Теорема 9. *Никакое простое число не может быть представлено в виде суммы квадратов двух целых чисел существенно разными (т. е. 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 8.

Упражнение 34 (М1288*). Докажите, что число $1000009 = 235^2 + 972^2$ составное.

Можно обойтись в доказательстве теоремы 9 и без комплексных чисел. Предположим, что простое число p двумя существенно разными (т. е. отличающимися не только порядком слагаемых) способами разложено в сумму квадратов натуральных чисел:

$$p = a^2 + b^2 = c^2 + d^2.$$

Тогда $a^2 \equiv -b^2$ и $c^2 \equiv -d^2 \pmod p$. Следовательно, $a^2c^2 \equiv \equiv \left(-b^2\right)\left(-d^2\right) \pmod p$, т. е. число $a^2c^2 - b^2d^2$ кратно p. (Если рассуждения со сравнениями по модулю p непривычны и потому подозрительны, вы можете получить то же самое, рассматривая тождество $a^2c^2 - b^2d^2 = a^2\left(c^2 + d^2\right) - \left(a^2 + b^2\right)d^2$.)

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 (1):

$$p^2 = (ac + bd)^2 + (ad - bc)^2.$$

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 $p^2 = (ac - bd)^2 + (ad + bc)^2$.

Упражнение 35. Представьте число $1000009 = 235^2 + 972^2$ в виде произведения двух отличных от 1 натуральных чисел.

Итак, простое число нельзя двумя существенно разными способами представить в виде суммы квадратов двух натуральных чисел. Число, единственным образом представимое в виде суммы квадратов двух натуральных чисел, не всегда является простым: $10 = 1^2 + 3^2$, $25 = 3^2 + 4^2$. Легко сформулировать условия, при которых число имеет единственное представление в виде суммы двух квадратов. Но давайте не будем тратить на это свои силы, а ответим на более общий вопрос.

Сколькими способами число можно представить в виде суммы двух квадратов?

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

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

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

Следующий пример – число 25. Тот, кто решил упражнение 1, знает, что 25 – наименьшее число, двумя способами представимое в виде суммы квадратов двух целых чисел. Оба эти разложения легко получить, поразному 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 сопряженные множители. Поэтому разложим рассматриваемое число сначала на простые натуральные, а затем и на простые гауссовы множители:

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

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

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

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

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

или

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

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

Аналогично можно найти число представлений в виде суммы двух квадратов любого натурального числа $n = 2^a p_1^{a_1} \ldots p_r^{a_r} Q$, где $p_1, \ldots, p_r$ – попарно различные простые числа, каждое из которых дает остаток 1 при делении на 4, Q – число, не имеющее простых делителей кроме тех, которые дают остаток 3 при делении на 4. А именно, если Q не является точным квадратом, то n не представимо в виде суммы двух квадратов; если же Q – точный квадрат, то, применив необходимое число раз теорему 2, получаем: количество представлений числа n в виде суммы двух квадратов равно количеству представлений числа $m = 2^a p_1^{a_1} \ldots p_r^{a_r}$ в виде суммы двух квадратов. Формулу для этого количества нашел немец Петер Густав Лежен Дирихле (1805–1859).

Теорема 10. *Количество представлений числа m в виде суммы квадратов двух целых чисел равно $[(a_1 + 1) \cdot \ldots \ldots \cdot (a_r + 1) + 1)/2]$. (Если число сомножителей равно 0, то произведение считается равным 1. Представления, отличающиеся порядком слагаемых, не различаются.)*