Суммы квадратов

«Зачем складывать простые числа?» —
недоумевал великий физик Л.Д. Ландау. —
«Простые числа созданы для того, чтобы их
умножать, а не складывать!»

Зачем складывать квадраты целых чисел? Почему бы не складывать их кубы или 66-е степени? Вопросы эти весьма серьёзны и встают перед каждым, кто начинает изучать математику. Из огромного разнообразия задач не все достойны пристального внимания. Задача о сумме квадратов — в высшей степени достойна. К сожалению для философа, это трудно объяснить, не рассказав её 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! Хотя эта статья содержит лишь малую часть теории делимости алгебраических чисел, надеемся, её очарование никого не оставит равнодушным.

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 убеждён, 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.

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

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.

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. Эта гипотеза верна. 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:

ВНИМАНИЕ! В этой и следующих таблицах линейки стоят со смыслом!!!

Квадрат	0	1	4	9	16	25	36	49	64	81	100	121
Остаток	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, то есть представимо в виде $x = 3k$, где k — целое число, и остаток равен 1, если x не кратно 3, то есть 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 $x^2 = 9k^2 \pm 6k + 1$ даёт 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:

Квадрат	0	1	4	9	16	25	36	49	64	81	100	121	144	169
Остаток	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.*

Указание. $21 = 3 \cdot 7$.

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.*

а) 0, 1, 3, 4, 5 или 9.

Остатки от деления на 19

Полезные истины следует говорить и
повторять как можно чаще.
П. Буаст

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

Квадрат	0	1	4	9	16	25	36	49	64	81	100	121	144	169	196	225	256	289	324
Остаток	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, $0 \leqslant r \leqslant 18$, и при этом число $x^2 = 19^2q^2 + 38qr + r^2$ даёт 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. Все 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.

Итак, простые числа $p = 3$, 7, 11 и 19 обладают тем свойством, что если сумма квадратов кратна p, то каждое из слагаемых кратно p. Обратите внимание: числа 3, 7, 11 и 19 при делении на 4 дают остаток 3, то есть $3 = 4 \cdot 0 + 3$, $7 = 4 \cdot 1 + 3$, $11 = 4 \cdot 2 + 3$ и $19 = 4 \cdot 4 + 3$.

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 нечётного числа даёт 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 трёх целых чисел.*
г) *Если число $8n + 3$, где n — целое неотрицательное число, представимо в виде суммы трёх квадратов, то число n представимо в виде суммы трёх треугольниых чисел, то есть 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 трёх 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. Серра. Оно использует p-адические числа, символ Гильберта и теорему Минковского–Хассе.*

а) *Первый способ.* Нечётное 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 $n+1$ чётно.
Третий способ. $x^2 = (x-1)(x+1)+1$, где при нечётном x один множитель чётен, а другой кратен 4.
в) Если все три числа x, y, z чётны, то разделим обе части уравнения $x^2+y^2+z^2 = 4^m(8n+7)$ на 4. Так будем делать до тех пор, пока одно из чисел x, y, z не станет нечётным. Поскольку квадрат нечётного числа при делении на 8 даёт остаток 1, а квадрат любого целого числа — остаток 0, 1 или 4, и поскольку ни одна из сумм $1+0+0$, $1+0+1$, $1+0+4$, ..., $1+4+4$ не даёт при делении на 8 ни остатка 7, ни остатка 4, ни остатка 0, получаем желанное противоречие.
г) Чтобы сумма трёх квадратов давала остаток 3 при делении на 8, слагаемые должны быть нечётны. Поэтому

$$8n+3 = (2x+1)^2+(2y+1)^2+(2z+1)^2,$$

что равносильно искомому равенству.

7. а) *Остаток от деления на 16 четвёртой степени нечётного числа равен 1. Докажите это.* б) *Решите в целых числах уравнение* $x_1^4 + x_2^4 + x_3^4 + \ldots + x_{14}^4 = 1\,000\,000\,001\,983$.

а) $x^4 - 1 = (x-1)(x+1)(x^2+1)$. Множители чётны. Из чисел $x-1$ и $x+1$ одно делится не только на 2, но даже на 4.
б) Остаток деления на 16 левой части равен количеству нечётных чисел среди x_1, x_2, ..., x_{14}, поэтому не превосходит 14. Остаток правой части — 15.

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

$60 = 3\cdot 5\cdot 4$. 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 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 чётные, очевиден. Если числа a и b оба нечётны, 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 чётности. Для определённости, пусть a нечётно, а b чётно. Поскольку квадрат любого нечётного 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.

9. *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.*

10. *Какое наибольшее количество натуральных чисел, ни одно из которых не представимо в виде ab^2, где числа a и b взаимно просты, причём $b>1$, идут подряд?*

Число $8n+4$, где n — целое, представимо в виде $(2n+1)\cdot 2^2$. Ряд из 7 чисел существует: например, таковы числа 29, 30, 31, 32, 33, 34 и 35.

Делимость суммы квадратов на простое число

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 — без малой теоремы Ферма. Рассмотрим числа $1, 2, \ldots, p-1$. Пусть x — любое из них. Числа x, $2x$, $\ldots$, $(p-1)x$, как легко убедиться, не делятся на p и дают разные остатки при делении на p; поэтому в точности одно из них даёт остаток 1 при делении на p, так что существует такое число y, что $xy \equiv 1 \pmod p$ и $1 \leqslant y < p$.

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, разберём ясности ради несколько примеров. 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 трёх рассмотренных случаях множество M_1 двухэлементное, а остальные множества состоят из четырёх элементов каждое.

Множество M_x не всегда состоит из четырёх разных остатков. Например, если $x \equiv 1$ или $x = p-1$, то $y \equiv x$ и $-y \equiv -x \pmod p$. Верно и обратное: если $x \equiv y$, то $x^2 \equiv 1$, так что $(x-1)(x+1) = (x^2-1) \vdots p$, то есть $x \equiv \pm 1 \pmod p$.

Априори вообразима ситуация, когда $x \equiv -y$, то есть $x^2 \equiv -1 \pmod p$. Поскольку сравнение $x \equiv -x \pmod p$ невозможно (вы помните, что $0 < x < p$, а p нечётно), приходим к основной мысли этого доказательства: кроме двухэлементного множества M_1 двухэлементным может быть лишь такое множество M_x, что $x^2 \equiv -1 \pmod p$. Поскольку удовлетворяющих этому сравнению второй степени остатков существует не более чем два, 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 $\{2, 3, \ldots, 4n+1\}$. Поскольку кроме M_1 двухэлементным, как мы только что доказали, может быть самое большее одно из рассматриваемых множеств, то M_1 — *единственное* двухэлементное множество, что и доказывает теорему 1: ни для какого целого x сумма x^2+1 не делится на простое число $p = 4n+3$.

Упражнения

11. *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 даёт остаток 3, то числа x и y кратны p^m. Докажите это.*

12. *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.*

Рассмотрите числа вида $21 \cdot 5^n$ или $3^{2n-1} \cdot 7$, где n — натуральное.

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

а) Предположим, что множество M простых чисел, сравнимых с 3 по модулю 4, конечно: $M = \{3, 7, 11, 19, 23, \ldots, p\}$. Перемножим их все, умножим произведение на 4 и вычтем из произведения единицу:

$$n = 4 \cdot 3 \cdot 7 \cdot 11 \cdot 19 \cdot 23 \cdot \ldots \cdot p - 1.$$

Число n нечётно 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 даёт при делении на 4 остаток 1. Следовательно, хотя бы один простой делитель q числа n удовлетворяет сравнению $q \equiv 3 \pmod 4$. Поскольку n не делится ни на один из элементов множества M, получили желанное противоречие.

б) Предположим, что множество M простых чисел, сравнимых с 1 по модулю 4, конечно: $M = \{5, 13, 17, 29, 37, \ldots, p\}$. Перемножим их квадраты, умножим произведение на 4 и прибавим к произведению единицу:

$$n = (2 \cdot 5 \cdot 13 \cdot 17 \cdot 29 \cdot 37 \cdot \ldots \cdot p)^2 + 1.$$

В силу теоремы 1, ни один простой делитель числа n не даёт остаток 3 при делении на 4. Осталось заметить, что n нечётно и не делится ни на один из элементов множества M.

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

$$16! = 1 \cdot (2 \cdot 9) \cdot (3 \cdot 6) \cdot (4 \cdot 13) \cdot (5 \cdot 7) \cdot (8 \cdot 15) \cdot (10 \cdot 12) \cdot (11 \cdot 14) \cdot 16 \equiv 16 \equiv -1 \pmod{17}.$$

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

Упражнения

14 (М1357). *Числа* а) $97!\cdot 1901!-1$; б) $98!\cdot 1900!+1$ *кратны 1999. Докажите это. (*Указание. *Число 1999 простое.)*

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

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

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

18. *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.*

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,

$$-1\equiv(n+1)!=(n+1)n\cdot(n-1)!\equiv(-1)(-2)\cdot(n-1)!=2\cdot(n-1)!\pmod{n+2},$$

следовательно, $4\cdot(n-1)!\equiv-2\pmod{n+2}$ и

$$4+4\cdot(n-1)!+n\equiv4-2+n\equiv0\pmod{n+2}.$$

Поскольку числа n и $n+2$ простые, то они взаимно простые и 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, $n\neq2$ и $n\neq4$. Предполагая, что $n=2k$, где $k\geqslant3$, 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 нечётно, 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 $4(1+(n-1)!)+n=2(1+2\cdot(n-1)!)+n+2$ на $n+2$ следует, что на $n+2$ делится число $1+2\cdot(n-1)!=1+(n+2-n)(n+2-n-1)\cdot(n-1)!\equiv1+(-n)(-n-1)\cdot(n-1)!=1+(n+1)!\pmod{n+2}$ и, опять в силу предыдущего упражнения, $n+2$ — простое.

Теперь докажем теорему 2. Годится $m=(2n)!$. В самом деле,

$$(p-1)!=1\cdot2\cdot\ldots\cdot(2n-1)\cdot(2n)\cdot(2n+1)\cdot(2n+2)\cdot\ldots\cdot(4n-1)\cdot(4n)=$$
$$=1\cdot2\cdot\ldots\cdot(2n-1)\cdot(2n)\cdot(p-2n)\cdot(p-(2n-1))\cdot\ldots\cdot(p-2)\cdot(p-1).$$

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

$$1\cdot2\cdot\ldots\cdot(2n-1)\cdot(2n)\cdot(-1)^{2n}\cdot(2n)\cdot(2n-1)\cdot\ldots\cdot2\cdot1=m^2.$$

Значит, $m^2\equiv(p-1)!\pmod p$. Сумма $(p-1)!+1$ кратна p по теореме Вильсона.

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

Упражнения

19. 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?*

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.

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

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

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: $x\leqslant 0$. По той же самой причине $y\leqslant 0$. Замечание. Рассматриваемое уравнение имеет бесконечно много решений в целых отрицательных числах.

22. 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 $x^2y^2=x^2+y^2+z^2$.*

а) Если n нечётно, то n^2-1 кратно 4, а число m^2+1 не кратно 4 ни при каком целом m. Если же $n=2k$, то $n^2-1=4k^2-1$ даёт остаток 3 при делении на 4, и остаётся применить утверждение теоремы 1.
б) Перенесём 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 упражнения, $x=y=0$, откуда $z=0$.

Часть II. Критерий Жирара

Мария Ивановна: *«Тождество — 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 маленькая область определения! В первом одна точка, а во втором — вообще 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! Тождество испортится!»*

Если $n=x^2+y^2$, то

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

Значит, если n представимо, то представимо и $2n$. Далее,

$$(2x+y)^2+(x-2y)^2=4x^2+4xy+y^2+x^2-4xy+4y^2=5(x^2+y^2)=5n.$$

Легко проверить и формулы

$$(2x+3y)^2+(3x-2y)^2=13n,$$
$$(4x+y)^2+(x-4y)^2=17n.$$

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:

$$(a^2+b^2)(x^2+y^2) = a^2x^2+b^2x^2+a^2y^2+b^2y^2 = \\ = a^2x^2-2axby+b^2y^2+b^2x^2+2bxay+a^2y^2 = (ax-by)^2+(bx+ay)^2.$$

Упражнение 23. *Докажите, что*
а) *если чётное 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.*

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 чётное, а другое нечётное, то сумма квадратов x^2+y^2 нечётна. Значит, x и y оба чётны или оба нечётны, 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 $3^2x^2 \equiv 2^2y^2$, то есть $(3x+2y)(3x-2y) \equiv 0 \pmod{13}$, откуда следует, что хотя бы одно из чисел $3x+2y$ и $3x-2y$ кратно 13. Дальнейшее очевидно.

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 ещё 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 её (при помощи любимого Ферма метода бесконечного спуска) Леонард Эйлер (1707–1783). Перед

тем, как её доказывать, сформулируем критерий того, какие числа представимы в виде суммы двух квадратов.

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 и упражнение 11 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 чётной 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

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

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

а) $x = y = z = t = 0$.
б) Поскольку y^2 не может дать остаток 3 при делении на 4, число x должно быть нечётным. Имеем: $y^2 + 1 = x^2 + 8 = (x + 2)(x^2 - 2x + 4)$. Число $x^2 - 2x = x(x - 2)$ — произведение двух соседних нечётных чисел — при делении на 4 даёт остаток 3.
в) *Указание.* Сначала докажите, что x нечётно, а затем запишите уравнение в виде $x(x + 2)(x - 1) = y^2 + 1$ и заметьте, что $x(x - 2)$ даёт остаток 3 при делении на 4. *Ответ*: $x = -1$, $y = 1$ или -1.

26 (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.*

б) *Указание.* Если числа $n-1$, n и $n+1$ отмеченные, причём число $n=a^2+b^2$ нечётное, 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.
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 $2\cdot 100^m-1$ даёт остаток 3 при делении на 4, а число $2\cdot 100^m+1$ даёт 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 13).

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 всё 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 трёх натуральных чисел a, b и c нарисуем 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°, 180° и 270°, получим ещё три прямоугольника размером $b \times c$ каждый. Возникла фигура площади $a^2 + 4bc$.

На рисунках 6, 7, 8 и 9 показаны все существующие 7 способов представить число 37 в виде a^2+4bc, где a, b и c — натуральные числа. Как видите, существует 7 таких представлений; они естественным образом разбиваются на представление $37 = 1^2 + {} + 4 \cdot 9 \cdot 1$ и три пары представлений.

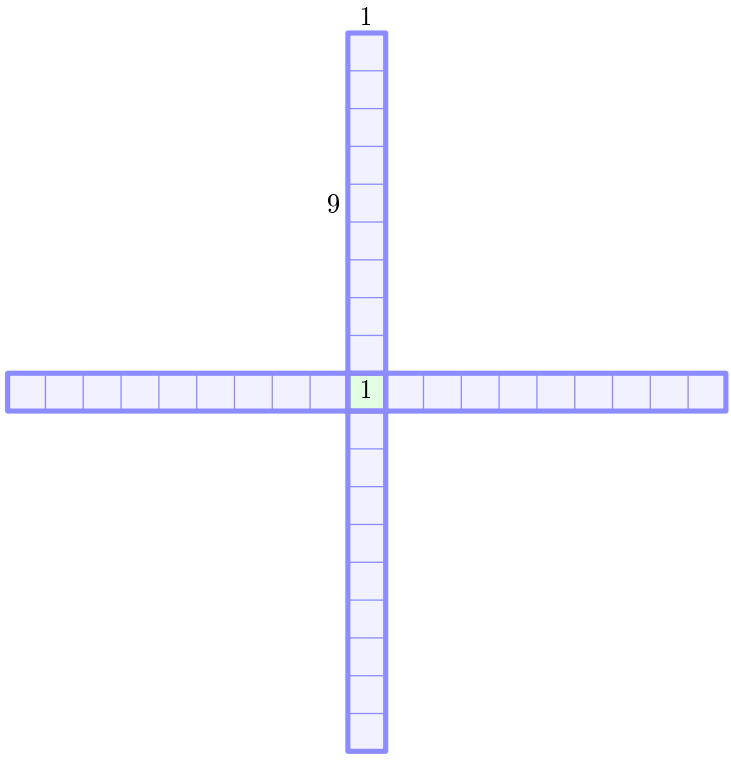

Рисунок 6

В общем виде конструкция такова: поскольку имеется одно представление в виде «креста» $p = 1+4 \cdot n \cdot 1$ и ещё несколько пар (это слово — главное!), то количество решений уравнения $p = a^2 + {} + 4bc$ в натуральных числах a, b и c нечётно. Поскольку можно каждому решению (a, b, c) сопоставить решение (a, c, b), а количество решений нечётно, то хотя бы в одном решении $b = c$. А это и есть теорема Ферма-Эйлера.

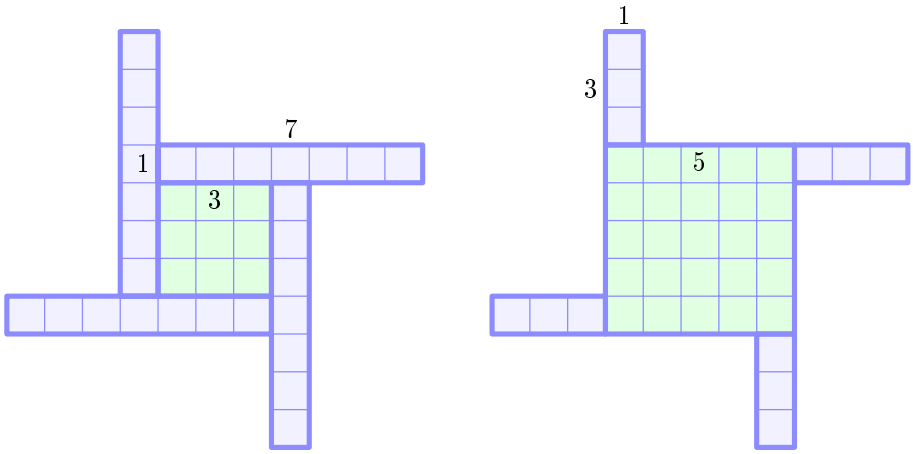

Рисунок 7

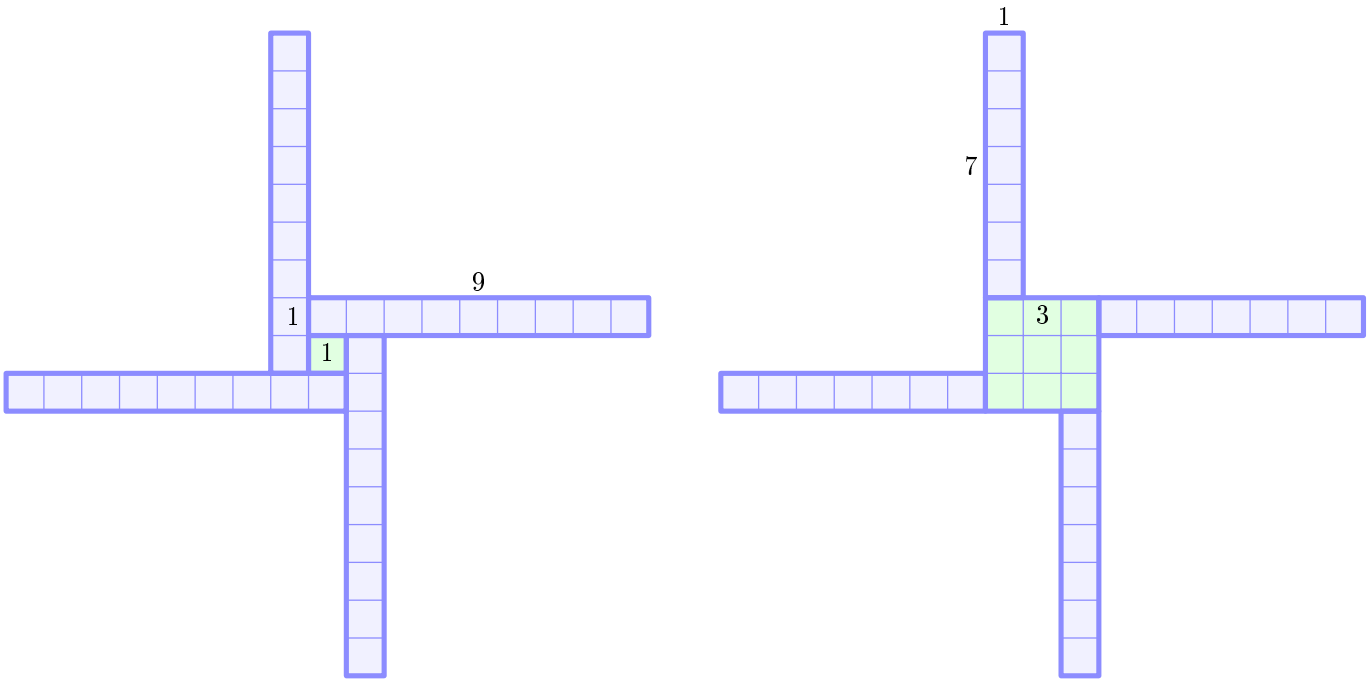

Рисунок 8

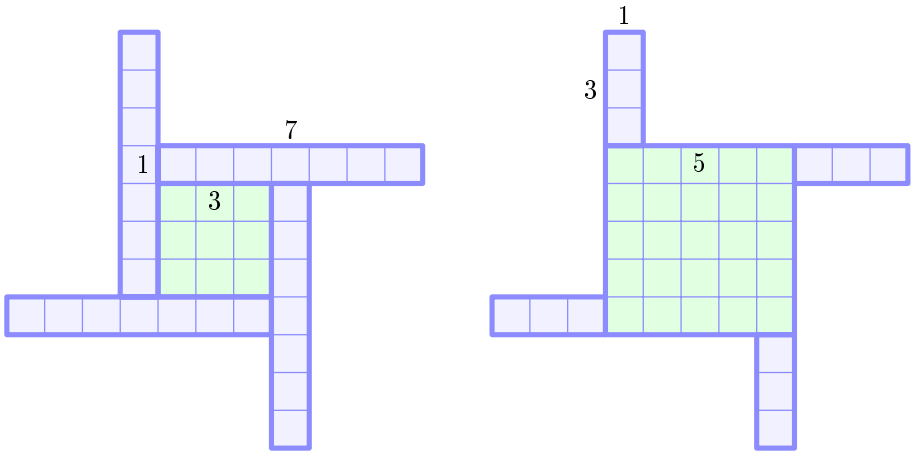

Рисунок 9

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, то есть $f(f(a, b, c)) = (a, b, c)$ 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

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

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

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

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

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

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

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

Очевидно, она равносильна системе

$$\begin{cases} a = c, \\ a^2+4ab = p, \end{cases}$$

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 *нечётно*. 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, с клетчатой бумагой это доказательство гораздо понятнее!)

Упражнения

27. *Поймите, как именно в доказательстве использована простота числа p.*

28. *Роджер Хит–Броун в придуманном в 1971 и опубликованном в 1984 году доказательстве рассмотрел множества*

$$F = \{(a,b,c) \mid a^2 + 4bc = p, \quad a \in \mathbb{Z}, \quad b,c \in \mathbb{N}\},$$
$$G = \{(a,b,c) \in F \mid a + c > b\},$$
$$H = \{(a,b,c) \in F \mid a > 0\}$$

и отображения $f\colon F \to F$, $g\colon G \to G$, $h\colon H \to H$, определённые формулами

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

Доказательство состоит из следующих соображений.
а) *f — инволюция, то есть $f(f(a,b,c)) = f(-a,c,b) = (a,b,c)$; 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 нечётно — значит, нечётно 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 нечётного 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, то есть удовлетворяет равенству $b = c$, что и завершает доказательство теоремы Ферма-Эйлера.*

II способ. Доказательство Лагранжа

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

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 $0 \leqslant r,s < \sqrt{p}$, 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.

При этом число $r+ms$, где $r = r_1 - r_2$ и $s = s_1 - s_2$, кратно p. Поэтому число

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

тоже кратно p. Заметим, что $0 < r^2+s^2 < p+p = 2p$. Единственное кратное p число, которое больше 0, но меньше $2p$, — само число p. Значит, $r^2+s^2 = p$.

Упражнение 29. *Как доказано в статье «Уравнения Пелля», для любого вещественного числа ξ и любого натурального числа n существуют такие целое число t и натуральное число s, что $s \leqslant n$ и $|s\xi - t| \leqslant \frac{1}{n+1}$. Рассмотрев $\xi = m/p$ и $n = [\sqrt{p}]$, докажите теорему Ферма–Эйлера.*

$\left|\frac{sm}{p} - t\right| \leqslant \frac{1}{n+1} = \frac{1}{[\sqrt{p}]+1} < \frac{1}{\sqrt{p}}$. Обозначим $ms - tp = r$. Тогда $|r| = p\left|\frac{sm}{p} - t\right| < \sqrt{p}$ и число

$$r^2 + s^2 = (ms - tp)^2 + s^2 = s^2(m^2 + 1) - 2mstp + t^2p^2$$

делится на p. Поскольку $s \leqslant n < \sqrt{p}$ и $r < \sqrt{p}$, то $r^2 + s^2 < 2p$. Следовательно, $r^2 + s^2 = p$.

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 ещё 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». Вполне возможно, что Ферма действительно знал такое доказательство, как и доказательства двух аналогичных его 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 даёт остаток 3 или 7, представимо в виде $p = x^2 + 5y^2$, где x и y — целые.

Лишь Л. Эйлер в 1747—1749 годах превратил изложенный в письме Ферма 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

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

Значит, $ar - bs$ или $ar + bs$ кратно p. Если $ar - bs \vdots p$, 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 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

$$c^2+d^2 = (a-mx)^2+(b-my)^2 = (a^2+b^2) - 2amx + m^2x^2 - 2bmy + m^2y^2 \vdots m.$$

Значит, $c^2+d^2 = mn$, где n — целое, причем $n = \frac{c^2+d^2}{m} \leqslant \frac{(m/2)^2+(m/2)^2}{m} = \frac{m}{2}$. 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 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, аналогично получаем меньшее число, являющееся делителем суммы квадратов взаимно простых чисел и не представимое в виде суммы квадратов, и так далее. Но бесконечной убывающей последовательности натуральных чисел не существует. Осталось сослаться на теорему 2 — и теорема Ферма–Эйлера доказана! Впрочем, Эйлер в 1749 году так не рассуждал, а 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}, $\ldots$, $(4n-1)^{4n}$, $(4n)^{4n}$ даёт 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 $1 \leqslant a < 4n$, 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 $a = 1, 2, \ldots, p-1$; но многочлен степени $2n$ не может иметь $4n$ корней.

Упражнения

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

[*)] Между прочим, число 21 представимо в виде суммы квадрата и упятерённого квадрата двумя способами: $21 = 4^2+5\cdot 1^2 = 1^2+5\cdot 2^2$, а числа 3 и 7 не представимы. Таким образом, задача о сумме двух квадратов значительно проще задачи о сумме квадрата и упятерённого квадрата.

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, $a^2c^2 \equiv (-b^2)(-d^2) \pmod p$, то есть число $a^2c^2 - b^2d^2$ кратно 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 один из множителей кратен p. Если число $ac + bd$ кратно p, то 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 $ac - bd$ кратно p, можно рассмотреть аналогично, воспользовавшись формулой $p^2 = (ac - bd)^2 + (ad + bc)^2$.

31 (М1288*). *Число* $1\,000\,009 = 235^2 + 972^2$ *составное.* а) *Докажите это.* б) *Представьте его в виде произведения двух отличных от 1 натуральных чисел.*

б) Пусть $a = 1\,000$, $b = 3$, $c = 235$, $d = 972$. Тогда $ac + bd = 237\,916$ и $ac - bd = 232\,084$. Произведение $237\,916 \cdot 232\,084$ кратно $1\,000\,009$. Применим алгоритм Евклида. Поскольку $1\,000\,009 = 4 \cdot 237\,916 + 48\,345$, имеем $\text{НОД}(1\,000\,009; 237\,916) = \text{НОД}(48\,345; 237\,916)$. Далее, $237\,916 = 5 \cdot 48\,345 - 3809$. Значит, $\text{НОД}(48\,345; 237\,916) = \text{НОД}(48\,345; 3809) = \text{НОД}(13 \cdot 3809 - 1\,172; 3809) = \text{НОД}(1172; 3809) = \text{НОД}(1172; 3 \cdot 1172 + 293) = \text{НОД}(1172; 293) = 293$. (Аналогично можно было бы найти $\text{НОД}(1\,000\,009; 232\,084) = 3413$.)
Ответ: $1\,000\,009 = 293 \cdot 3413$.

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

33. *Если p — простое число, m — натуральное число, причём $pm = a^2 + nb^2$ 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.*

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 $m = \left(\frac{ar - nbs}{p}\right)^2 + n\left(\frac{as + br}{p}\right)^2$.

34. *а) Если q — нечётное простое число, m — натуральное число, причём $q^2m = a^2 + nb^2$ и $q^2 = r^2 + ns^2$, где a, b — целые числа, r, s, n — натуральные числа, то и число m представимо в виде $m = x^2 + ny^2$, где x и y — целые числа. Докажите это.*
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. Докажите это.

а) Поскольку $(as-br)(as+br)=(a^2+nb^2)s^2-b^2(r^2+ns^2)$ делится на q^2, то достаточно рассмотреть три случая: $as-br$ делится на q^2; $as+br$ делится на q^2; каждое из чисел $as+br$ и $as-br$ делится на q. В первом случае годится представление

$$m=\frac{(a^2+nb^2)(r^2+ns^2)}{q^4}=\left(\frac{ar+nbs}{q^2}\right)^2+n\left(\frac{as-br}{q^2}\right)^2;$$

во втором — представление $m=\left(\frac{ar-nbs}{q^2}\right)^2+n\left(\frac{as+br}{q^2}\right)^2$.

В третьем случае $2as=(as+br)+(as-br)\vdots q$. Поскольку q нечётное и простое, а $1\leqslant s<q$, то $a\vdots q$. Аналогичным образом из равенства $2br=(as+br)-(as-br)$ следует, что $b\vdots q$. 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.

35. *Докажите следующие утверждения.*

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

б) Число -2 есть квадратичный невычет по любому простому модулю, дающему остаток 5 или 7 по модулю 8.

в) Для любого простого числа p, дающего остаток 1 при делении на 8, существует квадрат, дающий остаток 2 при делении на p. Указание. *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 $(x^2+1)^2\equiv 2x^2\pmod p$.*

г) Число 2 является квадратичным вычетом по модулю простого числа p тогда и только тогда, когда $p\equiv\pm1\pmod 8$.

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

а) Предположим противное: существуют простое число p, сравнимое с 3 или 5 по модулю 8, и целые числа x и y, удовлетворяющие равенству $x^2-2=py$. Рассмотрим *наименьшее* из таких простых чисел p. Заменяя при необходимости x на остаток от деления числа x на p, приходим к неравенству $0<x<p$. Далее, заменяя при необходимости x на $p-x$, видим, что можно считать число x нечётным и удовлетворяющим неравенствам $0<x<p$.

Поскольку $py=x^2-2<p^2$, то $y<p$. Число x^2-2 сравнимо по модулю 8 с 1 или с -1. Следовательно, y сравнимо с 3 или с -3 по модулю 8. Поскольку произведение чисел, каждое из которых сравнимо по модулю 8 с 1 или -1, при делении на 8 даёт остаток 3 или -3, 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).

в) Для числа x, не делящегося на p, существует такое число y, что $xy\equiv 1\pmod p$. Если $x^4+1\vdots p$, то $(x^2+1)^2y^2\equiv 2x^2y^2\equiv 2\pmod p$.

г) Если $p\equiv 1\pmod 8$, то в силу пункта в) имеем $\left(\frac{2}{p}\right)=1$. Если $p\equiv\pm3\pmod 8$, то $\left(\frac{2}{p}\right)=-1$ в силу пункта а). Наконец, если $p\equiv 7\pmod 8$, то $\left(\frac{-2}{p}\right)=-1$ в силу пункта б) и $\left(\frac{-1}{p}\right)=-1$ в силу теоремы 1.

36*. *Всякое простое число p, которое даёт остаток 1 или 3 при делении на 8, представимо в виде $p=x^2+2y^2$, где x и y — целые числа. Докажите это.* Указание. *Для вычисления символа Лежандра $\left(\frac{-2}{p}\right)$ воспользуйтесь пунктом д) предыдущего упражнения или тем, что вследствие статьи «Квадратичный закон взаимности» «Арифметики» $\left(\frac{-2}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)=(-1)^{(p-1)/2}(-1)^{(p^2-1)/8}$.*

37*. *Всякое простое число p, которое даёт остаток 1 при делении на 3, представимо в виде $p = x^2 + 3y^2$, где x и y — целые числа. Докажите это.* Указание. $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}(-1)^{(3-1)(p-1)/4}\left(\frac{p}{3}\right)$.

Неоткрытие Эйлера

... всё уже сочинено в далёкие средние века —
и современными авторами только воруется.
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

Леонард Эйлер — автор огромного числа научных работ. В частности, он не только доказал теорему Ферма–Эйлера, но и сформулировал несколько гипотез: 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;[*)]
- 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 четвёртой степени некоторого целого числа на p.[†)]

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 $p = 2x^2 + 2xy + 3y^2$, 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

$$(2a^2 + 2ab + 3b^2)(2x^2 + 2xy + 3y^2) = (2ax + bx + ay + 3by)^2 + 5(bx - ay)^2$$

показывает, что верна и гипотеза Ферма о том, что произведение любых двух простых чисел, каждое из которых при делении на 20 даёт 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 «взятой с потолка» формулы.)

[*)]Об этой гипотезе мы ничего не расскажем. Заинтересованному читателю советуем «Классическое введение в современную теорию чисел» К. Айерлэнда и М. Роузена.

[†)]Доказательство Петера Густава Лежёна Дирихле (1805–1859) этой гипотезы Эйлера — в упражнении 33.

В 2006 году Йинг Жанг придумал доказательство теоремы о числах, представимых в виде x^2+5y^2, которое построено 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 нечётного 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 нечётных простых чисел p, которые удовлетворяют одному из сравнений $p\equiv 1$, 3, 5, 7 или 9 $(\mathrm{mod}\ 20)$.

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, причём $q\equiv 3$ или 7 $(\mathrm{mod}\ 20)$ и $Q=2$ или $Q\equiv 3$ или 7 $(\mathrm{mod}\ 20)$, то произведение qQ представимо в виде $qQ=x^2+5y^2$, где x и y — натуральные числа.*

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

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 $(\mathrm{mod}\ 20)$, представимы в виде суммы квадрата и упятерённого квадрата натуральных чисел, а все простые числа $q<P$, удовлетворяющие сравнению $q\equiv 3$ $(\mathrm{mod}\ 20)$ или сравнению $p\equiv 7$ $(\mathrm{mod}\ 20)$, обладают тем свойством, что для любого простого числа $Q<P$, где $Q=2$, $Q\equiv 3$ или 7 $(\mathrm{mod}\ 20)$, произведение qQ представимо в виде суммы квадрата и упятерённого 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 $a^2+5\vdots P$. Заменив число a на наименьшее по модулю число, сравнимое с a по модулю P, мы видим, что можно считать выполненным неравенство $|a|\leqslant(P-1)/2$, а вместе с ним и неравенства

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

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

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

причём $m<P$. При рассматриваемом P мы можем из всех таких равенств выбрать то, где m — наименьшее возможное. Очевидно, для наименьшего возможного m числа x и y взаимно простые — иначе m можно было бы разделить на квадрат наибольшего общего делителя.

Как вы помните, перед формулировкой теоремы 3 мы вывели из квадратичного закона взаимности, что любой нечётный простой делитель числа m при делении на 20 даёт один из остатков 1, 3, 5, 7 и 9.

Если m делится на простое число p, сравнимое с 1 или 9 по модулю 20, то в силу предположения индукции число p представимо в виде суммы квадрата и

упятерённого квадрата. Вспоминая упражнение 27, 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 нечётные числа q, дающие остаток 3 или 7 при делении на 20. Рассмотрим два случая.

Если m делится на q^2, то достаточно вспомнить упражнение 28. Если m делится на qQ, где $q \neq Q$, причём 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 упятерённого квадрата. В силу формулы упражнения 26, представимо в таком виде и произведение $qQ \cdot Pm$. Поскольку $qQPm = q^2Q^2 \cdot P\frac{m}{qQ}$, то, дважды применив утверждение упражнения 28, видим, что в виде суммы квадрата и упятерённого 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 даёт при делении на 20 остаток 3 или 7. По предположению индукции, число mQ представимо в виде суммы квадрата и упятерённого квадрата. В силу упражнения 26, произведение $mP \cdot mQ = m^2 \cdot PQ$ тоже представимо. Осталось вспомнить упражнение 28 — и теорема 3 доказана.

Упражнения

38. *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.*

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

39. *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?*

Нет, ибо $(a + b)^2 - (a + b)b + b^2 = a^2 + ab + b^2$.

40. *Всякое простое число p, которое даёт 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.*

В силу теоремы 3, существуют такие целые числа b и c, что $2p = c^2 + 5b^2$. Числа b и c нечётные, поэтому $c = 2a + b$ для некоторого целого числа a. Очевидно, $2p = (2a + b)^2 + 5b^2 = 4a^2 + 4ab + 6b^2$, откуда $p = 2a^2 + 2ab + 3b^2$.

41. *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 чётности, можно считать, что a нечётно, а b чётно. Пусть f — такое целое число, что $b \equiv af \pmod{p}$. Применяя свойства символа Якоби и критерий Эйлера, убедитесь в следующем:*

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

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

в) $f^2 \equiv -1 \pmod{p}$;

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

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, то есть когда b делится на 8. Таким образом, из статьи «Малая теорема Ферма» первой части книги следует, что 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 четвёртой степени некоторого целого числа на p.*

IV способ. Доказательство Минковского

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

Рисунок 12 — это рисунок страницы 405 энциклопедии.

Доказательство. Выбрав находящиеся на наименьшем расстоянии ρ точки решетки A_0 и A_1 (рис. 12), видим, что решетка содержит все точки A_k, где $k \in \mathbb{Z}$ и $\overrightarrow{A_0A_k} = k\overrightarrow{A_0A_1}$, и не содержит ни одной точки внутри кругов радиуса ρ с центрами в этих точках; поэтому высота основного параллелограмма $A_0A_1B_1B_0$ решетки, опущенная на сторону A_0A_1, не меньше $\rho\sin 60^\circ$, откуда $S \geqslant \rho^2\sqrt{3}/2$.

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 $\overrightarrow{OA}$ и $\overrightarrow{OC}$ длин $\sqrt{a}$ и $\sqrt{c}$ соответственно, угол φ между которыми выберем так, чтобы скалярное произведение равнялось b, то есть $\cos\varphi = b/\sqrt{ac}$. Площадь S параллелограмма $OABC$ равна

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

Существуют такие целые числа x и y, хотя бы одно из которых отлично от нуля, что $|x\overrightarrow{OA} + y\overrightarrow{OC}| \leqslant \sqrt{2/\sqrt{3}}$. Следовательно,

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

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 Германа Минковского (1864–1909) о квадратичной форме доказана.

Применяя её 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

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

Упражнения

42. *Всякая выпуклая и симметричная относительно начала координат фигура, площадь которй больше 4, содержит кроме начала координат ещё хотя бы одну точку с целыми координатами. Докажите это. (Это утверждение называют леммой Минковского о выпуклом теле.)*

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 $\overrightarrow{O_1N} = \overrightarrow{MO_2}$ (рис. 13). 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.

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

Площадь фигуры, заданной на координатной плоскости неравенством $ax^2 + 2bxy + cy^2 \leqslant 2$, 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, то есть равна 1.

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 даёт не только ещё 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 её 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, то есть расширение множества $\mathbb{N} = \{1, 2, 3, \dots\}$ натуральных чисел до множества $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$, даёт возможность решить, например, уравнение $x + 7 = 5$. Построив более широкое множество $\mathbb{Q} = \{\frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{N}\}$ 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 $Q[\sqrt{2}]$ 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 всё 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», то есть формулы $z_1+z_2=z_2+z_1$ (переместительный закон, или коммутативность сложения), $z_1z_2=z_2z_1$ (коммутативность умножения), $(z_1+z_2)+z_3=z_1+(z_2+z_3)$ (сочетательный закон, или ассоциативность сложения), $(z_1z_2)z_3=z_1(z_2z_3)$ (ассоциативность умножения), $(z_1+$ $+z_2)z_3=z_1z_3+z_2z_3$ (распределительный закон, или дистрибутивность).

Упражнения

44. *Выполните эту проверку.*

45. *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, то есть 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 всё 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 $u=vw$.)*

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

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 (то есть 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 $z=(x;y)$ 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.

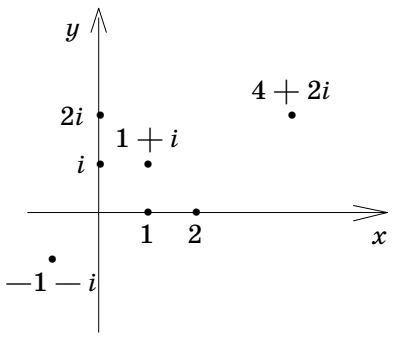

Рис. 14

Рисунки 14–18 — это рисунки 1–5 страниц 18–19 номера 3 за 1999 год.

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

Упражнения

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

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 $x^2=\left(\sqrt{a^2+b^2}+a\right)/2$ и $y^2=\left(\sqrt{a^2+b^2}-a\right)/2$.

Ответ: если $b\geqslant 0$, то $x=\pm\sqrt{\left(\sqrt{a^2+b^2}+a\right)/2}$ и $y=\pm\sqrt{\left(\sqrt{a^2+b^2}-a\right)/2}$; если $b<0$, то $x=\pm\sqrt{\left(\sqrt{a^2+b^2}+a\right)/2}$ и $y=\mp\sqrt{\left(\sqrt{a^2+b^2}-a\right)/2}$.

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

Сопряжённые 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 *сопряжёнными*. Число, сопряжённое с $z = x + yi$, обозначают $\overline{z} = x - yi$ (рис. 15). Геометрический смысл перехода от числа к сопряжённому — симметрия относительно оси абсцисс. Легко проверить тождества

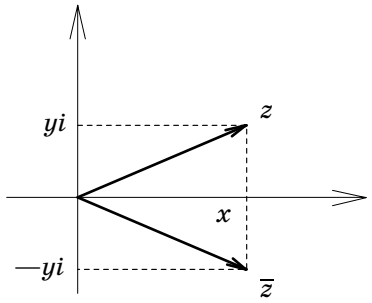

Рис. 15

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

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

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

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

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 — комплексные 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 всё, 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° С. 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 решётку (рис. 16). Интересно, что числа, кратные данному числу z, тоже образуют решётку (рис. 17).

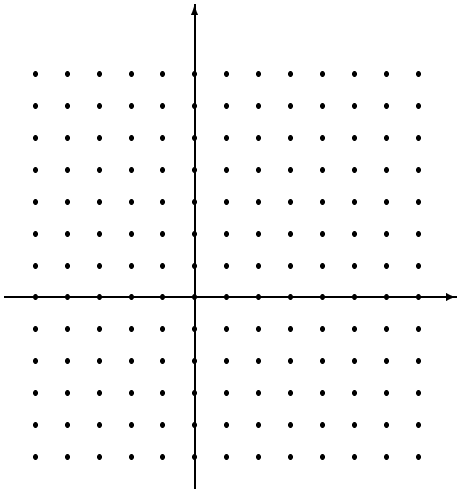

Рис. 16

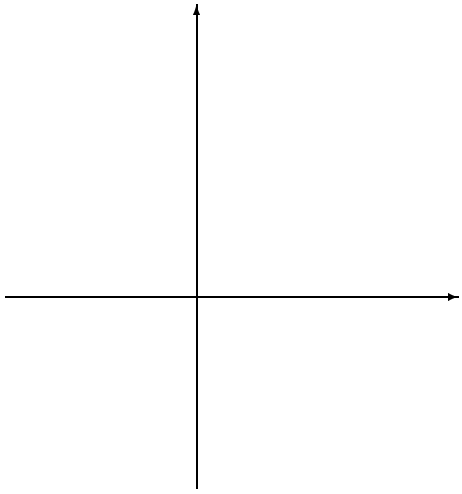

Рис. 17

На рисунке 18 кружочком выделены кратные числа $2 + i$, звёздочками — кратные числа $2 - i$. Спросим себя, какие целые гауссовы числа кратны и числу $2+i$, и числу $2-i$. Ответ очевиден: пересечение множеств «синих» и «красных» чисел 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 сопряжённого к нему числа $\bar{z} = a - bi$ является числом вещественным. Поэтому для любого ненулевого целого гауссова числа z существует кратное ему натуральное число $z\bar{z} = a^2 + b^2$.

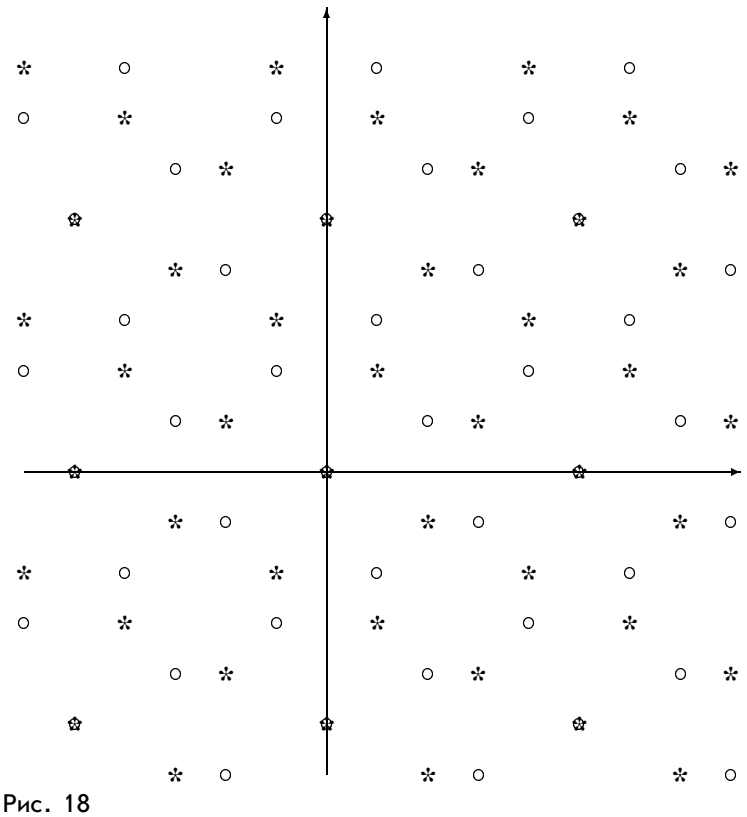

Рис. 18

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

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

Тогда и только тогда, когда a и b — одной чётности, то есть когда сумма $a+b$ чётна.

50. *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?*

в) Кратные числа $5+5i$.

51. *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

Как относиться к трудностям? В области неведомого 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

Очевидно, $1 = 1\cdot 1 = i\cdot(-i) = (-1)\cdot(-1) = (-i)\cdot i$. 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, то есть 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

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

53. *Ассоциированные с числом z числа — это в точности числа вида εz, где ε — делитель единицы. Докажите это.*

54. *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 вида $p \equiv 1 \pmod 4$ существует такое целое число m, что $m^2 + 1 \vdots p$. 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 своеобычна, 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 точке решётки, 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 всё 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 $p_1, \ldots, p_r$ не ассоциировано ни с одним из чисел $q_1, q_2, \ldots, q_s$ (в противном случае мы сократили бы обе части равенства на общий множитель, получив меньшее по модулю число).

Обозначим $P = p_2 \ldots p_r$ и $Q = q_2 \ldots q_s$. Тогда $z = p_1 P = q_1 Q$. Не ограничивая общности, можно считать, что $|p_1| \leqslant |q_1|$. При этом $|P| \geqslant |Q|$ и, значит, $|p_1 Q| \leqslant |z|$. Рассмотрим число $w = \varepsilon z - p_1 Q$, где ε — такой делитель единицы, что $|w| < |z|$. (Почему такой делитель единицы ε 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:

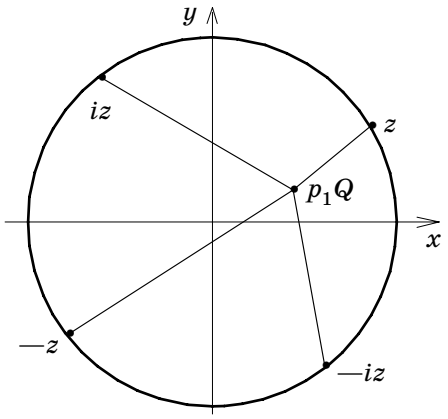

Рис. 19

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

Поскольку $|w| < |z|$, для числа w должна иметь место единственность разложения на простые гауссовы множители. Значит, хотя бы один из множителей $\varepsilon q_1 - p_1$, $q_2, \ldots, q_s$ 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. Ещё очевиднее противоречие в случае, когда кратен числу p_1 один из множителей $q_2, \ldots, q_s$.

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

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

то есть $p^2 = (a^2+b^2)(c^2+d^2)$, 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

Начнёшь читать с начала и дочитаешь до того места, где совсем ничего не будешь понимать. Потом снова начнёшь с начала и будешь так работать с книгой до тех пор, пока не разберёшься со всем.
Совет Ричарда Фейнмана его сестре Джоан

По теореме Ферма–Эйлера любое простое число p, которое при делении на 4 даёт 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*): «Простое число, которое на единицу превосходит кратное четырёх, только один раз является гипотенузой прямоугольного треугольника, его квадрат — два раза, куб — три раза, биквадрат†) — четыре и т. д. до бесконечности.

Это же простое число и его квадрат только одним способом разлагаются на два квадрата*), 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 четырьмя 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. Берём все простые делители числа 15: это 3 и 5. Вычитаем из каждого единицу и берём половины остатков; получаем 1 и 2. Возьмём 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 четырёх 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 четырёх,— это 5 и 13; последнее — один раз, а первое — в квадрате. Возьмём 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 даёт 17. Прибавляем к нему единицу, будет 18; половина есть 9. Столькими способами предложенное число составляется из двух квадратов.

Если последнее число, которое нужно разделить пополам, нечётно, тогда от него следует отнять единицу и взять половину остатка†).»

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 $5 = (2 + i)(2 - i)$,

*)См. «Исследования по теории чисел и диофантову анализу», под редакцией И. Г. Башмаковой, М., «Наука», 1992 год.

†)Биквадрат — четвёртая степень, квадрато-куб — пятая, кубо-куб — шестая.

*)Натуральных чисел. Во времена Ферма к отрицательным числам и нулю всё ещё относились настороженно.

†)Не удивляйтесь тому, что Ферма не вычитает, а прибавляет единицу: дело в том, что Ферма не признаёт разложений вида $n^2 + 0^2$.

$13 = (3 + 2i)(3 - 2i)$ и продолжил бы свои объяснения следующим образом:

$$65 = (2 + i)(3 + 2i) \cdot (2 - i)(3 - 2i) = (4 + 7i) \cdot (4 - 7i) = 4^2 + 7^2 =$$
$$= (2 + i)(3 - 2i) \cdot (2 - i)(3 + 2i) = (8 - i) \cdot (8 + i) = 8^2 + 1^2.$$

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:

$$25 = (2 + i)^2 \cdot (2 - i)^2 = (3 + 4i) \cdot (3 - 4i) = 3^2 + 4^2 =$$
$$= (2 + i)(2 - i) \cdot (2 + i)(2 - i) = 5 \cdot 5 = 5^2 + 0^2.$$

Последний пример — число 5746. Как мы хорошо знаем, всякому представлению $5746 = a^2 + b^2$ соответствует разложение $5746 = (a + bi)(a - bi)$ на сопряжённые 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 ещё два варианта:

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

или

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

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 поймёте 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 даёт 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 ... 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 — нечётно, 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 $\frac{1}{2}(\alpha+1)(\beta+1)(\gamma+1)\ldots$ разложений числа M, когда хотя бы одно из чисел α, β, γ, ... нечётно, и $\frac{1}{2}(\alpha+1)(\beta+1)(\gamma+1)\ldots+\frac{1}{2}$ разложений, когда α, β, γ, ... все чётны.»

Короче, мы можем сформулировать следующую теорему:

Теорема 10. *Количество представлений числа m в виде суммы квадратов двух целых чисел равно $[((a_1+1)\cdot\ldots\cdot(a_r+1)+1)/2]$. (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 поймёте, почему эта формула верна).

Упражнения

55. *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?*

а) 1, б) $\sqrt{5}$, в) $\sqrt{25}$, г) $\sqrt{65}$.

56. 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.*

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

$4(a_1+1)\cdot\ldots\cdot(a_r+1)$.

58*. *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?*

Нет.

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

а) В разложение n на натуральные простые множители простые числа вида $4k-1$ должны входить только в чётных степенях, а простой множитель вида $4k+1$ может быть не более чем один, причём 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, $\alpha \leqslant 2$, $Q = 1$ или Q — произведение одного или нескольких простых чисел вида $4k-1$, причём m должно быть чётным при $\alpha = 2$ и нечётным — 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.

60. *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.*

61*. *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 учетверённой 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

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

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, ..., $\left(\frac{p-1}{2}\right)^2$. Если какие-то два из них дают один и тот же остаток при делении на p, то есть если $x^2 \equiv y^2 \pmod p$, где $0 \leqslant x < y \leqslant (p-1)/2$, 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: $-1-0^2$, $-1-1^2$, $-1-2^2$, ..., $-1-\left(\frac{p-1}{2}\right)^2$. 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 $m - a \leqslant m - \frac{m+1}{2} = \frac{m-1}{2}$.)

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:

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

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 четырёх квадратов в виде суммы четырёх 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 $zj = j\overline{z}$ для любого комплексного числа z. Сумму кватернионов $z_1 + w_1 j$ и $z_2 + w_2 j$ определяем формулой $(z_1 + z_2) + (w_1 + w_2)j$, а произведение — формулой $(z_1 z_2 - w_1\overline{w_2}) + (z_1 w_2 + w_1\overline{z_2})j$.

Нетрудно убедиться, что алгебра кватернионов является телом, то есть ассоциативна и не имеет делителей нуля (произведение любых двух её 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 $z + wj = a + bi + cj + dk$.

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 $ik = -j$.

Рисунок 20 — это рисунок маленький страницы 410 энциклопедии.

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, то есть 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.

Рисунок 21 — это большой рисунок страницы 410 энциклопедии.

Сопряженным кватерниона $u = a + bi + cj + dk$ называют кватернион $\overline{u} = a - bi - cj - dk$. Модуль кватерниона — это число $|u| = \sqrt{u\overline{u}} = \sqrt{a^2 + b^2 + c^2 + d^2}$. Для любых двух кватернионов u и v имеем

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

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