Локальные и глобальные методы в арифметике

А. А. Панчишкин

1. p-адические числа и сравнения

Идея расширения поля $\mathbb{Q}$ в теории чисел встречается в различных вариантах. Например, вложение $\mathbb{Q} \subset \mathbb{R}$ часто дает полезные необходимые условия существования решений диофантовых уравнений над $\mathbb{Q}$ и над $\mathbb{Z}$. Важное свойство поля $\mathbb{R}$ — его полнота: любая фундаментальная последовательность (последовательность Коши) $\{\alpha_n\}_{n=1}^{\infty}$ в $\mathbb{R}$ имеет предел. Фундаментальность означает, что абсолютная величина разности $\alpha_n - \alpha_m$ стремится к 0, когда n и m стремятся к бесконечности. Кроме того, все элементы поля $\mathbb{R}$ являются пределами фундаментальных последовательностей $\{\alpha_n\}_{n=1}^{\infty}$ с $\alpha_n \in \mathbb{Q}$. Таким образом, можно сказать, что поле $\mathbb{R}$ получается из $\mathbb{Q}$ «присоединением пределов фундаментальных последовательностей». Такая конструкция называется *пополнением*.

Определение предела и фундаментальной последовательности дается в терминах абсолютной величины числа. Абсолютная величина обладает следующими свойствами:

$$\text{а) } |a| \geqslant 0, \text{ причем } |a| = 0 \text{ тогда и только тогда, когда } a = 0; \quad (1)$$

$$\text{б) } |ab| = |a| \cdot |b|; \quad (2)$$

$$\text{в) } |a + b| \leqslant |a| + |b|. \quad (3)$$

Всякая вещественная функция $|\cdot|$ на каком-либо поле K, обладающая этими свойствами, называется (мультипликативным) *нормированием* поля K. Для поля $\mathbb{Q}$, помимо абсолютной величины, существуют и другие нормирования. Так, для любого простого p можно определить так называемое *p-адическое нормирование* $|\cdot|_p$:

$$|a/b|_p = p^{\mathrm{ord}_p b - \mathrm{ord}_p a}, \quad |0|_p = 0,$$

где $\mathrm{ord}_p a$ есть наивысшая степень числа p, делящая целое число a. Согласно теореме Островского, всякое нормирования поля $\mathbb{Q}$ с точностью до постоянного (положительного) множителя есть либо абсолютная величина, либо p-адическое нормирование для некоторого простого p.

Пополнение поля $\mathbb{Q}$ относительно p-адического нормирования называется *полем p-адических чисел* и обозначается через $\mathbb{Q}_p$. Легко видеть, что нормирование (в данном случае p-адическое) однозначно продолжается на пополнение.

Использование вложений поля $\mathbb{Q}$ в его пополнения по всем нормированиям, то есть в $\mathbb{R}$ и в $\mathbb{Q}_p$ для всех простых p, часто значительно упрощает ситуацию в арифметических задачах. Замечательный пример дает *теорема Минковского – Хассе* (см.[1], глава 1): уравнение

$$\sum_{i,j} a_{ij} x_i x_j = 0 \ (a_{ij} \in \mathbb{Q}) \tag{4}$$

имеет нетривиальное решение в рациональных числах в том и только в том случае, когда оно нетривиально разрешимо над $\mathbb{R}$ и над $\mathbb{Q}_p$ для всех простых чисел p. Для нахождения решений уравнений над $\mathbb{Q}_p$ можно эффективно применять такие приемы, взятые из вещественного анализа, как «метод касательных Ньютона», который в p-адическом случае известен как *лемма Гензеля*.

Наиболее простым способом можно ввести p-адические числа как выражения вида

$$\alpha = a_m p^m + a_{m+1} p^{m+1} + \dots, \tag{5}$$

где $a_i \in \{0, 1, \dots . p-1\}$ – цифры (по основанию p), а $m \in \mathbb{Z}$. При этом число α называется целым, если $m \geqslant 0$. Удобно записывать α в виде последовательности цифр, бесконечной влево:

$$\alpha = \begin{cases} \cdots a_{m+1} a_m \overbrace{000\dots0}^{m-1}{}_{(p)}, & \text{если } m \geqslant 0, \\ \cdots a_1 a_0, a_{-1} \cdots a_{m(p)}, & \text{если } m < 0. \end{cases}$$

Эти выражения образуют поле, в котором сложение и умножение выполняются так же, как для рациональных чисел вида $p^m n \, (m \in \mathbb{Z}, n \in \mathbb{N})$, записанных по основанию p (с конечным числом цифр после запятой). На самом деле в этом поле лежат все рациональные числа. Например,

$$-1 = \frac{p-1}{1-p} = (p-1) + (p-1)p + (p-1)p^2 + \cdots = \cdots (p-1)(p-1)_{(p)}.$$

Если $n \in \mathbb{N}$, то выражение для $-n = n \cdot (-1)$ вида (5) получается, если перемножить такие выражения для n и для -1. Если n не делится на p, то выражение для $-\dfrac{1}{n}$ может быть получено следующим образом. По теореме Эйлера $p^{\varphi(n)} - 1 = un$, где $u \in \mathbb{N}$. Положим $\varphi(n) = r$. Тогда

$$-\frac{1}{n} = \frac{u}{1-p^r} \, .$$

Так как $u < un = p^r$, то запись по основанию p числа u имеет вид $a_{r-1}\cdots a_{0(p)}$ (где, быть может, первые несколько цифр равны 0). Следовательно,

$$-\frac{1}{n} = \cdots a_0\overbrace{a_{r-1}\cdots a_0}^{r}\overbrace{a_{r-1}\cdots a_0}^{r}{}_{(p)}.$$

Пользуясь этим, легко получить p-адическое выражение для любого рационального числа. Например, для $p = 5$ имеем

$$\frac{9}{7} = 2 - \frac{5}{7} = 2 + \frac{5\cdot 2232}{1-5^6}.$$

Так как

$$2232 = 3\cdot 5^4 + 2\cdot 5^3 + 4\cdot 5^2 + 1\cdot 5 + 2,$$

то

$$\frac{9}{7} = \cdots\overbrace{032412032412}\,2_{(5)}.$$

Нетрудно проверить, что пополнение поля $\mathbb{Q}$ относительно p-адической метрики $|\cdot|_p$ отождествляется с полем «p-адических разложений» вида (5) (см. [2]). При этом $|\alpha|_p = p^m$, если в выражении (5) для α имеем $a_m \neq 0$.

Разложения (5) p-адических чисел можно рассматривать как аналоги разложения функции f переменной x в окрестности точки a по степеням $(x-a)$, причем p является аналогом $(x-a)$.

Любопытно также сравнить разложения (5), «бесконечные влево», с десятичными разложениями действительных чисел $\alpha \in \mathbb{R}$, «бесконечными вправо»:

$$\alpha = a_m a_{m-1}\cdots a_0, a_{-1}\cdots = \\ = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_0 + a_{-1}10^{-1} + \cdots, \quad (6)$$

где $a_i \in \{0, 1, \cdots, 9\}$. Разложения такого типа по любому основанию приводят к одному и тому же полю $\mathbb{R}$. Их можно рассматривать как аналоги разложения функции f переменной x в окрестности бесконечности по степеням x^{-1}.

Поле $\mathbb{Q}_p$ является *полным метрическим пространством*. Более того, из любой ограниченной по норме последовательности p-адических чисел можно выбрать сходящуюся подпоследовательность. Это легко доказывается с помощью последовательного рассмотрения p-адических цифр справа налево, с учетом того, что у всех членов последовательности число знаков после запятой ограничено фиксированным числом. Иначе говоря, всякий «открытый диск» $U(r) = \{x \in \mathbb{Q}_p \mid |x|_p < r\}$, а также всякий «замкнутый диск» $D(r) = \{x \in \mathbb{Q}_p \mid |x|_p \leqslant r\}$, компактны. При этом и $U(r)$, и $D(r)$ являются открыто-замкнутыми подмножествами в $\mathbb{Q}_p$.

В частности, кольцо целых p-адических чисел

$$\mathbb{Z}_p = D(1) = \{x \in \mathbb{Q}_p \mid \ |x|_p \leqslant 1\} = \left\{x = a_0 + a_1 p + a_2 p^2 + \cdots\right\}$$

— это компактное топологическое кольцо. Оно совпадает с замыканием множества $\mathbb{Z}$ обычных целых чисел в $\mathbb{Q}_p$.

Множество обратимых элементов («единиц») кольца $\mathbb{Z}_p$ — это

$$\mathbb{Z}_p^\times = \mathbb{Z}_p \backslash p\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid \ |x|_p = 1\} = \left\{x = a_0 + a_1 p + a_2 p^2 + \cdots \mid a_0 \neq 0\right\}.$$

Оно является группой по умножению. Для описания этой группы положим $\nu = 1$, если $p > 2$, и $\nu = 2$, если $p = 2$, и рассмотрим подгруппу

$$U_p = \left\{x \in \mathbb{Z}_p^\times \mid x \equiv 1 \pmod{p^\nu}\right\}.$$

Отображение, определяемое степенным рядом

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}\,,$$

задает гомоморфизм аддитивной группы $p^\nu\mathbb{Z}_p$ в мультипликативную группу U_p. На самом деле это изоморфизм, так как существует обратное отображение, задаваемое рядом

$$\log(x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(x-1)^n}{n}\,.$$

Можно показать, что

$$\mathbb{Q}_p^\times = \{p^m \mid m \in \mathbb{Z}\} \times \mathbb{Z}_p^\times, \quad \mathbb{Z}_p^\times \cong (\mathbb{Z}/p^\nu\mathbb{Z})^\times \times U_p, \tag{7}$$

где $\nu = 1$, если $p > 2$, $\nu = 2$, если $p = 2$.

1.1. Приложения p-адических чисел к решению сравнений

Возникновение p-адических чисел в работах Гензеля было связано с проблемой решения сравнений по модулю p^n, а применение их к теории квадратичных форм его учеником Хассе привело к элегантной формулировке теории квадратичных форм над рациональными числами, не использующей рассмотрений в кольцах вычетов $\mathbb{Z}/p^n\mathbb{Z}$, работать с которыми затруднительно из-за наличия в них делителей нуля.

Нетрудно видеть, что если $f(x_1, \ldots, x_n) \in \mathbb{Z}_p[x_1, \ldots, x_n]$, то сравнения

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{p^n}$$

разрешимы при любом $n \geqslant 1$ тогда и только тогда, когда уравнение

$$f(x_1, \ldots, x_n) = 0$$

разрешимо в целых p-адических числах. Эти решения в $\mathbb{Z}_p$ можно находить с помощью p-адического варианта метода касательных Ньютона.

Теорема 1 (лемма Гензеля). *Пусть $f(x) \in \mathbb{Z}_p[x]$ — многочлен одной переменной x, $f'(x) \in \mathbb{Z}_p[x]$ — его формальная производная и для некоторого $\alpha_0 \in \mathbb{Z}_p$ выполнено начальное условие*

$$|f(\alpha_0)/f'(\alpha_0)^2|_p < 1 \tag{8}$$

Тогда существует единственное такое $\alpha \in \mathbb{Z}_p$, что

$$f(\alpha) = 0, \quad |\alpha - \alpha_0|_p < 1.$$

Доказательство проводится с помощью рассмотрения последовательности

$$\alpha_n = \alpha_{n-1} - \frac{f(\alpha_{n-1})}{f'(\alpha_{n-1})}\,.$$

С учетом формального разложения Тейлора многочлена $f(x)$ в точке $x = \alpha_{n-1}$ проверяется, что последовательность фундаментальна, а ее предел α обладает всеми необходимыми свойствами (см. [1], [6]).

Например, если $f(x) = x^{p-1} - 1$, то любое $\alpha_0 \in \{1, 2, \ldots, p-1\}$ удовлетворяет условию $|f(\alpha_0)|_p < 1$, в то время как $f'(\alpha_0) = (p-1)\alpha_0^{p-2} \not\equiv \not\equiv 0 \pmod p$, так что начальное условие (8) выполнено. Корень $\alpha \equiv \alpha_0 \pmod p$ называется представителем Тейхмюллера числа α_0 и обозначается через $\omega(\alpha_0)$. Например, для $p = 5$ имеем

$$\begin{aligned}
&\omega(1) = 1;\\
&\omega(2) = 2 + 1\cdot 5 + 2\cdot 5^2 + 1\cdot 5^3 + 3\cdot 5^4 \cdots;\\
&\omega(3) = 3 + 3\cdot 5 + 2\cdot 5^2 + 3\cdot 5^3 + 1\cdot 5^4 + \cdots;\\
&\omega(4) = 4 + 4\cdot 5 + 4\cdot 5^2 + 4\cdot 5^3 + 4\cdot 5^4 + \cdots = -1;
\end{aligned}$$

Описанный метод применим и к многочленам многих переменных, но уже без единственности находимого решения, (см. [1], [6]).

Еще одно приложение леммы Гензеля связано с описанием квадратов поля $\mathbb{Q}_p$: для произвольного элемента

$$\alpha = p^m \cdot v \ \in \ \mathbb{Q}_p \ \ (m \in \mathbb{Z},\ v \in \mathbb{Z}_p^\times)$$

свойство α быть квадратом в $\mathbb{Q}_p$ равносильно тому, что

а) если $p > 2$, то $m \in 2\mathbb{Z}$, а $\overline{v} \equiv v \pmod p \in (\mathbb{Z}/p\mathbb{Z})^{\times 2}$ (то есть $\left(\frac{\overline{v}}{p}\right) = 1$, где $\left(\frac{\overline{v}}{p}\right)$ — символ Лежандра);

б) если $p = 2$, то $m \in 2\mathbb{Z}$, а $v \equiv 1 \pmod 8$.

Разрешимость уравнения $x^2 = \alpha$ в $\mathbb{Q}_p$ при условиях а) и б) выводится из леммы Гензеля, а необходимость этих условий вытекает из простых рассмотрений по модулю p и по модулю 8. Как следствие мы получаем, что факторгруппа $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$

а) при $p > 2$ изоморфна $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ с системой представителей $\{1, p, v, pv\}$, $\left(\frac{v}{p}\right) = -1$;

б) при $p = 2$ изоморфна $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ с системой представителей $\{\pm 1, \pm 5, \pm 2, \pm 10\}$.

2. Диофантовы системы линейных уравнений и сравнений

2.1. Вычисления с классами вычетов.

С точки зрения алгебры множество $\mathbb{Z}$ целых чисел является коммутативным ассоциативным кольцом с единицей, то есть множеством с двумя коммутативными и ассоциативными операциями (сложение и умножение), связанными друг с другом законом дистрибутивности.

Пусть N — фиксированное натуральное число. Остатки от деления на N подразделяют все целые числа на непересекающиеся классы

$$\bar{a} = a + N\mathbb{Z}, \quad 0 \leqslant a \leqslant N - 1,$$

которые также образуют кольцо

$$\mathbb{Z}/N\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{N-1}\},$$

называемое кольцом вычетов по модулю N. При этом равенство $\bar{a} = \bar{b}$ равносильно сравнению $a \equiv b \pmod N$.

Часто в задачах теории чисел вычисления в кольце $\mathbb{Z}$ можно сводить к вычислениям в кольцах вычетов $\mathbb{Z}/N\mathbb{Z}$. Это доставляет ряд удобств. Например, на многие элементы из $\mathbb{Z}/N\mathbb{Z}$ можно делить, оставаясь в пределах этого кольца (в отличие от целых чисел, где всегда определено только деление на ± 1). Действительно, если число a взаимно просто с N, то есть $(a, N) = 1$, класс $\bar{a}$ обратим, так как в этом случае существуют такие целые числа $x,\ y$, что $ax + Ny = 1$, и поэтому $\bar{a} \cdot \bar{x} = \bar{1}$. Так получаются все обратимые элементы кольца вычетов $\mathbb{Z}/N\mathbb{Z}$. Они образуют группу по умножению, обозначаемую $(\mathbb{Z}/N\mathbb{Z})^\times$. Порядок этой группы обозначается через $\varphi(N)$ (функция Эйлера). Название происходит от обобщения малой теоремы Ферма, принадлежащего Эйлеру:

$$a^{\varphi(N)} \equiv 1 \pmod N \tag{9}$$

для всех таких чисел a, что $(a, N) = 1$, то есть $\bar{a}^{\varphi(N)} = \bar{1}$ для всех обратимых элементов $\bar{a}$ в кольце $\mathbb{Z}/N\mathbb{Z}$.

Доказательство Эйлера, применимое к любой конечной абелевой группе порядка f, показывает, что порядок любого элемента a делит f. А именно, умножение на a является перестановкой элементов группы (в нашем случае группы $(\mathbb{Z}/N\mathbb{Z})^\times$ порядка $f = \varphi(N)$). Произведение всех элементов группы при этой перестановке умножается на a^f. Поэтому $a^f = 1$.

Если число N разложено в произведение $N = N_1 N_2 \cdot \ldots \cdot N_k$ попарно взаимно простых чисел, то имеется разложение

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/N_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/N_k\mathbb{Z} \tag{10}$$

в прямую сумму колец, что эквивалентно китайской теореме об остатках: для любых вычетов $a_i \bmod N_i$, $i = 1, \ldots, k$, найдется такое целое число a, что $a \equiv a_i \pmod{N_i}$ для всех i. Практический поиск числа a можно быстро осуществить, применяя повторно алгоритм Евклида. Положим $M_i = N/N_i$; тогда числа M_i и N_i по условию взаимно просты и, значит, существуют такие целые числа X_i, что $X_i M_i \equiv 1 \pmod{N_i}$. Искомым числом тогда будет

$$a = \sum_{i=1}^{k} a_i X_i M_i. \tag{11}$$

Из разложения (10) вытекает и разложение мультипликативной группы:

$$(\mathbb{Z}/N\mathbb{Z})^\times \cong (\mathbb{Z}/N_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/N_k\mathbb{Z})^\times, \tag{12}$$

из которого, в частности, следует, что $\varphi(N) = \varphi(N_1) \cdot \ldots \cdot \varphi(N_k)$. Поскольку для простого числа p имеем $\varphi(p^a) = p^{a-1}(p-1)$, мы можем найти $\varphi(N)$, исходя из разложения числа N на простые множители.

В специальном случае, когда N — простое число, кольцо вычетов $\mathbb{Z}/N\mathbb{Z}$ является полем: в нем обратим любой элемент, отличный от нуля.

2.2. Системы линейных уравнений с целыми коэффициентами

В этом параграфе все буквы (коэффициенты и неизвестные в уравнениях) означают целые числа.

Из алгоритма Евклида вытекает, что уравнение

$$ax + by = c \tag{13}$$

разрешимо тогда и только тогда, когда c делится на $d = (a, b)$.

Уравнение (13) дает первый пример общей проблемы: для системы алгебраических уравнений с целыми коэффициентами

$$F_1(x_1,\dots,x_n)=0,\ \cdots\ ,F_m(x_1,\dots,x_n)=0 \tag{14}$$

найти все целочисленные (или все рациональные) решения. Для уравнения (13) задача нахождения рациональных решений тривиальна. Если в системе (14) все уравнения линейные, то и для нее все рациональные решения легко находятся последовательным исключением неизвестных (например, по методу Гаусса).

Опишем общий прием нахождения всех целочисленных решений системы целочисленных линейных уравнений

$$Ax=b, \tag{15}$$

где

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n}\\ \dots & \dots & \ddots & \dots\\ a_{m1} & a_{m2} & \cdots & a_{mn}\end{pmatrix}\in M_{m,n}(\mathbb{Z}),\quad x=\begin{pmatrix} x_1\\ \cdots\\ x_n\end{pmatrix},\quad b=\begin{pmatrix} b_1\\ \cdots\\ b_m\end{pmatrix}.$$

Эта задача также сводится к применению алгоритма Евклида.

Элементарным преобразованием над $\mathbb{Z}$ строк матрицы назовем преобразование, при котором к некоторой строке прибавляют другую, умноженную на целое число, а остальные строки не меняют. Проверяется, что применение такого преобразования эквивалентно умножению исходной матрицы слева на некоторую матрицу из $\mathrm{SL}_m(\mathbb{Z})$ (целочисленную матрицу с определителем, равным 1). Аналогичное преобразование столбцов равносильно умножению матрицы справа на некоторую матрицу из $\mathrm{SL}_n(\mathbb{Z})$.

Применение нескольких элементарных преобразований приводит матрицу A к виду UAV с $U\in\mathrm{SL}_m(\mathbb{Z}), V\in\mathrm{SL}_n(\mathbb{Z})$, а целочисленные решения соответствующей системы уравнений

$$UAVy=Ub \tag{16}$$

и исходной системы (15) взаимно однозначно соответствуют друг другу по формуле $x=Vy$.

Действуя, как в алгоритме Евклида, с помощью описанных преобразований и, быть может, умножений каких-то строк на -1 матрицу A можно привести к диагональному виду

$$D=\begin{pmatrix} d_1 & 0 & 0 & \dots & 0\\ 0 & d_2 & 0 & \dots & 0\\ \dots & \dots & \ddots & \dots & 0\\ 0 & 0 & \dots & d_r & \dots\\ \dots & \dots & \dots & \dots & \dots\end{pmatrix} \tag{17}$$

(где на диагонали после выписанных элементов стоят нули). Система уравнений примет тогда вид

$$d_i y_i = c_i \text{ для } i \leqslant r, \quad c_i = 0 \text{ для остальных } i.$$

Эта система легко решается, причем критерий ее совместности (а значит, и совместности исходной системы) над $\mathbb{Z}$ состоит в том, что $d_i \mid c_i$ для всех $i \leqslant r$ и $c_i = 0$ для остальных i.

В частности, отсюда следует, что для совместности над $\mathbb{Z}$ системы (15) необходимо и достаточно, чтобы была разрешима соответствующая система сравнений

$$Ax \equiv b \pmod{p^m}$$

для любого простого p и любого натурального m, а это, в свою очередь, равносильно совместности системы (15) над $\mathbb{Z}_p$ для любого простого p. Критерий такого рода называется принципом Минковского – Хассе, и он часто встречается в задачах диофантовой геометрии.

3. Уравнения второй степени

3.1. Квадратичные формы и квадрики

Для диофантова уравнения

$$f(x_1, x_2, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j + \sum_{i=1}^{n} b_i x_i + c = 0 \tag{18}$$

находить целочисленные решения значительно труднее, чем рациональные, хотя и последняя задача уже нетривиальна.

Известный пример — рациональная параметризация окружности $x^2 + y^2 = 1$ по формулам универсальной подстановки

$$x = \frac{2t}{1+t^2}\,,\ y = \frac{1-t^2}{1+t^2} \quad \left(x = \cos\varphi,\ y = \sin\varphi,\ t = \operatorname{tg}\left(\frac{\varphi}{2}\right)\right). \tag{19}$$

Полагая $t = u/v$, получаем отсюда следующее описание всех примитивных пифагорейских троек (X, Y, Z), то есть натуральных решений уравнения $X^2 + Y^2 = Z^2$ с $(X,\ Y,\ Z) = 1$:

$$X = 2uv,\ Y = u^2 - v^2,\ Z = u^2 + v^2,$$

где $u > v > 0$ — взаимно простые натуральные числа противоположной четности.

При отыскании рациональных решений уравнения (18) удобно перейти к квадратичной форме

$$F(X_0, X_1, \cdots, X_n) = \sum_{i,j=0}^{n} f_{ij} X_i X_j = \\ = \sum_{i,j=1}^{n} f_{ij} X_i X_j + 2\sum_{i=1}^{n} f_{i0} X_i X_0 + f_{00} X_0^2, \qquad (20)$$

где $f_{ij} = f_{ji} = a_{ij}$ для $1 \leqslant i < j \leqslant n$, $f_{0i} = f_{i0} = b_i/2$ для $1 \leqslant i \leqslant n$ и $f_{00} = c$. Для этого надо заменить «неоднородные координаты» $x_1, \ldots, x_n$ на «однородные» $X_0, \ldots, X_n$ по формулам $x_i = X_i/X_0$ $(i = 1, 2, \ldots, n)$. Квадратичная форма F является однородным многочленом второй степени, который удобно записывать в матричной форме

$$F(X) = X^t A_F X, \quad X^t = (X_0, X_1, \ldots, X_n),$$

где $A_F = (f_{ij})$ — матрица коэффициентов. Если существует ненулевое рациональное решение уравнения $F(X) = 0$, то говорят, что форма F представляет нуль над полем $\mathbb{Q}$.

Рассмотрим квадрику

$$Q_F = \{(X_0 : X_1 : \cdots : X_n) \in \mathbb{CP}^n \mid F(X_0, X_1, \ldots, X_n) = 0\}$$

в комплексном проективном пространстве $\mathbb{CP}^n$. Ненулевое рациональное решение X^0 уравнения $F(X) = 0$ определяет точку на квадрике Q_F. Остальные рациональные точки (рациональные решения) легко найти: они совпадают с точками пересечения квадрики Q_F со всевозможными прямыми, выходящими из X^0 в направлении векторов с рациональными координатами. Пусть Y^0 — какая-либо рациональная точка. Проективная прямая, проходящая через X^0 и Y^0, состоит из точек $uX^0 + vY^0$. Уравнение $F(uX^0 + vY^0) = 0$ сводится к уравнению

$$u\sum_{i=1}^{n} \frac{\partial F}{\partial X_i}(X^0) Y_i^0 + vF(Y^0) = 0.$$

Если точка X^0 не является вершиной квадрики, то есть если $\dfrac{\partial F}{\partial X_i}(X^0) \neq 0$ хотя бы для одного i, то для любого Y^0 находится точка пересечения квадрики Q_F с этой прямой:

$$v = -u\sum_{i=1}^{n} \frac{\partial F}{\partial X_i}(X^0) Y_i^0 / F(Y^0). \qquad (21)$$

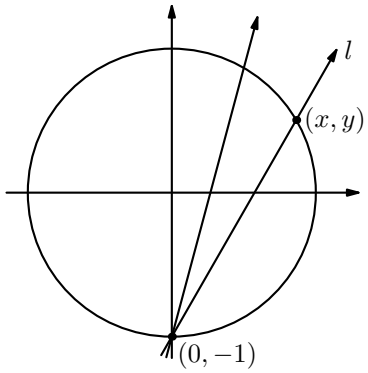

Рис. 1.

(Если $F(Y^0) = 0$, то Y^0 уже на Q_F.)

Примером рассмотренной конструкции, записанным в неоднородных координатах, являются формулы (19). Чтобы найти все пары (x, y) рациональных чисел, для которых $x^2 + y^2 = 1$, рассмотрим прямую l, проходящую через точки $(0, -1)$ и (x, y) (рис. 1). Эта прямая имеет угловой коэффициент $t = \dfrac{y+1}{x}$, который может быть любым рациональным числом. Находя точку пересечения этой прямой с окружностью, получаем формулы (19).

При нахождении рациональных решений уравнения

$$F(X_0, X_1, \ldots, X_n) = 0 \tag{22}$$

(с квадратичной формой F из (20)) можно считать, что форма F диагональна: метод Лагранжа выделения полных квадратов дает замену переменных $X = CY$ с невырожденной рациональной матрицей C, приводящую форму F к диагональному виду.

Для однородных уравнений типа (22) нет существенной разницы между их целочисленными и рациональными решениями: после умножения на подходящее целое число любое рациональное решение становится целочисленным, и его можно считать примитивным, то есть имеющим взаимно простые в совокупности координаты. Наиболее фундаментальным фактом теории квадратичных форм над полем рациональных чисел является следующий результат.

3.2. Принцип Минковского – Хассе для квадратичных форм

Теорема 2. *Невырожденная рациональная квадратичная форма $F(x_1, x_2, \ldots, x_n)$ представляет нуль над полем рациональных чисел тогда*

и только тогда, когда она представляет нуль над полем $\mathbb{R}$ *вещественных чисел (то есть является неопределенной) и над полем* $\mathbb{Q}_p$ *p-адических чисел для любого простого* p.

(См. [1], глава 1. Конечно, утверждение «только тогда» тривиально.)

Приведем красивое доказательство этой теоремы для ключевого случая $n = 3$, рассмотренного Лежандром ([1]).

Путем линейной замены переменных с рациональными коэффициентами приведем форму F к диагональному виду. Пусть

$$F = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 \qquad (a_1a_2a_3 \neq 0).$$

Неопределенность формы F означает, что не все коэффициенты a_1, a_2, a_3 одного знака. Умножив форму при необходимости на -1, мы придем к случаю, когда два коэффициента положительны, а один отрицателен. Кроме того, мы можем считать эти числа целыми, свободными от квадратов и взаимно простыми в совокупности, так как их можно сократить на наибольший общий делитель. Далее, если, например, a_1 и a_2 имеют общий простой делитель p, то, умножив форму на p и взяв px и py за новые переменные, мы получим форму с коэффициентами a_1/p, a_2/p и pa_3. Повторяя этот процесс несколько раз, мы заменим нашу форму формой вида

$$F = ax^2 + by^2 - cz^2, \tag{23}$$

в которой a, b, c — попарно взаимно простые свободные от квадратов натуральные числа.

Пусть теперь p — какой-нибудь простой делитель числа c, и пусть (x_0, y_0, z_0) — ненулевое решение уравнения $F = 0$ над полем $\mathbb{Q}_p$. Можно считать, что x_0, y_0, z_0 — целые p-адические числа, не делящиеся одновременно на p. Рассматривая равенство

$$ax_0^2 + by_0^2 - cz_0^2 = 0$$

по модулю p^2, мы видим, что x_0 и y_0 не могут одновременно делиться на p (так как тогда и z_0 делилось бы на p). Пусть для определенности y_0 не делится на p. Тогда можно считать, что $y_0 = 1$. При этом условии мы получаем разложение на множители

$$F \equiv a(x + x_0y)(x - x_0y) \pmod{p}.$$

Аналогичные разложения имеют место по модулю простых p, делящих a и b. Таким образом, для любого простого $p \mid abc$ существуют такие целочисленные линейные формы $L^{(p)}$, $M^{(p)}$ от x, y, z, что

$$F \equiv L^{(p)}M^{(p)} \pmod{p}.$$

Теперь с помощью китайской теоремы об остатках найдем такие целочисленные линейные формы L, M, что

$$L \equiv L^{(p)} \pmod{p}, \quad M \equiv M^{(p)} \pmod{p}$$

для всех $p \mid abc$, и мы получим

$$F \equiv LM \pmod{abc}. \tag{24}$$

Будем придавать переменным x, y, z целые значения, удовлетворяющие условиям

$$0 \leqslant x < \sqrt{bc}, \quad 0 \leqslant y < \sqrt{ac}, \quad 0 \leqslant z < \sqrt{ab}. \tag{25}$$

Если исключить из рассмотрения тривиальный случай $a = b = c = 1$, то не все числа $\sqrt{bc}$, $\sqrt{ac}$, $\sqrt{ab}$ целые и число троек (x, y, z), удовлетворяющих условиям (25), строго больше, чем $\sqrt{bc}\sqrt{ac}\sqrt{ab} = abc$. Следовательно, для каких-то двух различных троек форма L принимает одно и то же значение по модулю abc, откуда в силу линейности формы L получаем

$$L(x_0, y_0, z_0) \equiv 0 \pmod{abc} \tag{26}$$

для некоторых $|x_0| < \sqrt{bc}$, $|y_0| < \sqrt{ac}$, $|z_0| < \sqrt{ab}$. Поэтому

$$ax_0^2 + by_0^2 - cz_0^2 \equiv 0 \pmod{abc} \tag{27}$$

и имеют место неравенства

$$-abc < ax_0^2 + by_0^2 - cz_0^2 < 2abc.$$

Таким образом,

$$ax_0^2 + by_0^2 - cz_0^2 = 0 \text{ или } abc.$$

В первом случае теорема доказана. Во втором случае доказательство следует из равенства

$$a(x_0z_0 + by_0)^2 + b(y_0z_0 - ax_0)^2 - c(z_0^2 + ab)^2 = 0.$$

В формулировке Лежандра диофантово уравнение $ax^2 + by^2 - cz^2 = 0$ рассмотренного выше вида имеет нетривиальное целочисленное решение в том и только в том случае, когда классы вычетов

$$bc \,(\mathrm{mod}\, a), \quad ac \,(\mathrm{mod}\, b), \quad -ab \,(\mathrm{mod}\, c)$$

являются квадратами.

Можно доказать, что рациональная квадратичная форма ранга $\geqslant 5$ всегда представляет нуль над $\mathbb{Q}$.

В общем случае существуют эффективные методы (основанные на принципе Минковского – Хассе) выяснения того, представляет ли нуль данная рациональная квадратичная форма. Эти методы используют символ Гильберта.

3.3. Символ Гильберта

В этом пункте мы допускаем значение $p = \infty$, считая, что $\mathbb{Q}_\infty = \mathbb{R}$ и $|\cdot|_\infty = |\cdot|$.

Символ Гильберта (символ норменного вычета) $(a,b)_p$ для $a, b \in \mathbb{Q}_p^\times$ определяется равенством

$$(a,b)_p = \begin{cases} 1, \text{ если уравнение } ax^2 + by^2 = 1 \text{ имеет решение в } \mathbb{Q}_p, \\ -1 \text{ в противном случае.} \end{cases}$$

Ясно, что $(a,b)_p$ не меняется при умножении a и b на квадраты любых элементов из $\mathbb{Q}_p^\times$, то есть зависит только от классов a и b по модулю подгруппы квадратов в $\mathbb{Q}_p^\times$.

Заметим, что если квадратичная форма $ax^2 + by^2$ представляет нуль в поле $\mathbb{Q}_p$, то она разлагается на линейные множители и, следовательно, принимает все значения в $\mathbb{Q}_p$. В частности, в этом случае $(a,b)_p = 1$.

Иногда бывает полезна несимметричная форма определения символа Гильберта. Именно, $(a,b)_p = 1$ тогда и только тогда, когда уравнение

$$z^2 - by^2 = a \tag{28}$$

имеет решение в $\mathbb{Q}_p$. Действительно, пусть $z_0^2 - by_0^2 = a$. Если $z_0 \neq 0$, то $(1/z_0, y_0/z_0)$ — решение уравнения $ax^2+by^2 = 1$. Если же $z_0 = 0$, то $(1, y_0)$ — нетривиальный нуль формы $ax^2 + by^2$ и $(a,b)_p = 1$ согласно сказанному выше. Обратно, пусть (x_0, y_0) — решение уравнения $ax^2 + by^2 = 1$. Если $x_0 \neq 0$, то $(y_0/x_0, 1/x_0)$ — решение уравнения (28). Если же $x_0 = 0$, то $(y_0, 1)$ — нетривиальный нуль формы $z^2 - by^2$ и, следовательно, уравнение (28) также имеет решение.

Если b не является квадратом, то равенство (28) выражает тот факт, что a является нормой элемента $z + y\sqrt{b}$ квадратичного расширения $\mathbb{Q}_p(\sqrt{b})$ поля $\mathbb{Q}_p$ (см. [1], [6]). Отсюда, в частности, следует, что при фиксированном b все a, для которых $(a,b)_p = 1$, образуют подгруппу в группе $\mathbb{Q}_p^\times$ (содержащую подгруппу квадратов). Нетрудно показать, что это подгруппа индекса 2.

Локальные свойства символа Гильберта:

$$\text{(а) } (a,b)_p = (b,a)_p; \tag{29}$$

$$\text{(б) } (a_1a_2, b)_p = (a_1,b)_p(a_2,b)_p, \quad (a, b_1b_2)_p = (a,b_1)_p(a,b_2)_p; \tag{30}$$

$$\text{(в) если } (a,b)_p = 1 \text{ для всех } b, \text{ то } a \in \mathbb{Q}_p^{\times 2}; \tag{31}$$

$$\text{(г) } (a, 1-a)_p = 1 \text{ для всех } a; \tag{32}$$

$$\text{(д) если } p \neq 2, \infty \text{ и } |a|_p = |b|_p = 1, \text{ то } (a,b)_p = 1. \tag{33}$$

Свойства (а) и (б) тривиальны. Свойства (в) и (г) вытекают из описанной выше интерпретации символа Гильберта в терминах норм элементов поля $\mathbb{Q}_p(\sqrt{b})$. Свойство (д) выводится при помощи леммы Гензеля из того факта, что при любых целых a и b, не делящихся на p, сравнение $ax^2 + by^2 \equiv 1 \pmod p$ имеет решение. (Для доказательства последнего факта надо представить сравнение в виде $ax^2 \equiv 1 - by^2 \pmod p$ и посмотреть, сколько значений принимают левая и правая части при различных x и y.)

Вычисление символа Гильберта позволяет полностью решить вопрос о представлении нуля квадратичными формами над $\mathbb{Q}_p$ и, тем самым (с помощью теоремы Минковского – Хассе) — над $\mathbb{Q}$. В частности, из определения символа Гильберта и теоремы Минковского – Хассе следует, что форма

$$ax^2 + by^2 + cz^2 \quad (a, b, c \in \mathbb{Q}^\times), \tag{34}$$

представляет нуль над полем $\mathbb{Q}$ тогда и только тогда, когда $(-a/c, -b/c)_p = 1$ для всех p (включая $p = \infty$). Этот критерий является весьма эффективным, так как для почти всех p имеем $|a|_p = |b|_p = 1$, и в этом случае согласно свойству (д) $(a, b)_p = 1$, если только $p \neq 2, \infty$.

Очевидно, что $(a, b)_\infty = -1$, если a и b отрицательны, и $(a, b)_\infty = 1$ во всех остальных случаях. Выпишем теперь таблицы значений символа Гильберта для простых p.

Табл. 1. *Символ Гильберта для $p > 2$. Здесь v обозначает такое число $v \in \mathbb{Z}$, что $\left(\frac{v}{p}\right) = -1$; $\varepsilon = 1$, если $-1 \in \mathbb{Q}_p^{\times 2}$ (то есть если $p \equiv 1 \pmod 4$), и $\varepsilon = -1$ в противном случае.*

a / b	1	v	p	pv
1	$+1$	$+1$	$+1$	$+1$
v	$+1$	$+1$	-1	-1
p	$+1$	-1	ε	$-\varepsilon$
pv	$+1$	-1	$-\varepsilon$	ε

Отметим, в частности, что если a — целое число, не делящееся на p, то

$$(a, p)_p = \left(\frac{a}{p}\right). \tag{35}$$

Табл. 2. *Символ Гильберта в случае* $p = 2$.

a / b	1	5	-1	-5	2	10	-2	-10
1	$+1$	$+1$	$+1$	$+1$	$+1$	$+1$	$+1$	$+1$
5	$+1$	$+1$	$+1$	$+1$	-1	-1	-1	-1
-1	$+1$	$+1$	-1	-1	$+1$	$+1$	-1	-1
-5	$+1$	$+1$	-1	-1	-1	-1	$+1$	$+1$
2	$+1$	-1	$+1$	-1	$+1$	-1	$+1$	-1
10	$+1$	-1	$+1$	-1	-1	$+1$	-1	$+1$
-2	$+1$	-1	-1	$+1$	$+1$	-1	-1	$+1$
-10	$+1$	-1	-1	$+1$	-1	$+1$	$+1$	-1

В частности, если a и b — нечетные целые числа, то

$$(a, b)_2 = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}. \tag{36}$$

Глобальное свойство символа Гильберта (*формула произведения*). Пусть $a, b \in \mathbb{Q}^\times$. Тогда $(a, b)_p = 1$ для почти всех p и

$$\prod_p (a, b)_p = 1, \tag{37}$$

где произведение берется по всем p, включая ∞.

Формула (37) равносильна квадратичному закону взаимности. Действительно, ввиду мультипликативности символов Гильберта (свойство (б) выше) достаточно проверить ее для случаев, когда a и b — простые числа или -1. Предоставляя читателю рассмотрение остальных случаев, рассмотрим случай, когда a и b — различные нечетные простые числа. Так как в этом случае $(a, b)_p = 1$ для всех $p \neq a, b, 2$, то с учетом (35) и (36) формула произведения принимает вид

$$(-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}} \left(\frac{b}{a}\right)\left(\frac{a}{b}\right) = 1,$$

но это и есть квадратичный закон взаимности.

Отметим также следующее глобальное свойство нормирований $|\cdot|_p$, аналогичное свойству (37) и вытекающее непосредственно из их определения.

Формула произведения для нормирований. Пусть $a \in \mathbb{Q}^\times$. Тогда $|a|_p = 1$ для почти всех p и

$$\prod_p |a|_p = 1, \tag{38}$$

где произведение берется по всем p, включая ∞.

4. Кубические уравнения и эллиптические кривые

4.1. Проблема существования рационального решения

Для рациональных кубических форм $F(X, Y, Z)$ от трех переменных уже не известно никакого общего алгоритма, позволяющего установить существование нетривиального рационального решения уравнения $F = 0$, хотя изучено большое число конкретных уравнений, например уравнений вида

$$aX^3 + bY^3 + cZ^3 = 0.$$

Оказывается, для кубических форм перестает, вообще говоря, выполняться принцип Минковского – Хассе: например, уравнение $3X^3 + 4Y^3 + 5Z^3 = 0$ не имеет нетривиальных решений в рациональных числах, хотя имеет нетривиальные решения в поле вещественных чисел и во всех полях p-адических чисел (см. [1, гл. I, §7.6], где приведен план доказательства этого факта).

4.2. Сложение точек на кубической кривой

Кубическая форма $F(X, Y, Z)$ с комплексными коэффициентами задает кривую $\mathcal{C}$ на комплексной проективной плоскости $\mathbb{C}P^2$:

$$\mathcal{C} = \{(X : Y : Z) \in \mathbb{C}P^2 \mid F(X, Y, Z) = 0\}. \tag{39}$$

Форма F называется невырожденной, если частные производные $\dfrac{\partial F}{\partial X}$, $\dfrac{\partial F}{\partial Y}$, $\dfrac{\partial F}{\partial Z}$ не обращаются одновременно в нуль ни в какой точке $(X, Y, Z) \neq \neq (0, 0, 0)$. Геометрически это означает, что кривая $\mathcal{C}$ гладкая (не имеет особенностей).

Всякая прямая проективной плоскости пересекает гладкую кубическую кривую $\mathcal{C}$ ровно в трех точках, если считать точку касания с кратностью 2, а точку касания, являющуюся точкой перегиба кривой $\mathcal{C}$ — с кратностью 3.

Существует красивый геометрический способ определить сложение точек гладкой кубической кривой $\mathcal{C}$, превращающее ее в абелеву группу («метод секущих и касательных»), см. [8], [5], [13]. А именно, фиксируем точку $O \in \mathcal{C}$ (см. рис. 2). Если $P, Q \in \mathcal{C}$ — различные точки, то проведем через них прямую. Она пересечет $\mathcal{C}$ в однозначно определенной третьей точке R. Затем проведем прямую через R и O. Точку ее пересечения с $\mathcal{C}$ назовем суммой $P + Q$ точек P и Q. Аналогично определяется точка $2P$, но вместо секущей PQ следует взять касательную, проходящую через точку P (рис. 3).

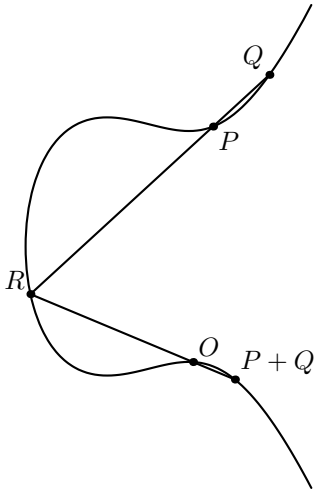

Рис. 2.

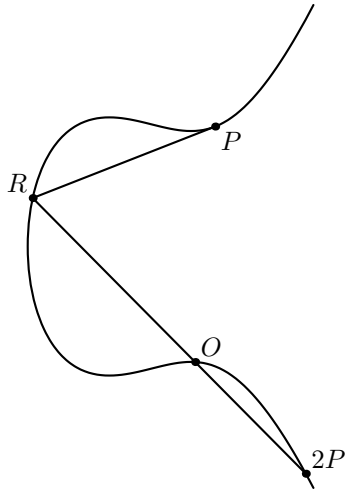

Рис. 3.

Коммутативность определенной таким образом операции сложения очевидна. Ее ассоциативность есть красивая теорема, обобщающая теорему Паскаля о шестиугольнике, вписанном в окружность (см., например, [5]). Роль нуля, как легко видеть, играет точка O. Точка, противоположная P, находится следующим образом. Проведем через точку O касательную. Она пересечет кривую $\mathcal{C}$ в некоторой точке O'. Теперь проведем прямую через O' и P. Третья точка ее пересечения с $\mathcal{C}$ и будет точкой, противоположной P.

Кубическая форма F называется неприводимой, если она не разлагается в произведение квадратичной и линейной форм. Геометрически это означает, что соответствующая кубическая кривая $\mathcal{C}$ не распадается на конику и прямую или на три прямые. Известно (см., например, [5]), что с помощью невырожденной линейной замены координат (над полем комплексных чисел) всякую неприводимую кубическую форму можно

привести к вейерштрассовой нормальной форме

$$Y^2Z - X^3 - aXZ^2 - bZ^3 \quad (a, b \in \mathbb{C}). \tag{40}$$

(см. также [8, т. 1, гл. 1, §6, следствие 3, с. 31]). Уравнение соответствующей кривой $\mathcal{C}$ в неоднородных координатах $x = X/Z$, $y = Y/Z$ примет тогда вид

$$y^2 = x^3 + ax + b, \tag{41}$$

Условие гладкости кривой (41) означает, что многочлен x^3+ax+b не имеет кратных корней, то есть его дискриминант $D = -4a^3 - 27b^2$ отличен от нуля.

Кривая (41) имеет единственную бесконечно удаленную точку $O = (0 : 1 : 0)$, являющуюся точкой перегиба. Если взять эту точку в качестве фиксированной точки при определении операции сложения, то легко найти явные выражения для координат суммы точек. А именно, сумма точек (x_1, y_1) и (x_2, y_2) при $x_1 \neq x_2$ есть точка с координатами

$$x_3 = -x_1 - x_2 + \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2, \quad y_3 = \frac{y_1 - y_2}{x_1 - x_2}(x_1 - x_3) - y_1. \tag{42}$$

Если $x_1 = x_2$, но $y_1 \neq y_2$, то $y_1 = -y_2$ и суммой данных точек является точка O; иными словами, точка $(x_1, -x_2)$ противоположна точке (x_1, x_2). Наконец, если $x_1 = x_2$ и $y_1 = y_2$, то

$$x_3 = -2x_1 + \left(\frac{3x_1^2 + a}{2y_1}\right)^2, \quad y_3 = \frac{3x_1^2 + a}{2y_1}(x_1 - x_3) - y_1. \tag{43}$$

4.3. Строение группы рациональных точек на кубической кривой

Предположим теперь, что кубическая форма $F(X, Y, Z)$ имеет рациональные коэффициенты. Если кривая $\mathcal{C}$, задаваемая уравнением $F = 0$, гладкая и имеет хотя бы одну рациональную точку, то она называется эллиптической кривой (над $\mathbb{Q}$). Метод секущих и касательных дает возможность «размножать» рациональные точки эллиптических кривых.

Более точно, если в качестве фиксированной точки O при определении операции сложения взята рациональная точка, то легко видеть, что сумма рациональных точек будет рациональна и точка, противоположная рациональной, также рациональна. Иными словами, рациональные точки кривой $\mathcal{C}$ образуют подгруппу в группе всех ее точек. Обозначим эту подгруппу через $\mathcal{C}(\mathbb{Q})$. Имеет место

Теорема 3 (теорема Морделла). *Абелева группа $\mathcal{C}(\mathbb{Q})$ конечно порождена.*

(См. [10], и приложение Ю. И. Манина к [3]).

Согласно теореме о строении конечнопорожденных абелевых групп, имеется разложение

$$\mathcal{C}(\mathbb{Q}) = \Delta \oplus \mathbb{Z}^r,$$

где Δ — конечная подгруппа, а $\mathbb{Z}^r$ — прямая сумма бесконечных циклических групп. Подгруппа Δ называется группой кручения, а ее элементы — точками кручения кривой $\mathcal{C}$. Число r называется рангом кривой $\mathcal{C}$ (над $\mathbb{Q}$).

О группе кручения Δ уже давно было кое-что известно. Так, Нагелль и позднее Лутц получили следующий интересный результат, дающий одновременно метод для явного определения точек кручения конкретных кривых: если $P = (x_P, y_P)$ — рациональная точка кручения на кривой, заданной уравнением $y^2 = x^3 + ax + b$, то ее координаты x_P и y_P являются целыми числами, причем либо $y_P = 0$, либо y_P^2 есть делитель дискриминанта $D = -4a^3 - 27b^2$ данной кривой.

Б. Мазур доказал в 1976 г., что группа Δ может быть изоморфна лишь одной из пятнадцати групп

$$\mathbb{Z}/m\mathbb{Z}\ (m \leqslant 10, m = 12),\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}\ (n \leqslant 4), \tag{44}$$

причем все возможности реализуются (см. [14], глава 6).

Вычисление ранга r остается открытой проблемой.

Приведение неприводимой кубической формы $F(X, Y, Z)$ к вейерштрассовой нормальной форме над полем рациональных чисел, вообще говоря, невозможно. Однако если соответствующая кубическая кривая $\mathcal{C}$ имеет хотя бы одну рациональную точку, то она изоморфна над $\mathbb{Q}$ некоторой кривой вида (41)(см. [8, §3, п.1] и [7, гл. III, §2, с. 113]). Изоморфизм задается рациональными функциями с рациональными коэффициентами и, в частности, переводит рациональные точки в рациональные (см. [8, §3, п.1]. Так как явный вид этого изоморфизма может быть достаточно легко найден, то, если известна одна рациональная точка кривой $\mathcal{C}$, нахождение всех остальных рациональных точек сводится к нахождению рациональных точек кривой вида (41).

Примеры. 1) Пусть кривая $\mathcal{C}$ задается уравнением

$$y^2 + y = x^3 - x,$$

целочисленные решения которого описывают все случаи, когда произведение двух последовательных целых чисел равно произведению некоторых других трех последовательных чисел. В этом примере группа Δ тривиальна и группа $\mathcal{C}(\mathbb{Q})$ (с бесконечно удаленной точкой в качестве нуля) является бесконечной циклической группой (то есть $r = 1$), причем в качестве ее образующей можно взять точку $P = (0, 0)$. Точки вида mP указаны на рис. 4.

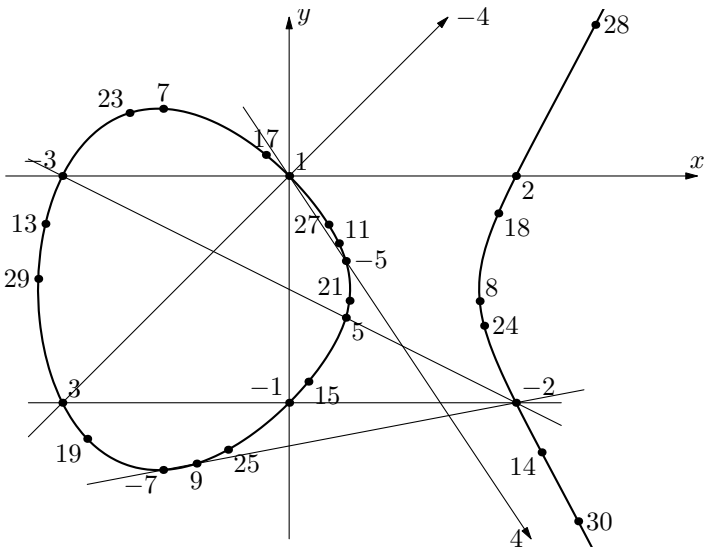

Рис. 4.

2) Пусть кривая $\mathcal{C}$ задается уравнением

$$y^2 + y = x^3 - 7x + 6.$$

Тогда $\mathcal{C}(\mathbb{Q}) = \mathbb{Z}^3$, причем в качестве свободных образующих этой группы можно взять точки $(1,0), (2,0), (0,2)$, см. [11].

3) Рассмотрим кривую $\mathcal{C} : y^2 = x^3 + 877x$. Можно показать, что образующая по модулю кручения группы $\mathcal{C}(\mathbb{Q})$ имеет x-координату

$$x = \frac{37549452812716219310550406994209279234620 1}{62159877768715054254632207806972380441 00}\,.$$

Этот пример дает определенное представление о трудностях нахождения рациональных точек бесконечного порядка на кубических кривых.

Для кубических кривых, имеющих особенности, описанный метод неприменим. Пусть, к примеру,

$$\mathcal{C} : \ y^2 = x^2 + x^3 \tag{45}$$

— кривая, изображенная на рис. 5. Тогда любая прямая, проходящая через точку $(0,0)$, имеет еще лишь одну общую точку с кривой $\mathcal{C}$. А именно, прямая $y = tx$ пересекает $\mathcal{C}$ в точке $(t^2-1, t(t^2-1))$. Поэтому, хотя и нельзя определить сложение точек, как в случае гладких кривых, мы находим все рациональные точки на $\mathcal{C}$ с помощью рациональной параметризации $x = t^2 - 1,\ y = t(t^2 - 1)$.

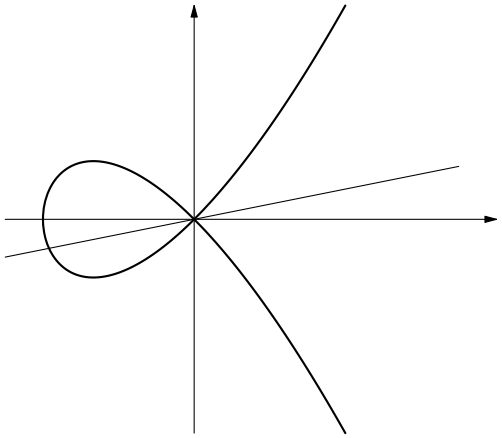

Рис. 5.

4.4. Кубические сравнения по простому модулю

Пусть p — простое число и $F(X,Y,Z)$ — невырожденная целочисленная кубическая форма. Решение сравнения $F \equiv 0 \pmod p$ равносильно решению уравнения $\overline{F} = 0$, где $\overline{F}$ обозначает кубическую форму над полем $\mathbb{Z}/p\mathbb{Z}$, полученную из F рассмотрением ее коэффициентов по модулю p.

Предположим, что форма F невырождена по модулю p. Это означает, что форма F и ее частные производные $\dfrac{\partial\overline{F}}{\partial X}$, $\dfrac{\partial\overline{F}}{\partial Y}$, $\dfrac{\partial\overline{F}}{\partial Z}$ не имеют общих нетривиальных нулей ни в каком конечном расширении поля $\mathbb{Z}/p\mathbb{Z}$.

Как и в случае поля рациональных чисел, если известно одно решение уравнения $\overline{F} = 0$ над $\mathbb{Z}/p\mathbb{Z}$, $p \neq 2,3$, то простые алгебро-геометрические идеи позволяют свести нахождение всех остальных решений к нахождению решений уравнения вида

$$y^2 = x^3 + ax + b,\ \ a, b \in \mathbb{Z}/p\mathbb{Z}. \tag{46}$$

Ясно, что число решений этого уравнения не превосходит $2p$, так как для каждого значения $x \in \mathbb{Z}/p\mathbb{Z}$ найдутся не больше двух значений $y \in \mathbb{Z}/p\mathbb{Z}$, таких, что (x,y) удовлетворяет уравнению. Однако лишь половина элементов из $(\mathbb{F}_p)^\times$ являются квадратами, поэтому можно ожидать, что число решений вдвое меньше (предположив, что значения x^3+ax+b разбросаны случайно в поле $\mathbb{Z}/p\mathbb{Z}$).

Более точно, пусть $\chi(x) = \left(\frac{x}{p}\right)$ при $x \neq 0$ и $\chi(0) = 0$. Тогда число решений уравнения $y^2 = u$ в $\mathbb{Z}/p\mathbb{Z}$ равно $1 + \chi(u)$ и мы получаем следующую формулу для числа точек кривой $\mathcal{C}$, заданной уравнением (46), над полем

$\mathbb{Z}/p\mathbb{Z}$ (с учетом бесконечно удаленной точки $(0:1:0)$):

$$\begin{aligned}\#\,\mathcal{C}(\mathbb{Z}/p\mathbb{Z}) &= 1+\sum_{x\in\mathbb{Z}/p\mathbb{Z}}(1+\chi(x^3+ax+b))\\ &= p+1+\sum_{x\in\mathbb{Z}/p\mathbb{Z}}\chi(x^3+ax+b).\end{aligned}$$

Коблиц сравнивает взятие суммы в этой формуле со случайным блужданием, при котором делается шаг вперед, если $\chi(x^3+ax+b)=1$, и шаг назад, если $\chi(x^3+ax+b)=-1$. Из теории вероятностей известно, что расстояние от исходной точки после p шагов при случайном блуждании будет иметь порядок $\sqrt{p}$. И действительно, это так: сумма всегда ограничена величиной $2\sqrt{p}$.

Теорема 4 (теорема Хассе). *Пусть* $N_p=\#\,\mathcal{C}(\mathbb{Z}/p\mathbb{Z})$. *Тогда*

$$|N_p-(p+1)|\leqslant 2\sqrt{p}.$$

Элементарное доказательство этого факта было дано Ю. И. Маниным в 1956 г.

4.5. От сравнений к рациональным точкам: гипотеза Бёрча и Суиннертона–Дайера

Знаменитый пример, связывающий локальную и глобальную информацию, дается гипотезой Бёрча и Суиннертона–Дайера для кубических кривых. Эта гипотеза принадлежит к числу семи проблем тысячелетия института Клея, за решение каждой из которых предложен приз в миллион долларов!

Пусть $\mathcal{C}$ — эллиптическая кривая, заданная уравнением

$$y^2=x^3+ax+b$$

с $a,b\in\mathbb{Z}$. Для $p\nmid\Delta=-16(4a^3+27b^2)$ положим $a_p=p+1-\#\mathcal{C}(\mathbb{Z}/p\mathbb{Z})$. Пусть

$$L(\mathcal{C},s)=\prod_{p\nmid\Delta}\frac{1}{1-a_pp^{-s}+p^{1-2s}}=\sum_{n=1}^{\infty}c_nn^{-s},\tag{47}$$

где c_n — какие-то целые числа. Из теоремы 4 следует, что последний ряд сходится абсолютно при $\operatorname{Re}(s)>\dfrac{3}{2}$.

Теорема 5 (Брёй, Конрад, Дайамонд, Тэйлор, Уайлс). *Функция $L(\mathcal{C},s)$ продолжается до аналитической функции на всей комплексной плоскости.*

Гипотеза 6 (Бёрча и Суиннертона–Дайера). *Разложение Тэйлора функции* $L(\mathcal{C}, s)$ *в* $s = 1$ *имеет вид*

$$L(\mathcal{C}, s) = c(s-1)^r + \text{члены высшей степени}, \tag{48}$$

где $c \neq 0$, *а* r *— ранг кривой* $\mathcal{C}$ *над* $\mathbb{Q}$.

(См. изложение в [14], главы 32–34, и в [15].)

Специальный случай гипотезы БСД утверждает, что $L(\mathcal{C}, 1) = 0$ тогда и только тогда, когда группа $\mathcal{C}(\mathbb{Q})$ бесконечна.

В статье [15] обсуждается история следующего результата:

Теорема 7 (Гросс, Колывагин, Загир и др.). *Предположим, что*

$$L(\mathcal{C}, s) = c(s-1)^r + \text{ члены высшей степени}$$

с $c \neq 0$ *и* $r \leqslant 1$. *Тогда гипотеза БСД справедлива для* $\mathcal{C}$, *то есть* r *— ранг кривой* $\mathcal{C}$ *над* $\mathbb{Q}$.

Джон Тэйт сделал доклад о гипотезе БСД для института Клея. Этот доклад можно посмотреть в интернете по адресу
`http://www.msri.org/publications/ln/hosted/cmi/2000/cmiparis/index-tate.html`

Отметим также, что гипотеза БСД допускает «экспериментальную» проверку. Для этого можно приближенно вычислять показатель r в разложении (48). Для вычислений с эллиптическими кривыми можно использовать компьютерную систему PARI (см. [9]). Например, для кривой $y^2+y = x^3-7x+6$ из примера 2) на с. 75 ранг равен 3. Приближенное вычисление показателя в формуле (48) дает значение 3.000011487248732705286325574.

* * * * * *

Статья основана на материалах лекций автора в Институте Фурье (Гренобль, Франция), в Эколь Нормаль (Лион, Франция), а также на материалах спецкурсов на мехмате МГУ в 1979–1991 и в 2001.

Искренне благодарю Эрнеста Борисовича Винберга за адаптирование первоначальной версии статьи для сборника «Математическое просвещение», посвященного p-адическим числам и их приложениям.

Список литературы

[1] Боревич З. И., Шафаревич И. Р. *Теория чисел*. Изд. 3е, доп. М.: Наука, 1985.

[2] Коблиц Н. *p-адические числа, p-адический анализ и дзета функции*. М.: Мир, 1982.

[3] Мамфорд Д. *Абелевы многообразия*. М.: Мир, 1971.

[4] Острик В. В., Цфасман М. А. *Алгебраическая геометрия и теория чисел: рациональные и эллиптические кривые*. М.: МЦНМО, 2005.

[5] Прасолов В. В., Соловьев Ю. П. *Эллиптические функции и алгебраические уравнения* М.: Факториал, 1997.

[6] Серр Ж.-П. *Курс арифметики*. М.: Мир, 1972.

[7] Степанов С. А. *Арифметика алгебраических кривых*. М.: Наука, 1991.

[8] Шафаревич И. Р. *Основы алгебраической геометрии*. Тт. 1–2. Изд. 2е. М.: Наука, 1988.

[9] Batut C., Belabas K., Bernardi H., Cohen H., Olivier M. *The PARI/GP number theory system*.
`http://pari.math.u-bordeaux.fr`

[10] Cassels J.W.S. *Diophantine equations with special reference to elliptic curves* // J. Lond. Math. Soc. Vol. 41, 1966. P. 193–291.

[11] Buhler J. P., Gross B. H., Zagier D. B. *On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank* 3 // Mathematics of Computation. Vol. 44, no. 170., 1985. P. 473–481.

[12] Manin Yu. I., *Selected papers of Yu. I. Manin*, World Scientific Series in 20th Century Mathematics, 3. World Scientific Publishing Co., Inc., River Edge, NJ, 1996. xii+600 pp.

[13] Manin Yu.I. and Panchishkin A.A., *Introduction to Modern Number Theory*, Encyclopaedia of Mathematical Sciences, vol. 49 (2nd ed.), Springer-Verlag, 2005, 514 p. (Русск. пер. М.: МЦНМО, 2008.)

[14] Stein W. *An Explicit Approach to Number Theory*.
`http://modular.fas.harvard.edu/edu/Fall2001/124/lectures/lectures_all/lectures.pdf`

[15] Wiles A. *The Birch and Swinnerton-Dyer Conjecture*.
`http://www.claymath.org/millennium/Birch_and_Swinnerton-Dyer_Conjecture/birchswin.pdf`

А. А. Панчишкин: Institut Fourier,Université de Grenoble I, France