$+ 1^2$, $13 = 3^2 + 2^2$, $17 = 4^2 + 1^2$, $29 = 5^2 + 2^2$, $37 = 6^2 + 1^2$, $41 = 5^2 + 4^2$, $53 = 7^2 + 2^2,\ldots$

Теорема 4. *Любое простое число p, которое при делении на 4 дает остаток 1, представимо в виде суммы квадратов двух натуральных чисел.*

Мы приведем доказательство, состоящее из следующих двух лемм.

Лемма 1. *Для любого простого числа $p = 4n + 1$, где $n \in \boldsymbol{N}$, существует такое целое число m, что $m^2 + 1$ кратно p.*

Лемма 2. *Любой простой делитель p числа $m^2 + 1$, где m – целое, представим в виде суммы квадратов двух натуральных чисел.*

Упражнение 9. Пользуясь формулой (1), объясните, почему в лемме 2 слова «любой простой» можно заменить на «любой натуральный».

Лемму 1 мы выведем из теоремы Вильсона (1741–1793), лемму 2 – из теории делимости целых гауссовых чисел. Но сначала сформулируем ответ на один важный вопрос.

Какие натуральные числа – суммы двух квадратов?

По теоремам 3 и 4, простое число $p > 2$ не представимо в виде суммы двух квадратов, если оно имеет вид $p = 4k + 3$, и представимо – если $p = 4k + 1$, где k – целое. Вспомнив формулу (1) и применив (еще не доказанную нами) теорему 2, получаем следующий элегантный критерий: *натуральное число представимо в виде суммы квадратов двух целых чисел тогда и только тогда, когда в его разложение на простые множители любой простой множитель вида $4k + 3$ входит в четной степени.*

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

Упражнения

10. Докажите, что 15 не представимо в виде суммы квадратов двух рациональных чисел. (Этот факт упомянут в «Арифметике» древнегреческого математика Диофанта.)

11. Выведите из критерия представимости числа в виде суммы двух квадратов, что если сумма квадратов $x^2 + y^2$ целых чисел кратна p^{2s-1}, где s – натуральное число, p – простое число, которое при делении на 4 дает остаток 3, то числа x и y кратны p^s.

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

13. а) Для любого делителя d числа $n^2 + 1$, где $n \in \boldsymbol{N}$, существует бесконечно много таких $m \in \boldsymbol{N}$, что $m^2 + 1$ кратно d. Докажите это. б) Сколько существует натуральных чисел $n < 1000$, для которых $n^2 + 1$ кратно 65?

14. Из леммы 2 и теоремы 3 выведите, что число вида $n^2 + 1$, где $n \in \boldsymbol{N}$, не имеет ни одного делителя вида $4k - 1$, где $k \in \boldsymbol{N}$.

15. Докажите, что если x, y, z – целые числа и $4xy - x - y = z^2$, то $x \le 0$ и $y \le 0$. (Это упражнение придумал Л. Эйлер.)

16. 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 $x^2y^2 = x^2 + y^2 + z^2$.

Доказательство леммы 1

В качестве числа m в лемме 1 годится $m = (2n)!$, т. е. произведение первых $2n$ натуральных чисел. Чтобы это увидеть, рассмотрим число

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

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

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

Значит, $m^2 + 1$ при делении на p дает такой же остаток, как и число $(p - 1)! + 1$. Последнее число кратно p по теореме Вильсона, которая впервые была сформулирована англичанином Эдуардом Варингом (1734–1798), а доказана французом Жозефом Луи Лагранжем (1736–1813).

Теорема Вильсона. *Для любого простого числа p сумма $(p - 1)! + 1$ кратна p. (Другими словами, произведение $1 \cdot 2 \cdot \ldots \cdot (p-1)$ дает остаток $(p-1)$ при делении на p.)*

Доказательство этой теоремы можно узнать, например, из статьи А. Егорова и А. Котовой «Необыкновенные арифметики» (Приложение к журналу «Квант» № 2 за 1994 год).

Итак, мы вывели лемму 1 из теоремы Вильсона. Идея доказательства леммы 2 – разложение на множители $m^2 + 1 = (m + i)(m - i)$. Что такое i и что делать дальше, вы узнаете, когда познакомитесь с комплексными числами.

Упражнения

17. Докажите, что числа а) $97! \cdot 1901! - 1$; б) $98! \cdot 1900!+1$ кратны 1999. *Указание.* 1999 – простое число.

18. Если p – простое число, $p > 2$, $m = ((p - 1)/2)!$, то $m^2 \equiv (-1)^{(p+1)/2} (\operatorname{mod} p)$, 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.

19. Докажите, что а) если составное число $n > 4$, то $(n - 1)!$ кратно n; б) если $(n - 1)! + 1$ кратно n, где $n > 1$ – натуральное число, то n – простое.

Комплексные числа

Что нам стоит дом построить?
Нарисуем – будем жить!

Что такое комплексное число?

Новые числа в математике вводят, когда старых оказывается недостаточно. Изобретение целых чисел, т. е. расширение множества $\boldsymbol{N} = \{1, 2, 3,\ldots\}$ натуральных чисел до множества $\boldsymbol{Z} = \{\ldots, -2, -1, 0, 1, 2,\ldots\}$, дает возможность решить, например, уравнение $x + 7 = 5$. Построив еще более широкое множество $\boldsymbol{Q} = \{\frac{m}{n} \mid m \in \boldsymbol{Z},\ n \in \boldsymbol{N}\}$ рациональных чисел, мы 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