рыл для нас мир, полный красоты и загадочности.

Следующая теорема, несомненно, принадлежит к числу высших достижений математики XVII—XVIII веков.

Взгляните на несколько первых нечетных простых чисел:

$$3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ \ldots$$

Числа 5, 13, 17 представимы в виде суммы двух квадратов: $5 = 2^2 + 1^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$, а остальные числа (3, 7, 11, 19) эти свойством не обладают. Можно ли объяснить этот феномен? Ответ на этот вопрос дает

Теорема 2. *Для того чтобы нечетное простое число было представимо в виде суммы двух квадратов, необходимо и достаточно, чтобы оно при делении на 4 давало в остатке 1.*

Немного истории

На рождество 1640 года в письме от 25 декабря Пьер Ферма извещал без доказательства знаменитого Мерсенна, друга Декарта и главного посредника в переписке ученых того времени, о том, что «всякое простое число, которое при делении на четыре дает единицу, единственным способом представимо как сумма двух квадратов».

Спустя почти двадцать лет после письма Мерсенну в письме к Каркави, отправленном в августе 1659 года, Ферма приоткрывает замысел доказательства сформулированной выше теоремы. Он пишет, что основная идея доказательства состоит в *методе спуска*, позволяющем из предположения, что для какого-то простого числа вида $4n + 1$ заключение теоремы неверно, получить, что оно неверно и для меньшего числа того же вида и т.д., пока мы не доберемся до числа 5, когда окончательно придем к противоречию.

Первые доказательства, которые впоследствии были опубликованы, найдены Эйлером между 1742 и 1747 годами. Причем, желая утвердить приоритет Ферма, к которому он испытывал чувства глубочайшего уважения, Эйлер придумал доказательство, соответствующее описанному выше замыслу Ферма.

Воздавая должное обоим великим ученым (об Эйлере речь еще впереди), мы называем эту теорему *теоремой Ферма—Эйлера.*

Есть свойство, присущее почти всякому прекрасному математическому результату, равно как и почти всякой неприступной и прекрасной горной вершине: его можно штурмовать с разных сторон, и все пути доставляют наслаждение тому, кто не устрашится ими последовать.

В своей статье в «Кванте»[1] я привел три совершенно различных доказательства. Одно из них было придумано Лагранжем в XVIII веке, другое – Германом Минковским в XIX веке, а третье – нашим современником Даном Цагиром. Есть также очень красивое доказательство, использующее теорию делимости чисел вида $n + mi$, где n, m – целые.[2] Здесь я ограничусь лишь первым из названных.

Доказательство Лагранжа

Это доказательство опирается на следующую *лемму Вильсона*: если p – простое число, то число $(p - 1)! + 1$ делится на p.

Чтобы не отвлекаться на доказательство этого вспомогательного факта, продемонстрирую лишь основную идею доказательства на примере простого числа 13. Для любого целого числа x $(2 \le x \le 11)$ найдется такое число y $(2 \le y \le 11)$, что $x \cdot y$ при делении на 13 дает в остатке 1. Действительно,

$$(13-1)! = 12! =$$
$$= (2\cdot 7)(3\cdot 9)(4\cdot 10)(5\cdot 8)(6\cdot 11)\cdot 12,$$

и при этом все произведения в скобках при делении на 13 дают в остатке 1, а значит, число 12! при делении на 13 даст в остатке 12, откуда (для выбранного нами числа 13) следует утверждение леммы Вильсона.

Из леммы Вильсона извлечем такое следствие: если p – простое число вида $p = 4n + 1$, где n – натуральное число, то $((2n)!)^2 + 1$ делится на p. Действительно, из леммы Вильсона следует, что $(4n)! + 1$ делится на p, и теперь необходимое утверждение вытекает из следующей выкладки:

$$(4n)!+1 = (2n)!(2n+1)\cdot\ldots\cdot(4n)+1 =$$
$$= (2n)!(p-2n)(p-2n-1)\cdot\ldots\cdot(p-1)+1 \equiv$$
$$\equiv (2n)!(-1)^{2n}(2n)!+1 \equiv$$
$$\equiv ((2n)!)^2 + 1 \pmod p.$$

[1] *«Квант» №10 за 1991 г.*
[2] *См. об этом: Шнирельман Л.Г. Простые числа (М.: ГИТТЛ, 1940); Сендеров В., Спивак А. Суммы квадратов и целые гауссовы числа («Квант» №3 за 1999 г.).*

Обозначим $(2n)!$ через N. Мы доказали, что $N^2 \equiv -1 \pmod p$.

Теперь нам предстоит преодолеть основную трудность. Рассмотрим все пары целых чисел (m, s) такие, что $0 \le m \le \left[\sqrt{p}\right]$, $0 \le s \le \left[\sqrt{p}\right]$ (где через $\left[\sqrt{p}\right]$ обозначена целая часть числа $\sqrt{p}$ – наибольшее целое число, не превосходящее $\sqrt{p}$). Число таких пар $\left(\left[\sqrt{p}\right]+1\right)^2 > p$. Значит, по крайней мере для двух *различных* пар (m_1, s_1) и (m_2, s_2) имеем: $m_1 + Ns_1 \equiv m_2 + Ns_2 \pmod p$, т.е. число $a + Nb$, где $a = m_1 - m_2$, $b = s_1 - s_2$, делится на p. При этом $|a| \le \left[\sqrt{p}\right]$, $|b| \le \left[\sqrt{p}\right]$. Но тогда число $a^2 - N^2b^2 = (a+Nb)(a-Nb)$ делится на p. Учитывая, что $N^2 \equiv -1 \pmod p$, получим, что $a^2 + b^2$ делится на p, т.е. $a^2 + b^2 = rp$, где r – натуральное число ($r \ne 0$, ибо иначе пары были бы одинаковы). С другой стороны, $a^2 + b^2 \le 2\left[\sqrt{p}\right]^2 < 2p$, т.е. $r = 1$ и $a^2 + b^2 = p$. Теорема 2 доказана.

Вопрос о представлении чисел в виде суммы двух квадратов исчерпывается следующим утверждением:

Натуральное число представимо в виде суммы целых чисел тогда и только тогда, когда все простые сомножители вида 4k + 3 входят в разложение этого числа на простые сомножители с четными показателями.

Эйлер и его формула $e^{\pi i} = -1$

Его [Эйлера] творчество изумительно и в науке беспримерно.
А.Н.Крылов

Однажды, когда я учился в восьмом классе, мой друг и одноклассник написал мне формулу Эйлера, которой я посвящаю этот раздел. Тогда я уже знал, что e – это число: две целых, семь десятых, год рождения Толстого, год рождения Толстого и дальше – другие десятичные знаки, запоминать которые уже необязательно(e = 2,718281828…). Я знал также, что

$$e = \lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n.$$

Разумеется, я имел представление о числе π, о том, что такое степень, и слышал о том, что i – это какое-то