О теореме Дирихле о единицах

Лекция 1: Диофантовы уравнения: линейные уравнения, пифагоровы тройки, уравнение Пелля.

Артём Авилов, Никон Курносов

Первая лекция курса посвящена различным диофантовым уравнениям - линейным, уравнению Пифагора, уравнению Пелля, мы разберём решения уравнений первых двух типов, а также простейшее уравнение Пелля.

1 Диофантовы уравнения

Уравнения, в которых обе части представляют собой многочлены, а решения необходимо найти в целых числах, называются *диофантовыми*. Наиболее простой случай - линейные диофантовы уравнения вида

$$ax + by = c,$$

где a, b, c - целые числа, при этом a и b не равны 0 одновременно. Очевидно, что решений нет, если c не делится на НОД a и b. Будем в дальнейшем предполагать, что c делится на НОД a и b.

Теорема 1.1 *Уравнение $ax + by = c$ имеет решение, если c делится на d, где d - НОД a и b. При этом общение решение имеет вид*

$$x = x_0 + \frac{b}{d}n, y = y_0 - \frac{a}{d}n,$$

где (x_0, y_0) - частное решение уравнения, а n - целое число.

Доказательство: Для существования решения достаточно рассмотреть случай c, равного НОД a и b. Действительно, решения искомого уравнения легко получить из решений уравнения $ax + by = d$, где d - НОД a и b, умножив их на $k = \frac{c}{d}$.

Теперь решим это уравнение. Разделим обе части на d, тогда уравнение примет вид $a_1x + b_1y = 1$, где $(a_1, b_1) = 1$. Это уравнение представляет собой

соотношение Безу, и его решение (u, v) можно найти по алгоритму Евклида. Таким образом, мы получаем некоторое решение уравнения $ax + by = d$

Найдём теперь и другие решения исходного уравнения $ax + by = c$. Обозначим частное решение, которое мы нашли выше из соотношения Безу (x_0, y_0). Легко видеть, что $(x_0, y_0) = (\frac{c}{d} \cdot u, \frac{c}{d} \cdot v)$, где (u, v) удовлетворяют соотношению $ax + by = d$.

Заметим, что чтобы найти все решения уравнения $ax + by = c$ надо к частному решению прибавить все решения уравнения

$$ax + by = 0,$$

то мы получим все решения исходного уравнения. Действительно, во-первых, если к частному решению (x_0, y_0) прибавить произвольное решение уравнения $ax + by = 0$, то получим решение. Во-вторых, почему мы так получим все решения? Пусть какое-то решение (x', y') мы не получили таким образом. Вычтем из него наше частное (x_0, y_0) - результат, $(x' - x_0, y' - y_0)$ - решение уравнения $ax + by = 0$. Противоречие.

Замечание 1.2 *Геометрическая интерпретация про параллельные прямые.*

Осталось найти решения $ax + by = 0$ Поделим обе части на d (НОД a и b), получим уравнение $a'x + b'y = 0$, где $(a', b') = 1$. Теперь, как легко видеть, из взаимной простоты следует, что $x = b'n$, $y = -a'n$. Таким образом, любое решение исходного уравнения имеет вид

$$x = x_0 + \frac{b}{d}n, y = y_0 - \frac{a}{d}n,$$

где (x_0, y_0) - частное решение уравнения, а n - целое число. □

Пример 1.1 *Посмотрим на уравнение* $5x + 7y = 11$. *Легко видеть, что пара (-2, 3) - решение. Если будем действовать по алгоритму Евклида, найдём пару* (x', y'), *такую, что* $5x' + 7y' = 1$, *то получим пару (-33, 22).*

Основные примеры нелинейных диофантовых уравнений:

- Уравнение Пифагора $x^2 + y^2 = z^2$.
- Уравнение Пелля $x^2 - qy^2 = 1$, где q не полный квадрат.
- Уравнение Баше $y^3 = x^2 + n$, где $n > 0$. Пример эллиптических кривых.
- Уравнение Ферма $x^n + y^n = z^n$, где $n > 2$.

2 Пифагоровы тройки

Ещё одним известным примером диофантового уравнения является уравнение

$$a^2 + b^2 = c^2,$$

которое связывает стороны прямоугольного уравнения по теореме Пифагора. Решения (a, b, c) этого уравнения называются *пифагоровыми тройками*. Пифагорова тройка называется простой, если у тройки (a, b, c) нет общих делителей. Для простых троек верна следующая

Теорема 2.1 *Тройка целых чисел (a, b, c) является простой пифагоровой титтк ровно одно из чисел a, b - чётное и верны следующие формулы (считаем, что чётное b):*

$$a = k^2 - l^2, b = 2kl, c = k^2 + l^2,$$

где $k > l$ - натуральные, взаимопростые числа, не сравнимые по модулю 2.

Доказательство:

Во-первых, простой проверкой убеждаемся, что тройка (a, b, c), задаваемая формулами выше, действительно простая пифагорова тройка. Во-вторых, нам достаточно доказать, что два, напрмиер, $k^2 - l^2, k^2 + l^2$, из трёх чисел не имеют общего делителя. Ну, и в правду, пусть они делятся на некоторое d, тогда, заметим, что d делит и $2k^2$ и $2l^2$, а, значит, и сами k^2 и l^2 (так как d нечётное). Но k и l взаимно простые, поэтому таковы и их квадраты, следовательно, $d = 1$.

В обратную сторону, проделаем следующее рассуждение. Во-первых, заметим, что a и b не могут быть одновременно нечётными. Действительно, если они оба нечётные, то при делении на 4 их квадраты дают остаток 1. А, следовательно, $c^2 = a^2 + b^2 \equiv 2(4)$, чего не бывает. Без ограничения общности, будем считать b чётным, а a - нечётным. Перепишем уравнение Пифагора в следующем виде:

$$b^2 = c^2 - a^2 = (c + a)(c - a).$$

Легко, видеть, что обе части делятся на 4, причем оба сомножителя в правой части чётны и взаимно простые (так как тройка примитивная). В то же время их произведение - полный квадрат. Пользуясь единственностью разложения на простые сомножители в $\mathbb{Z}$, получаем, что существуют такие целые k, l, что:

$$\frac{c + a}{2} = k^2, \frac{c - a}{2} = l^2.$$

Легко проверить, что такие k, l дают нужные выражения для a, b, c. Осталось проверим, что k, l разной чётности. Действительно, поскольку k, l взаимно простые, то они не могут быть одновременно чётными. Но и одновременно нечётными они быть не могут, поскольку в этом случае $k^2 + l^2, 2kl, k^2 - l^2$ все были бы нечётными, что невозможно. $\square$

Напомним, что многочлен с целыми коэффициентами называется *приводимым* над кольцом целых чисел, если он раскладывается в произведение многочленов с целыми коэффициентами.

Теорема 2.2 *Существует взаимно-однозначное соответствие между пифагоровыми тройками $(a,b,c)a<b<c$ и приводимыми многочленами $x^2+mx\pm n$, задаваемое следующим образом:*

$$(a,b,c)\mapsto x^2+cx\pm\frac{ab}{2}, x^2+mx\pm n\mapsto (\frac{e-d}{2},\frac{e+d}{2},m), \tag{1}$$

где $d^2=m^2-4n$ и $e^2=m^2+4n$.

Доказательство: В одну сторону очевидно, в обратную - нам необходимо, чтобы дискриминант обоих трёхчленов был полным квадратом, тогда у них будут целые корни и, значит, они будут приводимыми. Тогда, обозначив, первый дискриминант m^2-4n за d^2, а m^2+4n за e^2, получим, что $2m^2=d^2+e^2$, преобразуя, имеем Пифагорову тройку $(\frac{e-d}{2},\frac{e+d}{2},m)$. □

3 Уравнение Пелля

Уравнение, которому собственно и будет посвящена большая часть курса имеет вид:

$$x^2-qy^2=1.$$

Такое уравнение называется *уравнением Пелля*. Прежде чем решать это уравнение, посмотрим на несколько примеров:

Определение 3.1 *Число называется треугольным (Рис. 1), если оно соответствует числу точек в равностороннем треугольники с n точками на стороне.*

Легко видеть, что треугольные числа имеют вид $\frac{1}{2}n(n+1)$. Сумма двух последовательных треугольных чисел - полный квадрат. Когда само треугольное число является полным квадратом? Это условие выражается уравнением

$$(2n+1)^2-8m^2=1,$$

которое как раз и является уравнением Пелля.

Несколько ранее мы расмотрели так называемые пифагоровы тройки. Давайте, найдём все простые пифагоровы тройки, у которых два числа отличаются на 1. Без ограничения общности, можно считать, что a и b отличаются на 1. Тогда, пользуясь теоремой выше, получаем:

$$(k^2-l^2)-2kl=\pm1,$$

Рис. 1: Треугольные числа, $n = 2, 3, 4$.

что равносильно

$$(k-l)^2 - 2l^2 = \pm 1.$$

Таким образом, поиск простых Пифагоровых троек равносилен решению соответствующего уравнения Пелля $x^2 - 2y^2 = 1$.

Это самое простое уравнение Пелля $x^2 - 2y^2 = 1$ и давайте мы его решим. Если у нас есть какое-то решение (x, y) уравнения Пелля, то пара $(3x+4y, 2x+3y)$ - тоже решение (обозначим операцию составления нового решения за f). Таким образом, начиная с тривиального решения (1, 0) или с (3, 2), не важно, мы можем построить бесконечную серию решений. Могут ли быть какие-то другие решения (с точностью до знака)? Оказывается, что нет. Неотрицательные решения находятся на графике функции $y = \sqrt{\frac{x^2-1}{2}}$. Теперь решения уравнения Пелля можно естественным образом упорядочить, пользуясь монотонностью этой функции. Т.е. одно решение больше другого, когда у него больше и абсцисса, и ордината. Теперь заметим, что функция f монотонна, обратная к ней, $g(x, y) = (3x - 4y, 3y - 2x)$ монотонна. Вообще, общее утверждение из анализа гласит, что любое монотонное отображение имеет обратное, также являющееся монотонным. Будем действовать от противного. Пусть существует решение (x', y') уравнения Пелля $x^2 - 2y^2 = 1$, которое не совпадает ни с каким членом полученной нами бесконечной серии. Поскольку члены нашей серии неограниченно возрастают, то наше решение (x', y') лежит между какими-то двумя решениями, после чего применяем наше монотонное обратное отображение g нужное число раз, получим, что у нас должно быть ещё одно решение между (1, 0) и (3, 2), чего, очевидным образом, нет.

В древней Греции уравнение

$$x^2 - qy^2 = 1,$$

использовали для определения $\sqrt{2}$, рассматривая возрастающие решения (x_i, y_i). Для этого заметим, что исходное уравнение можно переписать в виде

$$\frac{x^2}{y^2} = 2 + \frac{1}{y^2} \iff \frac{x}{y} = \sqrt{2 + \frac{1}{y^2}} \to \sqrt{2},$$

когда $y \to \infty$. Почему так происходит, мы увидим в следующий раз.

Если обратимся к истории, то обнаружим, что уравнение Пелля встречается в знаменитой задаче Архимеда о быках (Archimedes cattle problem). Что касается самого Пелля, то в данном случае применим принцип Арнольда и само уравнение упоминается в работах Пелля, но решение получил Эйлер.

4 Цепные дроби

Любое нецелое число α можно представить в виде

$$\alpha = \alpha_0 + \frac{1}{\alpha_1},$$

где α_0, а $\alpha_1 > 1$. Действительно, в качестве α_0 берём просто целую часть, а в качестве α_1 - обратное число к его дробной части, если оно оказалось нецелым, то его в свою очередь можно представить в виде $\alpha_1 = a_1 + \frac{1}{\alpha_2}$. В результате получим представление α в виде

$$\alpha = \alpha_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \frac{1}{\alpha_n}}}$$

Если на каком-то шаге у нас получилось, что α_n целое число, то цепная дробь в этом случае называется *конечной*, в противном случае - *бесконечной*. Для удобства, будем в дальнейшем записывать цепные дроби в следующем виде $[a_0, a_1, a_2, ..., a_n]$.

Если бесконечную цепную дробь $[a_0, a_1, a_2, ...]$ на каком-то n месте обрубить, то получим рациональное число $\frac{p_n}{q_n}$, называемое n-ой подходящей дробью к нашей цепной дроби.

Предложение 4.1 *Цепная дробь конечно тогда и только тогда она является рациональным числом.*

Определение 4.2 *Пусть $[a_0, a_1, a_2, ...]$ - цепная дробь, такая что $a_n = a_{n+l}$ для достаточно больших n и фиксированного положительного l. Тогда эта дробь называется периодичной с периодом l.*

Теорема 4.3 *Иррациональное число является квадратично иррациональным тогда и только тогда его цепная дробь периодична.*

Определение 4.4 *Пусть α иррациональное число. Оно называется квадратично иррациональным, если оно является корнем многочлена второй степени с целыми коэффициентами. Второй корень этого многочлена β называется сопряжённым к α.*

Определение 4.5 *Пусть α квадратично иррациональное число. Оно называется приведённым, если $\alpha > 1$ и $-1 < \beta < 0$.*

Теорема 4.6 ***(Галуа)*** *Пусть α иррациональное. Тогда α чисто периодична тогда и только тогда α приведённое. Если $\alpha = \overline{[a_0, a_1, ..., a_n]}$ и β его сопряжённое, то $-\frac{1}{\beta} = \overline{[a_n, ..., a_2, a_1]}$.*

Следствие 4.7 *Пусть d - не полный квадрат, тогда существует набор чисел $a_1, ..., a_n$, таких что $\sqrt{d} = [[\sqrt{d}, \overline{a_1, a_2, ..., a_2, a_1, 2\sqrt{d}}]$ и $a_1, a_2, ..., a_2, a_1$ - палиндром.*

Доказательство:

Заметим, что $0 > [\sqrt{d}] - \sqrt{d} > -1$ и $1 < [\sqrt{d}] + \sqrt{d}$. Заметим, что они сопряжённые квадратичные иррациональности и $[\sqrt{d}] + \sqrt{d}$ приведённое, воспользуемся Теоремой 4.6 и получим, что цепная дробь для $[\sqrt{d}] + \sqrt{d}$ чисто периодическая. В результате, мы получаем цепную дробь для $\sqrt{d}$ в следующем виде

$$\sqrt{d} = [[\sqrt{d}; \overline{a_1, a_2, ..., a_n, 2\sqrt{d}}].$$

Используем разложение $\frac{-1}{[\sqrt{d}]-\sqrt{d}}$ в цепную дробь (Теоремой 4.6):

$$\frac{-1}{[\sqrt{d}] - \sqrt{d}} = [[\overline{a_n, a_{n-1}, ..., a_1, 2\sqrt{d}}].$$

Далее используем очевидное равенство

$$\sqrt{d} = [[\sqrt{d}; \frac{1}{\sqrt{d} - [\sqrt{d}]}]$$

Получаем, что

$$\sqrt{d} = [[\sqrt{d}, \overline{a_n, a_{n-1}, ..., a_2, a_1, 2\sqrt{d}}],$$

затем используем цепную дробь, полученную чуть выше, завершаем доказательство. □