Записки научных
семинаров ПОМИ
Том 400, 2012 г.

**Б. Б. Лурье**

# ОБ ОДНОМ МЕТОДЕ РЕШЕНИЯ ДИОФАНТОВЫХ УРАВНЕНИЙ

Рассмотрим вначале в качестве модели одну классическую задачу, решённую Пьером Ферма [1]: "Найти треугольник, у которого гипотенуза будет квадратом и сумма катетов также будет квадратом".

Сведём поставленную задачу к диофантову уравнению. Пусть искомый треугольник имеет катеты $a$, $b$ и гипотенузу $c$. Разумеется, данные числа предполагаются взаимно простыми. Используя параметрическое представление сторон пифагорова треугольника (известное ещё Диофанту), имеем: $a = p^2 - q^2$, $b = 2pq$, $c = p^2 + q^2$ при натуральных взаимно простых $p$, $q$ разной чётности. Задача свелась к системе диофантовых уравнений

$$p^2 + q^2 = s^2, \quad p^2 - q^2 + 2pq = t^2.$$

Поскольку $2pq$ кратно 4, получаем, что $p$ – нечётное, а $q$ – чётное число. Снова используя параметрическое выражение для первого уравнения, получаем $p = u^2 - v^2$, $q = 2uv$, и задача свелась к диофантову уравнению четвёртой степени

$$u^4 + 4u^3v - 6u^2v^2 - 4uv^3 + v^4 = t^2. \tag{1}$$

Как и ранее, числа $u$, $v$ – натуральные и взаимно простые разной чётности.

Деля (1) на $v^4$ и обозначая $w = u/v$, получаем уравнение

$$w^4 + 4w^3 - 6w^2 - 4w + 1 = r^2, \tag{2}$$

где $w$, $r$ рациональны. Полагая далее $r = w^2 + 2w - z$, получаем более простое уравнение

$$2(z-5)w^2 + 4(z-1)w - (z^2 - 1) = 0. \tag{3}$$

Очевидные значения для $z : z = 1$, $z = -1$ приводят к нулевому или отрицательному значению для $w$. При $z = 5$ получаем $w = 3/2$, что приводит к "треугольнику" со сторонами $a = -119$, $b = 120$, $c = 169$,

*Ключевые слова*: диофантовы уравнения, эллиптические кривые, задача Ферма.

который нас, естественно, не устраивает (вообще, условие $p^2 - q^2 > 0$ равносильно неравенству $w^2 - 2w - 1 > 0$, то есть $w > 1 + \sqrt{2}$).

Ясно, что всякое рациональное решение уравнения (3) при $w > 1 + \sqrt{2}$ приводит к нахождению искомого пифагорова треугольника.

Продемонстрируем два метода решения уравнения (3) – одно вполне традиционное, и другое, о котором ниже.

1. Для разрешимости уравнения (3) в рациональных числах необходимо и достаточно, чтобы его дискриминант (по $w$) был квадратом рационального числа. Таким образом,

$$4(z-1)^2 + 2(z-5)(z^2-1) = 2z^3 - 6z^2 - 10z + 14$$

должно быть квадратом. Полагая здесь $z = 2X+1$, приходим к такому уравнению эллиптической кривой

$$Y^2 = X^3 - 2X. \tag{4}$$

Всякой точке $(x_1, y_1)$ на кривой (4) отвечает значение

$$w_1 = (y_1 - x_1)/(x_1 - 2) = x_1(x_1 + 1)/(x_1 + y_1).$$

Удваивая точку (2,2) на кривой (4) (при которой $w_1 = 3/2$), приходим к точке $(9/4, -21/8)$, откуда $w = -39/2$ (симметричная точка $(9/4, 21/8)$ приводит к $w = 3/2$); поэтому данная точка также не даёт требуемый треугольник. Зато утроенная точка равна $(338, 6214)$, откуда $w = 1469/84$. Полагая теперь $u = 1469$, $v = 84$, имеем $p = 215095$, $q = 246792$, что даёт нам искомый треугольник со сторонами $a = 4565486027761$; $b = 1061652293520$; $c = 4687298610289$. При этом $c = 2165017^2$, $a + b = 2372159^2$.

Именно этот треугольник и нашёл П. Ферма.

2. Покажем теперь другой способ решения уравнения (3). Заметим, что это уравнение является уравнением второй степени как по $w$, так и по $z$:

$$z^2 - (2w^2 + 4w)z + (10w^2 + 4w - 1) = 0. \tag{3'}$$

Пусть $(z_1, w_1)$ – точка на кривой (3) (или, что то же самое, на (3')). Тогда на этой кривой лежит также точка $(z_1, w_2)$, где $w_1 + w_2 = -2(z_1 - 1)/(z_1 - 5)$ (формулы Виета!). Аналогично, на этой кривой лежит и точка $(z_2, w_1)$, где $z_1 + z_2 = 2w_1^2 + 4w_1$.

"Отталкиваясь" от точки $(z_1, w_1) = (5, 3/2)$, находим точку $(z_2, w_1)$, где $z_2 = 11/2$. Далее находим точку $(z_2, w_2)$, где $w_2 = -39/2$. Продолжая этот процесс, находим $z_3 = 677$, и, наконец, $w_3 = 1469/84$.

Проанализируем теперь предложенный метод в общей ситуации.

Пусть $Y^2 = F(X)$ – уравнение эллиптической кривой, где $F$ – полином третьей степени без кратных корней, и будем считать, что его старший коэффициент равен 1. Предположим, что на этой кривой лежит рациональная точка $(x_0, y_0)$, причём $y_0 \neq 0$. Для удобства будем считать, что $x_0 = 0$ (чего легко добиться сдвигом по оси абсцисс). Итак, наше уравнение имеет вид

$$Y^2 = X^3 + aX^2 + bX + y_0^2 \tag{5}$$

где $y_0 \neq 0$.

Свяжем с нашей кривой (5) другую кривую, задаваемую равносильными уравнениями

$$XW^2 + 2y_0W - (X^2 + aX + b) = 0, \tag{6}$$

$$X^2 - (W^2 - a)X + (b - 2y_0W) = 0. \tag{6'}$$

Точке $(0, y_0)$ на кривой (5) сопоставим точку $(0, b/2y_0)$ на кривой (6). Покажем, что кривые (5) и (6) бирационально эквивалентны. Эта эквивалентность задаётся формулой $w_1 = (y_1 - y_0)/x_1$ (соответственно, $y_1 = x_1w_1 + y_0$), где $(x_1, y_1)$ – точка на кривой (5), а $(x_1, w_1)$ – точка на кривой (6).

**Теорема.** *Пусть $(x_1, w_1)$ – точка на кривой* (6). *Перейдём к точке $(x_2, w_1)$, а затем к точке $(x_2, w_2)$ на этой кривой, дважды применив формулы Виета. Тогда точке $(x_2, w_2)$ на кривой* (5) *соответствует сумма точек $(x_1, y_1)$ и $(x_0, y_0)$.*

**Доказательство.** Угловой коэффициент прямой, проходящей через точки $(x_0, y_0)$, $(x_1, y_1)$ равен $w_1$ (напомним, что у нас $x_0 = 0$). Поэтому $x_2 = w_1^2 - a - x_1$ является абсциссой третьей точки пересечения этой секущей и кривой (5). Имеем далее $w_2 = -2y_0/x_2 - w_1$, откуда $y_2 = x_2w_2 + y_0 = -x_2w_1 - y_0$, то есть точка $(x_2, y_2)$ симметрична указанной точке пересечения, а потому есть сумма точек $(x_1, y_1)$ и $(x_0, y_0)$. □

Производя наши операции в обратном порядке (то есть находя сначала новое значение для $W$, а затем для $X$, мы получим точку, которой на кривой (5) отвечает разность точек $(x_1, y_1)$ и $(x_0, y_0)$.

Указанный метод интересен тем, что позволяет находить решения диофантовых уравнений, сводящихся к поиску рациональных точек на эллиптической кривой, без использования геометрической терминологии. Элементарность предложенного метода, возможно, даёт ключ к решению трудной проблемы в истории математики – каким образом

математики прошлого, незнакомые с геометрической интерпретацией уравнений, решали соответствующие задачи. Впрочем, это предположение вряд ли может быть убедительно обосновано.

## Литература

1. П. Ферма, *Исследования по теории чисел и диофантову анализу*. М., 1992.

Lur'e B. B. On a method of solving Diophantine equations.

The article proposes an elementary method of finding points on elliptic curves without using algebro-geometric techniques.

Санкт-Петербургское отделение
Математического института
им. В. А. Стеклова РАН,
Фонтанка 27, 191023 С.-Петербург,
Россия
*E-mail*: borislurje@mail.ru

Поступило 4 июня 2012 г.