

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 производящими 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	1
2	Производящие функции, модулярные формы и сравнения.	2
2.1	Производящие функции	2
2.2	Представление целых чисел квадратичными формами.	3
2.3	Мотивировка: функция Рамануджана τ и её контекст.	4
3	Классические модулярные формы	11
3.1	Фундаментальная область модулярной группы	12
3.2	Модулярные формы как вычислительное средство решения задач арифметики	14
4	Ряды Эйзенштейна и сравнения для функции Рамануджана.	16
4.1	Структура пространств модулярных форм относительно $SL_2(\mathbb{Z})$	20
4.2	Приложение: доказательство сравнения Рамануджана	22
5	Числа Бернулли и сравнения Куммера	22
5.1	Сравнения для коэффициентов рядов Эйзенштейна	22
5.2	p -адическое интегрирование и мера Мазура	25
5.3	p -адическая дзета-функция Куботы – Леопольдта	26
5.3.1	Область определения p -адических дзета-функций	26
5.3.2	Неархимедово преобразование Меллина	27
5.3.3	Пример: p -адическая дзета-функция Куботы – Леопольдта	27

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:

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

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

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

Действительно, непосредственное перемножение показывает, что

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

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

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

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

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

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

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

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

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

```
gp > {n=100;\
prod(i=1,n,(1-x^(2*i)))*prod(i=1,n,((1-x^(2*i-1))^-1)+0(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 + 0(x^101)
gp > ##
*** last result computed in 451 ms.
```

2.2 Представление целых чисел квадратичными формами.

Пусть

$$f(x) = f(x_1, \dots, x_n) = \sum_{i,j=1}^n a_{ij} x_i x_j = A[x] = x^t A x,$$

$$g(y) = g(y_1, \dots, y_m) = \sum_{i,j=1}^m b_{ij} y_i y_j = B[y] = y^t B y,$$

—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

$$f(Cy) = g(y), \quad A[C] = B. \quad (2.3)$$

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 $4^k(8l - 1)$, $k, l \in \mathbb{Z}$ (см. [Se70], [Ma-Pa05]).

Пусть

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

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]):

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

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

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

где

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

— тэта-функция, которая рассматривается как голоморфная функция на верхней комплексной полуплоскости $\mathbb{H} = \{z \in \mathbb{C} \mid \text{Im}(z) > 0\}$ 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

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

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 $\text{Im}(z) \rightarrow \infty$ в вершинах; заметим, что $2\pi idz = \frac{dq}{q}$, поэтому дифференциал мероморфен с простым полюсом в точке $q = 0 \iff z = i\infty$).

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 следующей производящей функции, определённой разложением в ряд следующего бесконечного произведения:

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

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

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

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

Свойство автоморфности имеет вид:

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

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 $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z})$, поскольку для всех $\gamma \in \text{SL}(2, \mathbb{Z})$, 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 $\text{SL}(2, \mathbb{Z})$ действует на множестве голоморфных функций $f(z)$ на $z \in \mathbb{H}$ по формуле: для $\gamma \in \text{SL}(2, \mathbb{Z})$, 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 $\forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Rightarrow \Delta|_{12}\gamma = \Delta$. Поэтому (2.8) достаточно проверить на образующих группы $\text{SL}(2, \mathbb{Z})$. Используем тот факт, что группа $\text{SL}(2, \mathbb{Z})$ порождена матрицами $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ и $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. 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 следующем смысле [обозначим через \mathbf{P} множество всех простых чисел]:

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

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.[Ma-Pa05]. Может оказаться, что же замечание относится и к теореме Ферма, доказанной 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 :

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

Этот ряд аналогичен ряду Дирихле задающему дзета-функцию Римана,

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

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

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

а доказательство рекуррентных формул сводится к равенству:

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

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 $\operatorname{Re}(s) > 13/2$.

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 функциональным 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 $p : \mathbb{N} \rightarrow \mathbb{N}$ причём полагают $p(0) = 1$.

Как мы видели, производящий ряд функции $p : \mathbb{N} \rightarrow \mathbb{N}$ 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} , $f : \mathbb{H} \rightarrow \mathbb{C}$ где

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

Имеет место равенство $\tilde{\Delta}(q) = q(f(q))^{-24}$ связывающее 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

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

В частности, $\tau(691) = -2747313442193908 \equiv 1 \pmod{691}$.

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

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

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 $\overline{\mathbb{Q}}$. Обозначим через $G_{\mathfrak{p}}$ и $I_{\mathfrak{p}}$ подгруппы группы Галуа $G = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ определенные равенствами:

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

Группа $G_{\mathfrak{p}}$ называемая группой разложения, отождествляется с группой Галуа алгебраического замыкания $\overline{\mathbb{Q}}_{\mathfrak{p}}$ поля $\mathbb{Q}_{\mathfrak{p}}$ 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 замыкания 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 $\rho_l : G \rightarrow \text{GL}(2, \mathbb{Z}_l)$, что для любого простого числа p отличного от l , группа инерции $I_{\mathfrak{p}}$ тривиально действует (т.е. ρ_l неразветвлено в p), и $\det(\text{Id} - \rho_l(Fr_p) \cdot X) = 1 - \tau(p)X + p^{11}X^2$. В случае $l = 691$ справедливо сравнение $\rho_l(Fr_p) \equiv \begin{pmatrix} p^{11} & * \\ 0 & 1 \end{pmatrix} \pmod{691}$, откуда $\tau(p) \equiv 1 + p^{11} \pmod{691}$.

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 $\tau(n)$, дающие 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 $\sigma_{11}(n) = \sum_{d|n} d^{11}$ а во внешней сумме $\sum^{*(n)}$ справа суммирование производится по всем целым решениям уравнения, $n = \Delta\Delta' + \delta\delta'$, которые “допустимы”, т.е. удовлетворяют условиям

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

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

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

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

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 интересная открытая проблема состоит в построении полиномиального алгоритма вычисления $\tau(p)$ для простого числа p . Аналогичный результат известен для коэффициентов $a(p)$ производящего 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 модулярной группы, в то время, как $\tau(p)$ являются коэффициентами модулярной формы веса 12 относительно полной модулярной группы.

3 Классические модулярные формы

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

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

где $Z = \left\{ \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} \mid x \in \mathbb{R}^\times \right\}$ центр группы $G(\mathbb{R})$ а $\text{O}(2)$ ортогональная группа. При этом группа $\text{GL}_2^+(\mathbb{R})$ 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 $\text{SL}_2(\mathbb{Z})$.

Определение 3.1 Голоморфная функция на верхней комплексной полуплоскости $\mathbb{H} = \{z \in \mathbb{C} \mid \text{Im } z > 0\}$ $f : \mathbb{H} \rightarrow \mathbb{C}$ называется модулярной формой целого веса k относительно Γ , если выполнены следующие условия а) и б):

а) Условие автоморфности

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

для всех $\gamma \in \Gamma$;

б) Регулярность в вершинах: f регулярна в вершинах $z \in \mathbb{Q} \cup i\infty$; это означает, что для каждого элемент $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$ 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

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

(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

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

где $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$ и B_k обозначает $k^{\text{е}}$ 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 $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ и $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Имеем

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

С другой стороны, пусть D подмножество \mathbb{H} состоящее из точек z таких, что $|z| \geq 1$ и $|\mathrm{Re}(z)| \leq 1/2$. Мы увидим, что D является фундаментальной областью для действия модулярной группы $\Gamma(1) = \mathrm{SL}(2, \mathbb{Z})$ на \mathbb{H} , т.е. естественное отображение проекции $D \rightarrow \Gamma(1) \backslash \mathbb{H}$ 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 $ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$;
 $z = -\bar{\rho} = e^{\pi i/3}$, 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 множеством классов изоморфизма эллиптических кривых над \mathbb{C} : точке $z \in \mathbb{H}$ сопоставляется комплексный тор $\mathbb{C}/(\mathbb{Z} + z\mathbb{Z})$ который

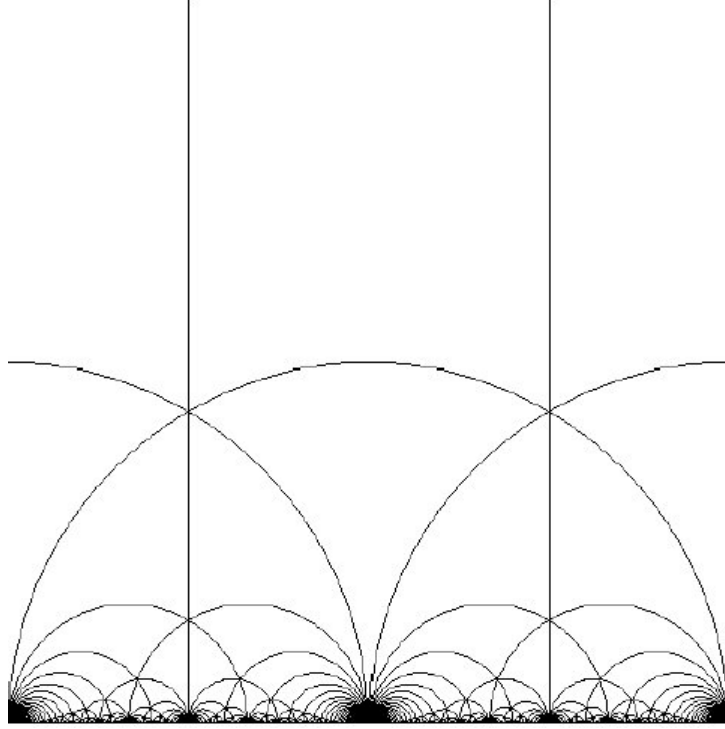


Рис. 2: Действие группы $SL(2, \mathbb{Z})$.

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

аналитически изоморфен римановой поверхности эллиптической кривой, записанной в форме Вейерштрасса:

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

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

При замене z на $\gamma(z)$ для $\gamma = \begin{pmatrix} a_\gamma & b_\gamma \\ c_\gamma & d_\gamma \end{pmatrix} \in SL_2(\mathbb{Z})$ 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 $\Gamma = SL_2(\mathbb{Z})$:

$$2^{-4}(g_2^3 - 27g_3^2) = \quad (3.15)$$

$$2^{-4}(2\pi)^{12} q \prod_{m=1}^{\infty} (1 - q^m)^{24} = 2^{-4}(2\pi)^{12} \sum_{n=1}^{\infty} \tau(n) q^n,$$

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

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

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

Ещё один метод вычисления функции Рамануджана:

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

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. [BBVCO]).

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

```
gp > h6=sum(d=1,20,d^5*q^d/(1-q^d)+0(q^20))
```

```
gp > h4=sum(d=1,20,d^3*q^d/(1-q^d)+0(q^20))
```

```
gp > Delta=((1+240*h4)^3-(1-504*h6)^2)/1728
```

$$\begin{aligned} & q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 - 16744q^7 \\ & + 84480q^8 - 113643q^9 - 115920q^{10} + 534612q^{11} \\ & - 370944q^{12} - 577738q^{13} + 401856q^{14} + 1217160q^{15} \\ & + 987136q^{16} - 6905934q^{17} + 2727432q^{18} + 10661420q^{19} + 0(q^{20}) \end{aligned}$$

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

```
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 + 0(q^20)
```

Вот ещё 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), 0(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 $a_n = p(n)$

Выражение через
модулярную форму,
например
 $\sum_{n=0}^{\infty} p(n)q^n$
 $= (\Delta/q)^{-1/24}$

Число
(ответ)

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-Ra05], 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 (a) *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 $q = e(z) = \exp(2\pi iz)$, 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:

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

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

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

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

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

поскольку $\langle cz+d, az+b \rangle = \langle 1, z \rangle$ для всех $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.

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

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

Логарифмическая производная (4.17) даёт

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

Заметим, что

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

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

$$\begin{aligned} \sum_{k=0}^{\infty} B_k \frac{x^k}{k!} + \frac{x}{2} &= 1 - \sum_{n=1}^{\infty} \frac{2 \left(\frac{x}{2\pi i n} \right)^2}{-\left(\frac{x}{2\pi i n} \right)^2 + 1} = \\ &= 1 - 2 \sum_{n=1}^{\infty} \sum_{k=2k' \geq 2} \left(\frac{x}{2\pi i n} \right)^k = 1 - 2 \sum_{k=2k' \geq 2} \frac{\zeta(k)}{(2\pi i)^k} x^k. \end{aligned}$$

Это непосредственно даёт

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

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:

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

Положим $a = mz$, тогда

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

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

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

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

$$\begin{aligned} \frac{d}{dz} \log(\Delta(z)) &= \frac{d}{dz} \log q + 24 \sum_{m=1}^{\infty} \frac{d}{dz} \log(1 - q^m) = \\ 2\pi i(1 - 24 \sum_{m=1}^{\infty} mq(1 - q^m)^{-1}) &= 2\pi i E_2(z), \quad \frac{dq}{dz} = 2\pi i q. \end{aligned}$$

Достаточно доказать следующее предложение:

Предложение 4.3

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

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

$$\begin{aligned} E_2(z) &= \frac{1}{2\zeta(2)} \sum_{m=-\infty}^{\infty} \left(\sum_{\substack{n=-\infty \\ n \neq 0}}^{\infty} (mz + n)^{-2} \right) = \\ 1 + \frac{3}{\pi^2} \sum_{m \neq 0} \left(\sum_{n=-\infty}^{\infty} (mz + n)^{-2} \right) &= 1 + \frac{6}{\pi^2} \sum_{m=1}^{\infty} \left(\sum_{n=-\infty}^{\infty} (mz + n)^{-2} \right). \end{aligned}$$

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

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

Получается модифицированный ряд

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

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

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

Остаётся вычислить последнюю сумму:

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

Однако

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

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

$$\begin{aligned} \sum_{m \neq 0} \left(\sum_{n=-N+1}^{n=N} b_{m,n} \right) &= \sum_{m \neq 0} \left(\frac{1}{(mz-N)} - \frac{1}{(mz+N)} \right) = \\ &= \frac{2}{z} \sum_{m=1}^{\infty} \left(\frac{1}{(-N/z+m)} + \frac{1}{(-N/z-m)} \right) = \frac{2}{z} \left(\pi \operatorname{ctg} \left(-\frac{\pi N}{z} \right) + \frac{z}{N} \right) \rightarrow -\frac{2\pi i}{z} \end{aligned}$$

при $N \rightarrow \infty$, $z \in \mathbb{H}$, 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 функция $f/(z-p)^n$ голоморфна и не обращается 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 $\Gamma \backslash \mathbb{H}$. 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:

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

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

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

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 $SL(2, \mathbb{Z})$)

(a)

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

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

(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

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691}. \quad (4.26)$$

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

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

и $\dots = \mathcal{O}(q^2)$. Поэтому

$$\alpha = -1008 - \frac{65520}{691} = \frac{a}{691} \quad \text{где } a \equiv -65520 \pmod{691},$$

и из разложения выводится, что

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

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

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

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

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

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

б) Пусть $k \equiv k' \pmod{(p-1)p^{N-1}}$, тогда для любых $c \in \mathbb{Z}$, $(c,p)=1$, $c > 1$ имеем: $(1-c^k)\mathbb{G}_k^* \equiv (1-c^{k'})\mathbb{G}_{k'}^* \pmod{p^N}$ (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 $f_k = \sum_{n \geq 0} a_k(n)q^n$

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 $h(x) = \sum_i \alpha_i x^i \in \mathbb{Z}[x]$ такой, что $h(a) \equiv 0 \pmod{p^N}$ для всех $a \in \mathbb{Z}_p^*$. Тогда $\sum_i \alpha_i \zeta_{(p)}^{(c)}(-i) \equiv 0 \pmod{p^N}$.

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

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

Отсюда вытекает

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

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

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

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

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

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

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

$$\zeta_{(p)}^{(c)}(-k) = (c^{k+1} - 1)(1 - p^k) \frac{B_{k+1}}{k+1} \equiv \frac{S_{k+1}(p^M)}{p^M} \cdot \frac{(c^{k+1} - 1)}{k+1} \pmod{p^N} \quad (5.27)$$

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

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

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

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

поэтому $\zeta_{(p)}^{(c)}(-k) \equiv \sum_{\substack{n=1 \\ p \nmid n}} t \cdot n_c^k \pmod{p^M}$ где $t_n = t(n, c)$ не зависит от k . Чтобы завершить до-

казательство, подставим это сравнение в линейную комбинацию из теоремы 5.2 используя предположение

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

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

$$\zeta_{(p)}^{(c)}(-k) \equiv \zeta_{(p)}^{(c)}(-k') \pmod{p^N}.$$

Доказательство следствия 5.3: По теореме Эйлера имеем $h(a) \equiv 0 \pmod{p^N}$, 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, $\mathbb{C}_p = \widehat{\mathbb{Q}_p}$ (полное алгебраическое замыкание 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 $\text{Step}(Y, R)$ – 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 $U \subset Y$:

$$\mu: \left\{ \begin{array}{c} \text{открытые подмножества} \\ U \subset Y \end{array} \right\} \longrightarrow \mathcal{M}.$$

Другими словами, μ – это гомоморфизм R -модулей

$$\mu: \text{Step}(Y, R) \rightarrow \mathcal{M}$$

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 $\text{Step}(Y, R) \subset \mathcal{C}(Y, R)$ определяет распределение, обозначаемое той же буквой μ , причём мера μ однозначно определена по соответствующему распределению, поскольку R -подмодуль $\text{Step}(Y, R)$ “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 $\int_{\mathbb{Z}_p^*} x^k d\mu^{(c)} = \zeta_{(p)}^{(c)}(1-k) = (1-c^k)(1-p^{k-1})\zeta(1-k)$. 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, удовлетворяющей условиям следствия, определим интеграл $\int_{\mathbb{Z}_p^\times} \phi(x) \mu^{(c)}$ для каждой непрерывной функции $\phi: \mathbb{Z}_p^\times \rightarrow \mathbb{Z}_p$. 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

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

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

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

состоящая из всех непрерывных гомоморфизмов проконечной группы \mathbb{Z}_p^\times в мультипликативную группу поля Тэйта, $\mathbb{C}_p = \widehat{\mathbb{Q}}_p$ (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 Леопольдта даёт существование p -адической аналитической функции $\zeta_p : X_p \rightarrow \mathbb{C}_p$ с единственным простым полюсом в точке $x = x_p^{-1}$, которая становится ограниченной аналитической функцией на X_p после умножения на регуляризирующий множитель $(cx(c) - 1)$, ($x \in X_p, c \in \mathbb{Z}_p^\times$); эта функция однозначно определена условием

$$\zeta_p(x_p^k) = (1 - p^k)\zeta(-k) \quad (k \geq 1). \quad (5.29)$$

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

$$i_p : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p \quad (5.30)$$

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

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

становится элементом подгруппы кручения

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

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

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

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

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

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

$$L_\mu : X_p \longrightarrow \mathbb{C}_p. \quad (5.33)$$

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 выражает 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 -адическая дзета-функция Куботы – Леопольдта

Для меры Мазура из следствия 5.4 функция на X_p

$$\zeta_p(x) = (1 - c^{-1}x(c)^{-1})^{-1} L_{\mu^{(c)}}(x) \quad (x \in X_p) \quad (5.34)$$

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 регуляризирующий 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.