p-адические числа, модулярные формы и их приложения

А. А. Панчишкин (Laboratoire J.-V.Poncelet /Институт Фурье, Гренобль, Франция)

Предлагаемый курс рассчитан на студентов и аспирантов, желающих познакомиться с теорией p-адических L-функций, связанных с модулярными формами, а также с их приложениями в диофантовой геометрии. Рассматриваются локальные и глобальные методы в арифметике. Дается обзор теории p-адических семейств модулярных форм, а также открытых проблем и задач теории p-адических L-функций.

Программа:

1. Сравнения и p-адические числа, лемма Гензеля. Поле Тэйта.
2. Непрерывные и аналитичические функции. Критерий Малера. Многоугольники Ньютона.
3. Меры, распределения и алгебра Ивасавы. Сравнения Куммера и p-адическая L-функция Куботы-Леопольдта.
4. Модулярные формы и L-функции.
5. Представления Галуа и сравнения между модулярными формами.
6. Метод проекции модулярных распределений. Примеры построения p-адических L-функций.

7 Обзор приложений к проблемам диофантовой геометрии.

8. Открытые проблемы и задачи в теории p-адических L-функций.

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. Серр Ж.-П. Курс арифметики. М.: Мир, 1972.
4. 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.)
5. Панчишкин А. А.. Локальные и глобальные методы в арифметике. Математическое просвещение, сер. 3, вып. 12, 2008 (55–79)
6. Панчишкин А. А.. Модулярные формы и p-адические числа. arXiv:0709.1611 (2007)
7. Panchishkin A.A.. A new method of constructing p-adic L-functions associated with modular forms, Московский Математический Журнал, 2 (2002), N 2, 1-16
8. Böcherer S., Panchishkin A.A. Admissible p-adic measures attached to triple products of elliptic cusp forms, Documenta Math. Extra volume : John H.Coates' Sixtieth Birthday (2006), 77-132.

Независимый Московский Университет,
Большой Власьевский пер. 11,
119002 Москва Российская Федерация

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:

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

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

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

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.

Математическое просвещение, сер. 3, вып. 12, 2008(55–79)

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

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

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

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

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:

$$\alpha = \begin{cases} \cdots a_{m+1}a_m\overbrace{000\dots0}^{m-1}{}_{(p)}, & \text{если } m \geqslant 0, \\ \cdots a_1a_0, a_{-1}\cdots a_{m(p)}, & \text{если } m < 0. \end{cases}$$

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

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

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

$$\frac{9}{7} = \cdots \overbrace{032412}\overbrace{032412}2_{(5)}.$$

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»:

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

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

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

— 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

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

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

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

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 $\alpha_0 \in \{1, 2, \dots, p-1\}$ удовлетворяет условию $|f(\alpha_0)|_p < 1$, в то время как $f'(\alpha_0) = (p-1)\alpha_0^{p-2} \not\equiv 0 \pmod p$, 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 $\frac{\partial F}{\partial X_i}(X^0) \neq 0$ хотя бы для одного i, то для любого Y^0 находится точка пересечения квадрики Q_F с этой прямой:

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

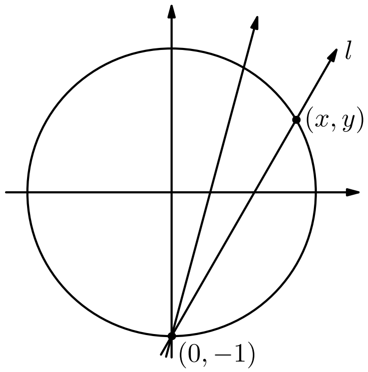

Рис. 1.

(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

$$F(X_0, X_1, \ldots, X_n) = 0 \qquad (22)$$

(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 $|x_0| < \sqrt{bc}, \quad |y_0| < \sqrt{ac}, \quad |z_0| < \sqrt{ab}$. 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:

(а) $(a,b)_p = (b,a)_p$; (29)

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

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

(г) $(a, 1-a)_p = 1$ для всех a; (32)

(д) если $p \neq 2, \infty$ и $|a|_p = |b|_p = 1$, то $(a,b)_p = 1$. (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.*

$b \backslash a$	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 $(X, Y, Z) \neq (0, 0, 0)$. 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).

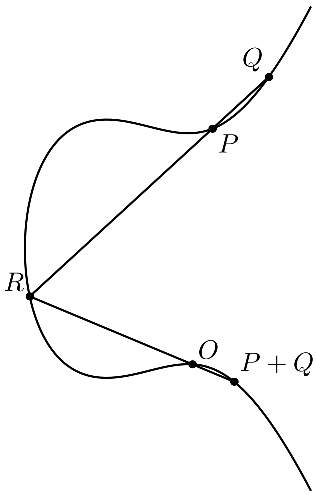

Рис. 2.

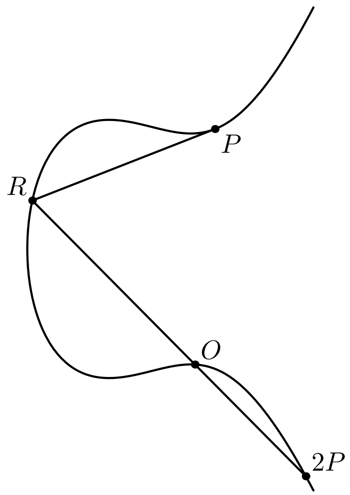

Рис. 3.

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.

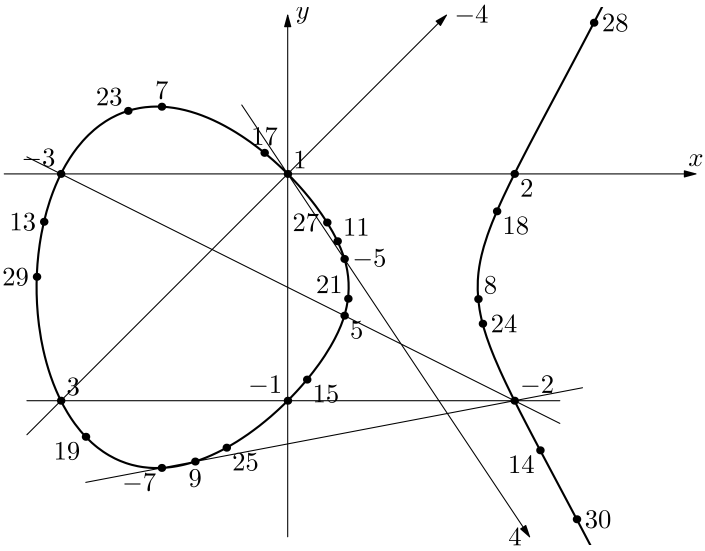

Рис. 4.

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

$$x = \frac{375494528127162193105504069942092792346201}{6215987776871505425463220780697238044100}.$$

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 $x = t^2 - 1,\ y = t(t^2 - 1)$.

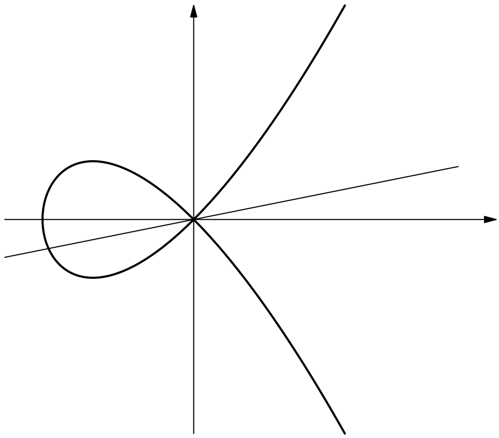

Рис. 5.

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

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

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

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

Модулярные формы и p-адические числа

А.А.Панчишкин

Аннотация

Пусть p – простое число. Обсуждаются p-адические свойства различных арифметических функций, связанных с коэффициентами модулярных форм и производяшими функциями. Модулярные формы рассматриваются как средство решения задач арифметики. Приведены примеры сравнений между модулярными формами, а также примеры компьютерных вычислений с модулярными формами и p-адическими числами.

Содержание

1 Введение

Статья основана на материалах спецкурсов автора в Университете Жозеф Фурье (Гренобль, Франция), лекций автора для французских педагогов в Институте Исследований Математического Просвещения (IREM, Гренобль, Франция) в 1998, в Эколь Нормаль (Лион, Франция), а также на материалах спецкурсов на мех-мате МГУ в 1979-1991 и в 2001.

В статье обсуждаются следующие темы:

1) Примеры производящих функций, модулярные формы и сравнения. Представление целых чисел квадратичными формами.

2) Ряды Эйзенштейна и сравнения для функции Рамануджана.

3) Числа и многочлены Бернулли, сравнения Куммера

4) Мера Мазура и p-адическое интегрирование.

2 Производящие функции, модулярные формы и сравнения.

2.1 Производящие функции

Традиционной областью применения производящих функций является комбинаторика и теория разбиений. Пусть $p(n)$ — число разбиений натурального числа n в сумму натуральных неубывающих слагаемых:

$$\begin{aligned}
&p(1) = 1 \quad : \quad 1 = 1;\\
&p(2) = 2 \quad : \quad 2 = 2, \quad 1+1;\\
&p(3) = 3 \quad : \quad 3 = 3, \quad 2+1, \quad 1+1+1;\\
&p(4) = 5; \quad p(5) = 7.
\end{aligned}$$

Тогда для производящей функции для $p(n)$ справедливо тождество Эйлера:

$$1 + \sum_{n=1}^{\infty} p(n) q^n = \prod_{m=1}^{\infty} (1 - q^m)^{-1}. \tag{2.1}$$

Действительно, непосредственное перемножение показывает, что

$$\begin{aligned}
&\prod_{m=1}^{\infty} (1-q^m)^{-1} = \prod_{m=1}^{\infty} (1 + q^m + q^{2m} + q^{3m} + \cdots) =\\
&(1 + q + q^2 + q^3 + \cdots) \times (1 + q^2 + q^4 + q^6 + \cdots) \times \cdots\\
&\cdots \times (1 + q^k + q^{2k} + q^{3k} + \cdots) \times \cdots = \sum_{a_1 \ge 0, a_2 \ge 0, a_3 \ge 0, \cdots} q^{a_1 + 2a_2 + 3a_3 + \cdots},
\end{aligned}$$

а $p(n)$ как раз и есть число решений целых числах $a_1, a_2, a_3, ..., > 0$ «уравнения с бесконечным числом переменных»

$$a_1 + 2a_2 + 3a_3 + \cdots = n.$$

Оказывается, что бесконечные произведения типа (2.1) тесно связаны с тэта-рядами. Например, при $|q| < 1,\ u \neq 0$ имеем(см. [And76])

$$\sum_{n=-\infty}^{\infty} u^n q^{n^2} = \prod_{m=0}^{\infty} (1 - q^{2m+2})(1 + uq^{2m+1})(1 + u^{-1} q^{2m+1}) \qquad \text{(Якоби)},$$

$$\sum_{n=0}^{\infty} q^{n(n+1)/2} = \frac{\prod_{m=1}^{\infty}(1-q^{2m})}{\prod_{m=1}^{\infty}(1-q^{2m-1})} \qquad (\text{Гаусс}),$$

которые выводятся из более общего тождества Коши: при $|q|<1,\ |t|<1,\ a\in\mathbb{C}$:

$$1+\sum_{n=1}^{\infty}\frac{(1-a)(1-qa)\dots(1-aq^{n-1})t^n}{(1-q)(1-q^2)\dots(1-q^n)} = \frac{\prod_{m=0}^{\infty}(1-atq^m)}{\prod_{m=0}^{\infty}(1-tq^m)}. \tag{2.2}$$

Вот иллюстрация вычисления с PARI-GP (см. [BBBCO]):

```
gp > {n=100;\\
prod(i=1,n,(1-x^(2*i)))*prod(i=1,n,((1-x^(2*i-1))^(-1))+O(x^(n+1)))
}
%5 = 1 + x + x^3 + x^6 + x^10 + x^15 + x^21 + x^28 + x^36 + x^45 + x^55 + x^66 +
 x^78 + x^91 + O(x^101)
gp > ##
  ***   last result computed in 451 ms.
```

2.2 Представление целых чисел квадратичными формами.

Пусть

$$f(x) = f(x_1,\dots,x_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j = A[x] = x^tAx,$$
$$g(y) = g(y_1,\dots,y_m) = \sum_{i,j=1}^{m} b_{ij}y_iy_j = B[y] = y^tBy,$$

—целочисленные квадратичные формы с матрицами A и B. Будем говорить, что квадратичная форма f *представляет* g *над* $\mathbb{Z}$ если для некоторой целочисленной матрицы $C\in M_{n,m}(\mathbb{Z})$ выполнено тождество

$$f(Cy) = g(y), \qquad A[C] = B. \tag{2.3}$$

В частности, при $m=1$ и $g(y)=by^2$, f представляет форму g если $f(c_1,\dots,c_n)=b$ для некоторых целых чисел $c_1,\dots,c_n$.

Лагранж доказал, что всякое целое число представимо суммой четырёх квадратов. Этот факт выводится также из (более трудной) теоремы Гаусса о том, что целое положительное число $b>0$ тогда и только тогда является суммой трех квадратов, когда оно не является числом вида $4^k(8l-1),\quad k,l\in\mathbb{Z}$ (см. [Se70], [Ma-Pa05]).

Пусть

$$r_k(n) = \mathrm{Card}\,\{(n_1,\dots,n_k)\in\mathbb{Z}^k \mid n_1^2+\dots+n_k^2 = n\}. \tag{2.4}$$

число представлений n в виде суммы k квадратов. Так, например, $r_2(5) = 8$, поскольку

$$\begin{aligned}5 &= 2^2 + 1^2 = 2^2 + (-1)^2 = (-2)^2 + 1^2 = (-2)^2 + (-1)^2 = \\ &= 1^2 + 2^2 = (-1)^2 + 2^2 = 1^2 + (-2)^2 = (-1)^2 + (-2)^2.\end{aligned}$$

В большом числе случаев найдены формулы для чисел представлений. Приведем лишь классический результат Якоби, (см. [And76], [Ma-Pa05]):

$$r_4(n) = \begin{cases} 8\sum_{d|n} d, & \text{если} \quad n \quad \text{нечётно,} \\ 24 \sum_{\substack{d|n \\ d\equiv 1(2)}} d, & \text{если} \quad n \quad \text{чётно.} \end{cases} \tag{2.5}$$

из которого также следует теорема Лагранжа. Метод доказательства этой теоремы основан на введении производящей функции для чисел $r_k(n)$:

$$\sum_{n=0}^{\infty} r_k(n) q^n = \sum_{(n_1,\ldots,n_k)\in\mathbb{Z}^k} q^{n_1^2+n_2^2+\cdots+n_k^2} = \theta(z)^k,$$

где

$$\theta(z) = \sum_{n\in\mathbb{Z}} q^{n^2}, \qquad q = e^{2\pi i z}. \tag{2.6}$$

— тэта-функция, которая рассматривается как голоморфная функция на верхней комплексной полуплоскости $\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}\,(z) > 0\}$ и обладает рядом замечательных аналитических свойств. Эти свойства позволяют однозначно охарактеризовать $\theta^4(z)$ как *модулярную форму веса* 2 относительно группы $\Gamma_0(4)$, где используется обозначения

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}) \;\middle|\; N|c \right\} \subset \mathrm{SL}(2,\mathbb{Z}). \tag{2.7}$$

Другими словами, голоморфный дифференциал $\theta^4(z)dz$ не меняется при дробно-линейных преобразованиях $z \mapsto (az+b)(cz+d)^{-1}$ с матрицей $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\Gamma_0(4)$ (и удовлетворяет оценкам регулярности роста при $\mathrm{Im}\,(z) \to \infty$ в вершинах; заметим, что $2\pi i dz = \frac{dq}{q}$, поэтому дифференциал мероморфен с простым полюсом в точке $q = 0 \Longleftrightarrow z = i\infty$).

2.3 Мотивировка: функция Рамануджана τ и её контекст.

В качестве иллюстрации к общей теории приведём несколько удивительных свойств функции Рамануджана τ.

Этот знаменитый пример происходит из происходит из следуюшей производяшей функции, определённой разложением в ряд следующего бесконечного произведения:

$$q \prod_{m\geq 1} (1-q^m)^{24} = \sum_{n\geq 1} \tau(n) q^n = q - 24q^2 + 252q^3 - 1472q^4 + \cdots$$

Положим $q = \exp(2i\pi z)$ для z из верхней комплексной полуплоскости $\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$, это голоморфное отображение $\mathbb{H}$ на единичный круг с выколотым центром $q : \mathbb{H} \to D(0,1)\backslash\{0\}$.

Определяется функция $\Delta : \mathbb{H} \to \mathbb{C}$, голоморфная на $\mathbb{H}$, по формуле:

$$\Delta(z) = \Delta_\infty(q) = q \prod_{m\geq 1} (1-q^m)^{24}$$

Эта функция даёт пример модулярной формы. Она обладает рядом замечательных свойств:

Автоморфность

Группа $\mathrm{SL}(2,\mathbb{Z})$ целочисленных квадратных 2×2-матриц с определителем 1 действует на $\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ по формуле

$$\forall\gamma = \begin{pmatrix} a\ b \\ c\ d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}), \quad \left(\begin{pmatrix} a\ b \\ c\ d \end{pmatrix}, z\right) \mapsto \gamma\cdot z = \frac{az+b}{cz+d}.$$

Свойство автоморфности имеет вид:

$$\forall\gamma = \begin{pmatrix} a\ b \\ c\ d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}),\ \forall z \in \mathbb{H} \Rightarrow \Delta(\gamma\cdot z) = (cz+d)^{12}\Delta(z). \tag{2.8}$$

Заметим, что свойство автоморфности (2.8)равносильно тому, что, голоморфный дифференциал

$\Delta(z)(dz)^6$ не меняется при дробно-линейных преобразованиях $z \mapsto (az+b)(cz+d)^{-1}$ с матрицей $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\mathrm{SL}(2,\mathbb{Z})$, поскольку для всех $\gamma \in \mathrm{SL}(2,\mathbb{Z})$, и для всех $z \in \mathbb{H}$, имеем

$$\gamma = \begin{pmatrix} a\ b \\ c\ d \end{pmatrix} \Rightarrow d(\gamma\cdot z) = (cz+d)^{-2}dz.$$

Отсюда непосредственно вытекает, что для любого натурального m группа $\mathrm{SL}(2,\mathbb{Z})$ действует на множестве голоморфных функций $f(z)$на $z \in \mathbb{H}$ по формуле: для $\gamma \in \mathrm{SL}(2,\mathbb{Z})$, и для $z \in \mathbb{H}$, имеем

$$\gamma = \begin{pmatrix} a\ b \\ c\ d \end{pmatrix} \Rightarrow (f|_{2m}\gamma)(z) = (cz+d)^{-2m}f(\gamma\cdot z),$$

(действие веса $2m$), а свойство автоморфности (2.8) означает, что $\forall\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \Rightarrow \Delta|_{12}\gamma = \Delta$. Поэтому (2.8) достаточно проверить на образующих группы $\mathrm{SL}(2,\mathbb{Z})$. Используем тот факт, что группа $SL(2,\mathbb{Z})$ порождена матрицами $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ и $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Чтобы в этом убедиться, используется алгоритм Евклида применительно к паре (a,b), а также степени элемента S, имеющего порядок 4.

Отсюда выводится, что свойство автоморфности (2.8) достаточно проверять для элементов S и T, т.е.

$$\Delta(z+1) = \Delta(z), \quad \Delta(-1/z) = z^{12}\Delta(z),$$

см. ниже.

Мультипликативность.

Функция Рамануджана τ мультипликативна в следуюшем смысле [обозначим через $\mathbf{P}$ множество всех простых чисел]:

$$\begin{cases} \forall m \in \mathbb{N}^*,\ \forall n \in \mathbb{N}^*,\ (m,n)=1 \Rightarrow \tau(mn)=\tau(m)\cdot\tau(n); \\ \forall p \in \mathbf{P},\ \forall r \in \mathbb{N}^*,\ \tau(p^{r+1})=\tau(p^r)\tau(p)-p^{11}\tau(p^{r-1}); \\ \forall m \in \mathbf{N}^*,\ \forall n \in \mathbb{N}^*,\ \tau(m)\tau(n)=\sum\limits_{d|(m,n)} d^{11}\tau(mn/d^2). \end{cases}$$

Эти свойства были предположены Рамануджаном и доказаны Морделлом и Гекке. Возможно, однако, что не существует “элементарного” доказательства этих свойств, в духе теоремы Гёделя о недоказуемости средствами элементарной арифметики, см.[Ма-Ра05]. Может оказаться, что же замечание относится и к теореме Ферма, доказаной Уайлсом в 1994 в высшей степени “неэлементарными” методами [включающими теорию модулярных форм, p-адический анализ, теорию деформаций представлений Галуа, алгебраическую геометрию, ...].

Естественная формулировка свойств мультипликативности функции Рамануджана использует ряд Дирихле, связанный с функцией τ:

$$L(\Delta,s)=\sum_{n\geq 1}\tau(n)n^{-s}=\prod_{p\in\mathbf{P}}\left(1-\tau(p)p^{-s}+p^{11-2s}\right)^{-1}.$$

Этот ряд аналогичен ряду Дирихле задающему дзета-функцию Римана,

$$\zeta(s)=\sum_{n\geq 1}n^{-s}=\prod_{p\in\mathbf{P}}\left(1-p^{-s}\right)^{-1},$$

где равенство выражает свойство существования и единственности разложения натурального числа в произведение простых чисел.

Точно так же и в случае функции Рамануджана τ, справедливо тождество

$$\sum_{n\geq 1}\tau(n)n^{-s}=\prod_{p\in\mathbf{P}}\left(\sum_{r\geq 0}\tau\big(p^r\big)p^{-rs}\right),$$

а доказательство рекуррентных формул сводится к равенству:

$$\left(1-\tau(p)p^{-s}+p^{11-2s}\right)\cdot\left(\sum_{r\geq 0}\tau(p^r)p^{-rs}\right)=1$$

Оценки.

Следующее свойство, первоначально предположенное Рамануджаном, было доказано Делинем:

$$\forall p\in\mathbf{P},\ |\tau(p)|<2p^{11/2}.$$

Это свойство эквивалентно отрицательности дискриминанта многочлена второй степени $X^2-\tau(p)X+p^{11}$, для всех простых чисел p. Для фиксированного p, пусть α_p и β_p – комплексно-сопряжённые корни этого многочлена. Из формулы мультипликативности следует, что:

$$\frac{1}{(1-\tau(p)X+p^{11}X^2)} = \frac{1}{(1-\alpha_p X)(1-\beta_p X)} = \left(\sum_{r\geq 0}\tau(p^r)X^r\right).$$

Для всех $r \geq 1$ выводится соотношение $\tau(p^r) = \sum_{j=0}^{r}\alpha_p^j\beta_p^{r-j} = \sum_{j=0}^{r}\alpha_p^{2j-r}p^{11(r-j)}$. Абсолютная величина α_p равна $p^{11/2}$, откуда следует оценка

$$|\tau(p^r)| < (r+1)p^{11r/2}.$$

Применение формального тождества даёт следующую оценку

$$\forall n \in \mathbb{N}^*,\ |\tau(n)| < \sigma_0(n)n^{11/2} = O(n^{\frac{11}{2}+\varepsilon})$$

где $\sigma_0(n)$ – число делителей числа n, где $O(\ln(n)) = O(n^\varepsilon)$ для любого $\varepsilon > 0$.

Отсюда, в частности, выводится, что ряд $L(\Delta, s)$ абсолютно сходится и определяет голоморфную функцию в правой полуплоскости $\mathrm{Re}(s) > 13/2$.

Функциональное уравнение для $L(\Delta, s)$.

Определим функцию $L^*(\Delta, s)$ по формуле $L^*(\Delta, s) = (2\pi)^{-s}\Gamma(s)L(\Delta, s)$. Эта функция, с одной стороны, продолжается до голоморфной функции на всей комплексной плоскости $\mathbb{C}$, и эта функция удовлетворяет функциональному уравнению $L^*(\Delta, 12-s) = L^*(\Delta, s)$. Можно сравнить это функциональное уравнение с функциональнум уравнением для дзета-функции Римана $\zeta(s)$

$$\zeta^*(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s) = \zeta^*(1-s).$$

Связь с числами разбиений.

Напомним,что разбиением натурального числа n называется неубывающая последовательность натуральных чисел с суммой, равной n. Функция числа разбиений обозначается через $p : \mathbb{N} \to \mathbb{N}$ причём полагают $p(0) = 1$.

Как мы видели, производящий ряд функции $p : \mathbb{N} \to \mathbb{N}$ даётся бесконечным произведением $\sum_{n\geq 0} p(n)q^n = \prod_{m\geq 1}(1-q^m)^{-1}$. Соответствующая голоморфная функция переменной q сходится в открытом круге. Поэтому получается голоморфная функция на $\mathbb{H}$, $f : \mathbb{H} \to \mathbb{C}$ где

$$f(q) = \sum_{n\geq 0} p(n)q^n = \prod_{m\geq 1}(1-q^m)^{-1}.$$

Имеет место равенство $\tilde{\Delta}(q) = q(f(q))^{-24}$ связываюшее функцию числа разбиений и функцию Рамануджана τ.

Используя свойство автоморфности, Харди и Рамануджан доказали следующую оценку для $p(n)$:

$$p(n) = \left(\frac{1}{4\sqrt{3}} + O\left(\frac{1}{\lambda(n)}\right)\right)\cdot\frac{\exp(K\cdot\lambda(n))}{\lambda(n)^2}$$

где $\lambda(n) = \sqrt{n - \frac{1}{2}}$ и $K = \pi\sqrt{2/3}$ (см. [Chand70]).

Сравнение Рамануджана и представления групп Галуа.

Сравнение Рамануджана утверждает, что

$$\forall n \in \mathbb{Z}^+,\ \tau(n) \equiv \sum_{d|n} d^{11} \bmod 691. \tag{2.9}$$

В частности, $\tau(691) = -2747313442193908 \equiv 1 \bmod 691$.

Достаточно проверить справедливость сравнения $\tau(p) \equiv 1+p^{11} \bmod 691$ для любого простого числа p отличного от 691. Действительно, тогда в силу мультипликативности и в силу рекуррентных соотношений по r будем иметь

$$\tau(p^{r+1}) \equiv \tau(p^r)\tau(p) - p^{11}\tau(p^{r-1}) \equiv \sum_{j=0}^{r+1} p^{11j} \bmod 691,$$

откуда будет следовать и общее сравнение (2.9). Серр нашёл объяснение этого курьёзного сравнения в рамках теории представлений групп Галуа.

Пусть $\overline{\mathbb{Q}}$ – алгебраическое замыкание поля $\mathbb{Q}$ рациональных чисел. Пусть p – простое число, отличное от 691 и $\mathfrak{p}$ – произвольный простой идеал над (p) в кольце $\mathcal{O}$ целых элементов $\bar{\mathbb{Q}}$. Обозначим через $G_\mathfrak{p}$ и $I_\mathfrak{p}$ подгруппы группы Галуа $G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ определенные равенствами:

$$\begin{aligned} G_\mathfrak{p} &= \{\sigma \in G \mid \sigma\mathfrak{p} = \mathfrak{p}\} \\ I_\mathfrak{p} &= \{\sigma \in G_\mathfrak{p} \mid \forall x \in \mathcal{O},\ \sigma x \equiv x \bmod \mathfrak{p}\}. \end{aligned}$$

Группа $G_\mathfrak{p}$ называемая группой разложения, отождествляется с группой Галуа алгебраического замыкыния $\overline{\mathbb{Q}}_p$ поля $\mathbb{Q}_p$ p-адических чисел, её нормальная подгруппа $I_\mathfrak{p}$ называется группой инерции, а фактор-группа $G_\mathfrak{p}/I_\mathfrak{p}$ отождествляется с группой Галуа алгебраического замыкыния конечного поля $\mathbb{F}_p$. Эта группа порождается элементом Фробениуса Fr_p.

Серр предположил, а Делинь доказал, что для любого простого числа l, существует такое представление Галуа $\rho_l : G \to \mathrm{GL}(2, \mathbb{Z}_l)$, что для любого простого числа p отличного от l, группа инерции $I_\mathfrak{p}$ тривиально действует (т.е. ρ_l неразветвлено в p), и $\det(\mathrm{Id} - \rho_l(Fr_p) \cdot X) = 1 - \tau(p)X + p^{11}X^2$. В случае $l = 691$ справедливо сравнение $\rho_l(Fr_p) \equiv \left(\begin{smallmatrix} p^{11} & \star \\ 0 & 1 \end{smallmatrix}\right) \bmod 691$, откуда $\tau(p) \equiv 1 + p^{11} \bmod 691$.

Впоследствии, такие представления Галуа послужили основой для доказательства теоремы Уайлса о модулярности эллиптических кривых (1994), а также гипотез Серра о модулярности всех нечётных двумерных представлений Галуа над конечными полями, доказанных в 2007 Ч.Кхаре и Ж.-П. Винтенберже с использованием методов М.Кисина, Ж.-М. Фонтэна и Р.Тэйлора (Летняя школа в Марселе-Люмини, июль 2007).

Формулы Ю.И.Манина

Используя цепные дроби и модулярные символы, Ю.И.Манин нашёл формулы для функции Рамануджана $\tau(n)$, даюшие гораздо более быстрый метод вычисления этой функции, чем метод разложения в ряд бесконечного произведения, или же метод основанный на рядах Эйзенштейна ($\Delta = (E_4^3 - E_6^2)/1728$). Эти формулы таковы:

$$\tau(n) = \sigma_{11}(n) - \sum{}^{*(n)} \left(\frac{691}{18}(\Delta^8\delta^2 - \Delta^2\delta^8) - \frac{691}{6}(\Delta^6\delta^4 - \Delta^4\delta^6) \right);$$

Рис. 1: Летняя школа "Гипотезы Серра о модулярности" в Марселе-Люмини, июль 2007

$$\tau(n) = \sigma_{11}(n) - \frac{691}{18} \sum{}^{*(n)} \Delta^2\delta^2(\Delta^2 - \delta^2)^3$$

где $\sigma_{11}(n) = \sum\limits_{d|n} d^{11}$ а во внешней сумме $\sum^{*(n)}$ справа суммирование производится по всем целым решениям уравнения, $n = \Delta\Delta' + \delta\delta'$, котрые "допустимы", т.е. удовлетворяют условиям

$$\big\{(\Delta, \delta)\big|n = \Delta\Delta' + \delta\delta',\ \Delta > \delta > 0,\ \Delta' > \delta' > 0,\ \text{где}$$
$$\Delta|n,\ \Delta' = \frac{n}{\Delta},\ \delta' = 0,\ 0 < \frac{\delta}{\Delta} \leq \frac{1}{2}\big\}.$$

Кроме того, члены с $\frac{\delta}{\Delta} = \frac{1}{2}$ берутся в сумме с коэффициентом $\frac{1}{2}$. Эта формула, в частности, даёт новое доказательство сравнений Рамануджана

$$\tau(n) \equiv \sigma_{11}(n)(\mathrm{mod} 691).$$

С помощью этих формул можно также найти $\tau(6911) = -615012709514736031488$, причём оказывается, что $\tau(6911) \equiv 1 + 6911^{11}(\mathrm{mod} 691)$, но $\tau(6911) \not\equiv 1 + 6911^{11}(\mathrm{mod} 691^2)$.

Вычисление с PARI-GP

(см. также

```
http://www.research.att.com/~njas/sequences/A000594, и
D. H. Lehmer, Tables of Ramanujan's function tau(n), Math. Comp., 24 (1970), 495-496.)

Программа на PARI-GP:
{
m=11;n=2 ;si(n,m)= p=0; fordiv(n,d, p+= d^m); p \\ сумма степеней делителей
}
{
s1(n)=d3=1; vd1=[]; c1=0;
\\ первая часть суммы (с \Delta>\delta>0,\ \Delta'>\delta'>0
for(d1=1,n-1, for(d2=1,n-1,if(n-d1*d2>0,
fordiv(n-d1*d2, d3,if(((d3<d1)& ((n-d1*d2)/d3<d2)),
d4=(n-d1*d2)/d3; c1=c1+1;
vd1=concat(vd1,[[d1,d2,d3,d4,c1]]);
print("Delta="d1,"\t", "Deltap="d2,"\t","delta="d3,"\t", " deltap=" (n-d1*d2)/d3,"\t",c1);
)))));vd1
}
{
s2(n)= c2=c1; vd2=[];fordiv(n, d1, d2=n/d1;d4=0;for(d3=0,d1/2, \\ вторая часть суммы (с \delta'=0)
if(d3==d1/2, c=1/2, c=1); c2=c2+1;
vd2=concat(vd2, [[d1,d2,d3,d4,c, c2]]);
print("Delta="d1,"\t", "Deltap="d2,"\t","delta="d3,"\t", "deltap="d4,"\t",  c ,"\t",c2)
)) ; vd2
}
{
tau(n)=s1(n); s2(n); lvd1=length(vd1); lvd2=length(vd2); sn=0;
for(i1=1,lvd1, sn+=
vd1[i1] [1]^2* vd1[i1] [3]^2*(vd1[i1] [1]^2- vd1[i1] [3]^2)^3);
for(i2=1,lvd2,sn+=
(vd2[i2] [5])*vd2[i2] [1]^2* vd2[i2] [3]^2*(vd2[i2] [1]^2- vd2[i2] [3]^2)^3);
si(n,11)-(691/18)*sn
}

gp > tau(100)
Delta=2 Deltap=34       delta=1  deltap=32      1
Delta=2 Deltap=35       delta=1  deltap=30      2
Delta=2 Deltap=36       delta=1  deltap=28      3
Delta=2 Deltap=37       delta=1  deltap=26      4

...................................................................

Delta=100       Deltap=1        delta=50        deltap=0        1/2     291

%3 = 37534859200 \\ \\ результат: tau(100)
gp > ##
```

```
***   last result computed in 160 ms.
```

Много других методов см. в [Sloane], [Leh70]. Отметим открытую проблему (проблема Лемера) о том, что $\tau(n)$ не обращается в нуль.

Другая нтересная открытая проблема состоит в построении полиномиального алгоритма вычисления $\tau(p)$ для простого числа p. Аналогичный результат известен для коэффициентов $a(p)$ производяшего ряда $f_E(z)$ эллиптической кривой E над $\mathbb{Q}$ ("алгоритм Схоофа"). По теореме Уайлса, такой ряд является модулярной формой веса 2 относительно некоторой конгруэнц-подгруппы модулярой группы, в то время,как $\tau(p)$ являются коэффициентами модулярной формы веса 12 относительно полной модулярой группы.

3 Классические модулярные формы

вводятся как некоторые голоморфные функции на верхней комплексной полуплоскости $\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}\ z > 0\}$, которую можно также рассмативать как однородное пространство группы $G(\mathbb{R}) = \mathrm{GL}_2(\mathbb{R})$:

$$\mathbb{H} = \mathrm{GL}_2(\mathbb{R})/\mathrm{O}(2) \cdot Z, \tag{3.10}$$

где $Z = \{\left(\begin{smallmatrix} x & 0 \\ 0 & x \end{smallmatrix}\right) \ |x \in \mathbb{R}^\times\}$ центр группы $G(\mathbb{R})$ а $\mathrm{O}(2)$ ортогональная группа. При этом группа $\mathrm{GL}_2^+(\mathbb{R})$ матриц $\gamma = \begin{pmatrix} a_\gamma & b_\gamma \\ c_\gamma & d_\gamma \end{pmatrix}$ с положительным определителем действует на $\mathbb{H}$ дробно-линейными преобразованиями; на левых смежных классах (3.10) это действие переходит в естественное действие групповыми сдвигами.

Пусть Γ – подгруппа конечного индекса в модулярной группе $\mathrm{SL}_2(\mathbb{Z})$.

Определение 3.1 *Голоморфная функция на верхней комплексной полуплоскости* $\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}\ z > 0\}$ $f : \mathbb{H} \to \mathbb{C}$ *называется модулярной форой целого веса* k *относительно* Γ, *если выполнены следуюшие условия a) и b):*

a) Условие автоморфности

$$f((a_\gamma z + b_\gamma)/(c_\gamma z + d_\gamma)) = (c_\gamma z + d_\gamma)^k f(z) \tag{3.11}$$

для всех $\gamma \in \Gamma$;

b) Регулярность в вершинах: f *регулярна в вершинах* $z \in \mathbb{Q} \cup i\infty$; *это означает, что для каждого элемент* $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ *функция* $(cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right)$ *разлагается в ряд Фурье по неотрицательным степеням* $q^{1/N} = e(z/N)$ *для некоторого натурального числа* N. *Модулярная форма*

$$f(z) = \sum_{n=0}^{\infty} a(n) e(nz/N)$$

называется параболической, если f *обращается в нуль во всех вершинах*

(т.е. их разложения Фурье содержат лишь строго положительные степени $q^{1/N}$*),*

see [Se70], [Ma-Pa05], глава 6. Комплексное векторное пространство всех модулярных форм (соотв. параболических) форм веса k относительно Γ обозначается $\mathcal{M}_k(\Gamma)$ (соотв. $\mathcal{S}_k(\Gamma)$).

Фундаментальный результат теории модулярных форм утверждает, что эти пространства конечномерны. Кроме того, имеем $\mathcal{M}_k(\Gamma)\mathcal{M}_l(\Gamma) \subset \mathcal{M}_{k+l}(\Gamma)$. Прямая сумма

$$\mathcal{M}(\Gamma) = \bigoplus_{k=0}^{\infty} \mathcal{M}_k(\Gamma)$$

является градуированной алгеброй над $\mathbb{C}$ с конечным числом образующих.

Пример модулярных форм относительно $\mathrm{SL}_2(\mathbb{Z})$ веса $k \geq 4$ даётся *рядами Эйзенштейна*

$$G_k(z) = \sum_{m_1,m_2\in\mathbb{Z}}{}' (m_1 + m_2 z)^{-k} \tag{3.12}$$

(прим означает, что $(m_1, m_2) \neq (0,0)$). Для этих рядов условие автоморфности (3.11) непосредственно выводится из определения. Имеем $G_k(z) \equiv 0$ для нечётных k и

$$G_k(z) = \frac{2(2\pi i)^k}{(k-1)!}\left[-\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n)e(nz)\right], \tag{3.13}$$

где $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$ и B_k обозначает k^{e} *число Бернулли.*

Градуированная алгебра $\mathcal{M}(\mathrm{SL}_2(\mathbb{Z}))$ изоморфна кольцу многочленов от независимых переменных G_4 и G_6.

3.1 Фундаментальная область модулярной группы

Пусть $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Имеем

$$S(z) = -z^{-1},\ T(z) = z + 1.$$

С другой стороны, пусть D подмножество $\mathbb{H}$ состояшее из точек z таких, что $|z| \;>\geq 1$ и $|\mathrm{Re}(z)| \leq 1/2$. Мы увидим, что D является фундаментальная областью для действия модулярной группы $\Gamma(1) = \mathrm{SL}(2,\mathbb{Z})$ на $\mathbb{H}$, т.е. естественное отображение проекции $D \to \Gamma(1)\backslash\mathbb{H}$ сюръективно, а его ограничение на внутренность D инъективно. В то же время мы видели, что S и T порождают $\Gamma(1) = \mathrm{SL}(2,\mathbb{Z})$.

Теорема 3.2 *1) Для всех $z \in \mathbb{H}$ существует матрица $\gamma \in \Gamma(1)$, такая, что $\gamma(z) \in D$.*
2) Предположим, что две различные точки $z, z' \in D$ эквивалентны при действии $\Gamma(1)$. Тогда или $\mathrm{Re}(z) = \pm 1/2$ и $z = z' + 1$, или $|z| = 1$ и $z' = -1/z$.
3) Пусть $z \in D$, и пусть $St(z) = \{\gamma \in \Gamma(1) \mid \gamma(z) = z\}$ стабилизатор точки z в $\Gamma(1)$. Тогда имеем $St(z) = \{\pm 1\}$ за исключением трёх следующих случаев:
$z = i$, при этом $St(z)$ группа порядка 4 порождённая S;
$z = \rho = e^{2\pi i/3}$, при этом $St(z)$ группа порядка 6 порождённая элементом $ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$;
$z = -\overline{\rho} = e^{\pi i/3}$, при этом $St(z)$ группа порядка 6 порождённая элементом $TS = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$.

Множество $\mathbb{H}/\,\mathrm{SL}_2(\mathbb{Z})$ можно отождествить с можеством классов изоморфизма эллиптических кривых над $\mathbb{C}$: точке $z \in \mathbb{H}$ сопоставляется комплексный тор $\mathbb{C}/(\mathbb{Z}+z\mathbb{Z})$ который аналитически изоморфен римановой поверхности эллиптической кривой, записанной в форме Вейерштрасса:

$$y^2 = 4x^3 - g_2(z)x - g_3(z) \tag{3.14}$$

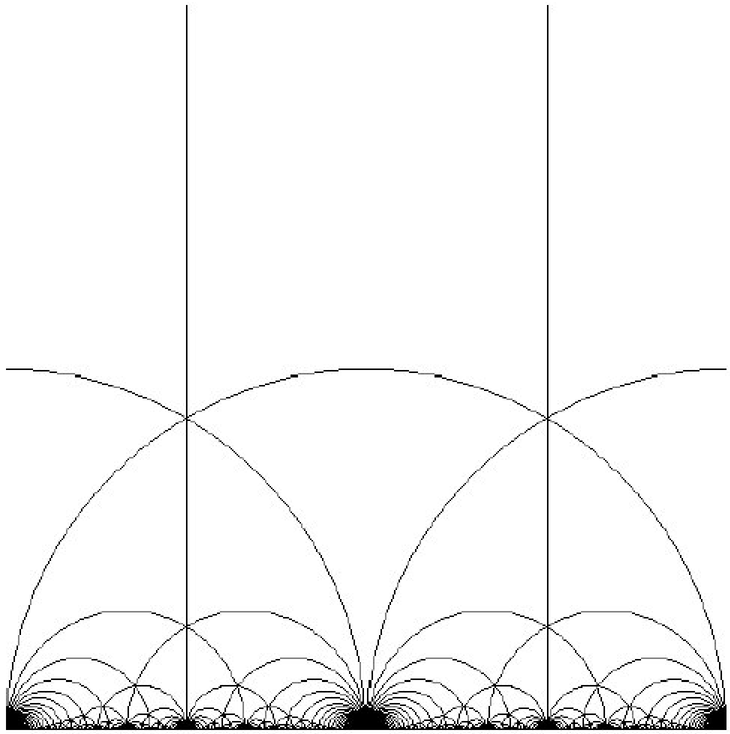

Рис. 2: Действие группы $\mathrm{SL}(2,\mathbb{Z})$.
На рисунке 2 представлено действие группы $\mathrm{SL}(2,\mathbb{Z})$ на верхней комплексной полуплоскости.

где $g_2 = 60G_4(z)$, $g_3(z) = 140G_6(z)$.

При замене z на $\gamma(z)$ для $\gamma = \begin{pmatrix} a_\gamma & b_\gamma \\ c_\gamma & d_\gamma \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ решётка $\Lambda_z = \mathbb{Z} + z\mathbb{Z}$ заменится на

$$\Lambda_{\gamma(z)} = \mathbb{Z} + \gamma(z)\mathbb{Z} = (cz+d)^{-1}(\mathbb{Z} + z\mathbb{Z}) = (cz+d)^{-1}\Lambda_z,$$

а кривая (3.14) примет каноническую форму Вейерштрасса с коэффициентами

$$g_2(\gamma(z)) = (cz+d)^4 g_2(z), \quad g_3(\gamma(z)) = (cz+d)^6 g_3(z).$$

Дискриминант кубического многочлена справа (3.14) является модулярной параболической формой веса 12 относительно группы $\Gamma = \mathrm{SL}_2(\mathbb{Z})$:

$$2^{-4}(g_2^3 - 27g_3^2) = \tag{3.15}$$
$$2^{-4}(2\pi)^{12} q \prod_{m=1}^{\infty}(1-q^m)^{24} = 2^{-4}(2\pi)^{12}\sum_{n=1}^{\infty}\tau(n)q^n,$$

где $\tau(n)$ функция Рамануджана. При этом функция

$$j(z) = 1728\frac{g_2^3}{g_2^3 - 27g_3^2} = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} c(n)q^n \tag{3.16}$$

мероморфна на $\mathbb{H}$ и в ∞, и не меняется при дробно-линейных преобразованиях с матрицами из $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. Эта функция доставляет важный пример *модулярной функции* и называется *модулярным инвариантом*

3.2 Модулярные формы как вычислительное средство решения задач арифметики

Таким образом, мы можем рассматривать модулярные формы как

1) *степенные ряды* $f = \sum_{n=0}^{\infty} a_n q^n \in \mathbb{C}[[q]]$ и как

2) *голоморфные функции на верхней полуплоскости*

$$\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}\ z > 0\},$$

где $q = \exp(2\pi i z)$, $z \in \mathbb{H}$, и рассмотрим L-функцию $L(f, s, \chi) = \sum_{n=1}^{\infty} \chi(n) a_n n^{-s}$ для любого характера Дирихле $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$, например, для символа Якоби $\chi(n) = \left(\frac{n}{N}\right)$.

Ещё один метод вычисления функции Рамануджана:

Положим $h_k := \sum_{n=1}^{\infty} \sum_{d|n} d^{k-1} q^n = \sum_{d=1}^{\infty} \frac{d^{k-1} q^d}{1 - q^d}$.

Доказывается: $\Delta = (E_4^3 - E_6^2)/1728$, где $E_4 = 1 + 240h_4$ и $E_6 = 1 - 504h_6$:

Вычисление с PARI-GP
(см. [BBBCO]).

$$h_k := \sum_{n=1}^{\infty} \sum_{d|n} d^{k-1} q^n = \sum_{d=1}^{\infty} \frac{d^{k-1} q^d}{1 - q^d} \Longrightarrow$$

```
gp > h6=sum(d=1,20,d^5*q^d/(1-q^d)+O(q^20))
gp > h4=sum(d=1,20,d^3*q^d/(1-q^d)+O(q^20)
gp > Delta=((1+240*h4)^3-(1-504*h6)^2)/1728

q - 24*q^2 + 252*q^3 - 1472*q^4 + 4830*q^5 - 6048*q^6 - 16744*q^7
+ 84480*q^8 - 113643*q^9 - 115920*q^10 + 534612*q^11
- 370944*q^12 - 577738*q^13 + 401856*q^14 + 1217160*q^15
+ 987136*q^16 - 6905934*q^17+ 2727432*q^18 + 10661420*q^19 + O(q^20)
```

Сравнение Рамануджана: $\tau(n) \equiv \sum_{d|n} d^{11} \mod 691:$

```
gp > (Delta-h12)/691
%10 = -3*q^2 - 256*q^3 - 6075*q^4 - 70656*q^5 - 525300*q^6
 - 2861568*q^7 - 12437115*q^8 - 45414400*q^9
 - 144788634*q^10 - 412896000*q^11 - 1075797268*q^12
 - 2593575936*q^13 - 5863302600*q^14 - 12517805568*q^15
 - 25471460475*q^16 - 49597544448*q^17
 - 93053764671*q^18 - 168582124800*q^19 + O(q^20)
```

Вот ешё три программы вычисления $\tau(n)$ (см. [Sloane])

```
 PROGRAM

(MAGMA) M12:=ModularForms(Gamma0(1), 12); t1:=Basis(M12)[2];
PowerSeries(t1[1], 100); Coefficients($1);

(PARI) a(n)=if(n<1, 0, polcoeff(x*eta(x+x*O(x^n))^24, n))

(PARI) {tau(n)=if(n<1, 0, polcoeff(x*(sum(i=1, (sqrtint(8*n-7)+1)\2,
(-1)^i*(2*i-1)*x^((i^2-i)/2), O(x^n)))^8, n));}
gp > tau(6911)
%3 = -615012709514736031488
gp > ##
  ***   last result computed in 3,735 ms.
```

Схема применения модулярных форм для решения задач теории чисел:

Производящая функция $f = \sum_{n=0}^{\infty} a_n q^n \in \mathbb{C}[[q]]$ для арифметической функции $n \mapsto a_n$, например $a_n = p(n)$	$\rightsquigarrow$	Выражение через модулярную форму, например $\sum_{n=0}^{\infty} p(n)q^n = (\Delta/q)^{-1/24}$	$\rightsquigarrow$	Число (ответ)
		$\uparrow$		$\uparrow$
Пример 1 (см. [Chand70]): (Харди-Рамануджан) $p(n) = \frac{e^{\pi\sqrt{2/3(n-1/24)}}}{4\sqrt{3}\lambda_n^2} + O(e^{\pi\sqrt{2/3}\lambda_n}/\lambda_n^3)$, $\lambda_n = \sqrt{n-1/24}$,		Хорошие базисы конечномерность много соотношений и тождеств		Значения L-функций, сравнения, ...

Пример 2 (см. в [Ma-Pa05], главы 6 и 7): теорема Ферма-Уайлса, гипотеза Бёрча-Суиннертона-Дайера, ...

4 Ряды Эйзенштейна и сравнения для функции Рамануджана.

Ряды Эйзенштейна и их разложение Фурье.

Пусть $k > 2$. Для решётки $\Lambda \subset \mathbb{C}$ положим

$$G_k(\Lambda) = \sum_{l \in \Lambda} l^{-k} = \sum_{m,n}{}' (m\omega_1 + n\omega_2)^{-k}, \quad \Lambda = \langle \omega_1, \omega_2 \rangle,$$

Этот ряд сходится абсолютно для $k > 2$.

Предложение 4.1 *(а) Имеем*

$$G_k(z) = \sum_{m,n \in \mathbb{Z}}{}' (mz+n)^{-k} \in \mathcal{M}_k(\Gamma(1));$$

(б)

$$G_k(z) = 2\zeta(k)\left[1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n\right] =: 2\zeta(k)E_k(z),$$

где $q = e(z) = \exp(2\pi i z)$, B_k *числа Бернулли определённые разложением*

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!}$$

Вот несколько численных значений:

$$B_0 = 1,\ B_1 = -\frac{1}{2},\ B_2 = \frac{1}{6},\ B_3 = B_5 = \cdots = 0,\ B_4 = -\frac{1}{30},\ B_6 = \frac{1}{42},$$
$$B_8 = -\frac{5}{66},\ B_{12} = \frac{691}{2730},\ B_{14} = -\frac{7}{6},\ B_{16} = \frac{3617}{510},\ B_{18} = -\frac{43867}{798},\ \ldots.$$

Имеем $\zeta(k) = -\dfrac{(2\pi i)^k}{2}\dfrac{B_k}{k!}$,

$$G_k(z) = \frac{(2\pi i)^k}{(k-1)!}\left[-\frac{B_k}{2k} + \sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n\right] =: \frac{(2\pi i)^k}{(k-1)!}\mathbb{G}_k(z).$$

Примеры.

$$E_4(z) = 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n \in \mathcal{M}_4(\mathrm{SL}(2,\mathbb{Z})),$$
$$E_6(z) = 1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n \in \mathcal{M}_6(\mathrm{SL}(2,\mathbb{Z})),$$
$$E_8(z) = 1 + 480\sum_{n=1}^{\infty}\sigma_7(n)q^n \in \mathcal{M}_8(\mathrm{SL}(2,\mathbb{Z})),$$
$$E_{10}(z) = 1 - 264\sum_{n=1}^{\infty}\sigma_9(n)q^n \in \mathcal{M}_{10}(\mathrm{SL}(2,\mathbb{Z})),$$
$$E_{12}(z) = 1 + \frac{65520}{691}\sum_{n=1}^{\infty}\sigma_{11}(n)q^n \in \mathcal{M}_{12}(\mathrm{SL}(2,\mathbb{Z})),$$
$$E_{14}(z) = 1 - 24\sum_{n=1}^{\infty}\sigma_{13}(n)q^n \in \mathcal{M}_{14}(\mathrm{SL}(2,\mathbb{Z})).$$

Доказательство. Автоморфность ясна, поскольку $G_k(\lambda\Lambda) = \lambda^{-k}G_k(\Lambda)$ поэтому G_k является *однородной функцией решётки* степени однородности $-k$, и

$$G_k(z) = G_k(\Lambda_z),\ G_k(\gamma z) = G_k(\Lambda_{\gamma z}) = G_k(\langle 1, \frac{az+b}{cz+d}\rangle)$$
$$= G_k((cz+d)^{-1}\langle cz+d, az+b\rangle) = (cz+d)^k G_k(\langle cz+d, az+b\rangle) = (cz+d)^k G_k(\Lambda_z) = (cz+d)^k G_k(z),$$

поскольку $\langle cz+d, az+b\rangle = \langle 1, z\rangle$ для всех $\begin{pmatrix} a & b \\ c & d\end{pmatrix} \in SL_2(\mathbb{Z})$.

Для нахождения разложения Фурье используется известное разложение синуса в бесконечное произведение:

$$\sin(\pi a) = \pi a \prod_{n=1}^{\infty} \left(1 - \frac{a^2}{n^2}\right). \tag{4.17}$$

Логарифмическая производная (4.17) даёт

$$\pi \mathrm{ctg} \pi a = \frac{1}{a} + \sum_{n=1}^{\infty} \left(\frac{1}{a+n} - \frac{1}{a-n}\right). \tag{4.18}$$

Заметим, что

$$\pi i \frac{e^{\pi i a} + e^{-\pi i a}}{e^{\pi i a} - e^{-\pi i a}} = \pi i + \frac{2\pi i}{e^{2\pi i a} - 1} = \pi i - 2\pi i \sum_{n=1}^{\infty} e^{2\pi i n a}, \tag{4.19}$$

и положим $x = 2\pi i a$; отсюда

$$\frac{x}{2} + \frac{x}{e^x - 1} = 1 + \sum_{n=1}^{\infty} \frac{2x^2}{x^2 - (2\pi i n)^2},$$

где

$$\sum_{k=0}^{\infty} B_k \frac{x^k}{k!} + \frac{x}{2} = 1 - \sum_{n=1}^{\infty} \frac{2\left(\dfrac{x}{2\pi i n}\right)^2}{-\left(\dfrac{x}{2\pi i n}\right)^2 + 1} =$$

$$1 - 2\sum_{n=1}^{\infty} \sum_{k=2k'\geq 2} \left(\frac{x}{2\pi i n}\right)^k = 1 - 2 \sum_{k=2k'\geq 2} \frac{\zeta(k)}{(2\pi i)^k} x^k.$$

Это непосредственно даёт

$$\zeta(k) = -\frac{(2\pi i)^k}{2} \frac{B_k}{k!}, \tag{4.20}$$

в частности,

$$\zeta(2) = \frac{\pi^2}{6}, \zeta(4) = \frac{\pi^4}{90}.$$

Чтобы доказать (б), проводится дифференцирование обеих частей (4.19) по переменной a $(k-1)$ раз:

$$-(2\pi i)^k \sum_{n=1}^{\infty} n^{k-1} e^{2\pi i n a} = (-1)^{k-1}(k-1)! \sum_{n\in\mathbb{Z}} (a+n)^{-k}, \quad (k \in 2\mathbb{Z}, k \geq 2). \tag{4.21}$$

Положим $a = mz$, тогда

$$\frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} n^{k-1} e^{2\pi i n m z} = \sum_{n\in\mathbb{Z}} (mz+n)^{-k}. \tag{4.22}$$

Если теперь $k > 2$, то можно просуммировать по m от 1 до ∞. В результате этого получим

$$G_k(z) = 2\zeta(k) + 2\sum_{m=1}\sum_{n=-\infty}^{\infty}(mz+n)^{-k} = 2\zeta(k)\left[1 - \frac{2k}{B_k}\sum_{m,d=1}^{\infty} d^{k-1}q^{md}\right]. \qquad (4.23)$$

Отметим, что двойной ряд в (4.23) абсолютно сходится при $k > 2$ но ряд (4.23) имеет смысл и при $k = 2$ как условно сходящийся ряд. Доказательство завершается подстановкой (4.20) в (4.23).

Теорема 4.2 *Пусть* $\Delta(z) = q\prod_{m\geq 1}(1-q^m)^{24}$. *Тогда имеем*

$$\Delta(-z^{-1}) = z^{12}\Delta(z).$$

(см. также [Se70]).

Доказательство. Положим

$$E_2(z) = 1 - 24\sum_{n=1}^{\infty}\sigma_1(n)q^n.$$

Имеем

$$\frac{d}{dz}\log(\Delta(z)) = \frac{d}{dz}\log q + 24\sum_{m=1}^{\infty}\frac{d}{dz}\log(1-q^m) =$$

$$2\pi i(1 - 24\sum_{m=1}^{\infty} mq(1-q^m)^{-1}) = 2\pi i E_2(z), \quad \frac{dq}{dz} = 2\pi i q.$$

Достаточно доказать следующее предложение:

Предложение 4.3

$$z^{-2}E_2(-z^{-1}) = E_2(z) + \frac{12}{2\pi i z}. \qquad (5.8)$$

Доказательство предложения. Используется ряд (4.23) с $k = 2$ сходящийся условно:

$$E_2(z) = \frac{1}{2\zeta(2)}\sum_{m=-\infty}^{\infty}\left(\sum_{\substack{n=-\infty\\ n\neq 0}}^{\infty}(mz+n)^{-2}\right) =$$

$$1 + \frac{3}{\pi^2}\sum_{m\neq 0}\left(\sum_{n=-\infty}^{\infty}(mz+n)^{-2}\right) = 1 + \frac{6}{\pi^2}\sum_{m=1}^{\infty}\left(\sum_{n=-\infty}^{\infty}(mz+n)^{-2}\right).$$

Для фиксированного m имеем

$$\sum_{n=-\infty}^{\infty}(mz+n)^{-2} = 1 - \frac{4}{B_2}\sum_{d=1}^{\infty} dq^{md} = 1 - 24\sum_{n=1}^{\infty}\sigma_1(n)q^n.$$

Выполним подстановку

$$z^{-2}E_2(-z^{-1}) = \frac{1}{2\zeta(2)} \sum_{m=-\infty}^{\infty} \left(\sum_{\substack{n=-\infty \\ n\neq 0}}^{\infty} (-m+nz)^2 \right) = 1 + \frac{3}{\pi^2} \sum_{n=-\infty}^{\infty} \sum_{m\neq 0} (mz+n)^{-2}.$$

Если положить $a_{m,n} = (mz+n)^{-2}$, то доказательство сводится к проверке равенства

$$-\sum_m \sum_n a_{m,n} + \sum_n \sum_m a_{m,n} = \frac{12}{2\pi i z}.$$

Для его доказательства вводится поправочный член

$$b_{m,n}(z) = \frac{1}{(mz+n-1)(mz+n)} = \frac{1}{(mz+n-1)} - \frac{1}{(mz+n)} \tag{4.24}$$

Получается модифицированный ряд

$$\tilde{E}_2(z) = 1 + \frac{3}{\pi^2} \sum_{m\neq 0} \sum_{n=-\infty}^{\infty} \big((mz+n)^{-2} - b_{m,n}(z) \big) \tag{4.25}$$

который уже абсолютно сходится поскольку

$$(mz+n)^{-2} - ((mz+n-1)(mz+n))^{-1} = (mz+n)^{-2}(mz+n-1)^{-1}.$$

С другой стороны,

$$\tilde{E}_2(z) =$$
$$1 + \frac{3}{\pi^2} \sum_{m\neq 0} \left(\sum_{n=-\infty}^{\infty} (mz+n)^{-2} \right) + \frac{3}{\pi^2} \sum_{m\neq 0} \sum_{n=-\infty}^{\infty} \left(\frac{1}{(mz+n)} - \frac{1}{(mz+n-1)} \right),$$

и последняя сумма преобразуется в нуль, поэтому

$$\tilde{E}_2(z) = E_2(z).$$

Изменение порядка суммирования в (4.25) обосновано в силу абсолютной сходимости, откуда

$$\tilde{E}_2(z) = 1 + \frac{3}{\pi^2} \sum_{n=-\infty}^{\infty} \sum_{m\neq 0} \big((mz+n)^{-2} - b_{m,n}(z) \big) =$$
$$z^{-2}E_2(-z^{-1}) - \frac{3}{\pi^2} \sum_{n=-\infty}^{\infty} \left(\sum_{m\neq 0} b_{m,n} \right).$$

Остаётся вычислить последнюю сумму:

$$\sum_{n=-\infty}^{\infty} \left(\sum_{m\neq 0} b_{m,n} \right) = \lim_{N\to\infty} \sum_{n=-N+1}^{n=N} \left(\sum_{m\neq 0} b_{m,n} \right).$$

Однако

$$\sum_{m\neq 0}(mz-n)^{-2} = \frac{1}{z^2}\sum_{m\neq 0}(n/z-m)^{-2} = -\frac{1}{n^2} - \frac{4\pi^2}{z^2}\sum_{d=1}^{\infty} de^{-2\pi ind(1/z)}$$

поэтому для всех z внешняя сумма сходится абсолютно, и преобразуется в

$$\sum_{m\neq 0}\left(\sum_{n=-N+1}^{n=N} b_{m,n}\right) = \sum_{m\neq 0}\left(\frac{1}{(mz-N)} - \frac{1}{(mz+N)}\right) =$$

$$\frac{2}{z}\sum_{m=1}^{\infty}\left(\frac{1}{(-N/z+m)} + \frac{1}{(-N/z-m)}\right) = \frac{2}{z}\left(\pi\mathrm{ctg}\left(-\frac{\pi N}{z}\right) + \frac{z}{N}\right) \to -\frac{2\pi i}{z}$$

при $N \to \infty$, $z \in \mathbb{H}$, откуда следует и предложение 4.3, и теорема 4.2.

4.1 Структура пространств модулярных форм относительно $\mathrm{SL}_2(\mathbb{Z})$.

(см. также [Se70], pp.127–178).

Пусть f ненулевая мероморфная функция на $\mathbb{H}$, и пусть p некоторая точка в $\mathbb{H}$. Назовём порядком f в p, и обозначим его через $v_p(f)$, целое число n такое, что функцмя $f/(z-p)^n$ голоморфна и необращается в нуль в точке p.

Пусть f модулярная функция веса k, то равенство

$$f(z) = (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right)$$

показывает, что $v_p(f) = v_{\gamma(p)}(f)$ для всех $\gamma \in \Gamma = \Gamma(1)$; другими словами, $v_p(f)$ зависит только от образа p в $\Gamma\backslash H$. Больше того, можно определить и $v_\infty(f)$ как порядок относительно $q = 0$ функции $\tilde{f}(q) = f(z)$ ассоциированной с f. Положим $e_p = 2$ (соотв.$e_p = 3$) если p эквивалентна относительно Γ точке i (соотв. точке ρ), и $e_p = 1$ в противном случае.

Предложение 4.4 (о степени дивизора модулярной формы) *Пусть f ненулевая модулярная функция веса k относительно $\Gamma(1)$. Имеем*

$$v_\infty(f) + \sum_{p\in\Gamma(1)\backslash\mathbb{H}} \frac{1}{e_p} v_p(f) = \frac{k}{12}$$

[Можно также записать этот результат в виде:

$$v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\rho(f) + \sum_{p\in\Gamma(1)\backslash\mathbb{H}}{}^{*\prime} v_p(f) = \frac{k}{12},$$

где символ $\sum_{p\in\Gamma(1)\backslash\mathbb{H}}{}^{*\prime}$ означает суммирование по всем классам точек $\Gamma(1)\backslash\mathbb{H}$, отличным от классов точек i et de ρ].

Естественное доказательство этого факта использует структуру римановой поверхности на $\Gamma(1)\backslash\overline{\mathbb{H}}$, где $\overline{\mathbb{H}} = \mathbb{H} \cup \mathbb{Q} \cup \infty$.

Теорема 4.5 (о функции Рамануджана Δ и рядах Эйзенштейна) *(i) Имеем* $\mathcal{M}_k(\Gamma(1)) = 0$ *pour* $k < 0$ *и* $k = 2$.

(ii) Для $k = 0, 4, 6, 8, 10$ *пространство* $\mathcal{M}_k(\Gamma(1))$ *имеет размерность 1 с базисом* $1, E_4, E_6, E_8, E_{10}$*; при этом* $\mathcal{S}_k(\Gamma(1)) = 0$.

(iii) Умножение на Δ *определяет изоморфизм* $\mathcal{M}_{k-12}(\Gamma(1))$ *на* $\mathcal{S}_k(\Gamma(1))$.

Теорема 4.6 (размерности пространств модулярных форм для $\mathrm{SL}(2,\mathbb{Z})$)

(а)

$$\dim \mathcal{M}_k(\Gamma(1)) = \begin{cases} \left[\frac{k}{12}\right], & k \equiv 2(\mathrm{mod} 12), k \geq 0, \\ 0, & k \equiv 1(\mathrm{mod} 2), \\ \left[\frac{k}{12}\right] + 1, & k \not\equiv 2(\mathrm{mod} 12), k \geq 0, k \in 2\mathbb{Z}. \end{cases}$$

$$\dim \mathcal{S}_k(\Gamma(1)) = \begin{cases} \left[\frac{k}{12}\right] - 1, & k \equiv 2(\mathrm{mod} 12), k \geq 12, \\ 0, & k \equiv 1(\mathrm{mod} 2), \\ \left[\frac{k}{12}\right], & k \not\equiv 2(\mathrm{mod} 12), k \geq 0, k \in 2\mathbb{Z}. \end{cases}$$

(б) Произведения

$$\{E_4^\alpha E_6^\beta \mid 4\alpha + 6\beta = k,\ \alpha, \beta \geq 0, \alpha, \beta \in \mathbb{Z}\}$$

образуют базис пространства $\mathcal{M}_k(\Gamma(1))$

Доказательство непосредственно следует из 4.5.

Следствие 4.7 *Справедливо равенство*

$$\Delta(z) = \frac{1}{1728}(E_4^3 - E_6^3).$$

Действительно, $\Delta(z) \in \mathcal{S}_{12}(\Gamma(1))$, и в силу 2.3 имеем $\dim \mathcal{S}_{12}(\Gamma(1)) = 1$, остаётся заметить, что функция $\frac{1}{1728}(E_4^3 - E_6^3)$ также принадлежит одномерному пространству $\mathcal{S}_{12}(\Gamma(1))$, так как обе функции E_4^3, E_6^3 имеют коэффициент при q, равный 1.

4.2 Приложение: доказательство сравнения Рамануджана

$$\tau(n) \equiv \sigma_{11}(n) \bmod 691. \tag{4.26}$$

Действительно,

$$E_6^2(z) - \left(1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n\right)^2 \in \mathbb{Z}[[q]],$$

поэтому можно разложить $E_6^2(z)$ в базисе $\{E_{12},\ \Delta\}$ пространства $\mathcal{M}_{12}(\Gamma(1))$ размерности 2: $E_6^2 = E_{12} + \alpha\Delta$, где

$$1 - 1008q + \cdots = 1 + \frac{65520}{691}q + \cdots + \alpha q + \ldots,$$

и $\dots = \mathcal{O}(q^2)$. Поэтому

$$\alpha = -1008 - \frac{65520}{691} = \frac{a}{691} \quad \text{где } a \equiv -65520 (\mathrm{mod} 691),$$

и из разложения выводится. что

$$\frac{65520}{691}\sigma_{11}(n) + \frac{a}{691}\tau(n) \in \mathbb{Z}, \quad \text{где} \;\; 65520(\sigma_{11}(n) - \tau(n)) \equiv 0 (\mathrm{mod} 691),$$

откуда вытекает сравнение (4.26).

5 Числа Бернулли и сравнения Куммера

5.1 Сравнения для коэффициентов рядов Эйзенштейна

Приведем пример сравнений между коэффициентами модулярных форм по модулю p^n.

Для этого рассмотрим ещё одну нормализацию рядов Эйзенштейна, заданную так, что коэффициенты Фурье $a(n)$ задают ряд Дирихле с эйлеровским произведением, при этом $a(1) = 1$:

$$\mathbb{G}_k = \frac{\zeta(1-k)}{2} E_k = -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n = \sum_{n=0}^{\infty} a(n) q^n \Rightarrow \sum_{n=1}^{\infty} a(n) n^{-s} = \zeta(s)\zeta(s+1-k),$$

а также p-нормализацию

$$\mathbb{G}_k^*(z) = \mathbb{G}_k(z) - p^{k-1}\mathbb{G}_k(pz).$$

Тогда

$$\mathbb{G}_k^* = \frac{\zeta^*(1-k)}{2} + \sum_{n=1}^{\infty} \sigma_{k-1}^*(n) q^n, \; \sigma_{k-1}^*(n) = \sum_{\substack{d|n \\ (d,p)=1}} d^{k-1}, \quad \text{где}$$

$$\zeta^*(s) = \zeta(s)(1-p^{-s}) = \sum_{\substack{n=1 \\ (p,n)=1}} n^{-s} \quad \text{обозначает дзета-функцию Римана с удалённым эйлеровским } p\text{-множителем.}$$

$$\mathbb{G}_k^* = \sum_{n=0}^{\infty} a_k^*(n) q^n \Rightarrow \sum_{n=1}^{\infty} a_k^*(n) n^{-s} = \zeta(s)\zeta^*(s+1-k).$$

Теорема 5.1 *а) Пусть* $k \equiv k' \bmod (p-1)p^{N-1}$ *тогда* $\mathbb{G}_k^* \equiv \mathbb{G}_{k'}^* \bmod p^N$ *в* $\mathbb{Q}[\![q]\!]$ *для всех* $k \not\equiv 0 \bmod (p-1)$.

б) Пусть $k \equiv k' \bmod (p-1)p^{N-1}$*, тогда для любых* $c \in \mathbb{Z}$*,* $(c,p) = 1$*,* $c > 1$ *имеем:* $(1-c^k)\mathbb{G}_k^* \equiv (1-c^{k'})\mathbb{G}_{k'}^* \bmod p^N$ *(без ограничения на* k*).*

в) Семейство классических модулярных форм

$$k \mapsto f_k = (1-c^k)\mathbb{G}_k^*$$

является p*-адически непрерывным* $\mathbb{Z}_p^*$ *с параметром из множества*

$$\mathcal{P} = \{y \mapsto y^k, k \geq 4\}$$

p*-адических характеров группы* $\mathbb{Z}_p^*$.

Доказательство теоремы 5.1: Утверждения а) и б) следуют из в). Для доказательства в) положим $f_k = \sum\limits_{n \geq 0} a_k(n) q^n$

Случай $n > 0$: Функции

$$k \mapsto a_k(n) = (1 - c^k) \sum_{\substack{d|n \\ (d,p)=1}} d^{k-1}$$

являются p-адически непрерывными по их элементарному описанию (по сравнениям теоремы Эйлера);

Случай $n = 0$: $a_k(0) = (1 - c^k)\zeta^*(1 - k)$ рассматривается с помощью классических сравнений Куммера: зафиксируем произвольное целое число $c \in \mathbb{Z}$, $(c, p) = 1$, $c > 1$.

Теорема 5.2 (Куммер) *Пусть* $\zeta_{(p)}^{(c)}(-k) = (1-c^{k+1})(1-p^k)\zeta(-k)$, $k \geq 0$, *и пусть* $h(x) = \sum\limits_i \alpha_i x^i \in \mathbb{Z}[x]$ *такой, что* $h(a) \equiv 0 \bmod p^N$ *для всех* $\alpha \in \mathbb{Z}_p^*$. *Тогда* $\sum\limits_i \alpha_i \zeta_{(p)}^{(c)}(-i) \equiv 0 \bmod p^N$.

Доказательство теоремы 5.2 использует суммы степеней $S_k(M) = \sum\limits_{n=1}^{M-1} n^k$, числа Бернулли B_k, и многочлены Бернулли $B_k(x)$:

$$S_k(M) = \sum_{n=1}^{M-1} n^k = \frac{1}{k+1}[B_{k+1}(M) - B_{k+1}], \text{ где } \sum_{m=1}^{\infty} \frac{B_k}{k!} t^k = \frac{t}{e^t - 1} \text{ и } B_k(x) = \sum_{i=0}^{k} \binom{k}{i} B_i x^{k-i}.$$

Отсюда вытекает

$$B_k = \lim_{N \to \infty} \frac{1}{p^N} S_k(p^N)$$

(p–адический предел явно вычсиляется по указанной формуле для $S_k(p^N)$ (в частности, $\frac{1}{p^N} S_1(p^N) = \frac{p^N(p^N-1)}{2p^N} \to -\frac{1}{2} = B_1$).

Далее, рассматривается регуляризованная сумма степеней

$$S_k^*(p^N) = \sum_{\substack{n=1 \\ p \nmid n}}^{p^N-1} n^k = S_k(p^N) - p^k S_k(p^{N-1}) \ ,$$

которая выражается через числа Бернулли в терминах $S_k(N)$ по формуле

$$B_{k+1} = \lim_{N \to \infty} \frac{1}{p^N} S_{k+1}(p^N).$$

Для всех n с $(p, n) = 1$ имеем сравнение $h(n) \equiv 0 (\mathrm{mod} p^N)$, и

$$\lim_{N \to \infty} \frac{1}{p^N} S_{k+1}^*(p^N) = \lim_{N \to \infty} \frac{1}{p^N} [S_{k+1}(p^N) - p^{k+1} S_k(p^{N-1})] =$$
$$\lim_{N \to \infty} \frac{1}{p^N} S_{k+1}(p^N) - p^k \lim_{N \to \infty} \frac{1}{p^N} S_{k+1}(p^{N-1}) = (1 - p^k) B_{k+1}.$$

Подставим $\zeta(-k) = -\dfrac{B_{k+1}}{k+1}$ тогда

$$\zeta^{(c)}_{(p)}(-k) = (c^{k+1}-1)(1-p^k)\frac{B_{k+1}}{k+1} \equiv \frac{S_{k+1}(p^M)}{p^M} \cdot \frac{(c^{k+1}-1)}{k+1} \bmod p^N \tag{5.27}$$

(для достаточно большого $M \geq N$). Правая часть (5.27) преобразуется к виду

$$\sum_{\substack{n=1 \\ p\nmid n}}^{p^M-1} \frac{(cn)^{k+1}-n^{k+1}}{p^M \cdot (k+1)} = \sum_{\substack{n=1 \\ p\nmid n}}^{p^M-1} \frac{(cn)^{k+1}-n_c^{k+1}}{p^M \cdot (k+1)} \tag{5.28}$$

где $n \mapsto n_c$ перестановка множества $\{1, 2, \ldots, p^M-1\}$ заданная $n_c \equiv nc \pmod{p^M}$. Подставим $cn = n_c + p^M t_n$, $t_n \in \mathbb{Z}$ в (5.28):

$$\frac{(nc)^{k+1}-n_c^{k+1}}{p^M \cdot (k+1)} \equiv t_n \cdot n_c^k \bmod p^M$$

поэтому $\zeta^{(c)}_{(p)}(-k) \equiv \sum\limits_{\substack{n=1 \\ p\nmid n}} t \cdot n_c^k \bmod p^M$ где $t_n = t(n,c)$ не зависит от k. Чтобы завершить доказательство, подставим это сравнение в линейную комбинацию из теоремы 5.2 используя предположение

$$h(x) \equiv 0 \bmod p^N : \quad \sum_i \alpha_i \zeta^{(c)}_{(p)}(-i) \equiv \sum_{\substack{n=1 \\ p\nmid n}} t_n \cdot h(n_c) \equiv 0 \bmod p^N \ . \quad \blacksquare$$

Следствие 5.3 *(p-адическая непрерывность $\zeta^{(c)}_{(p)}(-k)$ в прогрессиях по* $\bmod(p-1)$*). Если* $h(x) = x^k - x^{k'}$*,* $k \equiv k' \bmod (p-1)p^{N-1}$*, то*

$$\zeta^{(c)}_{(p)}(-k) \equiv \zeta^{(c)}_{(p)}(-k') \bmod p^N \ .$$

Доказательство следствия 5.3: По теореме Эйлера имеем $h(a) \equiv 0 \bmod p^N$, поскольку $a^{\varphi(p^N)} \equiv 1 \pmod{p^N}$, $(a,p) = 1$.

5.2 p-адическое интегрирование и мера Мазура

В p-адической теории интегрирования рассматривается *поле Тэйта*, $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}}}_p$ (пополнение алгебраического замыкания поля p-адических чисел $\mathbb{Q}_p$), которое служит аналогом поля комплексных чисел, так как $\mathbb{C}_p$ алгебраически замкнуто, и является топологически полным метрическим пространством с нормой $|\cdot|_p$, $|p|_p = \frac{1}{p}$.

Пусть R любое замкнутое подкольцо в $\mathbb{C}_p$, $\mathcal{M}$ – топологический R-модуль и $\mathcal{C}(Y,R)$ – топологический модуль всех R-значных непрерывных функций на проконечном множестве $Y = \mathbb{Z}_p^*$, и $\mathrm{Step}(Y,R)$ – R-модуль всех локально-постоянных функций на Y (в данном случае все ступенчатые функции непрерывны!).

Напомним, что *распределение* μ на Y со значениями в $\mathcal{M}$ это конечно-аддитивная функция на открытых подмножествах $U \subset Y$:

$$\mu\colon \left\{\begin{matrix}\text{открытые подмножества} \\ U \subset Y\end{matrix}\right\} \longrightarrow \mathcal{M}.$$

Другими словами, μ – это гомоморфизм R–модулей

$$\mu : \mathrm{Step}(Y, R) \to \mathcal{M}$$

Напомним, что *мерой* на Y со значениями в $\mathcal{M}$ называется *непрерывный* гомоморфизм R-модулей

$$\mu : \mathcal{C}(Y, R) \longrightarrow \mathcal{M}.$$

Ограничение μ на R–подмодуль $\mathrm{Step}(Y, R) \subset \mathcal{C}(Y, R)$ определяет распределение, обозначаемое той же буквой μ, причём мера μ однозначно определена по соответствующему распределению, поскольку R–подмодуль $\mathrm{Step}(Y, R)$ "плотен" в $\mathcal{C}(Y, R)$. Это утверждение выражает общий факт о равномерной непрерывности непрерывной функции на компакте Y.

Следствие 5.4 (Мазур) *Существует единственная $\mathbb{Q}_p$=значная мера $\mu^{(c)}$ на $\mathbb{Z}_p^*$ такая, что для всех $k \geq 1$ имеем $\int\limits_{\mathbb{Z}_p^*} x^k d\mu^{(c)} = \zeta_{(p)}^{(c)}(1-k) = (1-c^k)(1-p^{k-1})\zeta(1-k)$. Заметим, что $\zeta(0) = -\frac{1}{2}$, но $\zeta_{(p)}^{(c)}(0) = 0$.*

Действительно, если интегрировать $h(x)$ по $\mathbb{Z}_p^\times$, то получается сравнение Куммера из теоремы 5.1. С другой стороны, для определения меры, удовлетворяюшей условиям следствия, определим интеграл $\int_{\mathbb{Z}_p^\times} \phi(x)\mu^{(c)}$ для каждой непрерывной функции $\phi : \mathbb{Z}_p^\times \to \mathbb{Z}_p$. Для этого используется приближение непрерывной функции $\phi(x)$ многочленами (для них интеграл задан по определению), затем остаётся перейти к пределу. *Сравнения Куммера* из теоремы 5.1. показывают, что предел корректно определён, и даёт интеграл для любой непрерывной функции.

5.3 p-адическая дзета-функция Куботы – Леопольдта

5.3.1 Область определения p-адических дзета-функций

Областью определения комплексных дзета функций является группа

$$\mathbb{C} = \mathrm{Hom}_{\mathrm{cont}}(\mathbb{R}^\times, \mathbb{C}^\times), \quad s \mapsto (y \mapsto y^s).$$

По аналогии с классическим комплексным случаем областью определения p-адических дзета-функций является p-адическая группа

$$X_p = \mathrm{Hom}_{\mathrm{cont}}(\mathbb{Z}_p^\times, \mathbb{C}_p^\times),$$

состоящая из всех непрерывных гомоморфизмов проконечной группы $\mathbb{Z}_p^\times$ в мультипликативную группу поля Тэйта, $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}}}_p$ (пополнение алгебраического замыкания поля p-адических чисел $\mathbb{Q}_p$). Мы будем рассматривать целые числа k как гомоморфизмы $x_p^k : y \mapsto y^k$.

Конструкция Куботы и Леорольдта даёт существование p-адической аналитической функции $\zeta_p : X_p \to \mathbb{C}_p$ с единственным простым полюсом в точке $x = x_p^{-1}$, которая становится ограниченной аналитической функцией на X_p после умножения на регуляризующий множитель $(cx(c) - 1)$, $(x \in X_p, c \in \mathbb{Z}_p^\times)$; эта функция однозначно определена условием

$$\zeta_p(x_p^k) = (1 - p^k)\zeta(-k) \qquad (k \geq 1). \tag{5.29}$$

Этот результат имеет очень естественную интерпретацию в рамках теории p-адического интегрирования (в стиле результата Мазура, см. следствие 5.4)

Замечательное свойство этой конструкции состоит в том, что она применима и для всех характеров Дирихле χ по модулю степени простого числа p. Зафиксируем вложение

$$i_p : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p \tag{5.30}$$

и будем отождествлять поле $\overline{\mathbb{Q}}$ с подполем в $\mathbb{C}$ и в $\mathbb{C}_p$. Тогда характер Дирихле вида

$$\chi : (\mathbb{Z}/p^N\mathbb{Z})^\times \to \overline{\mathbb{Q}}^\times$$

становится элементом подгруппы кручения

$$X_p^{\text{tors}} \subset X_p = \operatorname{Hom}_{\text{cont}}(\mathbb{Z}_p^\times, \mathbb{C}_p^\times)$$

и равенство (5.29) остаётся в силе и для специальных значений $L(-k,\chi)$ соответствующих L-рядов Дирихле

$$L(s,\chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s} = \prod_{\substack{\ell \text{ простые} \\ \text{числа}}} (1-\chi(\ell)\ell^{-s})^{-1},$$

при этом мы имеем

$$\zeta_p(\chi x_p^k) = i_p\left[(1-\chi(p)p^k)L(-k,\chi)\right] \;\; (k \geq 1, \quad k \in \mathbb{Z}, \quad \chi \in X_p^{\text{tors}}). \tag{5.31}$$

5.3.2 Неархимедово преобразование Меллина

Пусть μ обозначает $\mathbb{C}_p$-значную меру $\mathbb{Z}_p^\times$. Тогда *неархимедово преобразование Меллина* меры μ определяется равенством

$$L_\mu(x) = \mu(x) = \int_{\mathbb{Z}_p^\times} x \mathrm{d}\mu, \qquad (x \in X_p), \tag{5.32}$$

и представляет некоторую ограниченную $\mathbb{C}_p$-аналитическую функцию

$$L_\mu : X_p \longrightarrow \mathbb{C}_p. \tag{5.33}$$

Действительно, ограниченность функции L_μ очевидна поскольку все характеры $x \in X_p$ принимают значения в $\mathcal{O}_p$ и μ также ограничена. Аналитичность L_μ вырыжает общее свойство интеграла (5.32), поскольку он аналитически зависит от параметра $x \in X_p$. Можно доказать (теорема Ивасава), что ограниченные $\mathbb{C}_p$-аналитические функции взаимно-однозначно соответствуют $\mathbb{C}_p$-значным мерам μ на $\mathbb{Z}_p^\times$ посредством неархимедова преобразования Меллина.

5.3.3 Пример: p-адическое преобразование Меллина меры Мазура и интегральное представление дзета-функции Куботы – Леопольдта

Для меры Мазура из следствия 5.4 функция на X_p

$$\zeta_p(x) = \left(1 - c^{-1}x(c)^{-1}\right)^{-1} L_{\mu^{(c)}}(x) \qquad (x \in X_p) \tag{5.34}$$

однозначно определена и голоморфна за исключением единственного простого полюса в точке $x = x_p^{-1}$, и становится ограниченной аналитической функцией на X_p после умножения на регуляризующий множитель $(cx(c)-1)$, $(x \in X_p, c \in \mathbb{Z}_p^\times)$; эта функция однозначно определена условием (5.29).

Признательность автора

Искренне благодарю Эрнеста Борисовича Винберга за приглашение подготовить статью для журнала “Математическое Просвещение” 2008, посвящённого p-адическим числам и их приложениям.

Список литературы

[And76] Andrews, G.E. (1976): The theory of partitions. Reading, Addison–Wesley (1976).

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

[BS85] Borevich, Z.I., Shafarevich, I.R. (1985): Number Theory. (in Russian). 3rd ed. Nauka, Moscow (1985). English transl.: New York/London: Academic Press, 1966.

[Chand70] Chandrasekharan, K. Arithmetical functions. Berlin–Heidelberg–New York, Springer–Verlag (1970).

[Leh70] D. H. Lehmer, Tables of Ramanujan's function tau(n), Math. Comp., 24 (1970), 495-496.)

[Kob77] Koblitz, N. (1977): $p-$adic numbers, $p-$adic analysis and zeta–functions. New York: Springer Verlag (1977).

[Kob84] Koblitz, N. (1984): Introduction to elliptic curves and modular forms. New York: Springer Verlag, 1984.

[KuLe64] Kubota, T., Leopoldt, H.–W. (1964): Eine $p-$adische Theorie der Zetawerte. I. J. reine u. angew. Math., **214/215**, 328-339 (1964).

[Man96] 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.

[Ma-Pa05] 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.

[Ri] Ribet K.A. (1990a): Raising the level of modular representations. Sémin. Theor. Nombres Paris, 1987-88 Progress in Math. **81** (1990), 259-271.

[Se70] Serre, J.– P. (1970): Cours d'arithmétique. Paris: Presses Univ. France, 1970.

[Sloane] Neil J. A. Sloane: Home Page The On-Line Encyclopedia of Integer. Contains 131774 sequences [Thu Aug 23 15:09:40 EDT 2007]
`http://www.research.att.com/ njas/sequences/A000594`

[TaWi] Taylor, R. and Wiles, A., *Ring theoretic properties of certain Hecke algebras*, Ann. of Math. 141 (1995), 553-572

[Wi95] Wiles A., *Modular elliptic curves and Fermat's Last Theorem*, Ann. Math., II. Ser. 141, No.3 (1995) 443–55.