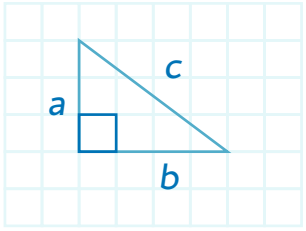
ПИФАГОРОВЫ ТРОЙКИ ОКОНЧАНИЕ

Продолжаем поиск пифагоровых троек, начатый на прошлом уроке.

Мы свели задачу о поиске таких целых взаимно простых a, b и c, что $a^2 + b^2 = c^2$, к поиску гауссовых чисел, таких что $(a + bi)(a - bi) = c^2$.



ДВА СЛУЧАЯ ДЛЯ $a + bi$

Нами доказано, что если НОД$(a, b, c) = 1$, то НОД$(a + bi, a - bi) = 1$.

Применяем следствие 1 из ОТА:

$$a + bi = \left\{ \begin{matrix} 1 \\ i \\ -1 \\ -i \end{matrix} \right\} \cdot (m + ni)^2$$

Так как $1 = 1^2$, $-1 = i^2$, фактически имеем два случая: $a + bi = (m + ni)^2$ и $a + bi = i(m + ni)^2$.

Приступаем к выводу формул.

1-й случай: $a + bi = (m + ni)^2$

$a + bi = m^2 + 2mni - n^2 \Rightarrow$

$a = m^2 - n^2$, $b = 2mn$.

2-й случай: $a + bi = i(m + ni)^2$

$a + bi = i(m^2 - n^2) - 2mn \Rightarrow$

$b = m^2 - n^2$, $a = -2mn$.

Это повтор предыдущего при замене a на b, m на — n (катеты равноправны, а m и n мы все равно выбираем так, чтобы $a, b > 0$).

ФОРМУЛЫ ДЛЯ ПИФАГОРОВЫХ ТРОЕК

Итак, мы получили формулы для пифагоровых троек: Если a, b и c — пифагорова тройка, и НОД$(a,b,c) = 1$, то:

$a = m^2 - n^2$

$b = 2mn$

$c = m^2 + n^2$, где $m, n > 0$, $m > n$.

Проверить, что такие формулы для a, b и c удовлетворяют условию $a^2 + b^2 = c^2$ легко. Но чтобы доказать, что других пифагоровых троек не существует, нам потребовалось привлечь теорию гауссовых чисел.

Пример: $m = 7$, $n = 2$. Получаем пифагорову тройку (45, 28, 53).

Решим еще одну красивейшую задачу в целых числах при помощи гауссовых чисел.

РЕШЕНИЕ УРАВНЕНИЯ $y^2 = x^3 - 1$ В ЦЕЛЫХ ЧИСЛАХ

ЗАДАЧА

Ребенок собрал из кубиков большой куб. Пришел папа и украл один кубик. Из оставшихся кубиков ребенок собрал квадрат. При каком количестве кубиков это возможно?

Математически эта задача выглядит так:
$x^3 - 1 = y^2$, где $x, y \in \mathbb{Z}$.

Эйлер изучал это уравнение и со знаком «–», и со знаком «+» (когда куб и квадрат могут соседствовать на числовой прямой).

РЕШЕНИЕ

Перепишем уравнение в виде $y^2 + 1 = x^3$ и рассмотрим его в гауссовых числах: $(y + i)(y - i) = x^3$.

Какой наибольший общий делитель может быть у этих двух чисел?

Может ли быть, что y — нечетное? Тогда было бы $y^2 + 1 \equiv 2 \bmod 4$. Но тогда $x \vdots 2$ и, следовательно, $x^3 \vdots 8$. Но тогда должно быть $x^3 \vdots 4$, противоречие.

Значит, y — четное. Тогда $y + i$ не делится на $1 + i$, так как y и 1 имеют различную четность.

Пусть $НОД(y + i, y - i) \neq 1$. Тогда существует гауссово простое число $\alpha + \beta i$, которое делит оба эти числа, а значит, и их разность, которая равна $2i$.

Тогда, с точностью до обратимого, $\alpha + \beta i = 1 + i$. Противоречие. Значит, $НОД(y + i, y - i) = 1$.

Тогда по следствию 1 из ОТА в $\mathbb{Z}[i]$
$y + i = (a + bi)^3$, где σ — обратимое.

Но любое обратимое есть куб:
$1 = 1^3$, $i = (-i)^3$, $-1 = (-1)^3$, $-i = i^3$.

Поэтому можем отправить σ внутрь скобок и считать, что $y + i = (a + bi)^3$.

ЗАВЕРШЕНИЕ РЕШЕНИЯ $y^2 = x^3 - 1$

$y + i = (a + bi)^3 = a^3 + 3a^2bi + 3a(bi)^2 + (bi)^3 =$
$= a^3 - 3ab^2 + i(3a^2b - b^3)$.

Тогда должно быть выполнено:

$$\begin{cases} y = a^3 - 3ab^2 \\ 1 = b(3a^2 - b^2) \end{cases}$$

Отсюда $b = \pm 1$, $3a^2 - b^2 = \pm 1$. Нужно решить две системы:

$$\begin{cases} 3a^2 - b^2 = 1 \\ b = 1 \end{cases} \quad \text{и} \quad \begin{cases} 3a^2 - b^2 = -1 \\ b = -1 \end{cases}$$

Первая неразрешима в целых числах, т.к. не может быть $3a^2 = 2$. А вторая система дает единственное решение $a = 0$, $b = -1$, откуда наше уравнение имеет в целых числах единственное решение $x = 1$, $y = 0$.

То есть у ребенка был только один кубик, а когда его забрали, он составил пустой квадрат.

3 УРАВНЕНИЕ $y^2 = x^3 + 1$

Второе уравнение из этой серии $y^2 = x^3 + 1$ трудно решается в кольце чисел Эйзенштейна $\mathbb{Z}[\omega]$, где $\omega = \frac{1}{2}(-1 + i\sqrt{3})$ — кубический корень из 1.

Единственное решение уравнения $y^2 = x^3 + 1$:
$x = 2$, $y = 3$.

ГИПОТЕЗА КАТАЛАНА (доказана в 2002 г.)

x^n и y^m в натуральном ряду соседствуют только в одном случае, когда $x = 2$, $n = 3$, $y = 3$, $m = 2$.

Обобщается эта идея через так называемую *abc* — гипотезу. Она описывает пределы разложений на множители у трех взаимно простых чисел, таких что $a + b = c$. Оказывается, их разложения существенно состоят из неповторяющихся простых (в эти разложения простые числа не входят в высоких степенях). Это далеко идущее обобщение великой теоремы Ферма*, которое на данный момент не доказано и не опровергнуто.

*Великая теорема Ферма утверждает, что уравнение $a^n + b^n = c^n$ не имеет целых ненулевых решений при натуральном $n > 2$. Была полностью доказана в 1994 г. (Эндрю Уайлс).