

В. А. ДЕМЬЯНЕНКО
О ВЫСОТЕ ТЭЙТА

(Представлено академиком И. М. Виноградовым 16 II 1973)

Пусть K — алгебраическое числовое поле степени n и T — эллиптическая кривая $y^2 = x^3 + rx + s$, определенная над этим полем.

В работе (1a) приводится изящное доказательство теоремы Тейта, дающей информацию о поведении высоты точек на абелевом многообразии. В частности, показывается, что если точки P_i , $i=1, 2, \dots, r$, взятые на T , рациональны над заданным полем K , то

$$c_1 < \ln \left\{ H \left(\sum_{i=1}^r t_i P_i \right) \right\} - \sum_{i,j=1}^r \alpha_{i,j} t_i t_j < c_2, \quad (1)$$

где $H(\sum_{i=1}^r t_i P_i)$ — высота Вейля точки $\sum_{i=1}^r t_i P_i$, c_1 и c_2 — некоторые константы, зависящие лишь от r , s и K .

Пусть $\sum_{i=1}^r t_i P_i = \{x_{(n)}, y_{(n)}\}$. Согласно формулам сложения точек на кривой T

$$x_{(m_i+n_i)} = \frac{-2y_{(m_i)}y_{(n_i)} + (x_{(m_i)} + x_{(n_i)})(x_{(m_i)}x_{(n_i)} + r) + 2s}{(x_{(n_i)} - x_{(m_i)})^2}, \quad (2)$$

$$y_{(m_i+n_i)} = \frac{(x_{(m_i)} + 3x_{(n_i)})(ry_{(m_i)} - x_{(m_i)}^2 y_{(n_i)}) + 4s(y_{(m_i)} - y_{(n_i)})}{(x_{(n_i)} - x_{(m_i)})^3} + \\ + \frac{(3x_{(m_i)} + x_{(n_i)})(x_{(n_i)}^2 y_{(m_i)} - ry_{(n_i)})}{(x_{(n_i)} - x_{(m_i)})^3}.$$

Поэтому

$$x_{(m_i+n_i)}x_{(m_i-n_i)} = \frac{(x_{(m_i)}x_{(n_i)} - r)^2 - 4s(x_{(m_i)} + x_{(n_i)})}{(x_{(n_i)} - x_{(m_i)})^2}, \quad (3)$$

$$y_{(m_i+n_i)}y_{(m_i-n_i)} = \frac{x_{(m_i)}^3 x_{(n_i)}^3 + r(x_{(m_i)}x_{(n_i)} - r)(x_{(m_i)}^2 + 3x_{(m_i)}x_{(n_i)} + x_{(n_i)}^2)}{(x_{(n_i)} - x_{(m_i)})^3} + \\ + \frac{s(x_{(m_i)} + x_{(n_i)})(x_{(m_i)}^2 + 8x_{(m_i)}x_{(n_i)} + x_{(n_i)}^2 - 2r) - r^3 - 8s^2}{(x_{(n_i)} - x_{(m_i)})^3}.$$

Пусть $u_{(m_i)}$, $v_{(m_i)}$, $w_{(m_i)}$ — произвольным образом выбранные целые числа из поля K , удовлетворяющие равенствам $x_{(m_i)} = u_{(m_i)}/w_{(m_i)}$, $y_{(m_i)} = v_{(m_i)}/w_{(m_i)}^3$ и (e_i) — система абсолютных наименьших вычетов индексов (m_i)

по mod 2. Тогда, ввиду (3), координатам точек $\sum_{i=1}^r m_i P_i$ можно поставить в соответствие тройку чисел $X_{(m_i)}$, $Y_{(m_i)}$, $Z_{(m_i)}$ по следующим рекуррент-

НЫМ СООТНОШЕНИЯМ:

$$x_{(m_i)} = X_{(m_i)} / Z_{(m_i)}^2, \quad y_{(m_i)} = Y_{(m_i)} / Z_{(m_i)}^3,$$

$$X_{(m_i)} X_{(e_i)} = (X_{(\alpha_i)} X_{(\beta_i)} - r Z_{(\alpha_i)}^2 Z_{(\beta_i)}^2)^3 - 4s (X_{(\alpha_i)} Z_{(\beta_i)}^2 + X_{(\beta_i)} Z_{(\alpha_i)}^2) Z_{(\alpha_i)}^2 Z_{(\beta_i)}^2,$$

$$Y_{(m_i)} Y_{(e_i)} = X_{(\alpha_i)}^3 X_{(\beta_i)}^3 + r (X_{(\alpha_i)} X_{(\beta_i)} - r Z_{(\alpha_i)}^2 Z_{(\beta_i)}^2) (X_{(\alpha_i)}^2 Z_{(\beta_i)}^4 +$$

$$+ 3 X_{(\alpha_i)} X_{(\beta_i)} Z_{(\alpha_i)}^2 Z_{(\beta_i)}^2 + X_{(\beta_i)}^2 Z_{(\alpha_i)}^4) + s (X_{(\alpha_i)} Z_{(\beta_i)}^2 + X_{(\beta_i)} Z_{(\alpha_i)}^2) (X_{(\alpha_i)}^2 Z_{(\beta_i)}^4 +$$

$$+ 8 X_{(\alpha_i)} X_{(\beta_i)} Z_{(\alpha_i)}^2 Z_{(\beta_i)}^2 + X_{(\beta_i)}^2 Z_{(\alpha_i)}^4 - 2r Z_{(\alpha_i)}^4 Z_{(\beta_i)}^4) - (r^3 + 8s^2) Z_{(\alpha_i)}^6 Z_{(\beta_i)}^6,$$

$$Z_{(m_i)} Z_{(e_i)} = \begin{cases} X_{(\beta_i)} Z_{(\alpha_i)}^2 - X_{(\alpha_i)} Z_{(\beta_i)}^2 & \text{при } (e_i) \neq (0), \\ 2Y_{(m_i/2)} Z_{(m_i/2)} & \text{при } (e_i) = (0); \end{cases}$$

$$(\alpha_i) = ((m_i + e_i)/2), \quad (\beta_i) = ((m_i - e_i)/2),$$

$$X_{(e_i)} = u_{(e_i)} / d_{(e_i)}^2, \quad Y_{(e_i)} = v_{(e_i)} / d_{(e_i)}^3, \quad Z_{(e_i)} = w_{(e_i)} / d_{(e_i)},$$

$$d_{(e_i)} = (u_{(e_i)}, v_{(e_i)}, w_{(e_i)}).$$

$$\text{Пусть } |N^{-1}(X_{(m_i)}^3, Y_{(m_i)}^2, Z_{(m_i)}^6)| = H_0 \text{ и } \max\{|X_{(m_i)}^{(j)}|^3, |Y_{(m_i)}^{(j)}|^2, |Z_{(m_i)}^{(j)}|^6\} =$$

$$= H_j. \text{ Очевидно, } H = \prod_{s=0}^n H_s.$$

Так как $(u_{(e_i)}, v_{(e_i)}, w_{(e_i)})$ определено лишь с точностью до единиц поля K , то выбор H_j будет неоднозначным. Поэтому будем брать такие значения $(u_{(e_i)}, v_{(e_i)}, w_{(e_i)})$, при которых $\sum_{j=1}^n H_j$ достигает своего минимума. В этом случае аналогично (1) будем иметь

$$c_{1,j} < \ln \left\{ H_j \left(\sum_{i=1}^r m_i P_i \right) \right\} - \sum_{j,s=1}^r \alpha_{j,s} m_j m_s < c_{2,j},$$

где $c_{1,j}, c_{2,j}$ — некоторые константы, зависящие лишь от $r^{(j)}, s^{(j)}, K^{(j)}, j=1, 2, \dots, n$.

Таким образом, высоту Тэйта h можно разложить на компоненты $h_j, j=1, 2, \dots, n$, по сопряженным полям $K^{(j)}$ таким образом, чтобы $h = \sum_{i=1}^n h_i$

и каждая из компонент h_i обладала квадратичностью относительно группового закона сложения точек.

Полученный результат имеет приложения к арифметическим вопросам теории алгебраических кривых. Рассмотрим некоторые из них.

Л. Морделл ⁽²⁾ предположил, что на всякой кривой рода $g > 1$ существует лишь конечное число рациональных точек. Как известно, самый сильный результат на пути доказательства этой гипотезы был получен Ю. И. Маниным ⁽¹⁶⁾, который установил ее справедливость над функциональным полем (совсем недавно доказательство указанного результата Ю. И. Манина было упрощено А. Н. Паршиным ⁽⁴⁾). Для наиболее трудного «числового случая» гипотезы Л. Морделла нами было доказано ⁽⁵⁾, что всякая кривая Φ , допускающая над полем K группу отображений G ранга R на одну и ту же эллиптическую кривую T ранга r , имеет конечное число K -точек, если только $R > r$. Впоследствии доказательство этого фак-

та было упрощено Дж. Касселсом ⁽³⁾ и распространено на якобиевы многообразия Ю. И. Маниным ^(1в).

Квадратичность компонент h_i относительно группового закона сложения точек на T позволяет доказать следующую более общую теорему.

Теорема 1. Если кривая Φ допускает над K группы отображений G_i , $i=1, 2, \dots, t$, рангов R_i на эллиптические кривые T_i рангов r_i , бирационально изоморфные над расширениями K , то Φ имеет конечное число K -точек, если только $R_i > r_i$ для некоторого $i \in (1, 2, \dots, t)$ или же

$$\left(\sum_{i=1}^t \frac{R_i + 1}{2} \right) > \sum_{i=1}^t r_i R_i.$$

Для иллюстрации этой теоремы укажем два конкретных примера.

Пример 1. Если над полем рациональных чисел сумма рангов кривых $u^4 + 1 = \alpha v^2$, $u^4 + v^2 = \alpha$ не превышает 3, то кривая $x^4 + y^4 = \alpha$ имеет конечное число рациональных точек.

Пример 2. Если сумма рангов кривых $u^3 + v^2 = \alpha$, $u^3 + v^2 = -\alpha^2$, $u^3 + v^2 = \alpha^3$ над полем рациональных чисел не превышает 8, то кривая $x^6 + y^6 = \alpha$ имеет конечное число рациональных точек.

Пусть $f_m(x, y)$ — бинарная однородная форма степени m относительно переменных x и y . С использованием разложения высоты Тэйта на компоненты доказываются еще две теоремы.

Теорема 2. Если r — ранг кривой $T: f_3(u, v) = A$ над K , то существует такая константа $c(r, n)$, зависящая лишь от r и n , что число целых K -точек на T со взаимно простыми координатами не превосходит $c(r, n)$.

Теорема 3. Если r — ранг кривой $f_4(u, 1) = Av^2$ над K , то существует такая константа $c(r, n)$, зависящая лишь от r и n , что число целых K -точек на $T: f_4(x, y) = A$ не превосходит $c(r, n)$.

Заметим, что на кривой $f_4(x, y) = A$ учитываются также целые точки и с не взаимно простыми координатами.

Из теорем 2 и 3 вытекают

Следствие 1. Пусть $K(s_1, s_2, \dots, s_n)$ — поле, получаемое присоединением к K корней уравнения $f_m(s) = 0$.

Тогда число целых K -точек на кривой $f_m(x, y) = 1$ не превышает константы $c(r, t, n)$, зависящей лишь от r , t и n , где r — наименьший над

полем $K(s_1, s_2, \dots, s_m)$ из рангов кривых $\prod_{s=1}^4 (u - s_i) = \epsilon v^2$, $\prod_{s=1}^3 (u - s_i v) = \epsilon$

(ϵ — единица из $K(s_1, s_2, \dots, s_m)$).

Следствие 2. Если над алгебраическим числовым полем K ранги кривых $f_3(u, v) = A$, $f_4(u, 1) = Av^2$ ограничены равномерно, то и число целых K -точек на них равномерно ограничено.

Следствие 3. Если число целых K -точек на кривых $f_3(u, v) = A$, $(u, v) = 1$, $f_4(x, y) = A$ ограничено неравномерно, то существуют такие кривые, ранги которых над фиксированным полем K превышают произвольное наперед заданное число c .

Институт математики и механики
Уральского научного центра Академии наук СССР
Свердловск

Поступило
13 II 1973

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

- ¹ Ю. И. Манин, Изв. АН СССР, а) 27, в. 6, 1395 (1963); б) 28, в. 6, 1363 (1964); в) 33, в. 3, 459 (1969). ² L. Mordell, Proc. Cambr. Phil. Soc., 21, 179 (1922). ³ J. W. S. Cassels, J. London Math. Soc., 43, 61 (1968). ⁴ А. Н. Паршин, УМН, 27, в. 4 (1972). ⁵ В. А. Демьяненко, Изв. АН СССР, 30, в. 5, 1373 (1966).