n+5) + 26$ , число  $n$  при делении на 5 должно давать остаток 2 или 3, а при делении на 13 — остаток 5 или 8. Таких чисел среди первых 65 натуральных чисел всего четыре: 8, 18, 47 и 57.  
*Ответ:* 62.

**22.** Умножив обе части уравнения на 4 и прибавив затем к обеим частям 1, получим:  $(4x-1)(4y-1) = (2z)^2 + 1$ . Поскольку правая часть не может иметь натуральных делителей вида  $4x-1$ , имеем:  $x \leq 0$ . По той же самой причине  $y \leq 0$ . *Замечание.* Рассматриваемое уравнение имеет бесконечно много решений в целых отрицательных числах.

**23. а)** Если  $n$  нечетно, то  $n^2 - 1$  кратно 4, а число  $m^2 + 1$  не кратно 4 ни при каком целом  $m$ . Если же  $n = 2k$ , то  $n^2 - 1 = 4k^2 - 1$  дает остаток 3 при делении на 4, и остается применить утверждение теоремы 1.

**б)** Перенесем  $x^2$  и  $y^2$  в левую часть и прибавим 1 к обеим частям. Получим:  $(x^2 - 1)(y^2 - 1) = z^2 + 1$ . В силу предыдущего пункта,  $x = y = 0$ , откуда  $z = 0$ .

**24. а)** Если  $n = x^2 + y^2$ , где  $x, y$  — целые числа, то  $\frac{n}{2} = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2$ . Если одно из чисел  $x, y$  четное, а другое нечетное, то сумма квадратов  $x^2 + y^2$  нечетна. Значит,  $x$  и  $y$  оба четны или оба нечетны, а числа  $(x+y)/2$  и  $(x-y)/2$  — целые.

**б)** Если  $x^2 + y^2$  кратно 5, то произведение  $(x-2y)(x+2y) = x^2 - 4y^2 = (x^2 + y^2) - 5y^2$  кратно 5. Если, например,  $x - 2y$  кратно 5, то  $2x + y = 2(x - 2y) + 5y$  тоже кратно 5.

**в)** Если  $x^2 + y^2$  кратно 13, то  $(2x-3y)(2x+3y) = 4x^2 - 9y^2 = 4(x^2 + y^2) - 13y^2$  кратно 13. Если, например,  $2x - 3y$  кратно 13, то  $3x + 2y = 8(2x - 3y) - 13x + 26y$  тоже кратно 13.

То же самое можно изложить на языке сравнений. Поскольку  $x^2 \equiv -y^2$  и  $3^2 \equiv 2^2 \pmod{13}$ , имеем  $3^2 x^2 \equiv 2^2 y^2$ , т.е.  $(3x+2y)(3x-2y) \equiv 0 \pmod{13}$ , откуда следует, что хотя бы одно из чисел  $3x+2y$  и  $3x-2y$  кратно 13. Дальнейшее очевидно.



26. а)  $x = y = z = t = 0$ .

б) Поскольку  $y^2$  не может дать остаток 3 при делении на 4, число  $x$  должно быть нечетным. Имеем:  $y^2 + 1 = x^2 + 8 = (x + 2)(x^2 - 2x + 4)$ . Число  $x^2 - 2x = x(x - 2)$  — произведение двух соседних нечетных чисел — при делении на 4 дает остаток 3.

в) *Указание.* Сначала докажите, что  $x$  нечетно, а затем запишите уравнение в виде  $x(x + 2)(x - 1) = y^2 + 1$  и заметьте, что  $x(x - 2)$  дает остаток 3 при делении на 4. *Ответ:*  $x = -1$ ,  $y = 1$  или  $-1$ .

27. б) *Первый способ. Указание.* Если числа  $n - 1$ ,  $n$  и  $n + 1$  отмеченные, причем число  $n = a^2 + b^2$  нечетное, то таковы же и числа  $n^2 - 1 = (n - 1)(n + 1)$ ,  $n^2 = (a^2 - b^2)^2 + (2ab)^2$  и  $n^2 + 1^2$ .

*Второй способ.* Рассмотрим тройку чисел  $289n^2 - 1 = (17n - 1)^2 + (34n - 2)^2$ ,  $289n^2 = (15n)^2 + (8n)^2$  и  $289n^2 + 1 = (17n)^2 + 1^2$ . Доказать, что для бесконечно многих натуральных  $n$  число  $34n - 2$  является квадратом натурального числа, легко:  $(34k + 10)^2 = 34(34k^2 + 20k + 3) - 2$ .

*Третий способ.* Рассмотрим тройки последовательных чисел  $2n^2 = n^2 + n^2$ ,  $2n^2 + 1$  и  $2n^2 + 2 = (n - 1)^2 + (n + 1)^2$ . Чтобы число  $2n^2 + 1$  было суммой двух квадратов, достаточно, чтобы для некоторого натурального числа  $k$  выполнялось равенство  $2n^2 + 1 = (n - k)^2 + (n + k - 1)^2$ , которое равносильно равенству  $n = k^2 + k$ .

в) *Первый способ.* Остаток от деления квадрата на 16 может равняться 0, 1, 4 или 9. Поэтому остаток от деления суммы двух квадратов на 16 может равняться 0, 1, 2, 4, 5, 8, 9, 10 и 13. В этом списке отсутствуют соседи числа 13. Следовательно, соседи числа  $(8a + 5)^2 + (8a + 6)^2$ , где  $a$  и  $b$  — целые числа, не представимы в виде суммы двух квадратов.

*Второй способ.*  $2 \cdot 100^m = (10^m)^2 + (10^m)^2$ . Число  $2 \cdot 100^m - 1$  дает остаток 3 при делении на 4, а число  $2 \cdot 100^m + 1$  дает остаток 3 при делении на 9.

*Третий способ.*  $(3^m)^2 + 1^2$  — сумма двух квадратов. Число  $9^m$  невозможно разложить в сумму квадратов двух натуральных чисел. Невозможно представить в виде суммы двух квадратов и число  $9^m + 2$ , ибо оно сравнимо с 3 по модулю 4.

г) Рассмотрите  $n = 100^m$ .

д) Воспользуйтесь китайской теоремой об остатках и бесконечностью множества простых чисел, дающих остаток 3 при делении на 4 (упражнение 14).

30. Обозначим  $ms - tp = r$ . Поскольку

$$|r| = p \left| \frac{sm}{p} - t \right| \leq \frac{p}{n+1} < \frac{p}{\sqrt{p}} = \sqrt{p}$$

и  $0 < s \leq n < \sqrt{p}$ , то

$$0 < r^2 + s^2 < 2p.$$

Число  $r^2 + s^2 = (ms - tp)^2 + s^2 = s^2(m^2 + 1) - 2mstp + t^2p^2$  делится на  $p$ . Следовательно,  $r^2 + s^2 = p$ .

**31.** Пусть  $p = a^2 + b^2 = c^2 + d^2$ . Тогда  $a^2 \equiv -b^2$  и  $c^2 \equiv -d^2 \pmod{p}$ . Следовательно,  $a^2c^2 \equiv (-b^2)(-d^2) \pmod{p}$ , т.е. разность  $a^2c^2 - b^2d^2$  кратна  $p$ . (Если рассуждения со сравнениями по модулю  $p$  непривычны и потому подозрительны, можете получить то же самое, рассматривая тождество  $a^2c^2 - b^2d^2 = a^2(c^2 + d^2) - (a^2 + b^2)d^2$ .)

Поскольку число  $p$  простое, из делимости произведения  $(ac + bd)(ac - bd)$  на  $p$  следует, что хотя бы один из множителей кратен  $p$ . Если сумма  $ac + bd$  кратна  $p$ , воспользуемся формулой

$$p^2 = (ac + bd)^2 + (ad - bc)^2.$$

Если  $ad - bc \neq 0$ , то противоречие очевидно, ибо первое слагаемое  $(ac + bd)^2$  кратно  $p^2$  и потому не меньше  $p^2$ . Если же  $ad - bc = 0$ , то  $ad = bc$ . Поскольку как числа  $a$  и  $b$ , так и числа  $c$  и  $d$  взаимно просты, имеем  $a = c$  и  $d = b$ .

Случай, когда разность  $ac - bd$  кратна  $p$ , рассмотрите аналогично, воспользовавшись формулой  $p^2 = (ac - bd)^2 + (ad + bc)^2$ .

**32. б)** Пусть  $a = 1000$ ,  $b = 3$ ,  $c = 235$ ,  $d = 972$ . Тогда  $ac + bd = 237916$  и  $ac - bd = 232084$ . Произведение  $237916 \cdot 232084$  кратно  $1000009$ . Применим алгоритм Евклида. Поскольку  $1000009 = 4 \cdot 237916 + 48345$ , имеем  $\text{НОД}(1000009; 237916) = \text{НОД}(48345; 237916)$ . Далее,  $237916 = 5 \cdot 48345 - 3809$ . Значит,

$$\text{НОД}(48345; 237916) =$$

$$= \text{НОД}(48345; 3809) = \text{НОД}(13 \cdot 3809 - 1172; 3809) =$$

$$= \text{НОД}(1172; 3809) = \text{НОД}(1172; 3 \cdot 1172 + 293) = \text{НОД}(1172; 293) = 293.$$

(Аналогично можно было бы найти  $\text{НОД}(1000009; 232084) = 3413$ .)

Ответ:  $1000009 = 293 \cdot 3413$ .

**34.** Поскольку произведение  $(as - br)(as + br) = a^2s^2 - b^2r^2 = (a^2 + nb^2)s^2 - b^2(r^2 + ns^2)$  делится на  $p$ , то хотя бы одно из чисел  $as - br$  и  $as + br$  делится на  $p$ . В первом случае годится представление

$$m = \frac{(a^2 + nb^2)(r^2 + ns^2)}{p^2} = \left( \frac{ar + nbs}{p} \right)^2 + n \left( \frac{as - br}{p} \right)^2,$$

во втором — представление  $m = \left( \frac{ar - nbs}{p} \right)^2 + n \left( \frac{as + br}{p} \right)^2$ .

**35. а)** Поскольку  $(as - br)(as + br) = (a^2 + nb^2)s^2 - b^2(r^2 + ns^2)$  делится на  $q^2$ , рассмотрим три случая: 1)  $as - br$  делится на  $q^2$ ; 2)  $as + br$  делится на  $q^2$ ; 3) каждое из чисел  $as + br$  и  $as - br$  делится на  $q$ . В первом случае годится представление

$$m = \frac{(a^2 + nb^2)(r^2 + ns^2)}{q^4} = \left(\frac{ar + nbs}{q^2}\right) + n\left(\frac{as - br}{q^2}\right)^2;$$

во втором – представление  $m = \left(\frac{ar - nbs}{q^2}\right)^2 + n\left(\frac{as + br}{q^2}\right)^2$ .

В третьем случае  $2as = (as + br) + (as - br) \div q$ . Поскольку  $q$  нечетное и простое, а  $1 \leq s < q$ , то  $a \div q$ . Аналогичным образом из равенства  $2br = (as + br) - (as - br)$  следует, что  $b \div q$ . Следовательно,  $m = (a/q)^2 + n(b/q)^2$  – искомое представление.

**б)** В первом из рассмотренных при решении пункта а) случаев числа  $as - br$  и  $ar + nbs$  делятся на  $q^2$ ; числа  $x = (ar + nbs)/q^2$  и  $y = (as - br)/q^2$  взаимно просты, поскольку иначе числа

$$a = r \frac{ar + nbs}{q^2} + ns \frac{as - br}{q^2} = rx + nsy,$$

$$b = s \frac{ar + nbs}{q^2} - r \frac{as - br}{q^2} = sx - ry$$

не были бы взаимно просты. Второй случай аналогичен первому, а третий невозможен.

**36. а)** Предположим противное: существуют целые числа  $x$  и  $y$ , удовлетворяющие равенству  $x^2 - 2 = py$ , где  $p$  – простое число, сравнимое с 3 или 5 по модулю 8. Рассмотрим *наименьшее* из таких чисел  $p$ . Заменяя при необходимости  $x$  на остаток от деления  $x$  на  $p$ , приходим к неравенству  $0 < x < p$ . Далее, заменяя при необходимости  $x$  на  $p - x$ , видим, что можно считать число  $x$  нечетным и удовлетворяющим неравенствам  $0 < x < p$ . Тогда  $py = x^2 - 2 < p^2$  и, следовательно,  $y < p$ .

Поскольку  $py = x^2 - 2 \equiv -1 \pmod{8}$  и  $p \equiv 3$  или  $5 \pmod{8}$ , то  $y \equiv 5$  или  $3 \pmod{8}$ . Поскольку произведение чисел, каждое из которых сравнимо с 1 или 7 по модулю 8, при делении на 8 дает остаток 1 или 7, то хотя бы один из простых множителей числа  $y$  сравним с 3 или 5 по модулю 8. Это противоречит выбору числа  $p$  как наименьшего.

**б)** Аналогично пункту а).

**37. а)** Пусть  $p = 8n + 3$  и  $a = (p + 1)/2$ . Тогда  $2a \equiv 1 \pmod{p}$  и, в силу малой теоремы Ферма,

$$0 \equiv 4(a^{8n+2} - 1) = (2a^{4n+1} - 2)(2a^{4n+1} + 2) \equiv (a^{4n} - 2)(a^{4n} + 2) \pmod{p}.$$

Сравнение  $a^{4n} \equiv 2$  невозможно вследствие предыдущего упражнения. Следовательно,  $a^{4n} + 2 \equiv 0 \pmod{p}$ .

б) Аналогично, пусть  $p = 8n + 7$  и  $a = (p+1)/2$ . Рассмотрите формулу

$$4(a^{8n+6} - 1) = (2a^{4n+3} - 2)(2a^{4n+3} + 2) \equiv (a^{4n+2} - 2)(a^{4n+2} + 2) \pmod{p}.$$

Сравнение  $a^{4n+2} \equiv -2$  невозможно вследствие предыдущего упражнения. Следовательно,  $a^{4n} \equiv 2 \pmod{p}$ .

**38.** а) Поскольку  $p - 1$  делится на 8, то  $x^{p-1} - 1$  делится на  $x^8 - 1 = (x^4 - 1)(x^4 + 1)$ . Как следует из статьи «Малая теорема Ферма» «Арифметики», существует целое число  $x$ , удовлетворяющее сравнению  $x^4 + 1 \equiv 0 \pmod{p}$  и, следовательно, сравнению  $(x^2 + 1)^2 \equiv 2x^2 \pmod{p}$ . Рассмотрев целое число  $y$ , для которого  $xy \equiv 1 \pmod{p}$ , получаем  $((x^2 + 1)y)^2 \equiv 2x^2y^2 \equiv 2 \pmod{p}$ .

б) Пусть  $p = 8n + 1$ . Рассмотрим последовательность чисел  $1^{8n}$ ,  $2^{8n}$ ,  $3^{8n}$ , ...,  $(8n)^{8n}$ . Поскольку

$$a^8 - b^8 = (a^4 - b^4)(a^4 + b^4),$$

то либо выполнены сравнения  $1^{4n} \equiv 2^{4n} \equiv 3^{2n} \equiv \dots \equiv (8n)^{4n} \pmod{p}$ , что невозможно в силу теоремы Лагранжа, либо сумма четвертых степеней некоторых соседних натуральных чисел  $a^n$  и  $b^n$  делится на  $p$ , и тогда на  $p$  делится число  $(a^{2n} - b^{2n})^2 + 2(a^n b^n)^2$ . Рассмотрев такое целое число  $c$ , что  $abc \equiv 1 \pmod{p}$ , приходим к выводу:

$$(a^{2n}c^n - b^{2n}c^n) \equiv -2(a^n b^n c^n)^2 \equiv -2 \pmod{p}.$$

**39.** Прочитайте статью «Квадратичный закон взаимности» «Арифметики» или воспользуйтесь таблицей значений символов Лежандра в зависимости от остатка, который дает простое число  $p$  при делении на 8 (в скобках указано упражнение, в котором найдено соответствующее значение):

$p \pmod{8}$	1	3	5	7
$\left(\frac{2}{p}\right)$	1(38a)	-1(36a)	-1(36a)	1(376)
$\left(\frac{-2}{p}\right)$	1(386)	1(37a)	-1(366)	-1(366)

ющее значение):

**41.** Случай, когда  $a$  и  $b$  четны, очевиден.

Пусть  $a$  и  $b$  нечетны. Поскольку любое нечетное число при делении на 4 дает остаток 1 или 3, то хотя бы одно из чисел  $a + b$  и  $a - b$  делится на 4. Если  $a + b$  делится на 4, то  $4(a^2 + 3b^2) = (1^2 + 3 \cdot 1^2)(a^2 + 3b^2) = (a - 3b)^2 + 3(a + b)^2$  и, следовательно,

$$\frac{a^2 + 3b^2}{4} = \left(\frac{a - 3b}{4}\right)^2 + 3\left(\frac{a + b}{4}\right)^2;$$

если же  $a - b$  делится на 4, то годится формула

$$\frac{a^2 + 3b^2}{4} = \left(\frac{a + 3b}{4}\right)^2 + 3\left(\frac{a - b}{4}\right)^2.$$

**42. Указание.**  $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}(-1)^{(3-1)(p-1)/4}\left(\frac{p}{3}\right).$

**44.**  $(b + a)^2 + (b + a)(b - a) + (b - a)^2 = a^2 + 3b^2.$

**45.** Нет, ибо  $(a + b)^2 - (a + b)b + b^2 = a^2 + ab + b^2.$

**46.** В силу теоремы 3, существуют такие целые числа  $b$  и  $c$ , что  $2p = c^2 + 5b^2$ . Числа  $b$  и  $c$  нечетные, поэтому  $c = 2a + b$  для некоторого целого числа  $a$ . Очевидно,  $2p = (2a + b)^2 + 5b^2 = 4a^2 + 4ab + 6b^2$ , откуда  $p = 2a^2 + 2ab + 3b^2$ .

**48.** Подвергните фигуру гомотетии с коэффициентом  $1/2$  и центром в начале координат. Полученную фигуру  $F$  подвергните всевозможным параллельным переносам вдоль осей координат на целые расстояния. Поскольку площади образов фигуры больше 1, то существует точка  $M$ , принадлежащая по крайней мере двум фигурам  $F_1$  и  $F_2$ . Обозначив их центры через  $O_1$  и  $O_2$ , рассмотрим такую точку  $N$ , что  $\overline{O_1N} = \overline{MO_2}$ . Точки  $M$  и  $N$  принадлежат выпуклой фигуре  $F_1$ , поэтому середина отрезка  $MN$  тоже принадлежит фигуре  $F_1$ . Поскольку  $O_1MO_2N$  — параллелограмм, то середины отрезков  $MN$  и  $O_1O_2$  совпадают и, следовательно, точка  $O_2$  принадлежит образу фигуры  $F_1$  при гомотетии с центром  $O_1$  и коэффициентом 2.

**49.** Площадь фигуры, заданной на координатной плоскости неравенством  $ax^2 + 2bxy + cy^2 \leq 2$ , равна  $2\pi/(ac - b^2) = 2\pi > 4$ . Следовательно, внутри эллипса лежит хотя бы одна точка  $(x; y) \neq (0; 0)$  с целыми координатами. Эта точка искомая, поскольку для нее величина  $ax^2 + 2bxy + cy^2$  меньше 2 и больше 0, т.е. равна 1.

**53.** Равенство комплексных чисел  $x^2 - y^2 + 2xyi = a + bi$  равносильно системе уравнений  $x^2 - y^2 = a$  и  $2xy = b$ . Любитель тождеств заметит, что  $(x^2 + y^2)^2 = (x^2 - y^2)^2 + (2xy)^2 = a^2 + b^2$ . (Впрочем, это следует из того, что модуль квадрата любого комплексного числа равен квадрату его модуля.) Зная величины  $x^2 + y^2 = \sqrt{a^2 + b^2}$  и  $x^2 - y^2 = a$ , находим

$$x^2 = (\sqrt{a^2 + b^2} + a)/2 \text{ и } y^2 = (\sqrt{a^2 + b^2} - a)/2.$$

**Ответ:** если  $b \geq 0$ , то  $x = \pm \sqrt{(\sqrt{a^2 + b^2} + a)/2}$  и

$$y = \pm \sqrt{(\sqrt{a^2 + b^2} - a)/2}; \text{ если } b < 0, \text{ то } x = \pm \sqrt{(\sqrt{a^2 + b^2} + a)/2} \text{ и}$$

$$y = \mp \sqrt{(\sqrt{a^2 + b^2} - a)/2}.$$

55. Тогда и только тогда, когда  $a$  и  $b$  — одной четности, т.е. когда сумма  $a + b$  четна.

56. в) Кратные числа  $5 + 5i$ .

61. а) 1; б)  $\sqrt{5}$ ; в)  $\sqrt{25}$ ; г)  $\sqrt{65}$ .

63.  $4(a_1 + 1) \dots (a_r + 1)$ .

64. Нет.

65. а) В разложение  $n$  на натуральные простые множители простые числа вида  $4k - 1$  должны входить только в четных степенях, а простой множитель вида  $4k + 1$  может быть не более чем один, причем не более чем в первой степени.

б) Число  $n$  должно иметь вид  $n = 2^m p^\alpha Q^2$ , где  $p = 4k + 1$  — простое число,  $\alpha \leq 2$ ,  $Q = 1$  или  $Q$  — произведение одного или нескольких простых чисел вида  $4k - 1$ , причем  $m$  должно быть четным при  $\alpha = 2$  и нечетным — при  $\alpha = 0$ .

в) В разложение  $n$  на натуральные простые множители не должны входить простые числа вида  $4k - 1$ , число 2 может войти в степени не выше первой, а простой множитель вида  $4k + 1$  может быть не более чем один.

### Уравнения Пелля

1. Поскольку по крайней мере две стороны «основного» квадрата граничат только с единичными квадратиками, то длина  $a$  стороны основного квадрата — натуральное число. Пусть искомая сторона равна  $b$ . Тогда  $a^2 = 35 + b^2$ , откуда  $35 = (a - b)(a + b)$ . Число 35 разлагается в произведение натуральных множителей лишь двумя способами:  $1 \cdot 35$  и  $5 \cdot 7$ . В первом случае  $a - b = 1$  и  $a + b = 35$ , откуда  $b = 17$  и  $a = 18$ . Во втором случае  $a - b = 5$  и  $a + b = 7$ , откуда  $b = 1$  и  $a = 6$ . Поскольку  $b > 1$ , подходит только  $b = 17$ .

2.  $999919 = 1000000 - 81 = 1000^2 - 9^2 = 991 \cdot 1009$ . Поскольку числа 991 и 1009 простые и  $991 < 1009$ , то кошек 991.

3. а)  $x^2 + 2xy - 3y^2 = (x + y)^2 - 4y^2 = (x - y)(x + 3y)$ ;

б)  $6x^2 - xy - 12y^2 = (2x - 3y)(3x + 4y)$ .

4. а) В виде разности квадратов представимы нечетные числа:  $2n + 1 = (n + 1)^2 - n^2$ . Представимы и числа, делящиеся на четыре:  $4n = (n + 1)^2 - (n - 1)^2$ . Четные числа, не кратные четырем, не представимы в виде разности двух квадратов, поскольку произведение двух чисел одной четности либо нечетно, либо делится на 4.

б) Воспользуйтесь равенством  $x^2 + 2xy = x(x + 2y)$  или сведите дело к пункту а) при помощи формулы  $x^2 + 2xy = (x + y)^2 - y^2$ .

в) Представимы числа вида  $4n + 1 = 1^2 + 4 \cdot 1 \cdot n$ , вида  $8n + 4 = 2^2 + 4 \cdot 2 \cdot n$  и вида  $16n = 4^2 + 4 \cdot 4 \cdot (n - 1)$ . Не представимы числа вида  $4n + 2$ ,  $4n + 3$  и  $16n + 8$ .

5. а)  $2 \cdot 99 = 198$ , поскольку  $(x; y) = \left( \pm \frac{2^k + 2^{100-k}}{2}; \frac{2^k - 2^{100-k}}{2} \right)$ , где  $1 \leq k \leq 99$ .

б)  $2 \cdot 101 = 202$ .

в) Решения имеют вид  $x = (A + B)/2$  и  $y = (A - B)/6$ , где  $AB = 10^6$ , причем  $A, B$  — целые числа. Числа  $A$  и  $B$  должны быть четными; разность  $A - B$  должна делиться на 3. Поскольку  $AB = 10^6 \equiv 1 \pmod{3}$ , последнее выполнено автоматически. Обозначив  $A = 2a$  и  $B = 2b$ , получаем  $ab = 2^{45}5^6$ . Интересующих нас пар  $(a; b)$  вдвое больше, чем делителей числа  $2^4 \cdot 5^6$ , т.е.  $2(4 + 1)(6 + 1) = 70$  штук.

6. а)  $41^2 = 1681$ ; б)  $4901^2 = 24019801$ ; в)  $\underbrace{49\dots90\dots01}_{n-1 \quad n-1}^2$ .

7. Нет. Пусть для определенности  $x \leq y$ . Тогда  $y^2 < y^2 + x \leq y^2 + y < (y + 1)^2$ , так что  $y^2 + x$  заключено между соседними квадратами.

8. Обозначим через  $x$  среднее из этих чисел. Получаем сумму  $(x - 12)^2 + (x - 11)^2 + (x - 10)^2 + \dots + (x + 10)^2 + (x + 11)^2 + (x + 12)^2$ . Раскрыв скобки и приведя подобные, приходим к уравнению

$$25x^2 + 1300 = y^2,$$

откуда  $(y - 5x)(y + 5x) = 1300$ . Поскольку числа  $y - 5x$  и  $y + 5x$  отличаются на  $10x$ , а их произведение оканчивается цифрой 0, то  $y - 5x$  и  $y + 5x$  должны оканчиваться нулями. Для натуральных  $x$  и  $y$  получаем систему  $y - 5x = 10$  и  $y + 5x = 130$ , которой удовлетворяют лишь  $x = 12$  и  $y = 70$ .

9.  $x = 1972$ . Очевидно,  $4^{27} + 4^{1000} + 4^x = 2^{54} (1 + 2 \cdot 2^{1945} + 2^{2x-54})$ . Если  $x = 1972$ , то  $2x - 54 = 2 \cdot 1945$ , а выражение в скобках является квадратом суммы.

Если же  $x > 1972$ , то число  $1 + 2 \cdot 2^{1945} + 2^{2(x-27)}$  больше  $2^{2(x-27)}$  и меньше  $(2^{x-27} + 1)^2$ , т.е. заключено между квадратами двух последовательных натуральных чисел и поэтому не является точным квадратом.

10. а)  $(x; y) = (0; 0), (0; -1), (-1; 0)$  или  $(-1; -1)$ . Уравнение можно записать в виде  $4x^2 + 4x + 1 = 4(4y^2 + 4y + 1) - 3$ , откуда  $4(2y + 1)^2 - (2x + 1)^2 = 3$ . Число 3 представимо в виде разности квадратов единственным образом:  $3 = 2^2 - 1^2$ . Значит,  $|2y + 1| = 1$  и  $|2x + 1| = 1$ , т.е.  $y = 0$  или  $-1$  и  $x = 0$  или  $-1$ .

б) Умножая  $x$  на  $x + 8$  и  $x + 1$  на  $x + 7$ , получаем:  $(x^2 + 8x) \cdot (x^2 + 8x + 7) = y^2$ . Решая в целых числах уравнение

$z(z+7) = y^2$ , получаем:  $(y; z) = (0; -7), (0; 0), (\pm 12; -16)$  или  $(\pm 12; 9)$ . Осталось решить квадратные уравнения  $x^2 + 8x = -16$ ,  $x^2 + 8x = -7$ ,  $x^2 + 8x = 0$  и  $x^2 + 8x = 9$ .

в)  $(x; y) = (0; -1), (-1; -1), (0; 0), (-1; 0), (5; 2)$  или  $(-6; 2)$ . Умножив обе части уравнения на 4 и прибавив к ним по 1, получим  $(2x+1)^2 = (2y^2 + y)^2 + 3y^2 + 4y + 1 = (2y^2 + y + 1)^2 - (y^2 - 2y)$ .

Если  $y$  целое и отлично от  $-1, 0, 1$  и  $2$ , то  $3y^2 + 4y + 1 > 0$  и  $y^2 - 2y > 0$ , так что  $(2y^2 + y)^2 < (2x+1)^2 < (2y^2 + y + 1)^2$ . Эти неравенства означают, что  $(2x+1)^2$  лежит между двумя последовательными квадратами, а это для целых  $x$  невозможно. Подставляя в уравнение по очереди  $y = -1, 0, 1$  и  $2$ , находим ответ.

г) Умножим обе части уравнения на 4. Получим:

$$(2x^2 + x)^2 = 4x^4 + 4x^3 + x^2 < (2y)^2 \leq 4x^4 + x^2 + 4 + 4x^3 + 8x^2 + 4x = \\ = (2x^2 + x + 2)^2.$$

Следовательно,

$$2y = 2x^2 + x + 1, \quad (2x^2 + x + 1)^2 = 4(1 + x + x^2 + x^3 + x^4),$$

т.е.  $x^2 - 2x - 3 = 0$ . Ответ:  $x = 3, y = 11$ .

д) Уравнение можно преобразовать к виду  $(x+y)^2 = xy(xy+1)$ .

е)  $y^3 = 8x^3 + 24x^2 + 32x + 16 = 8(x^3 + 3x^2 + 4x + 2)$ . Поэтому  $y = 2z$ , где  $z$  — целое,  $z^3 = x^3 + 3x^2 + 4x + 2$ .

Если  $x \geq 0$ , то  $(x+1)^3 = x^3 + 3x^2 + 3x + 1 < z^3 < x^3 + 6x^2 + 12x + 8 = (x+2)^3$ , поэтому  $x+1 < z < x+2$ , что невозможно.

Предположим, что  $x \leq -2$ . Тогда пара чисел  $(X; Y) = (-x - 2; y)$  тоже удовлетворяет исходному уравнению, так как  $(X+2)^4 - X^4 = x^4 - (x+2)^4 = -y^3 = Y^3$ . Но, как доказано выше, неравенство  $X \geq 0$  приводит к противоречию. Таким образом,  $-2 < x < 0$ , т.е.  $x = -1$ . При этом, очевидно,  $y = 0$ .

11. а) Обозначим  $x = m - n$ . Заменяя  $m$  на  $x + n$ , раскрыв скобки и упростив, получим равенство  $x(4n + 2x + 1) = n^2$ . Числа  $x$  и  $4n + 2x + 1$  взаимно просты. Поэтому  $x$  — квадрат натурального числа.

б) Обозначим  $y = 2m + 2n + 1$  и  $M = 2m + 1$ . Очевидно,  $m = (M - 1)/2$  и  $n = (y - M)/2$ ; после преобразований из равенства  $2m^2 + m = 3n^2 + n$  получаем равенство  $y(6M - 3y - 2) = M^2$ . Поскольку число  $y$  нечетное, из этого равенства легко вывести, что  $y$  — квадрат натурального числа.



**12.** Очевидно,  $(x-1)(x+1) = py^2$ . Если  $x$  четно, то  $\text{НОД}(x-1; x+1) = 1$ , так что  $x-1 = a^2$  и  $x+1 = pb^2$  или  $x-1 = pa^2$  и  $x+1 = b^2$ .

Если же  $x$  нечетно, то  $\text{НОД}(x-1; x+1) = 2$ . При этом  $x-1 = 2a^2$  и  $x+1 = 2pb^2$  или  $x-1 = 2pa^2$  и  $x+1 = 2b^2$ .

**13.** Рассуждайте по индукции.

**14.** Обозначим через  $f_n$  количество способов протанцевать расстояние длиной  $n$  шагов. Очевидно,  $f_0 = 1$  (никуда не ходить можно единственным способом) и  $f_1 = 2$  (можно сделать либо шаг вперед, либо два шага вперед и шаг назад). Пройти  $n+2$  шага можно трояко: либо пройти сначала  $n+1$  шаг и сделать шаг вперед, либо  $n$  шагов и сразу два шага вперед, наконец, можно пройти  $n+1$  шаг и затем сделать два шага вперед и шаг назад. Значит,  $f_{n+2} = f_{n+1} + f_n + f_{n+1} = 2f_{n+1} + f_n$ . Ответ:  $f_7 = 408$ .

**15.** а) Например,  $(x; y) = (3; 5), (20; 29)$  или  $(119; 169)$ . б) Например,  $a = 3, b = 2, c = 1, d = 4, e = 3, f = 2$ . Найти эти числа можно, выразив из равенств

$$z = 2x + 1,$$

$$Z = 2X + 1,$$

$$Z = 3z + 4y,$$

$$Y = 2z + 3y$$

числа  $X$  и  $Y$  через  $x$  и  $y$ .

**16.** Уравнение  $x^2 + (y^2 - 1)^2 = (y^2)^2$  эквивалентно уравнению  $x^2 - 2y^2 = -1$ .

**17.** Да. Например,  $f(x) = 2x^2 + 1$ .

**18.** Подставляя  $n = 1$  в искомые соотношения, получаем систему  $17 = 3a + b$  и  $12 = 2a$ , откуда  $a = 6, b = -1$ .

Докажем по индукции, что найденные значения удовлетворяют условию задачи. База – та система, из которой мы нашли  $a$  и  $b$ .

*Переход.* Пусть при некотором  $n$  выполнены равенства  $x_{n+1} = 6x_n - x_{n-1}$  и  $y_{n+1} = 6y_n - y_{n-1}$ . Тогда

$$\begin{aligned} x_{n+2} &= 3x_{n+1} + 4y_{n+1} = 3(6x_n - x_{n-1}) + 4(6y_n - y_{n-1}) = \\ &= 6(3x_n + 4y_n) - (3x_{n-1} + 4y_{n-1}) = 6x_{n+1} - x_n; \end{aligned}$$

аналогичная выкладка доказывает равенство  $y_{n+2} = 6y_{n+1} - y_n$ .

**19.** Нет. а)  $(x-1)^2 + x^2 + (x+1)^2 = 3x^2 + 2$ ; но квадрат не может дать остаток 2 при делении на 3.

б)  $(x-1)^2 + x^2 + (x+1)^2 + (x+2)^2 = 4x^2 + 4x + 6 \equiv 2 \pmod{4}$ ; но квадрат целого числа не может дать остаток 2 при делении на 4.

в)  $5x^2 + 10 = 5(x^2 + 2)$  не может быть квадратом, поскольку  $x^2 + 2$  ни при каком целом  $x$  не делится на 5.

г)  $6x^2 + 6x + 19 \equiv 3 \pmod{4}$ .

д)  $x^2 + 4 = 7z^2$ . Значит,  $x^2 + 4$  делится на 7, что невозможно.

е)  $2x^2 + 2x + 11 = z^2$ . Значит,  $z^2 \equiv 3 \pmod{4}$ .

ж)  $(x-4)^2 + (x-3)^2 + (x-2)^2 + \dots + (x+3)^2 + (x+4)^2 = 9x^2 + 60$  делится на 3, но не делится на 9 и поэтому не может быть точным квадратом.

з)  $2x(x+1) \not\equiv 3 \pmod{5}$ , поскольку  $(2x+1)^2 \not\equiv 7 \pmod{5}$ .

и)  $y^2 \not\equiv 2 \pmod{4}$ .

**20.** Если  $a^2 - db^2 = \pm 1$ , то

$$\frac{1}{a+b\sqrt{d}} = \frac{a-b\sqrt{d}}{(a-b\sqrt{d})(a+b\sqrt{d})} = \frac{a-b\sqrt{d}}{a^2-db^2} = \pm(a-b\sqrt{d}).$$

Обратно, пусть числа  $x$  и  $y$  целые. Рассмотрим равенство

$$(a+b\sqrt{d})(x+y\sqrt{d}) = 1$$

и сопряженное к нему:

$$(a-b\sqrt{d})(x-y\sqrt{d}) = 1.$$

Перемножив эти равенства, получаем

$$(a^2 - db^2)(x^2 - dy^2) = 1,$$

откуда  $a^2 - db^2 = \pm 1$ .

$$\begin{aligned} \mathbf{21. а)} \quad x_{2n} + y_{2n}\sqrt{2} &= (1 + \sqrt{2})^{2n} = \left((1 + \sqrt{2})^n\right)^2 = \\ &= (x_n + y_n\sqrt{2})^2 = x_n^2 + 2y_n^2 + 2x_ny_n\sqrt{2}. \end{aligned}$$

Поскольку  $x_n^2 - 2y_n^2 = (-1)^n$ , то  $x_{2n} + y_{2n}\sqrt{2} = (2x_n^2 - (-1)^n) + (2x_ny_n)\sqrt{2}$ .

$$\mathbf{22. а)} \quad (1 + \sqrt{2})^n = x_n + y_n\sqrt{2} = \sqrt{x_n^2} + \sqrt{2y_n^2} = \sqrt{x_n^2} + \sqrt{x_n^2 - (-1)^n}.$$

б) Пусть  $n$  нечетно. Возводя число  $\sqrt{m+d} + \sqrt{m}$  в  $n$ -ю степень и пользуясь тем, что  $(\sqrt{m+d})^2$  и  $(\sqrt{m})^2$  – натуральные числа, получаем равенство

$$(\sqrt{m+d} + \sqrt{m})^n = s\sqrt{m+d} + t\sqrt{m},$$

где  $s$  и  $t$  – натуральные числа. Заменяя  $\sqrt{m}$  на  $-\sqrt{m}$ , получим сопряженную формулу

$$(\sqrt{m+d} - \sqrt{m})^n = s\sqrt{m+d} - t\sqrt{m}.$$

Перемножим:

$$d^n = (m+d-m)^n = (s\sqrt{m+d} + t\sqrt{m})(s\sqrt{m+d} - t\sqrt{m}) = s^2(m+d) - t^2m.$$

Таким образом, достаточно положить  $k = t^2 m$  — при этом

$$(\sqrt{m+d} + \sqrt{m})^n = \sqrt{s^2(m+d)} + \sqrt{t^2 m} = \sqrt{k+d^n} + \sqrt{k}.$$

Решение для четных  $n$  аналогично:

$$(\sqrt{m+d} + \sqrt{m})^n = s + t\sqrt{m(m+d)},$$

где  $s, t$  — натуральные числа. Заменяя  $\sqrt{m}$  на  $-\sqrt{m}$ , получаем

$$(\sqrt{m+d} - \sqrt{m})^n = s - t\sqrt{m(m+d)}.$$

Следовательно,

$$d^n = (m+d-m)^n = (s + t\sqrt{m(m+d)})(s - t\sqrt{m(m+d)}) = s^2 - t^2 m(m+d).$$

Значит, если  $k = t^2 m(m+d)$ , то

$$(\sqrt{m+d} + \sqrt{m})^n = \sqrt{s^2} + \sqrt{t^2 m(m+d)} = \sqrt{k+d^n} + \sqrt{k},$$

что и требовалось.

Можно решить задачу и по-другому. Обозначим  $A = \sqrt{m} + \sqrt{m+d}$ .

Рассмотрим функцию  $y = \sqrt{x+d^n} + \sqrt{x}$ . Она непрерывна, а ее значение в точке  $x = 0$  меньше числа  $A^n$ . Поскольку эта функция стремится к бесконечности при  $x \rightarrow +\infty$ , то существует такое  $x$ , что

$$\sqrt{x+d^n} = A^n - \sqrt{x}.$$

Возводя обе части последнего равенства в квадрат, получаем после упрощения:

$$\begin{aligned} \sqrt{x} = \frac{A^{2n} - d^n}{2A^n} &= \frac{A^n - \left(\frac{d}{\sqrt{m+d} + \sqrt{m}}\right)^n}{2} = \\ &= \frac{(\sqrt{m+d} + \sqrt{m})^n - (\sqrt{m+d} - \sqrt{m})^n}{2}, \end{aligned}$$

откуда уже легко вывести, что  $x$  — натуральное число.

в) Число  $x = \frac{n + \sqrt{n^2 - 4}}{2}$  удовлетворяет равенству  $x + \frac{1}{x} = n$ .

Положим  $k_m = x^m + \frac{1}{x^m}$ . Тогда  $k_{m+1} = k_m \left(x + \frac{1}{x}\right) - k_{m-1} = nk_m - k_{m-1}$ .

Поскольку числа  $k_0 = 2$  и  $k_1 = n$  натуральные, то по индукции легко доказать, что все числа  $k_m$  натуральные. Решая квадратное уравне-

ние, находим  $x^m = \frac{k_m \pm \sqrt{k_m^2 - 4}}{2}$ . Поскольку  $x \geq 1$ , то нужно взять

знак «плюс».

**23.** Нет. Если бы такие числа  $a, b, c$  и  $d$  существовали, то при помощи перехода к сопряженным числам мы получили бы:

$$0 \leq (a - b\sqrt{2})^2 + (c - d\sqrt{2})^2 = 7 - 5\sqrt{2} < 0.$$

**24. а) Первый способ.** Пусть  $(5 + 3\sqrt{2})^m = (3 + 5\sqrt{2})^n$ . Переход к сопряженным числам дает равенство  $(5 - 3\sqrt{2})^m = (3 - 5\sqrt{2})^n$ , которое противоречит неравенствам  $0 < 5 - 3\sqrt{2} < 1$  и  $5\sqrt{2} - 3 > 1$ .

*Второй способ.* Если  $(5 + 3\sqrt{2})^m = (3 + 5\sqrt{2})^n$ , то и  $(5 - 3\sqrt{2})^m = (3 - 5\sqrt{2})^n$ . Перемножив эти равенства, получим:  $(25 - 9 \cdot 2)^m = (9 - 25 \cdot 2)^n$ , т.е.  $7^m = (-41)^n$ , что невозможно.

**б)** Пусть для определенности  $a < b$ . Тогда  $1 < b + a\sqrt{d} < a + b\sqrt{d}$  и поэтому  $m < n$ . Переходя к сопряженным числам и деля почленно полученное при этом равенство на исходное, получаем:

$$\left| \frac{a - b\sqrt{d}}{a + b\sqrt{d}} \right|^m = \left| \frac{b - a\sqrt{d}}{b + a\sqrt{d}} \right|^n.$$

Сравним величины  $\mu = \left| \frac{b\sqrt{d} - a}{a + b\sqrt{d}} \right|$  и  $\nu = \left| \frac{a\sqrt{d} - b}{b + a\sqrt{d}} \right|$ . Для этого достаточно сравнить числа

$$\left| (b\sqrt{d} - a)(b + a\sqrt{d}) \right| \text{ и } \left| (a\sqrt{d} - b)(a + b\sqrt{d}) \right|.$$

Первое из них равно  $\left| ab(d - 1) + (b^2 - a^2)\sqrt{d} \right|$ , а второе равно  $\left| ab(d - 1) - (b^2 - a^2)\sqrt{d} \right|$ . Обозначая  $S = ab(d - 1)$  и  $T = (b^2 - a^2)\sqrt{d}$ , сводим дело к сравнению чисел  $|S + T|$  и  $|S - T|$ . Поскольку  $S$  и  $T$  — положительные числа, то  $|S + T| > |S - T|$ . Значит,  $\mu > \nu$ . Тем более,  $\mu^m > \nu^m > \nu^n$ . Но, как вы помните,  $\mu^m = \nu^n$ .

**25. а)** Число  $x = (45 + \sqrt{1975})^{30}$  можно представить в виде  $a + b\sqrt{1975}$ , где  $a, b$  — натуральные числа. Рассмотрим сопряженное число  $y = (45 - \sqrt{1975})^{30} = a - b\sqrt{1975}$ . Поскольку  $x + y = 2a$  и  $0 < y < 1$ , то  $[x] = [2a - y] = 2a - 1$ .

**г)** Воспользуйтесь тем, что  $2 - \sqrt{3} > 0$ , число  $(2 + \sqrt{3})^n + (2 - \sqrt{3})^n$  целое и  $\lim_{n \rightarrow \infty} (2 - \sqrt{3})^n = 0$ .

**д)**  $a_n = (5 + 2\sqrt{6})^n + (5 - 2\sqrt{6})^n$ . Обозначим  $\alpha = 5 + 2\sqrt{6}$  и

$\beta = 5 - 2\sqrt{6}$ . Тогда

$$\begin{aligned} a_{n+2} &= \alpha^{n+2} + \beta^{n+2} = (5 + 2\sqrt{6})^2 \alpha^n + (5 - 2\sqrt{6})^2 \beta^n = \\ &= (49 + 20\sqrt{6})\alpha^n + (49 - 20\sqrt{6})\beta^n = \\ &= (50 + 20\sqrt{6})\alpha^n + (50 - 20\sqrt{6})\beta^n - \alpha^n - \beta^n = \\ &= 10(\alpha^{n+1} + \beta^{n+1}) - (\alpha^n + \beta^n) = 10a_{n+1} - a_n. \end{aligned}$$

Поскольку  $a_{n+4} = 10a_{n+3} - a_{n+2} = 10a_{n+3} - 10a_{n+1} + a_n$ , то числа  $a_{n+4}$  и  $a_n$  оканчиваются одной и той же цифрой. Поскольку  $a_0 = 2$ , то десятичная запись числа  $a_{1000}$  оканчивается цифрой 2. Далее,

$$\begin{aligned} a_{1000} &= (\sqrt{3} + \sqrt{2})^{2000} + (\sqrt{3} - \sqrt{2})^{2000} > (\sqrt{3} + \sqrt{2})^{2000} = \\ &= a_{1000} - (\sqrt{3} - \sqrt{2})^{2000} > a_{1000} - \left(\frac{1}{3}\right)^{2000} > a_{1000} - 10^{-666}, \end{aligned}$$

откуда и следует, что перед запятой в десятичной записи числа  $(\sqrt{3} + \sqrt{2})^{2000}$  стоит цифра 1, а после запятой – не менее 666 девяток. (При помощи компьютера можно проверить, что девяток 995 штук.)

**26.** Обозначим:  $a = 1 + \sqrt{2} + \sqrt{3}$ ,  $b = 1 - \sqrt{2} + \sqrt{3}$ ,  $c = 1 + \sqrt{2} - \sqrt{3}$  и  $d = 1 - \sqrt{2} - \sqrt{3}$ . Наряду с равенством

$$a^n = (1 + \sqrt{2} + \sqrt{3})^n = q_n + r_n\sqrt{2} + s_n\sqrt{3} + t_n\sqrt{6}$$

рассмотрим три сопряженных:

$$b^n = q_n - r_n\sqrt{2} + s_n\sqrt{3} - t_n\sqrt{6},$$

$$c^n = q_n + r_n\sqrt{2} - s_n\sqrt{3} - t_n\sqrt{6},$$

$$d^n = q_n - r_n\sqrt{2} - s_n\sqrt{3} + t_n\sqrt{6}.$$

Из этих четырех равенств находим:

$$4q_n = a^n + b^n + c^n + d^n,$$

$$4r_n\sqrt{2} = a^n - b^n + c^n - d^n,$$

$$4s_n\sqrt{3} = a^n + b^n - c^n - d^n,$$

$$4t_n\sqrt{6} = a^n - b^n - c^n + d^n.$$

Следовательно,

$$\frac{r_n}{q_n} = \frac{a^n - b^n + c^n - d^n}{(a^n + b^n + c^n + d^n)\sqrt{2}} = \frac{1 - \left(\frac{b}{a}\right)^n + \left(\frac{c}{a}\right)^n - \left(\frac{d}{a}\right)^n}{\left(1 + \left(\frac{b}{a}\right)^n + \left(\frac{c}{a}\right)^n + \left(\frac{d}{a}\right)^n\right)\sqrt{2}} \rightarrow \frac{1}{\sqrt{2}}.$$

(Стремление величин  $(b/a)^n$ ,  $(c/a)^n$  и  $(d/a)^n$  к нулю следует из того, что все три числа  $b/a$ ,  $c/a$  и  $d/a$  по модулю меньше 1.)

Аналогично можно доказать, что

$$\lim_{n \rightarrow \infty} \frac{s_n}{q_n} = 1/\sqrt{3} \text{ и } \lim_{n \rightarrow \infty} \frac{t_n}{q_n} = 1/\sqrt{6}.$$

**27. а)** Домножим обе части уравнения  $3x^2 + 3x + 1 = y^2$  на 4 и выделим полный квадрат:  $3(4x^2 + 4x + 1) + 1 = (2y)^2$ , т.е.  $(2y)^2 - 3(2x + 1)^2 = 1$ . Обозначая  $z = 2y$  и  $t = 2x + 1$ , получаем уравнение Пелля  $z^2 - 3t^2 = 1$ . Нас интересуют не все его решения, а лишь те, где  $z$  четно. В любом решении уравнения  $z^2 - 3t^2 = 1$  одно из чисел  $z$  и  $t$  четно, а другое нечетно. При переходе  $(z; t) \rightarrow (2z + 3t; z + 2t)$  пара (четное; нечетное) преобразуется в (нечетное; четное), и наоборот. Поэтому нужно рассматривать только «половину» решений, а именно  $(z; t) = (26; 15)$ ,  $(362; 209)$ ,  $(5042; 2911)$ ,  $(70226; 40545)$ ,  $(978122; 564719)$ ,  $(13623482; 7865521)$  и так далее. Этим решениям соответствуют пары  $(x; y) = (7; 13)$ ,  $(104; 181)$ ,  $(1455; 2521)$ ,  $(20272; 35113)$ ,  $(282359; 489061)$ ,  $(3932760; 6811741)$ , ... В частности,  $8^3 - 7^3 = 13^2$  и  $3932761^3 - 3932760^3 = 6811741^2$ . Впечатляет, не правда ли?

**б)**  $(2n - 1)(2n + 1) = 3(2x + 1)^2$ . Числа  $2n - 1$  и  $2n + 1$  взаимно просты, так что одно из них должно быть квадратом, а другое — утроенным квадратом. Значит, либо  $2n - 1 = 3t^2$  и  $2n + 1 = s^2$ , либо  $2n - 1 = t^2$  и  $2n + 1 = 3s^2$ . В первом случае  $s^2 - 3t^2 = 2$ , что невозможно, поскольку квадрат целого числа не может давать остаток 2 при делении на 3. Значит, имеет место второй случай:  $2n - 1 = t^2$ . Обозначив  $t = 2k + 1$ , из равенства  $2n - 1 = (2k + 1)^2$  получаем  $n = 2k^2 + 2k + 1 = k^2 + (k + 1)^2$ .

**в)**  $6x^2 + 12x + 8 \equiv 2 \equiv y^2 \pmod{3}$ .

**28.** Числа  $m$  и  $n$  удовлетворяют равенству  $m^2 - 3n^2 = 1$ , которое можно записать в виде  $(m - 1)(m + 1) = 3n^2$ .

**а)** Если  $k$  нечетно, то  $m$  четно, так что числа  $m - 1$  и  $m + 1$  взаимно просты и решение такое же, как решение пункта **б)** предыдущего упражнения.

**б)** Если  $k$  четно, то  $m$  нечетно и, следовательно,  $\text{НОД}(m - 1, m + 1) = 2$ . Значит, одно из чисел  $m - 1$  и  $m + 1$  имеет вид  $2a^2$ , а другое —  $6b^2$ . В случае, когда  $m - 1 = 2a^2$  и  $m + 1 = 6b^2$ , имеем  $a^2 = 3b^2 - 1$ , что невозможно. Следовательно,  $m + 1 = 2a^2$ , что и требовалось доказать.

**29.** Да. Например,  $x = 4$ ,  $y = 1$ ,  $d = 15$ .

**30.** Поскольку  $-1 < (1 - \sqrt{3})^{2n+1} < 0$  и число  $(1 + \sqrt{3})^{2n+1} + (1 - \sqrt{3})^{2n+1}$  целое,

$$\begin{aligned} \left[ (1 + \sqrt{3})^{2n+1} \right] &= (1 + \sqrt{3})^{2n+1} + (1 - \sqrt{3})^{2n+1} = \\ &= (1 + \sqrt{3})(4 + 2\sqrt{3})^n + (1 - \sqrt{3})(4 - 2\sqrt{3})^n = \\ &= 2^n \cdot \left( (1 + \sqrt{3})(2 + \sqrt{3})^n + (1 - \sqrt{3})(2 - \sqrt{3})^n \right) = \\ &= 2^n (2x_n + 6y_n) = 2^{n+1} (x_n + 3y_n), \end{aligned}$$

где  $x_n = \frac{(2 + \sqrt{3})^n + (2 - \sqrt{3})^n}{2}$  и  $y_n = \frac{(2 + \sqrt{3})^n - (2 - \sqrt{3})^n}{2\sqrt{3}}$  удовлетворяют равенству  $x_n^2 - 3y_n^2 = 1$ . Осталось заметить, что  $x_n$  и  $y_n$  — числа разной четности.

**31.** Рассмотрим 8 точек: вершины и середины сторон некоторого квадрата. Пусть все они лежат на гиперболах  $xy = \pm 1$ . Пусть на некоторой ветви лежат рассматриваемые точки  $K$  и  $L$ , не лежащие на одной стороне квадрата. С любой стороны от отрезка  $KL$  среди рассматриваемых вершин и середин сторон квадрата есть такая точка  $M$ , что углы  $MKL$  и  $MLK$  острые. Получили противоречие: точка  $M$  должна лежать в полуполосе, ограниченной отрезком  $KL$  и восстановленными в точках  $K$  и  $L$  перпендикулярами, направленной внутрь рассматриваемой ветви гиперболы.

Точки  $K$  и  $L$  не могут быть и соседними вершинами квадрата (иначе середина отрезка  $KL$  не лежит на гиперболах).

Поскольку никакая сторона квадрата не пересекает никакую ветвь гиперболы более чем в двух точках, то каждой ветви принадлежат вершина квадрата и середина одной из выходящих из нее сторон.

Рассмотрим две такие точки  $A$  и  $B$ . При симметрии относительно начала координат точки  $A$  и  $B$  переходят в точки  $A'$  и  $B'$ , лежащие на другой ветви той же гиперболы. При этом отрезок  $A'B'$  равен и параллелен отрезку  $BA$ . Если бы противоположная вершине  $B$  вершина квадрата и противоположная середине  $A$  середина стороны квадрата не совпадали с точками  $B'$  и  $A'$  соответственно, то на ветви гиперболы нашлись бы два разных отрезка, равных по длине и параллельных. Получили желанное противоречие: таких отрезков не бывает!

**32.** а) Воспользуйтесь индукцией или запишите тождество в виде

$\varphi_n^2 - \varphi_n \varphi_{n-1} - \varphi_{n-1}^2 = -(-1)^n$  и вспомните теорему 6.

$$\begin{aligned} \text{б) } \varphi_{n-2} \varphi_{n+2} &= (\varphi_n - \varphi_{n-1})(\varphi_n + \varphi_{n+1}) = \varphi_n^2 - \varphi_{n-1} \varphi_{n+1} + \varphi_n \varphi_{n+1} - \\ &- \varphi_{n-1} \varphi_n = -(-1)^n + \varphi_n (\varphi_{n+1} - \varphi_{n-1}) = \varphi_n^2 - (-1)^n. \end{aligned}$$

**33. а)** Одно решение очевидно:  $4^2 - 2 \cdot 1^2 = 14$ . Если  $x^2 - 2y^2 = 14$ , то  $(3x + 4y)^2 - 2(2x + 3y)^2 = 14$ , так что из всякого решения  $(x; y)$  можно получить еще одно решение  $(3x + 4y; 2x + 3y)$ . При положительных  $x$  и  $y$  числа  $3x + 4y$  и  $2x + 3y$  тоже положительны и  $3x + 4y > x$  (да и  $2x + 3y > y$ ).

б) Воспользуйтесь тем, что  $23 = 5^2 - 2 \cdot 1^2$ .

в) *Первый способ.* Пусть  $x^2 - 2y^2 = 3$ . Если хотя бы одно из чисел  $x$  и  $y$  делится на 3, то другое тоже должно делиться на 3, и  $x^2 - 2y^2$  делится на 9. Если же ни  $x$ , ни  $y$  не делятся на 3, то  $x^2$  и  $y^2$  дают остаток 1 при делении на 3, и левая часть уравнения не делится на 3.

Пусть теперь  $x^2 - 2y^2 = 2005$ . Если хотя бы одно из чисел  $x, y$  делится на 5, то второе тоже делится на 5, и тогда левая часть делится на 25, а 2005 на 25 не делится. В противном случае левая часть на 5 не делится, поскольку тогда каждое из чисел  $x^2$  и  $y^2$  при делении на 5 дает остаток 1 или 4, а ни одно из чисел  $1 - 2 \cdot 1$ ,  $1 - 2 \cdot 4$ ,  $4 - 2 \cdot 1$  и  $4 - 2 \cdot 4$  не делится на 5.

*Второй способ.* Если число  $x^2 - 2y^2$  нечетно, то  $x$  нечетно, так что  $x^2 \equiv 1 \pmod{8}$  и, следовательно,  $x^2 - 2y^2 \equiv 1$  или  $-1 \pmod{8}$ .

**34. а)**  $11^2 = (-4)^2 + (-3)^2 + \dots + 5^2 + 6^2$ . Уравнение  $(x - 5)^2 + (x - 4)^2 + \dots + (x + 4)^2 + (x + 5)^2 = y^2$  после раскрытия скобок и приведения подобных принимает вид  $11x^2 + 110 = y^2$ . Замена  $y = 11z$  и сокращение на 11 дают  $x^2 + 10 = 11z^2$ . Наименьшее по величине натуральное  $z$ , удовлетворяющее этому уравнению, равно 1. При этом  $y = 11$ .

б) Поскольку  $x^2 - 1 = 11z^2 - 11$ , то  $(x - 1)(x + 1) = x^2 - 1$  делится на 11. Значит,  $x = 11t \pm 1$ . Значения  $x = 1, 10, 12, 21$  не подходят, а при  $x = 23$  имеем  $z = 7$ , т.е.  $y = 77$ .

в) Поскольку  $1^2 - 11 \cdot 1^2 = -10$  и  $10^2 - 11 \cdot 3^2 = 1$ , то уравнение  $x^2 - 11z^2 = -10$  имеет бесконечно много решений в натуральных числах.

**35.** Случай  $b = 0$  тривиален: достаточно взять  $u = v = 0$  и  $w \neq 0$ .

Пусть  $b \neq 0$ . Если  $x^2 + ay^2 \neq 0$ , домножим обе части равенства  $x^2 + ay^2 = -b(z^2 + at^2)$  на  $x^2 + ay^2$  и воспользуемся формулой

$$(x^2 + ay^2)^2 = -b((xz - ayt)^2 + a(xt + yz)^2).$$



Следовательно,

$$-b = \left( \frac{b(xz - ayt)}{x^2 + ay^2} \right)^2 + a \left( \frac{b(xt + yz)}{x^2 + ay^2} \right)^2.$$

Значит, можно взять  $u = \frac{b(xz - ayt)}{x^2 + ay^2}$ ,  $v = \frac{b(xt + yz)}{x^2 + ay^2}$  и  $w = 1$ .

Если же  $x^2 + zy^2 = 0$ , то  $z^2 + at^2 = 0$  и можно в случае  $x^2 + y^2 \neq 0$  взять  $u = x$ ,  $v = y$ ,  $w = 0$ . А в случае  $x = y = 0$  можно взять  $u = z$ ,  $v = t$  и  $w = 0$ .

**37.** Можно считать, что  $x \geq 0$  и  $y \geq 0$ . Рассмотрим натуральные числа  $a$  и  $b$ , для которых  $a^2 - db^2 = 1$ . Тогда числа  $x_1 = ax + dby$  и  $y_1 = bx + ay$  натуральные. Формулы  $x_{n+1} = ax_n + dby_n$  и  $y_{n+1} = bx_n + ay_n$  дают бесконечную последовательность решений.

**38.** а) При любом натуральном  $a$ , не являющемся квадратом натурального числа, а также при  $a = 0$ . б) При  $a = 0$  число  $d$  должно быть квадратом, а при  $a \neq 0$  число  $d$  должно не быть квадратом.

**39.** б) Поскольку  $n^2 - (n^2 + 1) = -1$ , то  $(n - \sqrt{n^2 + 1})^2 (n + \sqrt{n^2 + 1})^2 = (-1)^2 = 1$ , откуда  $(2n^2 + 1 - 2n\sqrt{n^2 + 1})(2n^2 + 1 + 2n\sqrt{n^2 + 1}) = 1$ . Мы нашли решение  $(x; y) = (2n^2 + 1; 2n)$  уравнения Пелля в натуральных числах. А если есть одно, то есть и бесконечно много.

$$\text{в) } (n^2 + 1)^2 - (n^2 + 2)n^2 = 1.$$

$$\text{г) } (n^2 - 1)^2 - (n^2 - 2)n^2 = 1.$$

**40.** Воспользуйтесь предыдущим упражнением и тем, что а)  $(a^2 + 1)(a^2 + 1) = (a^2 + 1)^2$ ; б)  $(a^2 - 1)(a^2 - 1) = (a^2 - 1)^2$  (случай  $a = 1$  разберите отдельно; впрочем, он очевиден); в)  $(a^2 + 1)(0^2 + 1) = a^2 + 1$ ; г)  $(a^2 - 1)(1^2 - 1) = 1^2 - 1$  (случай  $a = 1$  требует отдельного рассмотрения); д)  $(a^2 + 1)(1^2 - 1) = 1^2 - 1$ ; е)  $(a^2 - 1)(0^2 + 1) = a^2 - 1$  (и опять случай  $a = 1$  требует отдельного рассмотрения).

**41.** а) Если  $y$  четно, то при делении на 4 правая часть уравнения дает остаток 3, а левая — 1. Если  $y$  нечетно, то правая часть делится на 8; поскольку ни  $a^2 + 1$ , ни  $x^2 + 1$  не делятся на 4, то левая часть на 8 не делится.

в) Если  $x$  нечетно, то  $x^2 - 1$  делится на 4 (и даже на 8); с другой стороны,  $y^2 + 1$  не делится на 4. Если  $x$  четно, то число  $x^2 - 1$  имеет хотя бы один простой делитель вида  $p = 4n - 1$ . Возведя обе части сравнения  $y^2 \equiv -1 \pmod{p}$  в степень  $2n - 1$ ,

получим:  $y^{p-1} = (y^2)^{2n-1} \equiv (-1)^{2n-1} = -1$ . Последнее сравнение противоречит малой теореме Ферма.

42. а) Если  $(x; y; z; t) = (2 + a; 2 - a; b - 1; -b - 1)$ , то  $x^3 + y^3 + z^3 + t^3 = (2 + a)^3 + (2 - a)^3 + (b - 1)^3 + (-b - 1)^3 = 14 + 12a^2 - 6b^2$ . Приходим к уравнению  $12a^2 - 6b^2 = -12$ , т.е.  $b^2 - 2a^2 = 2$ . б) Пусть  $x = 1$ . Замена  $Y = y + 1$  и  $Z = z + 1$  сводит задачу к уравнению  $Z^2 - 3Y^2 = -2$ , которое имеет бесконечно много решений.

в) Рассмотрите числа  $1, 2$  и  $y^2 + 1$ , где  $y$  — натуральное число, для которого существует такое натуральное число  $x$ , что  $x^2 - 2y^2 = 1$ .

г) Полагая  $x = 1$ , получаем уравнение  $(a^2 + 1)(v^2 + 1) = u^2 + 1$ , т.е.

$$u^2 - (a^2 + 1)v^2 = a^2.$$

Это уравнение имеет целочисленное решение  $(u; v) = (a; 0)$ . Поэтому оно имеет бесконечно много решений в натуральных числах.

д) Раскрыв скобки и приведя подобные в уравнении

$$x^2 = (y + 1)^2 + (y + 2)^2 + \dots + (y + k)^2,$$

получаем

$$x^2 = ky^2 + k(k + 1)y + \frac{k(k + 1)(2k + 1)}{6}.$$

Замена  $Y = y + \frac{k + 1}{2}$  приводит уравнение к виду

$$x^2 - kY^2 = \frac{k(k - 1)(k + 1)}{12}.$$

При  $k = 3n^2 - 1$  получаем уравнение

$$x^2 - (3n^2 - 1)Y^2 = \frac{(3n^2 - 2)(3n^2 - 1)n^2}{4}.$$

Если  $n$  четно, то это уравнение имеет целочисленное решение

$$(x : Y) = \left( \frac{n(3n^2 - 1)}{2}; \frac{n}{2} \right), \text{ а вследствие упражнения 24 — и бесконечно}$$

много решений в натуральных числах.

Если же  $n$  нечетно, то умножение обеих частей полученного уравнения на 4 и замена  $X = 2x$  и  $z = 2Y = 2y + k + 1$  приводят уравнение к виду

$$X^2 - (3n^2 - 1)z^2 = (3n^2 - 2)(3n^2 - 1)n^2,$$

причем  $X$  должно быть четно, а  $z$  нечетно. Пользуясь тем, что оно имеет целочисленное решение  $(X : z) = (n(3n^2 - 1); n)$ , где как раз  $X$  четно, а  $z$  нечетно, легко завершить решение. (Для этого достаточно убедиться, что в существующем в силу теоремы 10 решении уравне-

ния  $a^2 - (3n^2 - 1)b^2 = 1$  в натуральных числах число  $a$  нечетное. Четно или нечетно  $b$ , не столь уж важно: от этого зависит лишь то, сходятся ли все все решения соответствующей серии или же только каждое второе из них.)

43. а) Докажите, что существует бесконечно много таких пар натуральных чисел  $m$  и  $n$ , для которых  $n^2 + 1 = 5m^2$  и  $m > 5$ . При этом  $m = \sqrt{(n^2 + 1)/5} < n/2$  и  $n!$  делится на  $n^2 + 1$ , так как при  $m > 5$  в произведении  $1 \cdot 2 \cdot 3 \cdot 4 \cdot \dots \cdot (n-1) \cdot n$  есть множители 5,  $m$  и  $2m$ .

б) В силу равенства  $n^2 - (n^2 + 1) \cdot 1 = -1$  существуют сколь угодно большие натуральные числа  $d$ , для которых уравнение  $x^2 - dy^2 = -1$  имеет хотя бы одно решение в натуральных числах – а следовательно, и бесконечно много.

Есть и другие способы доказательства. Например, можно воспользоваться разложением многочлена  $x^{105} + 1$  на неприводимые многочлены с целыми коэффициентами (подробности – в статье «Многочлены деления круга», см. «Квант» №1 за 1998 г.) или разложением

$$64m^{12} + 1 =$$

$$= (4m^4 + 1)(4m^4 - 4m^3 + 2m^2 - 2m + 1)(4m^4 + 4m^3 + 2m^2 + 2m + 1).$$

44. В силу теоремы 10, существуют натуральные  $x$  и  $y$ , для которых  $x^2 - py^2 = 1$ . Рассмотрим *наименьшее* из таких чисел  $x$ . Если  $x$  четно, то  $y$  нечетно и, рассмотрев остаток от деления числа  $py^2$  на 4, получаем противоречие. Следовательно,  $x = 2a + 1$  и  $y = 2b$ , где  $a$  и  $b$  – целые числа. Поскольку

$$4pb^2 = py^2 = x^2 - 1 = 4a(a + 1),$$

то  $pb^2 = a(a + 1)$ . Если  $a = pz^2$  и  $a + 1 = t^2$ , где  $z$  и  $t$  – натуральные числа, то  $t^2 - pz^2 = 1$ , что противоречит минимальности числа  $x$ .

Значит,  $a = z^2$  и  $a + 1 = pt^2$ , где  $z$  и  $t$  – натуральные числа;  $z^2 - pt^2 = -1$ .

45. Неравенство  $\left| \frac{a^2}{4} - \frac{b^2}{4} - \frac{ab}{2} \right| < \frac{1}{2}$  можно записать в виде

$= |a^2 - b^2 - 2ab| < 2$ , откуда  $(a - b)^2 - 2b^2 = \pm 1$ . Значит,  $(a - b; b) = (1; 1), (3; 2), (7; 5), (17; 12)$  или  $(41; 29)$ , откуда  $(a; b) = (2; 1), (5; 2), (12; 5), (29; 12)$  или  $(70; 29)$ . Треугольник с катетами 29 и 12 расположить можно, ибо  $29 + \frac{12}{2} < 40$  и  $12 + \frac{29}{2} < 32$ .

А треугольник с катетом длины 70 расположить нельзя, ибо  $70^2 > 40^2 + 32^2$ .

**46.** Надо решить в натуральных числах уравнение

$$\frac{n(n+1)}{2} = \frac{k(k+1)}{2} - \frac{n(n+1)}{2},$$

т.е.  $2n(n+1) = k(k+1)$ . Умножив обе части на 2, получаем уравнение

$$(2n+1)^2 - 1 = 2k^2 + 2k.$$

Обозначим  $x = 2n + 1$  и еще раз умножим на 2 обе части уравнения:

$$2x^2 - 2 = (2k+1)^2 - 1.$$

Обозначив  $2k+1 = y$ , получаем уравнение  $2x^2 - 1 = y^2$ , которому, как

мы знаем, удовлетворяют числа вида  $x = \left( (1 + \sqrt{2})^{2m+1} - (1 - \sqrt{2})^{2m+1} \right) / (2\sqrt{2})$ . Следовательно,  $n = \left( (1 + \sqrt{2})^{2m+1} - (1 - \sqrt{2})^{2m+1} - 2\sqrt{2} \right) / (4\sqrt{2})$ , где  $m$  — натуральное число.

**47. а)** Применим индукцию для доказательства того, что соседние члены рассматриваемой последовательности удовлетворяют уравнению. *База.*  $0^2 - m \cdot 0 \cdot 1 + 1^2 = 1$ . *Переход.* В последовательности  $a_0, a_1, a_2, \dots$  за каждой парой  $a_k = x$ ,  $a_{k+1} = y$  следует пара  $(a_{k+1}, a_{k+2}) = (a_{k+1}, ma_{k+1} - a_k) = (y, my - x)$ . Очевидно,

$$\begin{aligned} y^2 - my(my - x) + (my - x)^2 &= \\ &= y^2 - (my - x)(my - (my - x)) = y^2 - (my - x)x = x^2 - mxy + y^2, \end{aligned}$$

что и требовалось.

Теперь докажем, что других решений в целых неотрицательных числах у рассматриваемого уравнения нет. Предположим, что  $X^2 - mXY + Y^2 = 1$  и  $0 \leq X \leq Y$ . Если при этом  $X = 0$ , то, очевидно,  $Y = 1$ . Если же  $X > 0$ , рассмотрим систему уравнений

$$\begin{cases} y = X, \\ my - x = Y. \end{cases}$$

Очевидно,  $x = mX - Y$  и  $y = X$ . Если  $mX - Y < 0$ , то  $mXY < Y^2$  и  $1 = X^2 - mXY + Y^2 > X^2 \geq 1$ , что невозможно. Значит,  $x = mX - Y \geq 0$ . Если  $x = 0$ , то  $y = 1$ . Если же  $x > 0$ , то пара натуральных чисел  $(x, y)$  удовлетворяет равенству  $x^2 - mxy + y^2 = 1$  и условиям  $x < y = X \leq Y$  (проверьте!). Переходя таким образом от пары  $(X, Y)$  к предшественнице  $(x, y)$ , затем от  $(x, y)$  — к ее предшественнице и так далее, мы рано или поздно должны будем остановиться, а остановиться сможем лишь тогда, когда получим решение  $(x, y) = (0, 1)$ . Значит, за конечное число операций вида  $(X, Y) \rightarrow (x, y)$  мы из любого решения в натуральных числах полу-

чим решение  $(0;1)$ . Поэтому, идя по этой цепочке в обратном направлении, т.е. начав с пары  $(0;1)$  и многократно выполняя преобразование  $(x;y) \rightarrow (X;Y)$ , мы получим любое решение уравнения в целых неотрицательных числах  $x \leq y$ .

б) *Первый способ.* Рассуждайте по индукции, предварительно доказав тождество  $\varphi_{n+4} = 3\varphi_{n+2} - \varphi_n$ .

*Второй способ.* Уравнение  $x^2 - 3xy + y^2 = 1$  заменой  $y = x - z$  можно привести к виду  $z^2 + zx - x^2 = 1$ . Решения  $(x;z) = (\varphi_{2n}; \varphi_{2n-1})$  соответствуют решениям исходного уравнения в неотрицательных целых числах  $x$  и  $y$ , удовлетворяющих неравенству  $x \geq y$ . Значит,  $(x;y) = (x; x-z) = (\varphi_{2n}; \varphi_{2n} - \varphi_{2n-1}) = (\varphi_{2n}; \varphi_{2n-2})$ .

*Третий способ.* Приведите уравнение к виду  $(2x - 3y)^2 - 5y^2 = 4$ , вспомните следствие теоремы 7 и рассмотрите два случая:  $2x - 3y > 0$  и  $2x - 3y < 0$ .

48. а) Для  $p = 2$  годятся  $x = y = 1$ . Для  $p = 17$  годятся  $x = 4, y = 0$ . Для любого другого простого  $p$  рассмотрим числа вида  $x^2$ , где  $x = 0, 1, \dots, (p-1)/2$ , и числа вида  $34y^2 - 1$ , где  $y = 0, 1, \dots, (p-1)/2$ . Докажите, что как  $(p+1)/2$  рассматриваемых чисел вида  $x^2$  дают разные остатки при делении на  $p$ , так и  $(p+1)/2$  рассматриваемых чисел вида  $34y^2 - 1$  дают разные остатки при делении на  $p$ . Поскольку  $\frac{p+1}{2} + \frac{p+1}{2} > p$ , то хотя бы одно число одного вида сравнимо по модулю  $p$  с числом другого вида, т.е. найдется такая пара  $(x; y)$ , что  $x^2 - 34y^2 + 1$  делится на  $p$ .

г) Воспользуйтесь китайской теоремой об остатках, т.е. тем, что существуют такие числа  $x$  и  $y$ , для которых  $x \equiv x_1 \pmod{m_1}$ ,  $x \equiv x_2 \pmod{m_2}$ ,  $y \equiv y_1 \pmod{m_1}$  и  $y \equiv y_2 \pmod{m_2}$ .

е) Если бы существовало решение в целых числах, то существовало бы и решение, где  $x$  и  $y$  — натуральные числа. Среди всех таких решений нашлось бы решение с наименьшей возможной величиной  $y$ . Поскольку

$$35^2 - 34 \cdot 6^2 = 35^2 - (35-1)(35+1) = 1,$$

то

$$\begin{aligned} x^2 - 34y^2 &= (x - y\sqrt{34})(x + y\sqrt{34}) = \\ &= (35x - 204y - (35y - 6x)\sqrt{34})(35x - 204y + (35y - 6x)\sqrt{34}). \end{aligned}$$

Докажем неравенства  $35x - 204y > 0$ ,  $35y - 6x > 0$  и  $35y - 6x < y$ .

Поскольку  $\frac{3}{17} > \frac{35}{204}$ , то достаточно доказать, что

$$\frac{6}{35}x < y < \frac{35}{204}x.$$

Первое совсем легко: если  $\frac{6}{35}x \geq y$ , то

$$-1 = x^2 - 34y^2 \geq \frac{35^2}{36}y^2 - 34y^2 = \frac{y^2}{36} > -1,$$

что неверно. Второе неравенство доказать чуть сложнее. Если  $y \geq \frac{35}{204}x$ , то

$$x^2 - 34y^2 \leq \frac{204^2}{35^2}y^2 - 34y^2 = \frac{-34y^2}{35^2}.$$

При  $y \geq 7$  противоречие очевидно:  $\frac{34y^2}{35^2} > 1$ . А для каждого из значений  $y = 1, 2, 3, 4, 5$  и  $6$  легко проверить, что  $34y^2 - 1$  не является квадратом целого числа.

$$\begin{aligned} 49. \text{ а) } 3a^2 - 2b^2 &= (a\sqrt{3} - b\sqrt{2})(a\sqrt{3} + b\sqrt{2}) = \\ &= (\sqrt{3} - \sqrt{2})^{2001} (\sqrt{3} + \sqrt{2})^{2001} = \\ &= ((\sqrt{3} - \sqrt{2})(\sqrt{3} + \sqrt{2}))^{2001} = (3 - 2)^{2001} = 1. \end{aligned}$$

б) Воспользуемся формулой  $(a\sqrt{3} + b\sqrt{2})(\sqrt{3} \pm \sqrt{2})^2 = (5a \pm 4b)\sqrt{3} + (5b \pm 6a)\sqrt{2}$ . Пусть  $a, b$  — натуральные числа и  $3a^2 - 2b^2 = 1$ . Тогда  $3(5a - 4b)^2 - 2(5b - 6a)^2 = 1$ . Если  $5a - 4b \leq 0$ , то  $3a^2 - 2b^2 \leq 3\left(\frac{4}{5}b\right)^2 = -\frac{2}{25}b^2 < 0$ . Значит,  $5a - 4b > 0$ . Если  $5b - 6a \leq 0$ , то  $3a^2 - 2b^2 \geq 3\left(\frac{5}{6}b\right)^2 - 2b^2 = \frac{1}{12}b^2$ . Осталось проверить значения  $b = 1, 2, 3$ . Подходит только  $b = 1$ , которому соответствует  $a = 1$ . Дальнейшие рассуждения аналогичны доказательствам теорем 2, 3, 5, 9.

50. а) Вспомнив пункт б) упражнения 20, видим: годятся  $a = \varphi_{2n-1}$  и  $b = \varphi_{2n+1}$ , где  $n$  — натуральное число.

в) Если  $a = b$ , то  $c = 2 + \frac{1}{a^2}$ , так что  $a = 1$  и  $c = 3$ . Пусть  $c \neq 3$  и  $a < b$ , причем  $b$  — наименьшее возможное. Положим  $A = ca - b$  и  $B = a$ . Очевидно,

$$A = ca - b = \frac{a^2 + 1}{b} < a + 1.$$

Значит,

$$0 < A \leq a = B < b$$

и

$$A^2 + B^2 + 1 = A^2 + a^2 + 1 = A^2 + Ab = A(A + b) = ABc.$$

Получили противоречие: число  $b$  оказалось не самым маленьким из возможных!

д) Пусть  $x^2 - (n^2 - 4)y^2 = -4$ , где  $x, y$  — натуральные числа. Число  $x$  той же четности, что и число  $ny$ . Значит, число  $a = (x + ny)/2$  натуральное. Как легко убедиться,

$$a^2 + y^2 + 1 = ayn.$$

51. а) Случай  $a = b$  невозможен: число  $\frac{2a^2}{a^2 - 1} = 2 + \frac{2}{a^2 - 1}$  не может быть целым ни при каком натуральном  $a$ .

Предположим, что при некотором натуральном  $t$  уравнение

$$x^2 - txy + y^2 + t = 0 \quad (*)$$

имеет решения в натуральных числах  $x, y$ . Рассмотрим наименьшее натуральное  $x = a$ , для которого существует натуральное  $y = b < a$ , удовлетворяющее равенству  $(*)$ . При фиксированных  $t$  и  $b$  уравнение  $x^2 - txb + b^2 + t = 0$  — квадратное относительно  $x$ . Если оно имеет натуральный корень  $a$ , то по теореме Виета оно имеет и целый корень  $A = tb - a$ . Если  $A \leq 0$ , то

$$a^2 - tab + b^2 + t = a(a - tb) + b^2 + t > 0,$$

что неверно. Значит,  $A \geq a$ . Если  $A = a$ , то дискриминант равен нулю:

$$(tb)^2 - 4(b^2 + t) = 0,$$

откуда  $4t = (t^2 - 4)b^2 \geq t^2 - 4$ , так что  $t \leq 4$ ; но при  $t = 1, 2, 3, 4$  равенство  $4t = (t^2 - 4)b^2$  не имеет места.

Итак,  $A > a$ . По теореме Виета,  $aA = b^2 + t$  и  $a + A = tb$ . Поэтому

$$b^2 + t - tb = aA - a - A = (a - 1)(A - 1) - 1 \geq b(b + 1) - 1 = b^2 + b - 1,$$

откуда

$$t(1 - b) \geq b - 1.$$

Это возможно лишь при  $b = 1$ , причем все неравенства должны обращаться в равенства, т.е.  $a = 2, A = 3, t = 5$ .

б) Два решения найти легко:  $(x; y) = (1; 2)$  или  $(1; 3)$ . Из каждого решения  $(x; y)$ , где  $x < y$ , можно получить новое решение  $(y; 5y - x)$ . Действительно,  $(5y - x)^2 - 5(5y - x)y + y^2 = x^2 - 5xy + y^2$ . При этом  $5y - x > 4y > y$ . Таким образом, любые два соседних

члена любой из последовательностей

$$1, 2, 9, 43, 206, 987, \dots,$$

$$1, 3, 14, 67, 321, 1538, \dots,$$

где каждый член получается из двух предыдущих  $x, y$  по формуле  $5y - x$ , дают решение интересующего нас уравнения.

На самом деле мы нашли все решения в натуральных числах! Докажем это. Пусть  $0 < X < Y$  и  $X^2 - 5XY + Y^2 + 5 = 0$ . Рассмотрим преобразование  $(X; Y) \rightarrow (x; y)$ , где  $x = 5X - Y$  и  $y = X$ . Если  $x < X$ , то  $\min(x, y) < \min(X, Y)$ , так что удалось получить «меньшее» решение в натуральных числах. Если же  $5X - Y \geq X$ , то  $5 = (5X - Y)Y - X^2 \geq XY - X^2 = X(Y - X) \geq X$ . Перебрав значения  $X = 1, 2, 3, 4, 5$ , находим:  $(X; Y) = (1; 2)$  или  $(1; 3)$ .

**52.** Поскольку  $-1 < 3 - \sqrt{11} < 0$  и поскольку число  $(3 + \sqrt{11})^{2n-1} + (3 - \sqrt{11})^{2n-1}$  целое, то

$$\left[ (3 + \sqrt{11})^{2n-1} \right] = (3 + \sqrt{11})^{2n-1} + (3 - \sqrt{11})^{2n-1}.$$

Пусть

$$(3 + \sqrt{11})^{2n-1} = X_n + Y_n \sqrt{11},$$

где  $X_n, Y_n$  — натуральные числа. Тогда

$$(3 + \sqrt{11})^{2n-1} + (3 - \sqrt{11})^{2n-1} = X_n + Y_n \sqrt{11} + X_n - Y_n \sqrt{11} = 2X_n.$$

Поскольку  $(3 + \sqrt{11})^2 = 2(10 + 3\sqrt{11})$ , то

$$\frac{X_n + Y_n \sqrt{11}}{2^{n-1}} = (3 + \sqrt{11}) \cdot (10 + 3\sqrt{11})^{n-1},$$

откуда легко усмотреть, что  $X_n/2^{n-1}$  — нечетное натуральное число. Это и требовалось доказать.

**53.** Обозначим для краткости  $\alpha = \frac{\sqrt{5}+1}{2}$  и  $\beta = \frac{\sqrt{5}-1}{2}$ . Тогда  $\left(\frac{3+\sqrt{5}}{2}\right)^n + \left(\frac{3-\sqrt{5}}{2}\right)^n - 2 = \alpha^{2n} + \beta^{2n} - 2(\alpha\beta)^n = (\alpha^n - \beta^n)^2$ . Осталось доказать, что число  $a_n = \alpha^n - \beta^n$  является целым, если  $n$  четно, и в  $\sqrt{5}$  раз больше целого числа, если  $n$  нечетно. Это можно сделать по индукции, проверив равенства  $a_1 = 1$  и  $a_2 = \sqrt{5}$  и рекуррентную формулу

$$a_{n+2} = \alpha^{n+2} - \beta^{n+2} = (\alpha^{n+1} - \beta^{n+1})(\alpha + \beta) - \alpha\beta(\alpha^n - \beta^n) = a_{n+1}\sqrt{5} - a_n.$$

**54. а) Первый способ.** Пусть  $\alpha = 2 + \sqrt{3}$  и  $\beta = 3 \cdot (2 + \sqrt{3})$ . Тогда



числа  $a = (2 + \sqrt{3})^m + (2 - \sqrt{3})^m$  и  $b = 3^n (2 + \sqrt{3})^n + 3^n (2 - \sqrt{3})^n$  целые, причем  $a$  не делится на 3, а  $b$  — делится. Очевидно,  $\left[(2 + \sqrt{3})^m\right] = a - 1$  и, поскольку  $3(2 - \sqrt{3}) = \frac{3}{2 + \sqrt{3}} < 1$ , то  $\left[3^n (2 + \sqrt{3})^n\right] = b - 1$ .

*Второй способ.* Числа  $a = \left((2 + \sqrt{3})^m + (2 - \sqrt{3})^m\right)/2$  и  $b = \left((1 + \sqrt{2})^n + (1 - \sqrt{2})^n\right)/2$  — натуральные, причем для некоторых натуральных  $c$  и  $d$  имеем:  $a^2 - 3c^2 = 1$  и  $b^2 - 2d^2 = (-1)^n$ . Если  $\left[(2 + \sqrt{3})^m\right] = \left[(1 + \sqrt{2})^n\right]$ , то в случае нечетного  $n$  имеем  $2a - 1 = 2b$ , что невозможно, а в случае четного  $n$  имеем  $2a - 1 = 2b - 1$ , так что  $a = b$ , откуда  $3c^2 = 2d^2$ , что невозможно для натуральных чисел  $c$  и  $d$ .

*Третий способ.* В статье «Пентиум хорошо, а ум лучше» («Квант» №4 за 1999 г.) доказано следующее утверждение: если  $\alpha$  и  $\beta$  — положительные иррациональные числа, причем  $\frac{1}{\alpha} + \frac{1}{\beta} = 1$ , то для любых натуральных чисел  $m$  и  $n$  целые части чисел  $m\alpha$  и  $n\beta$  различны. В таком случае числа  $\left[10^{n\alpha}\right]$  и  $\left[10^{m\beta}\right]$  имеют разное количество цифр, так что достаточно доказать существование таких положительных иррациональных  $\alpha$  и  $\beta$ , что  $\frac{1}{\alpha} + \frac{1}{\beta} = 1$  и числа  $10^\alpha$  и  $10^\beta$  иррациональны. Это легко сделать, воспользовавшись несчетностью континуума.

*Четвертый способ* естественен для студента, изучившего теорему о стягивающихся отрезках и счетность множества рациональных чисел. Зафиксируем любое нецелое  $\alpha > 4$  и покажем, что для него существует иррациональное  $\beta$ , удовлетворяющее условиям. Для этого обозначим  $a_1 = [\alpha] + 1,01$  и  $b_1 = [\alpha] + 1,99$ . Тогда

$$b_1 > a_1 > 5$$

и

$$b_1^2 - a_1^2 = (b_1 + a_1)(b_1 - a_1) > 5.$$

Перенумеруем все рациональные числа отрезка  $[a_1; b_1]$ , т.е. выпишем все их в виде последовательности  $c_1, c_2, c_3, \dots$ . Построим такую последовательность отрезков  $[a_k; b_k]$ , что

- отрезок  $[a_{k+1}; b_{k+1}]$  лежит в отрезке  $[a_k; b_k]$ ;
- $c_k \notin [a_{k+1}; b_{k+1}]$ ;
- $b_k^{k+1} - a_k^{k+1} > 5$ ;

• для любого числа  $\beta \in [a_k; b_k]$  целая часть ни одного из чисел  $\beta^n$ , где  $n \leq k$ , не равна целой части ни одного из чисел  $\alpha^m$  ни при каком натуральном  $m$ .

Поскольку  $4^2 - 4 = 12$ , то целые части степеней числа  $\alpha$  различаются не менее чем на 11. Пусть отрезок  $[a_k; b_k]$  построен. Поскольку длина отрезка  $[a_k^{k+1}; b_k^{k+1}]$  больше 5, то в нем содержатся хотя бы четыре отрезка с концами в соседних натуральных числах. Хотя бы в одном из них нет (нецелого!) числа  $c_k^{k+1}$  и нет ни одной степени числа  $\alpha$ ; пусть это отрезок  $[n; n+1]$ . Положим  $a_{k+1} = \sqrt[k+1]{n}$  и  $b_{k+1} = \sqrt[k+1]{n+1}$ . Тогда

$$b_{k+1}^{k+2} - a_{k+1}^{k+2} = b_{k+1}(n+1) - a_{k+1}n > a_{k+1}(n+1) - a_{k+1}n = a_{k+1} > 5.$$

Построение закончено. Очевидно, общая точка  $\beta$  всех построенных отрезков удовлетворяет условиям.

б) *Первый способ*. Если разрешить себе воспользоваться теоремой 10, то достаточно для каждого простого числа  $p$  рассмотреть такие натуральные числа  $a$  и  $b$ , что  $a^2 - pb^2 = 1$ , и положить  $\alpha = a + b\sqrt{p}$ .

*Второй способ* обходится без использования теоремы 10. А именно, для любого натурального числа  $k > 1$  рассмотрим  $\alpha_k = k + \sqrt{k^2 - 1}$ . Докажем существование такого бесконечного множества натуральных чисел  $k_n$ , что  $k_n > 1$  и  $(k_r^2 - 1)/(k_s^2 - 1)$  не является квадратом рационального числа ни для каких двух различных натуральных  $r$  и  $s$ . (Тогда натуральные числа

$$x = ([\alpha_k^m] + 1)/2 = \left( (k + \sqrt{k^2 - 1})^m + (k - \sqrt{k^2 - 1})^m \right) / 2$$

и

$$y = \left( (k + \sqrt{k^2 - 1})^m - (k - \sqrt{k^2 - 1})^m \right) / (2\sqrt{k^2 - 1})$$

удовлетворяют уравнению  $x^2 - (k^2 - 1)y^2 = 1$ . Поэтому аналогично второму способу решения пункта а) можно убедиться, что числа  $\alpha_{k_n}$  удовлетворяют требованию задачи.) Пусть  $k_1 = 2$  и  $k_{n+1} = (k_n^2 - 1)!$ , где  $n$  — натуральное число. Тогда  $k_{n+1}$  делится на каждое из чисел  $k_r^2 - 1$ , где  $r = 1, 2, \dots, n$ . Значит, числа  $k_{n+1}^2 - 1$  и  $k_r^2 - 1$  взаимно просты, откуда и следует нужное нам утверждение.

*Третий способ*. Достаточно построить такую последовательность положительных иррациональных чисел  $\alpha_1, \alpha_2, \alpha_3, \dots$  и такую последовательность простых чисел  $p_1, p_2, p_3, \dots$ , что для любых натуральных  $m$  и  $n$  число  $[\alpha_m^n] + 1$  делится на  $p_m$  и не делится на  $p_k$  ни при каком  $k < m$ .

**Лемма.** Для любого натурального числа  $a$  уравнение  $ax + 1 = y^2$  имеет бесконечно много решений в натуральных числах.

**Доказательство.** Для любого натурального  $r$  положим  $y = ar + 1$  и  $x = ar^2 + 2r$ .

Лемма доказана. Начнем построение. Положим  $p_1 = 3$  и  $\alpha_1 = 3(2 + \sqrt{3})$ . Тогда при любом натуральном  $n$  число  $[\alpha_1^n] + 1 = 3^n(2 + \sqrt{3})^n + 3^n(2 - \sqrt{3})^n$  целое и даже кратное  $p_1 = 3$ .

Предположим, что числа  $\alpha_1, \dots, \alpha_n$  и  $p_1, \dots, p_n$  уже найдены. Рассмотрим произведение  $a = p_1 p_2 \dots p_n$ . Выберем простое число  $p_{n+1} > a$  и натуральные числа  $x$  и  $y$ , для которых  $y^2 = ax + 1$  и  $y > p_{n+1}$ . Пусть  $\alpha_{n+1} = p_{n+1}(y + \sqrt{ax})$ . Тогда

$$[\alpha_{n+1}^m] + 1 = p_{n+1}^m (y + \sqrt{ax})^m + p_{n+1}^m (y - \sqrt{ax})^m$$

делится на  $p_{n+1}$  и не делится ни на одно из чисел  $p_1, \dots, p_n$ .

**55.** Примените утверждение теоремы 12 к положительному из чисел  $x + y\sqrt{d}$  и  $-(x + y\sqrt{d})$ .

**56.**  $q = 10 + 3\sqrt{11}$ . Как легко посчитать,

$$\frac{10 + 3\sqrt{11} + 17}{2\sqrt{11}} < 5.$$

Поэтому достаточно проверить значения  $y = 1, 2, 3, 4$ .

**57. а)** Обозначив среднее из 11 последовательных чисел буквой  $y$ , получаем уравнение

$$(y - 5)^2 + (y - 4)^2 + (y - 3)^2 + \dots + (y + 4)^2 + (y + 5)^2 = 11x^2,$$

т.е.

$$11x^2 + 110 = 11y^2.$$

Сократив на 11, получаем уравнение

$$x^2 - 11y^2 = -10.$$

Его решения таковы:

$$x + y\sqrt{11} = a(10 + 3\sqrt{11})^n,$$

где  $a \in \{1 + \sqrt{11}; 23 + 7\sqrt{11}\}$ ,  $n$  — целое число.

**б)** Аналогично пункту а), получаем уравнение  $x^2 - 23y^3 = -11$ . Его решения таковы:

$$x + y\sqrt{23} = a(24 + 5\sqrt{23})^n,$$

где  $a \in \{9 + 2\sqrt{23}; 14 + 3\sqrt{23}\}$ ,  $n$  — целое число.

**58.** Поскольку квадрат натурального числа может оканчиваться лишь на одну из цифр 0, 1, 4, 5, 6, 9, нужно решить в натуральных числах уравнения  $x^2 - 10y^2 = 0$ , 1, 4, 5, 6 или 9. Два из них – а именно, уравнение  $x^2 - 10y^2 = 0$  и уравнение  $x^2 - 10y^2 = 5$  – решений в натуральных числах не имеют. А остальные – имеют:  $x + y\sqrt{10} = a(19 - 6\sqrt{10})^n$ , где  $n$  – целое неотрицательное число,  $a = 1, 2, 4 + \sqrt{10}, 16 + 5\sqrt{10}, 3, 7 + 2\sqrt{10}$  или  $13 + 4\sqrt{10}$ .

**59.** а)  $x + y\sqrt{17} = \pm a(4 + \sqrt{17})^{2m}$ , где  $a \in \{-1 + \sqrt{17}; 1 + \sqrt{17}; 16 + 4\sqrt{17}\}$ , а  $m$  – целое число.

**61.** а) Пусть  $a$  четно. Тогда  $b$  нечетно. Поскольку квадрат нечетного числа при делении на 4 дает остаток 1, а квадрат четного – остаток 0, то  $pb^2 \equiv 1 \pmod{4}$  и  $a^2 - 1 \equiv 3 \pmod{4}$ . Получили желанное противоречие.

б) Воспользуемся разложением  $pb^2 = (a-1)(a+1)$ , основной теоремой арифметики и тем, что  $\text{НОД}(a-1; a+1) = \text{НОД}(a-1; 2) = 2$ .

в) Воспользуемся равенством

$$(u^2 - pv^2)^2 = (u^2 + pv^2)^2 - p(2uv)^2 = a^2 - pb^2 = 1$$

и тем, что  $v < b$ .

**62.** При  $n \rightarrow \infty$  имеем:

$$x = \frac{1}{2} \left( (z + t\sqrt{d})q^n + \frac{z - t\sqrt{d}}{q^n} \right) \rightarrow +\infty,$$

$$y = \frac{1}{2\sqrt{d}} \left( (z + t\sqrt{d})q^n - \frac{z - t\sqrt{d}}{q^n} \right) \rightarrow +\infty.$$

**63.**  $q = (a - \sqrt{a^2 + 1})^2 = 2a^2 + 1 - 2a\sqrt{a^2 + 1}$ . Множеству  $M$  принадлежат числа  $-1 + \sqrt{a^2 + 1}$ ,  $1 + \sqrt{a^2 + 1}$  и  $a^2 + a\sqrt{a^2 + 1}$ .

**64.** а)  $(s; r) = (1; 1)$  или  $(2; 3)$ . Если  $s$  нечетно и  $r > 1$ , то  $3^s \equiv 3 \not\equiv 1 \equiv 2^r + 1 \pmod{4}$ . Если же  $s = 2k$  четно, то  $2^r = (3^k - 1)(3^k + 1)$ , откуда  $3^k - 1 = 2^a$  и  $3^k + 1 = 2^b$  для некоторых целых неотрицательных  $a$  и  $b$ , так что  $2^b - 2^a = 2$ , откуда  $b = 2, a = 1, k = 1, s = 2$  и, наконец,  $r = 3$ .

б)  $(x; y; z) = (1; 1; 1), (1; 3; 2), (5; 2; 3)$  или  $(7; 5; 4)$ . Пусть  $y > 1$ . Поскольку  $x$  нечетно, то  $x \equiv 1 \pmod{4}$ . Следовательно,  $z$  четно, т.е.  $z = 2s$ . Значит,

$$2^y = (3^s)^2 - x^2 = (3^s - x)(3^s + x),$$

так что

$$\begin{cases} 3^s - x = 2^a, \\ 3^s + x = 2^b, \end{cases}$$

где  $a, b$  – целые неотрицательные числа. Сложив уравнения и поделив на 2, находим

$$3^s = 2^{a-1} + 2^{b-1}.$$

Поскольку число  $3^s$  нечетно, то  $a = 1$ . Значит,  $x = 3^s - 2$ . Подставив найденное выражение во второе уравнение системы, получаем

$$3^s = 2^{b-1} + 1.$$

В силу пункта а), имеем  $(s; b) = (1; 2)$  или  $(2; 4)$ . Этим двум случаям соответствуют ответы  $(x; y; z) = (1; 3; 2)$  и  $(7; 5; 4)$ .

Пусть теперь  $y = 1$ . Если  $z$  четно, то  $2 = (3^{z/2})^2 - x^2$ , что невозможно, так как число 2 нельзя представить в виде разности квадратов целых чисел. Значит,  $z$  нечетно:  $z = 2s + 1$ . Обозначим  $t = 3^s$ . Тогда  $x^2 - 3t^2 = -2$ . Значит,  $x + t\sqrt{3} = (1 + \sqrt{3})(2 + \sqrt{3})^n$  для некоторого целого неотрицательного числа  $n$ . Поскольку  $2 \pm \sqrt{3} = \frac{1}{2}(1 \pm \sqrt{3})^2$ , то

$$\begin{aligned} 3^s = t &= \frac{(x + t\sqrt{3}) - (x - t\sqrt{3})}{2\sqrt{3}} = \frac{(1 + \sqrt{3})(2 + \sqrt{3})^n - (1 - \sqrt{3})(2 - \sqrt{3})^n}{2\sqrt{3}} = \\ &= \frac{(1 + \sqrt{3})^{2n+1} - (1 - \sqrt{3})^{2n+1}}{2^{n+1}\sqrt{3}}. \end{aligned}$$

Докажем, что  $2n + 1$  – степень тройки. Если  $q$  – простой делитель числа  $2n + 1$ , отличный от 3, то

$$(1 + \sqrt{3})^{2n+1} - (1 - \sqrt{3})^{2n+1} = C \left( (1 + \sqrt{3})^q - (1 - \sqrt{3})^q \right),$$

где  $C$  – натуральное число. Но  $(1 + \sqrt{3})^q - (1 - \sqrt{3})^q = 2m\sqrt{3}$ , где  $m$  – целое число, не делящееся на 3. Нетрудно проверить, что  $m$  – не степень двойки. (В противном случае также и некоторое  $T$ , являющееся решением уравнения  $V^2 - 3T^2 = -2$ , было бы степенью двойки, а это невозможно.) Мы пришли к противоречию: число  $t = 3^s$  не имеет простого делителя, отличного от 3.

Итак,  $2n + 1$  – степень тройки. Если  $2n + 1$  делится на 9, то из равенства  $(1 \pm \sqrt{3})^9 = 16(27 \pm 153\sqrt{3})$  следует, что  $z = 3^s$  делится на 17. Значит,  $2n + 1 = 3$ , откуда  $n = 1$ ,  $x = 5$  и  $z = 3$ .

**65. а)** Выполнив замену  $x = X - 4y$ , получаем уравнение

$$X^2 + 2X - 15y^2 - 12y + 1 = 0,$$

которое можно записать в виде

$$(X + 1)^2 - 3(5y^2 - 4y) = 0.$$

Обозначив  $u = X + 1$  и домножив обе части уравнения на 5, получаем

$$5u^2 - 3(25y^2 - 20y) = 0,$$

откуда

$$5u^2 - 3(5y - 2)^2 = -12.$$

Домножив обе части на 5 и обозначив  $v = 5u$  и  $w = 5y - 2$ , получаем уравнение

$$v^2 - 15w^2 = -60.$$

Поскольку  $q = 4 + \sqrt{15}$  и

$$\frac{4 + \sqrt{15} + 60}{2\sqrt{15}} < 9,$$

то для нахождения множества  $M$  достаточно проверить значения  $w = 1, 2, \dots, 8$ . Подходит только  $w = 8$ , которому соответствует значение  $v = 30$ . Значит,

$$v + w\sqrt{15} = \pm(30 + 8\sqrt{15})(4 + \sqrt{15})^n,$$

где  $n \in \mathbb{Z}$ . Поскольку нас интересуют только те пары  $(v; w)$ , для которых  $v \equiv 0$  и  $w \equiv 3 \pmod{5}$ , то, как легко проверить, подходит лишь

$$v + w\sqrt{15} = (30 + 8\sqrt{15})(-4 - \sqrt{15})^n.$$

Теперь легко выписать ответ:

$$y = \frac{w + 2}{5} = \frac{(15 + 4\sqrt{15})(-4 - \sqrt{15})^n - (15 - 4\sqrt{15})(-4 + \sqrt{15})^n + 2\sqrt{15}}{5\sqrt{15}},$$

$$x = u - 4y - 1 = (15 + 4\sqrt{15})(-4 - \sqrt{15})^n + (15 - 4\sqrt{15})(-4 + \sqrt{15})^n - 4y - 1.$$

**67.** Взяв  $r = 9$ , имеем  $221^2 - 67 \cdot 27^2 = -2$ ; далее опять  $r = 9$  и  $1899^2 - 67 \cdot 232^2 = -7$ ; потом  $r = 5$  и  $3577^2 - 67 \cdot 437^2 = 6$ ; на предпоследнем шаге  $r = 7$  приводит к равенству  $9053^2 - 67 \cdot 1106^2 = -3$ ; наконец,  $r = 8$  дает ответ.

Оригинальное индийское решение этой задачи использует прием, сокращающий вычисления. Обе части равенства  $221^2 - 67 \cdot 27^2 = -2$  возводят в квадрат, получая  $(221^2 + 67 \cdot 27^2)^2 - 67(2 \cdot 27 \cdot 221)^2 = (-2)^2$ , после сокращения которого на 4 получаем искомый ответ.

**74.** Если  $2x < 3y$ , то  $y^2 - y = x(3y - x - 1) > x\left(\frac{3}{2}y - 1\right)$ , откуда

$$x < \frac{y^2 - y}{\frac{3}{2}y - 1} < y.$$

75. а) Обозначим  $\varphi_n = a$  и  $\varphi_{n+1} = b$ . Тогда  $\varphi_{n+3} + \varphi_{n+5} = 2\varphi_{n+3} + \varphi_{n+4} = \varphi_{n+2} + 3\varphi_{n+3} = 3\varphi_{n+1} + 4\varphi_{n+2} = 4a + 7b$  и  $\varphi_{n-1} + \varphi_{n+1} = 2b - a = 4a + 7b - 5(a + b)$ .

в) Обозначим для краткости  $\varphi_m = a$  и  $\varphi_{m+1} = b$ . Тогда

$$\begin{aligned}\varphi_{2m} + \varphi_{2m+2} - 5\varphi_m\varphi_{m+1} &= \varphi_{m+1}^2 - \varphi_{m-1}^2 + \varphi_{m+2}^2 - \varphi_m^2 - 5\varphi_m\varphi_{m+1} = \\ &= b^2 - (b-a)^2 + (a+b)^2 - a^2 - 5ab = b^2 - ab - a^2 = (-1)^m.\end{aligned}$$

76. б) Допустим, что данное уравнение имеет решение  $(x; y)$ , тогда

$$4x^n = (y - x - 1)(y + x + 1).$$

Сомножители в правой части имеют одинаковую четность и, следовательно, четны. Пусть  $y - x - 1 = 2a$ , тогда  $y + x + 1 = 2(a + x + 1)$ , т.е.  $x^n = a(a + x + 1)$ . Поскольку любой общий делитель чисел  $a$  и  $a + x + 1$  должен одновременно делить  $x^n$  и  $x + 1$ , то числа  $a$  и  $a + x + 1$  взаимно просты и потому существуют такие натуральные числа  $u$  и  $v$ , что  $a = u^n$ ,  $a + x + 1 = v^n$ ,  $x = uv$ . Но тогда при  $n \geq 3$  имеем

$$uv + 1 = x + 1 = v^n - u^n = (v - u)(v^{n-1} + v^{n-2}u + \dots + u^{n-1}) \geq v^2 + vu + u^2.$$

Полученное противоречие показывает, что исходное уравнение не имеет решений в натуральных числах.

### Избранные задачи

1. Если при некотором натуральном  $m$  число  $1978^m - 1$  делится на  $1000^m - 1$ , то на  $1000^m - 1$  делится и разность

$$(1978^m - 1) - (1000^m - 1) = 1978^m - 1000^m = 2^m(889^m - 500^m).$$

Поскольку число  $1000^m - 1$  нечетное, то оно взаимно просто с числом  $2^m$  и поэтому на  $1000^m - 1$  должна делиться разность  $989^m - 500^m$ . Однако

$$989^m - 500^m < 1000^m - 1.$$

2. а) Пусть мудрец, который говорит первым, скажет «черный», если видит нечетное число черных колпаков, и «белый» в противном случае. Поскольку другие мудрецы знают, какого цвета его колпак, они по тому, казнит его король или нет, вычисляют, четное или нечетное число черных колпаков надето на всех мудрецах на самом деле. Этой информации – вместе с тем, что каждый из них видит всех, кроме себя самого, – достаточно для того, чтобы все мудрецы, кроме (быть может) первого, избежали казни.

б) Решение по сути такое же, как в предыдущем пункте, только вместо четности первому говорящему можно порекомендовать рас-

смотреть остаток от деления суммы количества синих колпаков и удвоенного количества красных колпаков на 3.

**3.** Занумеруем цвета числами от 1 до  $n$ . Обозначим через  $s$  остаток от деления на  $n$  суммы номеров цветов на головах мудрецов (номер каждого цвета учитываем столько раз, на скольких мудрецах колпак такого цвета). Если известна величина  $s$  и цвета всех колпаков, кроме одного, то цвет этого колпака устанавливается однозначно. Поэтому мудрецы могут договориться, что один из них исходит из гипотезы, что  $s = 0$ , другой считает, что  $s = 1$ , еще один — что  $s = 2$ , и так далее вплоть до  $s = n - 1$ . При таком способе один и только один мудрец (тот, чье предположение о величине  $s$  истинно) угадает цвет своего колпака.

4. а) Если  $11^m > 5^n$ , то  $|11^m - 5^n|$  оканчивается цифрой 6, иначе — цифрой 4. Очевидно,  $|11^2 - 5^3| = 4$ .

б) Если  $36^m > 5^n$ , то  $|36^m - 5^n|$  оканчивается на 1, иначе — на 9. Если  $36^m - 5^n = 1$ , то  $5^n = 36^m - 1 = (6^m - 1)(6^m + 1)$ . Число  $6^m + 1$  оканчивается на 7 и поэтому не является степенью числа 5. Равенство  $5^n - 36^m = 9$  невозможно, поскольку 5 не делится на 9. Осталось заметить, что  $36^1 - 5^2 = 11$ .

в) Числа 53 и 37 сравнимы с 1 по модулю 4, поэтому  $53^m - 37^n$  делится на 4. Числа 53 и 37 сравнимы по модулю 9 с  $-1$  и 1 соответственно. Поэтому  $53^m - 37^n$  сравнимо с 0 или  $-2$  по модулю 9. Следовательно,  $|53^m - 37^n|$  при делении на 9 дает остаток 0, 2 или 7. Числа 4, 8 и 12 таких остатков не дают, а  $|53^1 - 37^1| = 16$ .

**5.** Докажем сначала две леммы.

**Лемма 1.** *Исследуемая последовательность содержит бесконечно много четных чисел.*

**Доказательство.** Предположим, что все члены исследуемой последовательности  $a_1, a_2, a_3, \dots$ , начиная с некоторого, нечетны. Поскольку все члены последовательности различны, то найдется такое  $n$ , что  $a_{n+1}$  нечетно и при этом больше как всех  $n$  предыдущих членов последовательности, так и всех четных ее членов.

Обозначим буквой  $p$  наименьший простой делитель числа  $a_n$ . Тогда  $a_{n+1} \geq a_n + p$ . Более того, поскольку сумма  $a_n + p$  четна, то  $a_{n+1} \geq a_n + 2p > a_n + p$ , что противоречит определению числа  $a_{n+1}$  как наименьшего натурального числа, отличного от  $a_n, a_2, \dots, a_n$  и не взаимно простого с  $a_n$ .

**Лемма 2.** *Пусть  $p$  — простое число. Если последовательность содержит бесконечно много чисел, кратных  $p$ , то она содержит все кратные числа  $p$ .*

**Доказательство.** Пусть число  $pk$  не принадлежит последовательности. Почти все (т.е. все, начиная с некоторого номера  $m$ )



члены последовательности больше  $pk$ . Рассмотрим такое  $n > m$ , что  $a_n$  делится на  $p$ . Число  $pk$  претендует на роль  $a_{n+1}$ . Противоречие.

Теперь – собственно решение задачи. По лемме 1, последовательность содержит бесконечно много четных чисел. Следовательно, по лемме 2 она содержит все четные числа и, значит, для любого простого  $p$  последовательность содержит бесконечно много чисел, кратных  $p$ , а поэтому в силу леммы 2 она содержит все числа, кратные  $p$ .

*Замечание.* Вычисления подсказывают гипотезу: если  $a_n$  – простое число, то  $a_n \approx n/2$ ; если  $a_n$  – утроенное простое число, то  $a_n \approx 3n/2$ ; в остальных случаях  $a_n \approx n$ . Доказаны, однако, лишь

неравенства

$$\frac{1}{14} < \frac{a_n}{n} < 260.$$

**6.** Пожалуй, самое неожиданное в этой задаче – форма записи решения. Как только вы поймете, что на самом деле эта задача скорее арифметическая, а не геометрическая, решение уложится «в одну строчку». Но не так уж легко догадаться, что фраза «поместим центры 2-ежей в целочисленные точки  $(x; y; z)$ , для которых  $x + 3y + 4z$  делится на 13», дает решение пункта в).

Начнем с простой задачи: покроем плоскость «крестами» из пяти квадратиков  $1 \times 1$ . Это сделать легко (рис.1). Покажем, как это решение можно было бы объяснить слепому (или компьютеру).

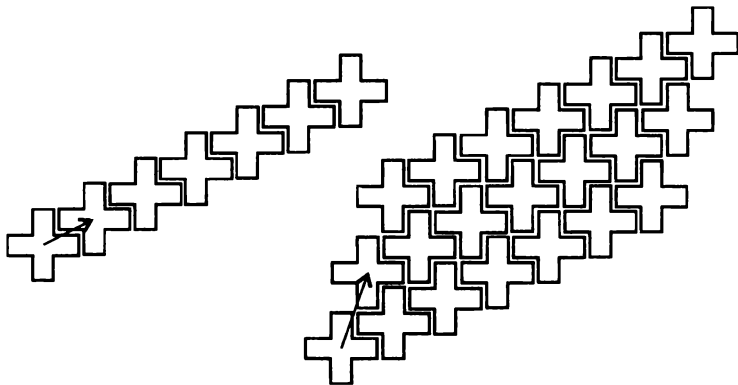


Рис. 1

В системе координат  $Oxy$ , оси которой параллельны сторонам квадратиков, а начало расположено в центре одного из крестов,

укажем множество  $M$  центров всех других крестов: оно состоит из точек  $(x; y)$ , где  $x, y$  – целые числа, а  $x + 2y$  делится на 5, т.е.  $x + 2y \equiv 0 \pmod{5}$ . Каждый крест с центром  $(x, y)$  содержит пять клеток – с центрами  $(x; y)$ ,  $(x \pm 1; y)$ ,  $(x; y \pm 1)$ .

Доказать, что кресты с центрами в  $M$  покрывают в один слой всю плоскость, можно и без рисунка: в следующей таблице указано, к какому кресту относится клетка с центром  $(x; y)$  при  $x + 2y \equiv r \pmod{5}$ , где  $r = 1, 2, 3$  или  $4$ . А именно, чтобы попасть в центр соответствующего креста, надо

при $r =$	1	2	3	4
из координаты	$x$	$y$	$y$	$x$
вычесть	1	1	-1	-1

Легко убедиться, что после этой операции из любой пары  $(x, y)$  получится точка множества  $M$ : например, если  $x + 2y \equiv 2 \pmod{5}$ , то

$$x + 2(y - 1) = x + 2y - 2 \equiv 2 - 2 \equiv 0 \pmod{5},$$

а если  $x + 2y \equiv 3$ , то

$$x + 2(y + 1) = x + 2y + 2 \equiv 3 + 2 \equiv 0 \pmod{5}.$$

Число 5 в решении появилось не случайно; это – число клеток в одном кресте. Оказывается, таким же способом можно описать и нужные нам пространственные примеры: пространство, разбитое на единичные кубики с центрами в целочисленных точках  $(x; y; z)$ , удастся заполнить параллельными переносами фигуры из  $m$  кубиков в точки некоторой решетки, задаваемой условием вида

$$F(x, y, z) = x + ay + bz \equiv 0 \pmod{m},$$

а для каждого кубика с центром  $(x; y; z)$ , где  $x + ay + bz \equiv r \pmod{m}$  и  $1 \leq r < m$ , можно указать, к какому именно сдвигу центрального кубика он относится.

Проверьте следующие конструкции.

а) Кнопка:  $m = 6$ , центральный кубик  $(x, y, z)$  и еще пять:  $(x \pm 1; y; z)$ ,  $(x; y \pm 1; z)$ ,  $(x; y; z + 1)$ ;  $F(x, y, z) = x + 2y + 3z$ ;

$r$	1	2	3	4	5
	$x$	$y$	$z$	$y$	$x$
	1	1	1	-1	-1

б) Ёж:  $m = 7$ , центральный кубик  $(x, y, z)$  и еще шесть:  $(x \pm 1; y; z)$ ,  $(x; y \pm 1; z)$ ,  $(x; y; z \pm 1)$ ;  $F(x, y, z) = x + 2y + 3z$ ;

$r$	1	2	3	4	5	6
	$x$	$y$	$z$	$z$	$y$	$x$
	1	1	1	-1	-1	-1

в) 2-ёж:  $m = 13$ , центральный кубик  $(x, y, z)$  и еще двенадцать:  $(x \pm d; y; z)$ ,  $(x; y \pm d; z)$  и  $(x; y; z \pm d)$ , где  $d = 1$  или  $2$ ;  $F(x, y, z) = x + 3y + 4z$ ;

$r$	1	2	3	4	5	6	7	8	9	10	11	12
	$x$	$x$	$y$	$z$	$z$	$y$	$y$	$z$	$z$	$y$	$x$	$x$
	1	2	1	1	-2	2	-2	2	-1	-1	-2	-1

Можно придумать и другие заполнения пространства. Например, на рисунках 2–6 показаны фигурки (знак «+» означает, что еще нужно положить кубик сверху, а знак «-» требует еще кубика снизу; для ясности на первых двух рисунках показаны вид спереди –

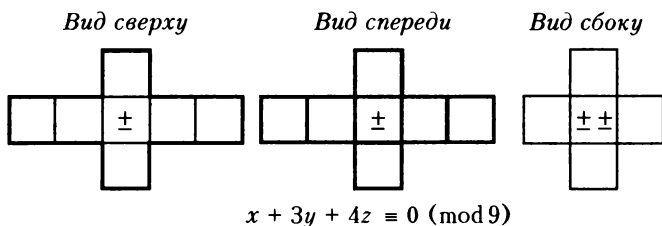


Рис. 2

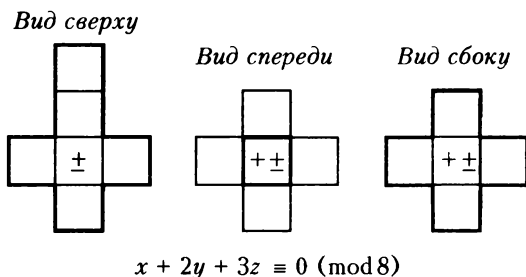


Рис. 3

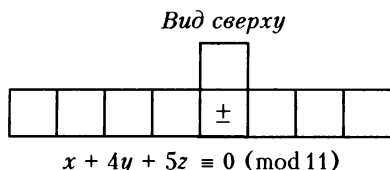


Рис. 4

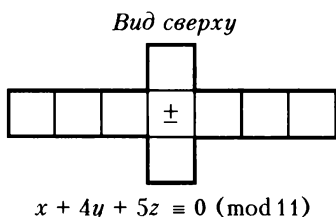


Рис. 5

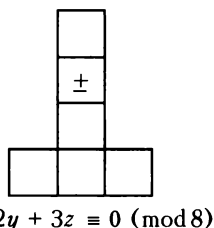


Рис. 6

проекция вдоль оси ординат, и сбоку – проекция вдоль оси абсцисс), для покрытия которыми пространства тоже достаточно рассмотреть сравнения.

Интересно было бы узнать, на какие еще фигурки из кубиков пространство можно разбить, а на какие нельзя. Например, 3-ёж (состоящий из 19 кубиков) кажется очень колючим. Но как доказать, что на 3-ежи пространство не разбить? Даже на плоскости заполнения и упаковки различными фигурками из клеточек дают богатую пищу для размышлений. Особенно трудны доказательства невозможности замощения (или оценка доли клеток, которые остаются непокрытыми).

В заключение я хочу признаться, что задача возникла при чтении замечательного сборника В.В.Прасолова и И.Ф.Шарыгина «Задачи по стереометрии». В первом параграфе, который называется «Знакомство со стереометрией» и должен воспитать пространственное воображение читателя, есть задача (№12) – разбить пространство на 1-ежи. Решение лаконично (рис.7):

«Можно. Разобьем пространство на слои толщиной 1, а слои разобьем на единичные кубики. В нечетных слоях поместим центры крестов в клетках, отмеченных цифрой 1, а в четных слоях – в клетках, отмеченных цифрой 2.»

		2			1		
	1			2			1
2			1			2	
		2			1		
	1			2			1
2			1			2	
		2			1		
	1			2			1

Рис. 7

Однако эта конструкция не дает разбиения на ежи; она разбивает пространство на кнопки! (В четных слоях поместите, остриями вверх, центры кнопок в клетки, помеченные цифрой 2, а в нечетных – остриями вниз в клетки, помеченные цифрой 1). Эта оплошность не случайна. Геометрия иногда для *наглядного* изображения должна использовать формулы.

***Александр Васильевич Спивак***

## **Арифметика-2**

Библиотечка «Квант». Выпуск 109

Приложение к журналу «Квант» №5/2008

Редактор *А.Ю.Котова*

Обложка *А.Е.Пацхверия*

Макет и компьютерная верстка *Е.В.Морозова*

Компьютерная группа *Е.А.Митченко, Л.В.Калиничева*

ИБ № 95

Формат 84×108 1/32. Бум. офсетная. Гарнитура кудряшевская

Печать офсетная. Объем 5 печ.л. Тираж 3000 экз.

Заказ № 4360.

119296 Москва, Ленинский пр., 64-А, «Квант»

Тел.: (495)930-56-48, e-mail: [admin@kvant.info](mailto:admin@kvant.info)

Отпечатано в ОАО Ордена Трудового Красного Знамени

«Чеховский полиграфический комбинат»

142300 г.Чехов Московской области.

Сайт: [www.chpk.ru](http://www.chpk.ru). E-mail: [marketing@chpk.ru](mailto:marketing@chpk.ru)

Факс: 8(49672)6-25-36, факс: 8(499)270-73-00

Отдел продаж услуг многоканальный: 8(499) 270-73-59

**ВЫШЛИ ИЗ ПЕЧАТИ книги  
СЕРИИ «БИБЛИОТЕЧКА «КВАНТ»**

1. *М.П.Бронштейн*. Атомы и электроны
2. *М.Фарадей*. История свечи
3. *О.Оре*. Приглашение в теорию чисел
4. Опыты в домашней лаборатории
5. *И.Ш.Слободецкий, Л.Г.Асламазов*. Задачи по физике
6. *Л.П.Мочалов*. Головоломки
7. *П.С.Александров*. Введение в теорию групп
8. *В.Г.Штейнгауз*. Математический калейдоскоп
9. Замечательные ученые
10. *В.М.Глушков, В.Я.Валах*. Что такое ОГАС?
11. *Г.И.Копылов*. Всего лишь кинематика
12. *Я.А.Сморodinский*. Температура
13. *А.Е.Карпов, Е.Я.Гук*. Шахматный калейдоскоп
14. *С.Г.Гиндикин*. Рассказы о физиках и математиках
15. *А.А.Боровой*. Как регистрируют частицы
16. *М.И.Каганов, В.М.Цукерник*. Природа магнетизма
17. *И.Ф.Шарыгин*. Задачи по геометрии: планиметрия
18. *Л.В.Тарасов, А.Н.Тарасова*. Беседы о преломлении света
19. *А.Л.Эфрос*. Физика и геометрия беспорядка
20. *С.А.Пикин, Л.М.Блинов*. Жидкие кристаллы
21. *В.Г.Болтянский, В.А.Ефремович*. Наглядная топология
22. *М.И.Башмаков, Б.М.Беккер, В.М.Гольховой*. Задачи по математике: алгебра и анализ
23. *А.Н.Колмогоров, И.Г.Журбенко, А.В.Прохоров*. Введение в теорию вероятностей
24. *Е.Я.Гук*. Шахматы и математика
25. *М.Д.Франк-Каменецкий*. Самая главная молекула
26. *В.С.Эдельман*. Вблизи абсолютного нуля
27. *С.Р.Филонович*. Самая большая скорость
28. *Б.С.Бокштейн*. Атомы блуждают по кристаллу
29. *А.В.Бялко*. Наша планета – Земля
30. *М.Н.Аршинов, Л.Е.Садовский*. Коды и математика
31. *И.Ф.Шарыгин*. Задачи по геометрии: стереометрия
32. *В.А.Займовский, Т.Л.Колупаева*. Необычные свойства обычных металлов
33. *М.Е.Левинштейн, Г.С.Симин*. Знакомство с полупроводниками
34. *В.Н.Дубровский, Я.А.Сморodinский, Е.Л.Сурков*. Релятивистский мир
35. *А.А.Михайлов*. Земля и ее вращение
36. *А.П.Пурмаль, Е.М.Слободецкая, С.О.Травин*. Как превращаются вещества

37. Г.С.Воронов. Штурм термоядерной крепости
38. А.Д.Чернин. Звезды и физика
39. В.Б.Брагинский, А.Г.Полнарев. Удивительная гравитация
40. С.С.Хилькевич. Физика вокруг нас
41. Г.А.Звенигородский. Первые уроки программирования
42. Л.В.Тарасов. Лазеры: действительность и надежды
43. О.Ф.Кабардин, В.А.Орлов. Международные физические олимпиады школьников
44. Л.Е.Садовский, А.Л.Садовский. Математика и спорт
45. Л.Б.Окунь.  $\alpha$ ,  $\beta$ ,  $\gamma$  ... Z: элементарное введение в физику элементарных частиц
46. Я.Е.Гегузин. Пузыри
47. Л.С.Марочник. Свидание с кометой
48. А.Т.Филиппов. Многоликий солитон
49. К.Ю.Богданов. Физик в гостях у биолога
50. Занимательно о физике и математике
51. Х.Рачлис. Физика в ванне
52. В.М.Липунов. В мире двойных звезд
53. И.К.Кикоин. Рассказы о физике и физиках
54. Л.С.Понтрягин. Обобщения чисел
55. И.Д.Данилов. Секреты программируемого микрокалькулятора
56. В.М.Тихомиров. Рассказы о максимумах и минимумах
57. А.А.Силин. Трение и мы
58. Л.А.Ашкинази. Вакуум для науки и техники
59. А.Д.Чернин. Физика времени
60. Задачи московских физических олимпиад
61. М.Б.Балк, В.Г.Болтянский. Геометрия масс
62. Р.Фейнман. Характер физических законов
63. Л.Г.Асламазов, А.А.Варламов. Удивительная физика
64. А.Н.Колмогоров. Математика – наука и профессия
65. М.Е.Левинштейн, Г.С.Симин. Барьеры: от кристалла до интегральной схемы
66. Р.Фейнман. КЭД – странная теория света и вещества
67. Я.Б.Зельдович, М.Ю.Хлопов. Драма идей в познании природы
68. И.Д.Новиков. Как взорвалась Вселенная
69. М.Б.Беркинблит, Е.Г.Глаголева. Электричество в живых организмах
70. А.Л.Стасенко. Физика полета
71. А.С.Штейнберг. Репортаж из мира сплавов
72. В.Р.Полищук. Как исследуют вещества
73. Л.Кэрролл. Логическая игра
74. А.Ю.Гросберг, А.Р.Хохлов. Физика в мире полимеров
75. А.Б.Мигдал. Квантовая физика для больших и маленьких
76. В.С.Гетман. Внуки Солнца
77. Г.А.Гальперин, А.Н.Земляков. Математические бильярды



78. *В.Е.Белонучкин*. Кеплер, Ньютон и все-все-все...
79. *С.Р.Филонович*. Судьба классического закона
80. *М.П.Бронштейн*. Солнечное вещество
81. *А.И.Буздин, А.Р.Зильберман, С.С.Кротов*. Раз задача, два задача...
82. *Я.И.Перельман*. Знаете ли вы физику?
83. *Р.Хонсбергер*. Математические изюминки
84. *Ю.Р.Носов*. Дебют оптоэлектроники
85. *Г.Гамов*. Приключения мистера Томпкинса
86. *И.Ш.Слободецкий, Л.Г.Асламазов*. Задачи по физике (2-е изд.)
87. Физика и...
88. *А.В.Спивак*. Математический праздник
89. *Л.Г.Асламазов, И.Ш.Слободецкий*. Задачи и не только по физике
90. *П.Гнэдиг, Д.Хоньек, К.Райли*. Двести интригующих физических задач
91. *А.Л.Стасенко*. Физические основы полета
92. Задачник «Кванта». Математика. Часть 1. Под редакцией Н.Б.Васильева
93. Математические турниры имени А.П.Савина
94. *В.И.Белотелов, А.К.Звездин*. Фотонные кристаллы и другие метаматериалы
95. Задачник «Кванта». Математика. Часть 2. Под редакцией Н.Б.Васильева
96. Олимпиады «Интеллектуальный марафон». Физика
97. *А.А.Егоров, Ж.М.Раббот*. Олимпиады «Интеллектуальный марафон». Математика
98. *К.Ю.Богданов*. Прогулки с физикой
99. *П.В.Блиох*. Радиоволны на земле и в космосе
100. *Н.Б.Васильев, А.П.Савин, А.А.Егоров*. Избранные олимпиадные задачи. Математика
101. У истоков моей судьбы...
102. *А.В.Спивак*. Арифметика
103. *Я.А.Сморodinский*. Температура
104. *А.Н.Васильев*. История науки в коллекции монет
105. *И.Ф.Акулич*. Королевские прогулки
106. Исаак Константинович Кикоин в жизни и в «Кванте»
107. *Г.С.Голицын*. Макро- и микромиры
108. *П.С.Александров*. Введение в теорию групп.

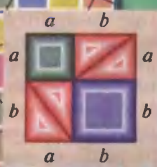


# Библиотечка КВАНТ



Арифметика-

2



Арифметика-

2

ВЫПУСК

109