Доклады Академии наук СССР
1972. Том 204, № 2

УДК 517.862 МАТЕМАТИКА

Л. А. КОГАН

ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ И МОДУЛЯРНЫЕ ФОРМЫ

(Представлено академиком Ю. В. Линником 22 XI 1971)

А. Вейль ([8]) высказал гипотезу, относящуюся к построению модулярных форм веса —2. Доказательство этой гипотезы А. Вейля известно для всех эллиптических кривых с комплексным умножением и для эллиптических кривых без комплексного умножения в случае, когда род поля модулярных функций $\Gamma_0(N)$ равен 1 (N — кондуктор кривой). Об этом А. Вейль сообщил в работе ([9]). В монографии ([3]) автор высказал гипотезу (А), которая является обобщением гипотезы А. Вейля ([8]) и относится к построению модулярных форм веса $-l$ ($l > 2$).

Как сообщено в работах ([3], [4]), гипотеза (А) была доказана автором с помощью обобщенных тэта-рядов для кривых

$$y^2 = x^3 + 1, \qquad y^2 = x^3 - x.$$

А. Вейль сообщил *, что гипотеза (А) в случае ее справедливости может быть проверена на основе результатов его работы ([8]) и работы Дойринга ([6]).

В статье приводится набросок доказательства гипотезы (А) для всех кривых с комплексным умножением (при l четных) на основе результатов ([8]) и ([6]). Кроме этого в заметке приводится функциональное уравнение для функции (6), построенной с помощью эллиптических кривых с комплексным умножением, определенных над алгебраическими полями.

Сформулируем гипотезу А. Вейля и гипотезу (А).

Пусть C — эллиптическая кривая, определенная над полем рациональных чисел Q посредством уравнения Вейерштрасса

$$y^2 = x^3 + Ax + B \tag{1}$$

с рациональными коэффициентами. Для каждого простого p кривой C однозначно соответствует модель Нерона C_p, бирационально эквивалентная C над p-адическим полем Q_p, заданная посредством уравнения

$$Y^2 + \lambda XY + \mu Y = X^3 + \alpha X^2 + \beta X + \gamma$$

с целыми p-адическими коэффициентами.

Далее редуцируем кривую C_p по $\operatorname{mod} p$. Обозначим через $\overline{C}_p$ уравнение редуцированной кривой. Возможны три случая:

a) редукция $\overline{C}_p = C_p (\operatorname{mod} p)$ «хорошая» (невырожденная); тогда положим

$$L_p^{(s)} = (1 - a_p p^{-s} + p^{1-2s})^{-1},$$

где $p + 1 - a_p$ — число рациональных точек на редуцированной кривой;

b) $\overline{C}_p$ имеет двойную точку с раздельными касательными; в этом случае положим $L_p^{(s)} = (1 - \varepsilon_p p^{-s})^{-1}$, $\varepsilon_p = 1$ или -1, в зависимости от того, рациональны или нет касательные над F_p;

* Письмо от 18 марта 1970 г.

c) $\bar{C}_p$ имеет точку возврата; в этом случае положим $L_p^{(s)} = 1$. Пусть N — кондуктор кривой C; $L^{(s)} = \prod_p L_p^{(s)} = \sum_{n=1}^{\infty} a_n n^{-s}$ — дзета-функция кривой C. А. Вейль предположил, что тогда $\sum_{n=1}^{\infty} a_n e^{2\pi i\tau n}$ — параболическая форма типа $(-2, N, 1)$.

Известно [1], что для p «хороших» $a_p = \mathrm{Tr}(\pi(p))$, где $\pi(p)$ — след эндоморфизма Фробениуса кривой C_p, редуцированной по модулю p.

Гипотеза (А). В тех же обозначениях, что были введены при формулировке гипотезы А. Вейля, пусть редукция $\bar{C}_p$ «хорошая», тогда положим

$$L_{p,k}^{(s)} = (1 - b_{p,k} p^{-s} + p^{k-1-2s})^{-1}, \quad \text{где} \quad (k-1) \geqslant 1, \quad k \text{ четное},$$

$b_{p,k} = \mathrm{Tr}\,(\pi^{k-1}(p))\,\pi^{k-1}(p) - (k-1)$ — степень эндоморфизма Фробениуса эллиптической кривой C_p. Тогда существует такой множитель, отнесенный к «плохим» p,

$$F_k = \prod_p L_{p,k}^{(s)}, \quad \text{«плохие»}$$

(при p «плохих» $L_{p,k}^{(s)}$ равно 1 или $(1 - C_k(p)p^{-s})^{-1}$, $C_k(p)$ — некоторая функция от p), что определенный по L-ряду

$$L_k^{(s)} = F_k \prod_p L_{p,k}^{(s)} = \sum_{n=1}^{\infty} b_{n,k} n^{-s}, \quad p \text{ «хорошие»}, \tag{2}$$

ряд Фурье

$$\sum_{n=1}^{\infty} b_{n,k} e^{2\pi i\tau n}$$

является некоторой параболической формой веса $-k$. Причем для кривых с комплексным умножением ряд

$$\sum_{n=1}^{\infty} b_{n,k} e^{2\pi i\tau n}$$

при $(k-1)$ нечетных является параболической формой геккевского типа $(-k, N_k, 1)$, где N_k — делитель кондуктора кривой C.

Для дальнейшего нам понадобятся следующие утверждения.

Лемма 1 (следует из результатов Дойринга [6]). *Пусть C — алгебраическая кривая рода 1 над числовым полем K, определенная посредством уравнения*

$$f(x;\, y) = 0 \tag{3}$$

с коэффициентами из K.

Пусть на кривой (3) имеется по крайней мере одна точка с координатами из K и кривая (3) имеет комплексное умножение. И пусть комплексные умножения образуют порядок K_2 в мнимом квадратичном поле $K_1 = Q(\sqrt{-d})$ и пусть $K_1 \subseteq K$, $\mathfrak{p}$ — простой дивизор числового поля K.

Обозначим для $\mathfrak{p}$ «хороших»

$$L_k''(s, C, K, \mathfrak{p}) = (1 - \pi_\nu^{k-1} N\mathfrak{p}^{-s})^{-1} (1 - \bar{\pi}_\nu^{k-1} N\mathfrak{p}^{-s})^{-1}, \tag{4}$$

где π_ν, $\bar{\pi}_\nu$ — собственные числа эндоморфизма Фробениуса кривой (3), редуцированной по mod $\mathfrak{p}$.

Тогда существует такой множитель $F_k''(s)$, отнесенный к «плохим» $\mathfrak{p}$ («плохих» $\mathfrak{p}$ конечное число), что

$$L_k''(s) = (F_k(s))^{-1}\prod_{\mathfrak{p}}(1-\pi_\nu^{k-1}N\mathfrak{p}^{-s})^{-1}(1-\bar{\pi}_\nu^{k-1}N\mathfrak{p}^{-s})^{-1} =$$
$$= L^*\left(s-\frac{k-1}{2},\ \lambda^{k-1}, K\right)L^*\left(s-\frac{k-1}{2}, \overline{\lambda^{k-1}}, K\right), \tag{5}$$

где $L^*(s, \lambda, K)$ — ряд Гекке поля K с гроссенхарактером λ. В ведущий модуль характера λ входят только простые дивизоры, отнесенные к плохим $\mathfrak{p}$; λ — неглавный характер; $L(s, K, \lambda)$ — целая функция. Функция

$$\psi(s, K, \lambda^{\pm1}) = (d\,/\,(2\pi)^n)^{1/2 s}(Nf_\nu)^{1/2 s}\Gamma^{1/2 n}(s+1/2)L(s, K, \lambda^{\pm1}) \tag{6}$$

(f_ν — ведущий модуль λ, n — порядок поля K) — целая функция от s и удовлетворяет функциональному уравнению

$$\psi(1-s, K, \lambda^{\mp1}) = w(\lambda^{\pm1})\psi(s, K, \lambda^{\pm1}),\ w(\lambda)w(\bar{\lambda}) = 1. \tag{7}$$

Лемма 2 (следует из результатов Дойринга [6]). *Пусть C — алгебраическая кривая рода 1 над числовым полем Q, определенная посредством уравнения*

$$f(x;\ y) = 0 \tag{8}$$

с коэффициентами из Q (поле рациональных чисел).

Пусть на кривой (8) имеется по крайней мере одна точка с координатами из Q и кривая (8) имеет комплексное умножение; пусть комплексные умножения образуют порядок K_2 в мнимом квадратичном поле $K_1 = Q(\sqrt{-d})$. Обозначим для p «хороших»

$$L_k'(s, C, Q, p) = (1-\pi_\nu^{k-1}p^{-s})^{-1}(1-\bar{\pi}_\nu^{k-1}p^{-s}), \tag{9}$$

где π_ν, $\bar{\pi}_\nu$ — собственные числа эндоморфизма Фробениуса кривой (8), редуцированной по $\operatorname{mod} p$.

Тогда существует такой множитель $F_k'(s)$, отнесенный к «плохим» p («плохих» p конечное число), что

$$L_k^{(s)} = (F_k'(s))^{-1}\prod_{p}(1-\pi_\nu^{k-1}p^{-s})^{-1}(1-\bar{\pi}_\nu^{k-1}p^{-s})^{-1} =$$
$$= L\left(s-\frac{k-1}{2},\ \lambda^{k-1}, K_2\right) = \sum_{n=1}^{\infty}\frac{b_{n,k}}{n^s}, \tag{10}$$

где $L(s, \lambda, K_2)$ — L-ряд Гекке с гроссенхарактером λ над K_2, причем

$$L(s, \lambda, K_2) = L(s, \bar{\lambda}, K_2).$$

Пользуясь леммой 2 и результатами [7], автор вывел функциональные уравнения для $L_k'(s) = \sum_{n=1}^{\infty}\frac{b_{n,k}}{n^s}$ (где $L_k'(s)$ определено по формуле (10)) и $L_{k,\chi}'(s) = \sum_{n=1}^{\infty}\frac{b_{n,k}\chi(n)}{n^s}$, где $\chi(n)$ — любой примитивный характер с ведущим модулем m (m — натуральное число, удовлетворяющее условиям теоремы 2 работы [8], $(k-1)$ нечетные).

На основе этого с помощью критерия А. Вейля (теорема 2 из ([8])) получено доказательство * гипотезы (A) в случае ($k-1$) нечетных.

Заметим, что для коэффициентов Фурье $b_{n,k}$, построенных модулярных форм выполняется оценка ** $|b_{n,k}| < B_\varepsilon n^{\frac{1}{2}(k-1)+\varepsilon}$, которая следует из известной оценки ***

$$|b_{p,2}| = |a_p| \leqslant 2\sqrt{p},$$

рекуррентных формул

$$b_{p,k} = b_{p,k-1}b_{p,2} - pb_{p,k-2} \quad \text{при} \quad k > 3,$$
$$b_{p,k} = b_{p,k-1}^2 - 2p \quad \text{при} \quad k = 3$$

и мультипликативных свойств $b_{n,k}$.

На основе леммы 1 получено функциональное уравнение

$$\Lambda_k(s) = CA^{\frac{1}{2}k-s}\Lambda_k^{(k-s)},$$

где

$$\Lambda_k(s) = \left(\frac{1}{(2\pi)^n}\right)^s \{\Gamma(s)\}^n L_k''(s)$$

($L_k''(s)$ определено по формуле (5)).

Лемма 1 позволяет также сформулировать аналог гипотезы (А) для кривых, определенных над алгебраическими полями.

В заключение считаю своим долгом выразить глубокую благодарность А. Вейлю, Ю. И. Манину за ценные указания и советы и А. И. Виноградову за большое внимание к работе и советы.

Поступило
2 XI 1971

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] А. О. Гельфонд, Ю. В. Линник, Элементарные методы в аналитической теории чисел, М., 1962. [2] Д. Касселс, Сборн. пер. Математика, **12**, **1**, 114 (1968); **12**, 2, 3 (1968). [3] Л. А. Коган, О представлении целых чисел положительно определенными квадратичными формами, Ташкент, 1971. [4] Л. А. Коган, Сообщ. АН ГрузССР, **59**, № 3 (1971). [5] Ю. И. Манин, Изв. АН СССР, сер. матем., **120**, 673 (1956). [6] M. Deuring, Nachr. Akad. Wiss. Göttingen, Math.-Phys. Kl., Math.—Phys.—Chem. Abt., 85 (1953); 13 (1955); 37 (1956); 55 (1957). [7] Hecke, Math. Zs., **6**, 11 (1920). [8] A. Weil, Math. Annal., **168**, 149 (1967). [9] A. Weil, Proc. of the Bombey Colloquium on Algebraic Geometry, 1968.

* Без полного уточнения ступени построенной модулярной формы и с точностью до конечного числа множителей в (2), отнесенных к «плохим» p эллиптической кривой (1).

** Эта оценка подтверждает известную гипотезу Рамануджана — Петерсона.

*** Элементарное доказательство этой оценки Хассе дано Ю. И. Маниным в ([5]), смотрите также ([1]).