

Рис. 4

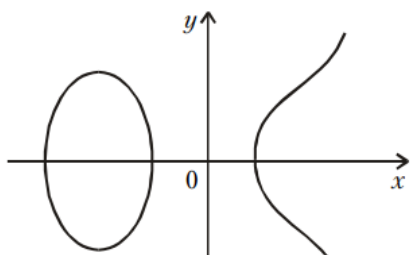


Рис. 5

Для кривой, заданной в канонической форме (2), дискриминант Δ определяется формулой

$$\Delta = -(4a^3 + 27b^2).$$

Пусть E - некоторая эллиптическая кривая, заданная уравнением

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

в котором a и b - целые числа. Для простого числа p рассмотрим сравнение

$$y \equiv x^3 + \bar{a}x + \bar{b} \pmod{p} \quad (3)$$

где \bar{a} и \bar{b} - остатки от деления целых чисел a и b на p , и обозначим через n_p число решений этого сравнения. Числа n_p , очень полезны при исследовании вопроса о разрешимости уравнений вида (2) в целых числах: если какое-то n_p равно нулю, то уравнение (2) не имеет целочисленных решений. Однако вычислить числа n_p удастся лишь в редчайших случаях. В то же время известно, что $|p - n_p| \leq 2\sqrt{p}$ (теорема Хассе).

Рассмотрим те простые числа p , которые делят дискриминант Δ эллиптической кривой (2). Можно доказать, что для таких p многочлен $x^3 + \bar{a}x + \bar{b}$ можно записать одним из двух способов:

$$x^3 + \bar{a}x + \bar{b} \equiv (x + \bar{\alpha})^2(\bar{\beta}) \pmod{p}$$

или

$$x^3 + \bar{a}x + \bar{b} \equiv (x + \bar{\gamma})^3 \pmod{p},$$

где $\bar{\alpha}, \bar{\beta}, \bar{\gamma}$ - некоторые остатки от деления на p . Если для всех простых

p , делящих дискриминант кривой, реализуется первая из двух указанных возможностей, то эллиптическая кривая называется *полустабильной*.

Простые числа, делящие дискриминант, можно объединить в так называемый *кондуктор* эллиптической кривой. Если E - полустабильная кривая, то ее кондуктор N задается формулой

$$N = \prod_{p|\Delta} p^{\epsilon_p}, \quad (4)$$

где для всех простых чисел $p \geq 5$, делящих Δ , показатель ϵ_p , равен 1. Показатели ϵ_2 и ϵ_3 , вычисляются с помощью специального алгоритма.

Модулярные формы и модулярные эллиптические кривые

Обозначим через \mathbb{H} верхнюю комплексную полуплоскость. Пусть N - натуральное и k - целое числа. *Модулярной параболической формой* веса k уровня N называется аналитическая функция $f(z)$, заданная в верхней полуплоскости и удовлетворяющая соотношению

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z) \quad (5)$$

для любых целых чисел a, b, c, d таких, что $ad-bc = 1$ и c делится на N . Кроме того, предполагается, что

$$\lim_{t \rightarrow +0} f(r+it) = 0,$$

где r - рациональное число, и что

$$\lim_{t \rightarrow \infty} f(it) = 0.$$

Пространство модулярных параболических форм веса k уровня N обозначается через $S_k(N)$. Можно показать, что оно имеет конечную размерность.

В дальнейшем нас будут особо интересовать модулярные параболические формы веса 2. Для малых N размерность $\dim S_2(N)$ пространства $S_2(N)$ представлена в таблице:

$N < 10$	11	12	13	14	15	16
0	1	0	0	1	1	0
	17	18	19	20	21	22
	1	0	1	1	1	2

В частности,

$$\dim S_2(2) = 0. \quad (6)$$

Отметим, что эта нехитрая формула сыграет важную роль в доказательстве теоремы Ферма.

Из условия (5) следует, что $f(z+1) = f(z)$ для каждой формы $f \in S_2(N)$. Стало быть, f является периодической функцией. Такую функцию можно представить в виде

$$f(z) = \sum_{n=1}^{\infty} a_n q^n, \quad q = e^{2\pi iz}. \quad (7)$$

Назовем модулярную параболическую форму $f(z) \in S_2(N)$ собственной, если ее коэффициенты - целые числа, удовлетворяющие соотношениям

$$a_1 = 1;$$

$$a_{pr} a_p = a_{p^{r+1}} p c_{p^{r-1}} \text{ для простого } p, \text{ не делящего число } N; \quad (8)$$

$$a_{pr} = (a_p)^r \text{ для простого } p, \text{ делящего число } N;$$

$$a_{mn} = a_m a_n, \text{ если } (m, n) = 1.$$

Сформулируем теперь определение, играющее ключевую роль в доказательстве теоремы Ферма. Эллиптическая кривая с рациональными коэффициентами и кондуктором N называется *модулярной*, если найдется такая собственная форма

$$f(z) = \sum_{n=1}^{\infty} a_n q^n \in S_2(N), \quad (9)$$

что $a_p = p - n_p$ для почти все простых чисел p . Здесь n_p - число решений сравнения (3).

Гипотеза Таниямы

Определение модулярной эллиптической кривой является настолько жестким, что на первый взгляд кажется невероятным существование хотя бы одной такой кривой. Трудно представить, что функция $f(z)$, удовлетворяющая перечисленным выше весьма ограничительным условиям (5) и (8), разлагается в ряд (7), коэффициенты которого связаны с практически невычислимыми числами n_p . Однако эмпирический материал, полученный в первой по-