Суммы двух квадратов

Тутубалина А. А.

Какие числа представимы в виде суммы двух квадратов?

Лемма 1

Если числа x, y представимы в виде суммы двух квадратов, то их произведение xy — тоже.

Какие числа представимы в виде суммы двух квадратов?

Лемма 1

Если числа x, y представимы в виде суммы двух квадратов, то их произведение xy — тоже.

Доказательство.

Верно равенство

$$\left(a^2+b^2\right)\left(c^2+d^2\right) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 =$$

$$= (a^2c^2 - 2abcd + b^2d^2) + (a^2d^2 + 2abcd + b^2c^2) = (ac-bd)^2 + (ad+bc)^2.$$

□

Какие числа представимы в виде суммы двух квадратов?

Лемма 1

Если числа x, y представимы в виде суммы двух квадратов, то их произведение xy — тоже.

Доказательство.

Верно равенство

$$\left(a^2+b^2\right)\left(c^2+d^2\right) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 =$$

$$= (a^2c^2 - 2abcd + b^2d^2) + (a^2d^2 + 2abcd + b^2c^2) = (ac-bd)^2 + (ad+bc)^2.$$

□

Значит, в первую очередь нужно разобраться с простыми числами.

Какие числа представимы в виде суммы двух квадратов?

Лемма 1

Если числа x, y представимы в виде суммы двух квадратов, то их произведение xy — тоже.

Доказательство.

Верно равенство

$$\left(a^2+b^2\right)\left(c^2+d^2\right) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 =$$

$$= \left(a^2c^2 - 2abcd + b^2d^2\right) + \left(a^2d^2 + 2abcd + b^2c^2\right) = (ac-bd)^2 + (ad+bc)^2.$$

□

Значит, в первую очередь нужно разобраться с простыми числами.

$p = x^2 + y^2$	$p \neq x^2 + y^2$

Какие числа представимы в виде суммы двух квадратов?

Лемма 1

Если числа x, y представимы в виде суммы двух квадратов, то их произведение xy — тоже.

Доказательство.

Верно равенство

$$\left(a^2+b^2\right)\left(c^2+d^2\right) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 =$$

$$= (a^2c^2 - 2abcd + b^2d^2) + (a^2d^2 + 2abcd + b^2c^2) = (ac-bd)^2 + (ad+bc)^2.$$

□

Значит, в первую очередь нужно разобраться с простыми числами.

$p = x^2 + y^2$	$p \neq x^2 + y^2$
	3

Какие числа представимы в виде суммы двух квадратов?

Лемма 1

Если числа x, y представимы в виде суммы двух квадратов, то их произведение xy — тоже.

Доказательство.

Верно равенство

$$\left(a^2+b^2\right)\left(c^2+d^2\right) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 =$$

$$= (a^2c^2 - 2abcd + b^2d^2) + (a^2d^2 + 2abcd + b^2c^2) = (ac-bd)^2 + (ad+bc)^2.$$

□

Значит, в первую очередь нужно разобраться с простыми числами.

$p = x^2 + y^2$	$p \neq x^2 + y^2$
5	3

Какие числа представимы в виде суммы двух квадратов?

Лемма 1

Если числа x, y представимы в виде суммы двух квадратов, то их произведение xy — тоже.

Доказательство.

Верно равенство

$$\left(a^2+b^2\right)\left(c^2+d^2\right) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 =$$

$$= (a^2c^2 - 2abcd + b^2d^2) + (a^2d^2 + 2abcd + b^2c^2) = (ac-bd)^2 + (ad+bc)^2.$$

□

Значит, в первую очередь нужно разобраться с простыми числами.

$p = x^2 + y^2$	$p \neq x^2 + y^2$
5	3
	7

Какие числа представимы в виде суммы двух квадратов?

Лемма 1

Если числа x, y представимы в виде суммы двух квадратов, то их произведение xy — тоже.

Доказательство.

Верно равенство

$$\left(a^2+b^2\right)\left(c^2+d^2\right) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 =$$

$$= (a^2c^2 - 2abcd + b^2d^2) + (a^2d^2 + 2abcd + b^2c^2) = (ac-bd)^2 + (ad+bc)^2.$$

□

Значит, в первую очередь нужно разобраться с простыми числами.

$p = x^2 + y^2$	$p \neq x^2 + y^2$
5	3
	7
	11

Какие числа представимы в виде суммы двух квадратов?

Лемма 1

Если числа x, y представимы в виде суммы двух квадратов, то их произведение xy — тоже.

Доказательство.

Верно равенство

$$\left(a^2+b^2\right)\left(c^2+d^2\right) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 =$$

$$= (a^2c^2 - 2abcd + b^2d^2) + (a^2d^2 + 2abcd + b^2c^2) = (ac-bd)^2 + (ad+bc)^2.$$

□

Значит, в первую очередь нужно разобраться с простыми числами.

$p = x^2 + y^2$	$p \neq x^2 + y^2$
5	3
13	7
	11

Какие числа представимы в виде суммы двух квадратов?

Лемма 1

Если числа x, y представимы в виде суммы двух квадратов, то их произведение xy — тоже.

Доказательство.

Верно равенство

$$\left(a^2+b^2\right)\left(c^2+d^2\right) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 =$$

$$= (a^2c^2 - 2abcd + b^2d^2) + (a^2d^2 + 2abcd + b^2c^2) = (ac-bd)^2 + (ad+bc)^2.$$

□

Значит, в первую очередь нужно разобраться с простыми числами.

$p = x^2 + y^2$	$p \neq x^2 + y^2$
5	3
13	7
17	11

Какие числа представимы в виде суммы двух квадратов?

Лемма 1

Если числа x, y представимы в виде суммы двух квадратов, то их произведение xy — тоже.

Доказательство.

Верно равенство

$$\left(a^2+b^2\right)\left(c^2+d^2\right) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 =$$

$$= \left(a^2c^2 - 2abcd + b^2d^2\right) + \left(a^2d^2 + 2abcd + b^2c^2\right) = (ac-bd)^2 + (ad+bc)^2.$$

□

Значит, в первую очередь нужно разобраться с простыми числами.

$p = x^2 + y^2$	$p \neq x^2 + y^2$
5	3
13	7
17	11
	19

Какие числа представимы в виде суммы двух квадратов?

Лемма 1

Если числа x, y представимы в виде суммы двух квадратов, то их произведение xy — тоже.

Доказательство.

Верно равенство

$$\left(a^2+b^2\right)\left(c^2+d^2\right) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 =$$

$$= (a^2c^2 - 2abcd + b^2d^2) + (a^2d^2 + 2abcd + b^2c^2) = (ac-bd)^2 + (ad+bc)^2.$$

□

Значит, в первую очередь нужно разобраться с простыми числами.

$p = x^2 + y^2$	$p \neq x^2 + y^2$
5	3
13	7
17	11
	19
	23

Какие числа представимы в виде суммы двух квадратов?

Лемма 1

Если числа x, y представимы в виде суммы двух квадратов, то их произведение xy — тоже.

Доказательство.

Верно равенство

$$\left(a^2+b^2\right)\left(c^2+d^2\right) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 =$$

$$= (a^2c^2 - 2abcd + b^2d^2) + (a^2d^2 + 2abcd + b^2c^2) = (ac-bd)^2 + (ad+bc)^2.$$

□

Значит, в первую очередь нужно разобраться с простыми числами.

$p = x^2 + y^2$	$p \neq x^2 + y^2$
5	3
13	7
17	11
29	19
	23

Какие числа представимы в виде суммы двух квадратов?

Лемма 1

Если числа x, y представимы в виде суммы двух квадратов, то их произведение xy — тоже.

Доказательство.

Верно равенство

$$\left(a^2+b^2\right)\left(c^2+d^2\right) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 =$$

$$= \left(a^2c^2 - 2abcd + b^2d^2\right) + \left(a^2d^2 + 2abcd + b^2c^2\right) = (ac-bd)^2 + (ad+bc)^2.$$

□

Значит, в первую очередь нужно разобраться с простыми числами.

$p = x^2 + y^2$	$p \neq x^2 + y^2$
5	3
13	7
17	11
29	19
	23
	31

Какие числа представимы в виде суммы двух квадратов?

Лемма 1

Если числа x, y представимы в виде суммы двух квадратов, то их произведение xy — тоже.

Доказательство.

Верно равенство

$$\left(a^2+b^2\right)\left(c^2+d^2\right) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 =$$

$$= \left(a^2c^2 - 2abcd + b^2d^2\right) + \left(a^2d^2 + 2abcd + b^2c^2\right) = (ac-bd)^2 + (ad+bc)^2.$$

□

Значит, в первую очередь нужно разобраться с простыми числами.

$p = x^2 + y^2$	$p \neq x^2 + y^2$
5	3
13	7
17	11
29	19
37	23
	31

Какие числа представимы в виде суммы двух квадратов?

Лемма 1

Если числа x, y представимы в виде суммы двух квадратов, то их произведение xy — тоже.

Доказательство.

Верно равенство

$$\left(a^2+b^2\right)\left(c^2+d^2\right) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 =$$

$$= \left(a^2c^2 - 2abcd + b^2d^2\right) + \left(a^2d^2 + 2abcd + b^2c^2\right) = (ac-bd)^2 + (ad+bc)^2.$$

□

Значит, в первую очередь нужно разобраться с простыми числами.

$p = x^2 + y^2$	$p \neq x^2 + y^2$
5	3
13	7
17	11
29	19
37	23
41	31

Рождественская теорема Ферма

Утверждение 1

Натуральные числа вида $N = 4k + 3$ *не представимы в виде суммы двух квадратов:* $N \neq a^2 + b^2$ *для любых* $a, b \in \mathbb{N}$.

Рождественская теорема Ферма

Утверждение 1

Натуральные числа вида $N = 4k + 3$ не представимы в виде суммы двух квадратов: $N \neq a^2 + b^2$ для любых $a, b \in \mathbb{N}$.

Доказательство.

Посмотрим, какие остатки от деления на 4 могут давать квадраты:

a	0	1	2	3
a^2	0	1	0	1

Поэтому сумма двух квадратов может давать только остатки 0, 1 и 2 от деления на 4. □

Рождественская теорема Ферма

Утверждение 1

Натуральные числа вида $N = 4k + 3$ не представимы в виде суммы двух квадратов: $N \neq a^2 + b^2$ для любых $a, b \in \mathbb{N}$.

Доказательство.

Посмотрим, какие остатки от деления на 4 могут давать квадраты:

a	0	1	2	3
a^2	0	1	0	1

Поэтому сумма двух квадратов может давать только остатки 0, 1 и 2 от деления на 4. □

Теорема 1 (Ферма, Эйлер)

Любое простое число $p = 4k + 1$ (где $k \in \mathbb{N}$) представимо в виде суммы двух квадратов $p = a^2 + b^2$, где $a, b \in \mathbb{N}$.

Рождественская теорема Ферма

Утверждение 1

Натуральные числа вида $N = 4k + 3$ не представимы в виде суммы двух квадратов: $N \neq a^2 + b^2$ для любых $a, b \in \mathbb{N}$.

Доказательство.

Посмотрим, какие остатки от деления на 4 могут давать квадраты:

a	0	1	2	3
a^2	0	1	0	1

Поэтому сумма двух квадратов может давать только остатки 0, 1 и 2 от деления на 4. □

Теорема 1 (Ферма, Эйлер)

Любое простое число $p = 4k + 1$ (где $k \in \mathbb{N}$) представимо в виде суммы двух квадратов $p = a^2 + b^2$, где $a, b \in \mathbb{N}$.

Формулировка принадлежит Альберу Жирару (1625). Пьер Ферма в письме к Мерсенну (датировано 25.12.1640) привел более полную ее версию, описав количество представлений степеней простых в виде суммы двух квадратов.
Первое доказательство (методом бесконечного спуска) принадлежит Леонарду Эйлеру (1752-1755).

Доказательство «в одно предложение»

https://ru.wikipedia.org/wiki/Теорема_Ферма_–_Эйлера#Доказательства

Одно из самых коротких доказательств придумано немецким математиком Доном Цагиром[3]:

Инволюция конечного множества $S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$, определённая как

$$(x, y, z) \to \begin{cases} (x + 2z, z, y - x - z), & x < y - z \\ (2y - x, y, x - y + z), & y - z < x < 2y \\ (x - 2y, x - y + z, y), & x > 2y \end{cases}$$

имеет ровно одну неподвижную точку (а именно $(1, 1, k)$, так как $p = 4k + 1$ — простое), так что $|S|$ нечётно и инволюция $(x, y, z) \to (x, z, y)$ также имеет неподвижную точку.

Доказательство «в одно предложение»

https://ru.wikipedia.org/wiki/Теорема_Ферма_–_Эйлера#Доказательства

Одно из самых коротких доказательств придумано немецким математиком Доном Цагиром[3]:

Инволюция конечного множества $S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$, определённая как

$$(x, y, z) \to \begin{cases} (x + 2z, z, y - x - z), & x < y - z \\ (2y - x, y, x - y + z), & y - z < x < 2y \\ (x - 2y, x - y + z, y), & x > 2y \end{cases}$$

имеет ровно одну неподвижную точку (а именно $(1, 1, k)$, так как $p = 4k + 1$ — простое), так что $|S|$ нечётно и инволюция $(x, y, z) \to (x, z, y)$ также имеет неподвижную точку.

ЧТО???

Доказательство «в одно предложение»

Фиксируем простое число $p = 4k+1 \in \mathbb{N}$. Мы ищем решения $a, b \in \mathbb{N}$ диофантова уравнения

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

Доказательство «в одно предложение»

Фиксируем простое число $p = 4k+1 \in \mathbb{N}$. Мы ищем решения $a, b \in \mathbb{N}$ диофантова уравнения

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

Поскольку p нечетно, то один из квадратов четный, а другой — нет. Будем считать, что a нечетно, а $b = 2B$:

$$a^2 + 4B^2 = p.$$

Доказательство «в одно предложение»

Фиксируем простое число $p = 4k+1 \in \mathbb{N}$. Мы ищем решения $a, b \in \mathbb{N}$ диофантова уравнения

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

Поскольку p нечетно, то один из квадратов четный, а другой — нет. Будем считать, что a нечетно, а $b = 2B$:

$$a^2 + 4B^2 = p.$$

Вместо этого диофантова уравнения рассмотрим другое:

$$x^2 + 4yz = p.$$

Доказательство «в одно предложение»

Фиксируем простое число $p = 4k+1 \in \mathbb{N}$. Мы ищем решения $a, b \in \mathbb{N}$ диофантова уравнения

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

Поскольку p нечетно, то один из квадратов четный, а другой — нет. Будем считать, что a нечетно, а $b = 2B$:

$$a^2 + 4B^2 = p.$$

Вместо этого диофантова уравнения рассмотрим другое:

$$x^2 + 4yz = p.$$

Пусть $S = \{(x, y, z) \mid x^2 + 4yz = p;\ x, y, z \in \mathbb{N}\}$ — множество его натуральных решений.

Доказательство «в одно предложение»

Фиксируем простое число $p = 4k+1 \in \mathbb{N}$. Мы ищем решения $a, b \in \mathbb{N}$ диофантова уравнения

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

Поскольку p нечетно, то один из квадратов четный, а другой — нет. Будем считать, что a нечетно, а $b = 2B$:

$$a^2 + 4B^2 = p.$$

Вместо этого диофантова уравнения рассмотрим другое:

$$x^2 + 4yz = p.$$

Пусть $S = \{(x, y, z) \mid x^2 + 4yz = p;\ x, y, z \in \mathbb{N}\}$ — множество его натуральных решений.

Оно конечно (поскольку $x, y, z \leq p$) и непусто (так как $x = y = 1, z = k$ является решением).

Доказательство «в одно предложение»

Фиксируем простое число $p = 4k+1 \in \mathbb{N}$. Мы ищем решения $a, b \in \mathbb{N}$ диофантова уравнения

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

Поскольку p нечетно, то один из квадратов четный, а другой — нет. Будем считать, что a нечетно, а $b = 2B$:

$$a^2 + 4B^2 = p.$$

Вместо этого диофантова уравнения рассмотрим другое:

$$x^2 + 4yz = p.$$

Пусть $S = \{(x, y, z) \mid x^2 + 4yz = p;\ x, y, z \in \mathbb{N}\}$ — множество его натуральных решений.

Оно конечно (поскольку $x, y, z \leq p$) и непусто (так как $x = y = 1, z = k$ является решением).

Все решения из множества S можно разбить на пары, получающиеся друг из друга заменой y на z, а z на y.

Доказательство «в одно предложение»

Фиксируем простое число $p = 4k+1 \in \mathbb{N}$. Мы ищем решения $a, b \in \mathbb{N}$ диофантова уравнения

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

Поскольку p нечетно, то один из квадратов четный, а другой — нет. Будем считать, что a нечетно, а $b = 2B$:

$$a^2 + 4B^2 = p.$$

Вместо этого диофантова уравнения рассмотрим другое:

$$x^2 + 4yz = p.$$

Пусть $S = \{(x, y, z) \mid x^2 + 4yz = p;\ x, y, z \in \mathbb{N}\}$ — множество его натуральных решений.

Оно конечно (поскольку $x, y, z \leq p$) и непусто (так как $x = y = 1, z = k$ является решением).

Все решения из множества S можно разбить на пары, получающиеся друг из друга заменой y на z, а z на y.

Без пары может остаться только решение, в котором $y = z$, а тогда как раз получится $x^2 + 4y^2 = p$.

Доказательство «в одно предложение»

Фиксируем простое число $p = 4k+1 \in \mathbb{N}$. Мы ищем решения $a, b \in \mathbb{N}$ диофантова уравнения

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

Поскольку p нечетно, то один из квадратов четный, а другой — нет. Будем считать, что a нечетно, а $b = 2B$:

$$a^2 + 4B^2 = p.$$

Вместо этого диофантова уравнения рассмотрим другое:

$$x^2 + 4yz = p.$$

Пусть $S = \{(x, y, z) \mid x^2 + 4yz = p;\ x, y, z \in \mathbb{N}\}$ — множество его натуральных решений.

Оно конечно (поскольку $x, y, z \leq p$) и непусто (так как $x = y = 1, z = k$ является решением).

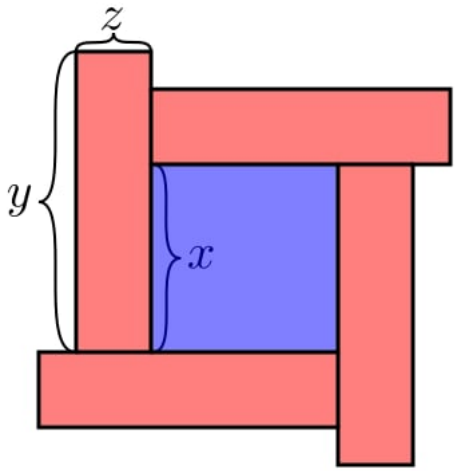
Все решения из множества S можно разбить на пары, получающиеся друг из друга заменой y на z, а z на y.

Без пары может остаться только решение, в котором $y = z$, а тогда как раз получится $x^2 + 4y^2 = p$.

Оказывается, в множестве S нечетное число решений, а значит какое-то из них обязательно останется без пары. Докажем это.

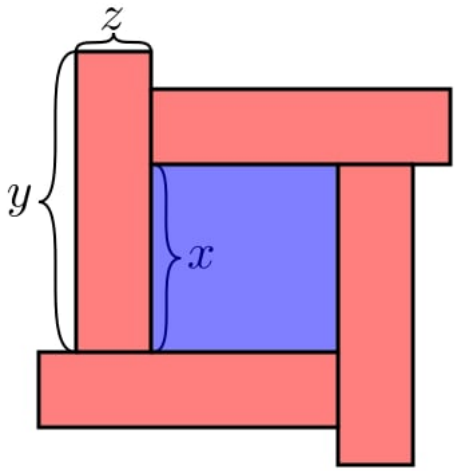
Доказательство «в одно предложение»

Все элементы множества $S = \{(x, y, z) \mid x^2 + 4yz = p;\ x, y, z \in \mathbb{N}\}$ можно изобразить на клетчатой бумаге в виде «крылатых квадратов» площади p.

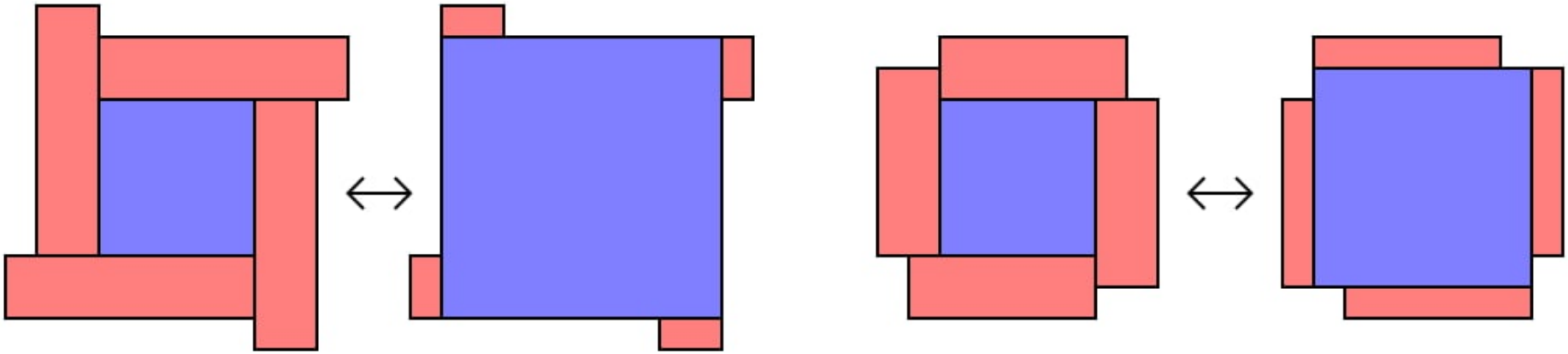


Доказательство «в одно предложение»

Все элементы множества $S = \{(x, y, z) \mid x^2 + 4yz = p;\ x, y, z \in \mathbb{N}\}$ можно изобразить на клетчатой бумаге в виде «крылатых квадратов» площади p.

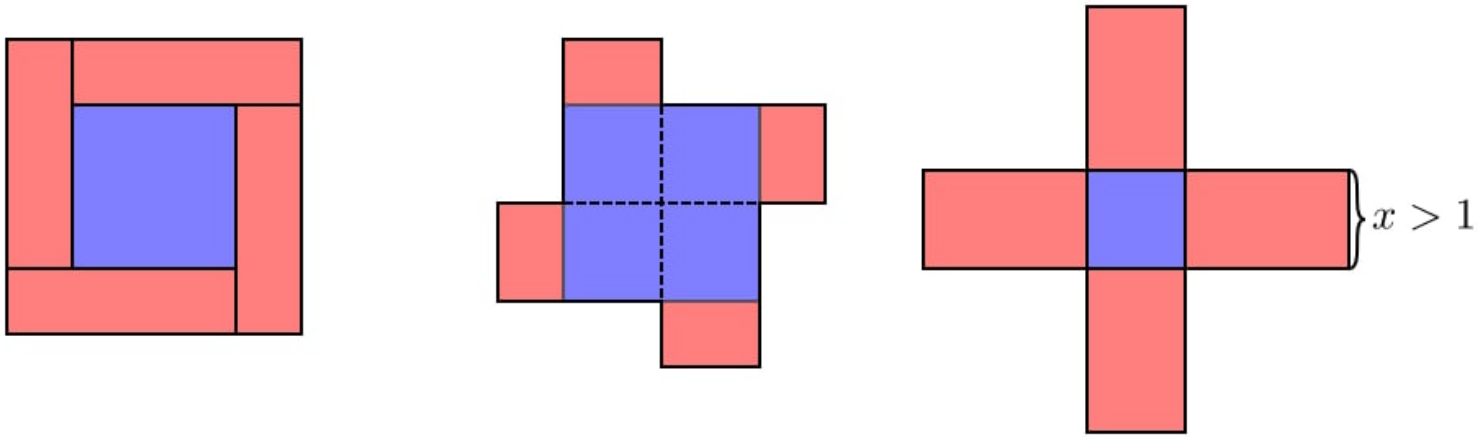


Их можно разбить на пары одной формы:



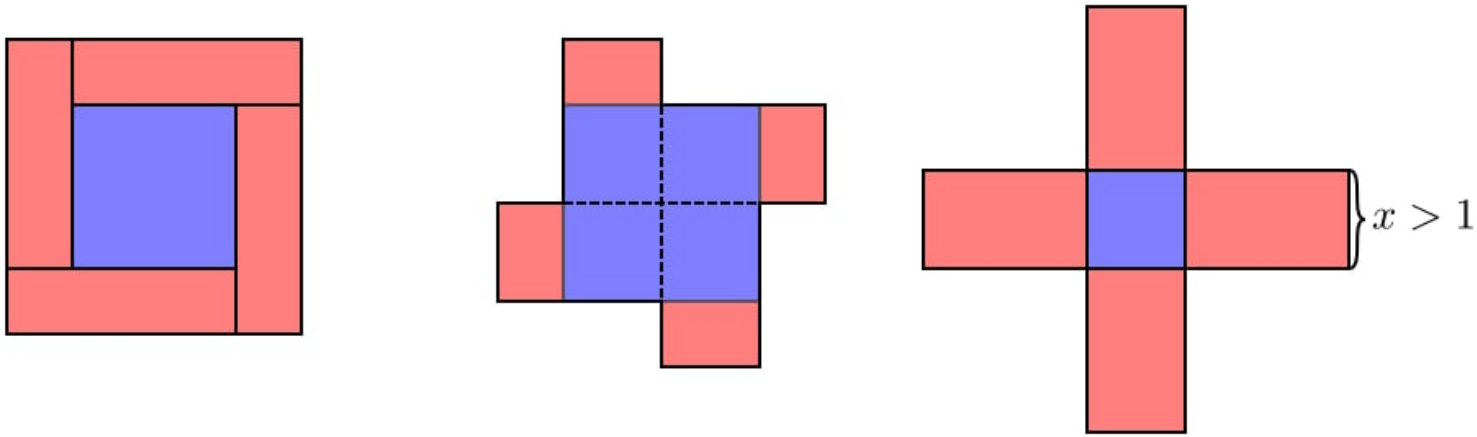
Доказательство «в одно предложение»

Поскольку p — простое число, и x нечетно, то следующие случаи невозможны:

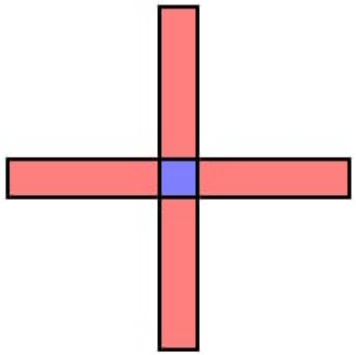


Доказательство «в одно предложение»

Поскольку p — простое число, и x нечетно, то следующие случаи невозможны:

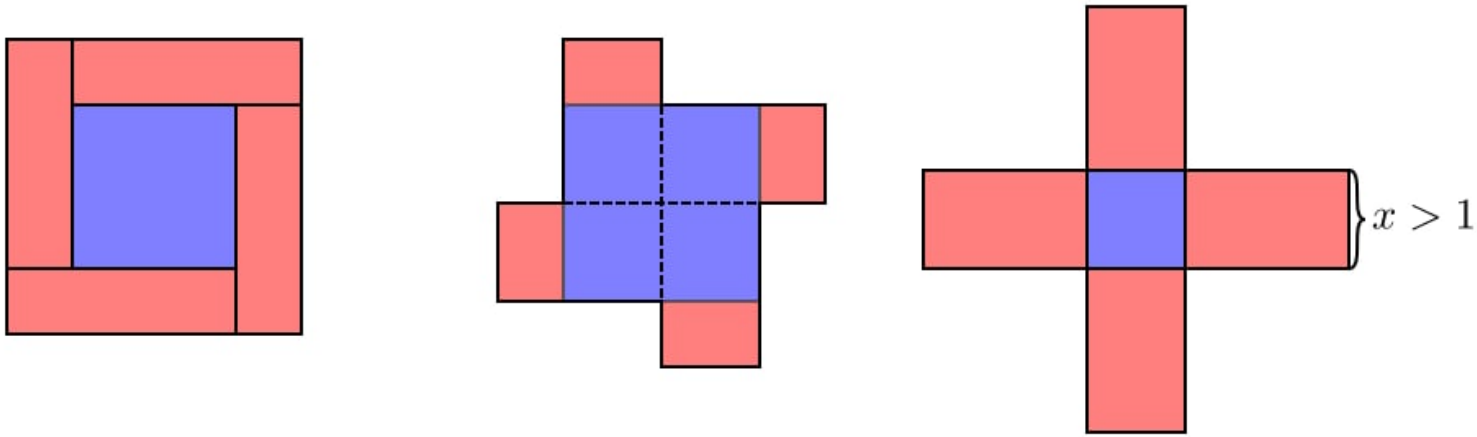


Поэтому без пары остается только крылатый квадрат, соответствующий решению $(1, 1, k)$

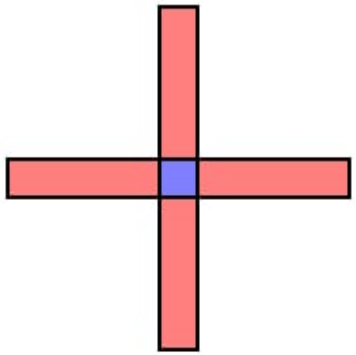


Доказательство «в одно предложение»

Поскольку p — простое число, и x нечетно, то следующие случаи невозможны:



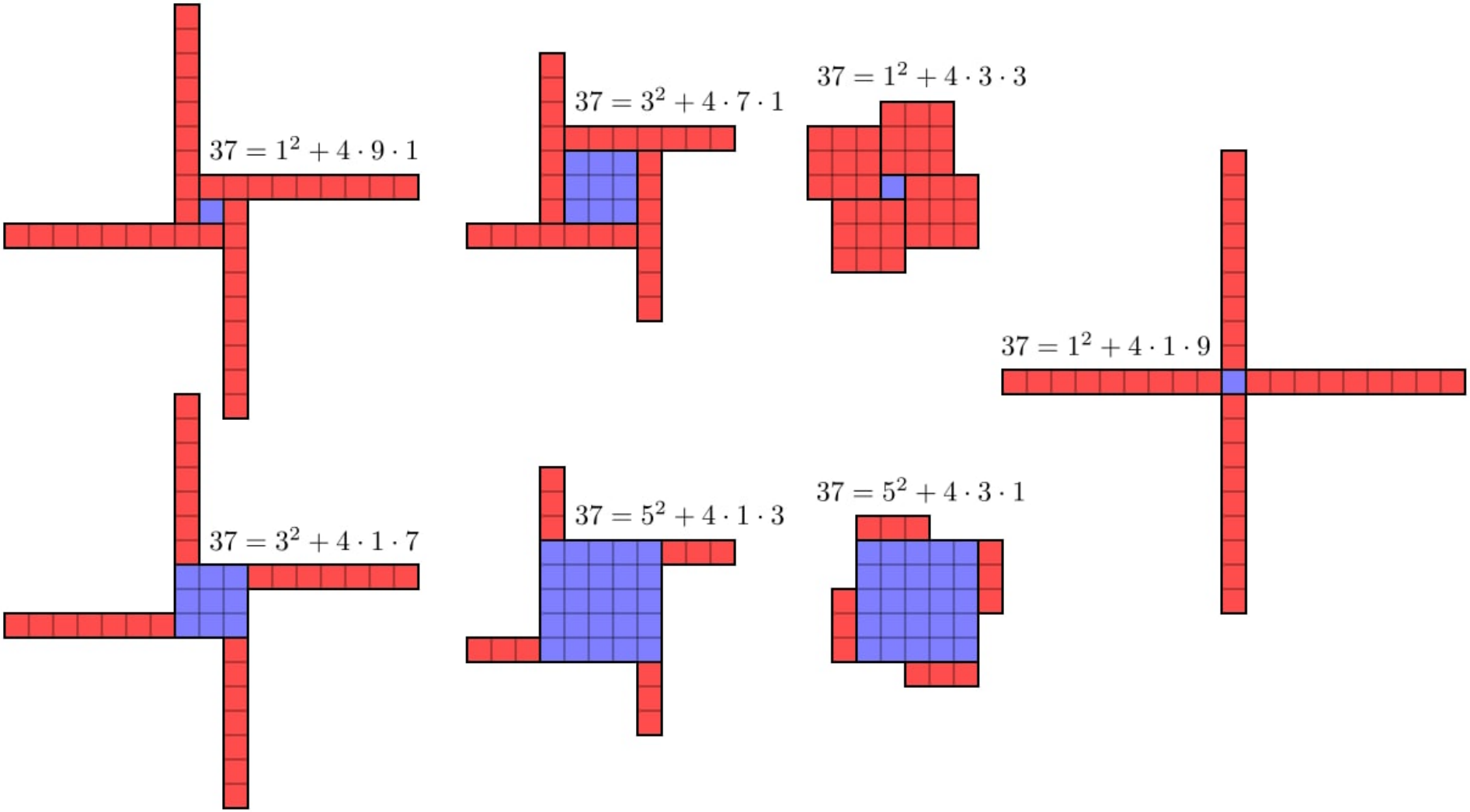
Поэтому без пары остается только крылатый квадрат, соответствующий решению $(1, 1, k)$



Значит, число крылатых квадратов (и число решений уравнения $x^2 + 4yz = p$) нечетно, что и требовалось доказать.

Доказательство «в одно предложение»

Пример для $p = 37$



Теорема 2

Пусть число $N \in \mathbb{N}$ раскладывается на простые множители следующим образом:

$$N = 2^s p_1^{\alpha_1} \dots p_m^{\alpha_m} q_1^{\beta_1} \dots q_r^{\beta_r},$$

где p_i — простые числа вида $4k+1$, а q_i — простые числа вида $4k+3$.
Число N представимо в виде суммы двух квадратов целых чисел в том и только том случае, когда все β_i четные.

Теорема 2

Пусть число $N \in \mathbb{N}$ раскладывается на простые множители следующим образом:

$$N = 2^s p_1^{\alpha_1} \dots p_m^{\alpha_m} q_1^{\beta_1} \dots q_r^{\beta_r},$$

где p_i — простые числа вида $4k+1$, а q_i — простые числа вида $4k+3$.
Число N представимо в виде суммы двух квадратов целых чисел в том и только том случае, когда все β_i четные.

Доказательство.

Поскольку числа $2, p_i$ и q_i^2 представимы в виде суммы двух квадратов, то и их произведение представимо в виде суммы двух квадратов.

Представление чисел в виде суммы двух квадратов

Тут уже пошло что-то страшное и непонятное, можно дальше не читать.

Доказательство.

$$N = 2^s p_1^{\alpha_1} \dots p_m^{\alpha_m} q_1^{\beta_1} \dots q_r^{\beta_r}$$

Представление чисел в виде суммы двух квадратов

Тут уже пошло что-то страшное и непонятное, можно дальше не читать.

Доказательство.

$$N = 2^s p_1^{\alpha_1} \dots p_m^{\alpha_m} q_1^{\beta_1} \dots q_r^{\beta_r}$$

В обратную сторону, пусть $N = x^2 + y^2$. Рассмотрим $q = q_i$ (для любого $i \in \{1, \dots, r\}$), $q = 4k + 3$. Тогда $x^2 \equiv -y^2 (\mathrm{mod}\, q)$.

Представление чисел в виде суммы двух квадратов

Тут уже пошло что-то страшное и непонятное, можно дальше не читать.

Доказательство.

$$N = 2^s p_1^{\alpha_1} \dots p_m^{\alpha_m} q_1^{\beta_1} \dots q_r^{\beta_r}$$

В обратную сторону, пусть $N = x^2 + y^2$. Рассмотрим $q = q_i$ (для любого $i \in \{1, \dots, r\}$), $q = 4k + 3$. Тогда $x^2 \equiv -y^2 (\mathrm{mod}\, q)$.

- $y \not\equiv 0 (\mathrm{mod}\, q)$.

Представление чисел в виде суммы двух квадратов

Тут уже пошло что-то страшное и непонятное, можно дальше не читать.

Доказательство.

$$N = 2^s p_1^{\alpha_1} \dots p_m^{\alpha_m} q_1^{\beta_1} \dots q_r^{\beta_r}$$

В обратную сторону, пусть $N = x^2 + y^2$. Рассмотрим $q = q_i$ (для любого $i \in \{1, \dots, r\}$), $q = 4k + 3$. Тогда $x^2 \equiv -y^2 (\mathrm{mod}\, q)$. Есть два варианта:

- $y \not\equiv 0 (\mathrm{mod}\, q)$. Тогда $\left(\frac{x}{y}\right)^2 \equiv -1 (\mathrm{mod}\, q)$.

Представление чисел в виде суммы двух квадратов

Тут уже пошло что-то страшное и непонятное, можно дальше не читать.

Доказательство.

$$N = 2^s p_1^{\alpha_1} \dots p_m^{\alpha_m} q_1^{\beta_1} \dots q_r^{\beta_r}$$

В обратную сторону, пусть $N = x^2 + y^2$. Рассмотрим $q = q_i$ (для любого $i \in \{1, \dots, r\}$), $q = 4k + 3$. Тогда $x^2 \equiv -y^2 (\mathrm{mod}\, q)$. Есть два варианта:

- $y \not\equiv 0 (\mathrm{mod}\, q)$. Тогда $\left(\frac{x}{y}\right)^2 \equiv -1 (\mathrm{mod}\, q)$. Возведем обе половины сравнения в степень $2k + 1$:

$$\left(\frac{x}{y}\right)^{q-1} \equiv \left(\frac{x}{y}\right)^{4k+2} \equiv (-1)^{2k+1} = -1 (\mathrm{mod}\, q).$$

Тут уже пошло что-то страшное и непонятное, можно дальше не читать.

Доказательство.

$$N = 2^s p_1^{\alpha_1} \dots p_m^{\alpha_m} q_1^{\beta_1} \dots q_r^{\beta_r}$$

В обратную сторону, пусть $N = x^2 + y^2$. Рассмотрим $q = q_i$ (для любого $i \in \{1, \dots, r\}$), $q = 4k + 3$. Тогда $x^2 \equiv -y^2 (\mathrm{mod}\, q)$. Есть два варианта:

- $y \not\equiv 0 (\mathrm{mod}\, q)$. Тогда $\left(\frac{x}{y}\right)^2 \equiv -1 (\mathrm{mod}\, q)$. Возведем обе половины сравнения в степень $2k + 1$:

$$\left(\frac{x}{y}\right)^{q-1} \equiv \left(\frac{x}{y}\right)^{4k+2} \equiv (-1)^{2k+1} = -1 (\mathrm{mod}\, q).$$

  Это противоречит малой теореме Ферма, согласно которой $a^{q-1} \equiv 1 (\mathrm{mod}\, q)$ для любого a, не делящегося на q. Следовательно, такой вариант невозможен.

Тут уже пошло что-то страшное и непонятное, можно дальше не читать.

Доказательство.

$$N = 2^s p_1^{\alpha_1} \dots p_m^{\alpha_m} q_1^{\beta_1} \dots q_r^{\beta_r}$$

В обратную сторону, пусть $N = x^2 + y^2$. Рассмотрим $q = q_i$ (для любого $i \in \{1, \dots, r\}$), $q = 4k + 3$. Тогда $x^2 \equiv -y^2 (\mathrm{mod}\, q)$. Есть два варианта:

- $y \not\equiv 0 (\mathrm{mod}\, q)$. Тогда $\left(\frac{x}{y}\right)^2 \equiv -1 (\mathrm{mod}\, q)$. Возведем обе половины сравнения в степень $2k + 1$:

$$\left(\frac{x}{y}\right)^{q-1} \equiv \left(\frac{x}{y}\right)^{4k+2} \equiv (-1)^{2k+1} = -1 (\mathrm{mod}\, q).$$

  Это противоречит малой теореме Ферма, согласно которой $a^{q-1} \equiv 1 (\mathrm{mod}\, q)$ для любого a, не делящегося на q. Следовательно, такой вариант невозможен.

- $x \equiv y \equiv 0 (\mathrm{mod}\, q)$.

Представление чисел в виде суммы двух квадратов

Тут уже пошло что-то страшное и непонятное, можно дальше не читать.

Доказательство.

$$N = 2^s p_1^{\alpha_1} \dots p_m^{\alpha_m} q_1^{\beta_1} \dots q_r^{\beta_r}$$

В обратную сторону, пусть $N = x^2 + y^2$. Рассмотрим $q = q_i$ (для любого $i \in \{1, \dots, r\}$), $q = 4k + 3$. Тогда $x^2 \equiv -y^2 (\mathrm{mod}\, q)$. Есть два варианта:

- $y \not\equiv 0 (\mathrm{mod}\, q)$. Тогда $\left(\frac{x}{y}\right)^2 \equiv -1 (\mathrm{mod}\, q)$. Возведем обе половины сравнения в степень $2k + 1$:

$$\left(\frac{x}{y}\right)^{q-1} \equiv \left(\frac{x}{y}\right)^{4k+2} \equiv (-1)^{2k+1} = -1 (\mathrm{mod}\, q).$$

  Это противоречит малой теореме Ферма, согласно которой $a^{q-1} \equiv 1 (\mathrm{mod}\, q)$ для любого a, не делящегося на q. Следовательно, такой вариант невозможен.

- $x \equiv y \equiv 0 (\mathrm{mod}\, q)$. Тогда $x = qx', y = qy'$ и

$$N = q^2 \left(x'^2 + y'^2\right), N = q^2 N', N' = x'^2 + y'^2.$$

□

Представление чисел в виде суммы двух квадратов

Тут уже пошло что-то страшное и непонятное, можно дальше не читать.

Доказательство.

$$N = 2^s p_1^{\alpha_1} \dots p_m^{\alpha_m} q_1^{\beta_1} \dots q_r^{\beta_r}$$

В обратную сторону, пусть $N = x^2 + y^2$. Рассмотрим $q = q_i$ (для любого $i \in \{1, \dots, r\}$), $q = 4k + 3$. Тогда $x^2 \equiv -y^2 (\mathrm{mod}\, q)$. Есть два варианта:

- $y \not\equiv 0 (\mathrm{mod}\, q)$. Тогда $\left(\frac{x}{y}\right)^2 \equiv -1 (\mathrm{mod}\, q)$. Возведем обе половины сравнения в степень $2k + 1$:

$$\left(\frac{x}{y}\right)^{q-1} \equiv \left(\frac{x}{y}\right)^{4k+2} \equiv (-1)^{2k+1} = -1 (\mathrm{mod}\, q).$$

  Это противоречит малой теореме Ферма, согласно которой $a^{q-1} \equiv 1 (\mathrm{mod}\, q)$ для любого a, не делящегося на q. Следовательно, такой вариант невозможен.

- $x \equiv y \equiv 0 (\mathrm{mod}\, q)$. Тогда $x = qx', y = qy'$ и

$$N = q^2 \left(x'^2 + y'^2\right), N = q^2 N', N' = x'^2 + y'^2.$$

  Если N' все еще делится на q, то таким же образом можно показать, что N' делится и на q^2, и так далее. Следовательно, q должен входить в разложение N в четной степени.

□

Теорема 3 (Лагранж)

Любое число $N \in \mathbb{N}$ представимо в виде суммы четырех квадратов целых чисел:

$$N = a^2 + b^2 + c^2 + d^2$$

Представление чисел в виде суммы четырех квадратов

Теорема 3 (Лагранж)

Любое число $N \in \mathbb{N}$ представимо в виде суммы четырех квадратов целых чисел:

$$N = a^2 + b^2 + c^2 + d^2$$

Лемма 2

Произведение двух сумм четырех квадратов тоже является суммой четырех квадратов.

Теорема 3 (Лагранж)

Любое число $N \in \mathbb{N}$ представимо в виде суммы четырех квадратов целых чисел:

$$N = a^2 + b^2 + c^2 + d^2$$

Лемма 2

Произведение двух сумм четырех квадратов тоже является суммой четырех квадратов.

$$\left(a^2 + b^2 + c^2 + d^2\right)\left(A^2 + B^2 + C^2 + D^2\right) =$$

$$= (aA+bB+cC+dD)^2+(aB-bA-cD+dC)^2+(aC+bD-cA-dB)^2+(aD-bC+cB-dA)^2$$

Представление чисел в виде суммы трех квадратов

Этот вопрос гораздо более сложный, чем предыдущие два. Одна из трудностей в том, что для сумм трех квадратов не существует аналогов лемм 1 и 2.

Представление чисел в виде суммы трех квадратов

Этот вопрос гораздо более сложный, чем предыдущие два. Одна из трудностей в том, что для сумм трех квадратов не существует аналогов лемм 1 и 2.
Действительно, $3 = 1^2 + 1^2 + 1^2, 5 = 2^2 + 1^2 + 0^2$, но $3 \cdot 5 = 15$ не представимо в виде суммы трех квадратов.

Представление чисел в виде суммы трех квадратов

Этот вопрос гораздо более сложный, чем предыдущие два. Одна из трудностей в том, что для сумм трех квадратов не существует аналогов лемм 1 и 2.
Действительно, $3 = 1^2 + 1^2 + 1^2, 5 = 2^2 + 1^2 + 0^2$, но $3 \cdot 5 = 15$ не представимо в виде суммы трех квадратов.

Лемма 3

Числа вида $4^l(8k + 7)$ не представимы в виде суммы трех квадратов.

Представление чисел в виде суммы трех квадратов

Этот вопрос гораздо более сложный, чем предыдущие два. Одна из трудностей в том, что для сумм трех квадратов не существует аналогов лемм 1 и 2.
Действительно, $3 = 1^2 + 1^2 + 1^2, 5 = 2^2 + 1^2 + 0^2$, но $3 \cdot 5 = 15$ не представимо в виде суммы трех квадратов.

Лемма 3

Числа вида $4^l(8k + 7)$ не представимы в виде суммы трех квадратов.

Доказательство.

Поскольку x^2 при делении на 4 может давать только остатки 0 и 1, то $a^2 + b^2 + c^2 \vdots 4 \Leftrightarrow a, b, c \vdots 2$. Значит, если число $4N$ представимо в виде суммы трех квадратов, то и число N тоже.

□

Представление чисел в виде суммы трех квадратов

Этот вопрос гораздо более сложный, чем предыдущие два. Одна из трудностей в том, что для сумм трех квадратов не существует аналогов лемм 1 и 2.
Действительно, $3 = 1^2 + 1^2 + 1^2, 5 = 2^2 + 1^2 + 0^2$, но $3 \cdot 5 = 15$ не представимо в виде суммы трех квадратов.

Лемма 3

Числа вида $4^l(8k + 7)$ не представимы в виде суммы трех квадратов.

Доказательство.

Поскольку x^2 при делении на 4 может давать только остатки 0 и 1, то $a^2 + b^2 + c^2 \vdots 4 \Leftrightarrow a, b, c \vdots 2$. Значит, если число $4N$ представимо в виде суммы трех квадратов, то и число N тоже.

При этом x^2 при делении на 8 может давать только остатки 0, 1 и 4, поэтому числа вида $8k + 7$ не представимы в виде суммы трех квадратов. □

Представление чисел в виде суммы трех квадратов

Этот вопрос гораздо более сложный, чем предыдущие два. Одна из трудностей в том, что для сумм трех квадратов не существует аналогов лемм 1 и 2.
Действительно, $3 = 1^2 + 1^2 + 1^2, 5 = 2^2 + 1^2 + 0^2$, но $3 \cdot 5 = 15$ не представимо в виде суммы трех квадратов.

Лемма 3

Числа вида $4^l(8k + 7)$ не представимы в виде суммы трех квадратов.

Доказательство.

Поскольку x^2 при делении на 4 может давать только остатки 0 и 1, то $a^2 + b^2 + c^2 \vdots 4 \Leftrightarrow a, b, c \vdots 2$. Значит, если число $4N$ представимо в виде суммы трех квадратов, то и число N тоже.

При этом x^2 при делении на 8 может давать только остатки 0, 1 и 4, поэтому числа вида $8k + 7$ не представимы в виде суммы трех квадратов. □

Теорема 4 (Лежандр, Дирихле, Гаусс)

Число N представимо в виде суммы трех квадратов тогда и только тогда, когда N не имеет вид $4^l(8k + 7)$.

Спасибо за внимание!