



УДК 512.74+512.552

Д.Ф. БАЗЫЛЕВ

## РАЦИОНАЛЬНЫЕ ТОЧКИ ЭЛЛИПТИЧЕСКИХ КРИВЫХ НУЛЕВОГО РАНГА

The method of calculation of rational points on the elliptic curves of zero rank is described.

Проблема нахождения ранга эллиптических кривых в общем случае является достаточно сложной. В данной статье мы предлагаем подход к доказательству того, что эллиптическая кривая имеет нулевой ранг. В этом случае группа рациональных точек эллиптической кривой  $E(\mathbf{Q})$  совпадает с ее подгруппой кручения, которая, как известно, является конечной, и, следовательно, группа  $E(\mathbf{Q})$  может быть описана явно, т. е. посредством перечисления элементов, а также с точки зрения абстрактной структуры.

Напомним, что всякая эллиптическая кривая над  $\mathbf{Q}$  может быть задана в форме Вейерштрасса  $E: y^2=f(x)=ax^3+bx^2+cx+d, f(x) \in \mathbf{Q}[x]$ .

В зависимости от типа разложения многочлена  $f(x)$  над  $\mathbf{Q}$  обычно различают три случая: неразложимый, полуразложимый и разложимый, каждый из которых рассмотрим отдельно.

1. Пусть  $f(x)$  неприводим над  $\mathbf{Q}$  и  $P_0(x_0, y_0) \in E(\mathbf{Q})$ . Положим  $t = \frac{y - y_0}{x - x_0}$ ,  $x \neq x_0$ . Тогда  $(y_0 + t(x - x_0))^2 = f(x)$ , причем  $f(x) - f(x_0) = (x - x_0) \times (a(x^2 + x x_0 + x_0^2) + b(x + x_0) + c)$ ,  $y_0^2 = f(x_0)$ .

Следовательно,

$$ax^2 + (ax_0 + b - t^2)x + ax_0^2 + bx_0 + c - 2ty_0 + t^2x_0 = 0. \quad (1)$$

Так как  $x \in \mathbf{Q}$ , то дискриминант уравнения (1) является полным квадратом, т. е.

$$(ax_0 + b - t^2)^2 - 4a(ax_0^2 + bx_0 + c - 2ty_0 + t^2x_0) = D^2, \quad (2)$$

где  $D \in \mathbf{Q}$ .

Пусть  $t = \frac{m}{n}$ ,  $(m, n)=1$ . Перепишем (2) в виде

$$a_1m^4 + b_1m^2n^2 + c_1n^4 + d_1mn^3 = k^2, \quad (3)$$

где  $a_1, b_1, c_1, d_1, k \in \mathbf{Z}$ . Далее к уравнению (3) применяем метод бесконечного спуска.

2. Пусть  $E: y^2=f(x)=(x-x_0)(ax^2+bx+c)$ , где  $g(x)=ax^2+bx+c$  – неразложимый многочлен над  $\mathbf{Q}$ ,  $x_0 \in \mathbf{Q}$ . Заметим, что  $(x_0, y_0) \in E(\mathbf{Q})$ , где  $y_0=0$ . Из ра-

венств (2), (3) получаем уравнение  $a_1m^4 + b_1m^2n^2 + c_1n^4 = k^2$ , к которому применяем метод бесконечного спуска.

3. Пусть  $E: y^2 = f(x) = a(x-x_1)(x-x_2)(x-x_3)$ , где  $a, x_1, x_2, x_3 \in \mathbb{Q}$ . Положим  $t = x - x_1$ . Тогда  $y^2 = t(at^2 + bt + c)$ , где многочлен  $g(t) = at^2 + bt + c$  разложим над  $\mathbb{Q}$ . Можно считать, что  $a, b, c \in \mathbb{Z}$ . В противном случае рассмотрим кривую, заданную уравнением  $y^2 = t(ad^2t^2 + bd^4t + cd^6)$ . Изоморфную кривой  $E$  с целочисленными коэффициентами для достаточно большого значения  $d$ .

Пусть  $t = \frac{m}{n}$ ,  $(m, n)=1$ . Тогда  $mn(am^2 + bmn + cn^2) = k^2$ , где  $k = n^2y$ . Если  $M = (m, am^2 + bmn + cn^2)$ ,  $N = (n, am^2 + bmn + cn^2)$ , то  $M$  делит  $c$ ,  $N$  делит  $a$ . С учетом  $(m, n)=1$  получаем  $a = Na_1$ ,  $c = Mc_1$ ,  $m = Mm_1$ ,  $n = Nn_1$ ,  $am^2 + bmn + cn^2 = MNL$ , где  $a_1, c_1, m_1, n_1, L \in \mathbb{Z}$ .

Далее имеем  $M^2N^2m_1n_1L = k^2$ , причем  $m_1n_1L$  попарно взаимно просты. Следовательно,  $m_1 = u^2$ ,  $n_1 = v^2$ ,  $L = w^2$  для некоторых целых  $u, v, w$ . Тогда  $a_1Mu^4 + bu^2v^2 + c_1Nv^4 = w^2$ , причем многочлен  $g(t)$  разложим над  $\mathbb{Q}$ . Следовательно,  $(p_1u^2 + q_1v^2)(p_2u^2 + q_2v^2) = w^2$  для некоторых целых  $p_1, p_2, q_1, q_2$ . Так как  $(m, n)=1$ , то  $(u, v)=1$  и  $h = (p_1u^2 + q_1v^2)(p_2u^2 + q_2v^2)$  делит  $p_1q_2 - p_2q_1$ . В результате получаем систему

$$\begin{cases} p_1u^2 + q_1v^2 = hw_1^2, \\ p_2u^2 + q_2v^2 = hw_2^2, \end{cases}$$

к которой снова используем метод бесконечного спуска.

Рассмотрим теперь описанную процедуру применительно к некоторым классам эллиптических кривых.

**Теорема 1.** Пусть задано семейство эллиптических кривых  $\{E_t\}_{t \in \mathbb{Q}}$ , где  $E_t: y^2 = x^3 - (3t+2)x^2 + (3t^2+4t-1)x - t^3 - 2t^2 + t$ .

Тогда для любого рационального значения  $t$  имеет место следующий изоморфизм  $E_t(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ , причем  $E_t(\mathbb{Q}) = \{O, (t, 0)\}$ .

**Доказательство.** Пусть  $z = x - t$ . Тогда  $E_t: y^2 = z^3 - 2z^2 - z$ . Если  $z \neq 0$ ,  $z = \frac{m}{n}$ ,  $(m, n)=1$ , то  $mn(m^2 - 2mn - n^2) = k^2$ , где  $k = n^2y$ .

Так как  $m, n, m^2 - 2mn - n^2$  попарно взаимно просты, то

$$\begin{cases} m = a^2, & n = b^2, & m^2 - 2mn - n^2 = c^2, \\ m = a^2, & n = -b^2, & m^2 - 2mn - n^2 = -c^2. \end{cases}$$

В первом случае имеем

$$a^4 - 2a^2b^2 - b^4 = c^2, \quad (4)$$

где  $a, b, c \in \mathbb{Z}$ ,  $b \neq 0$ . Предположим, что  $a \neq 0$ . Так как  $(m, n)=1$ , то  $(a, b)=1$ . Имеем

$$(a^2 - b^2 - c)(a^2 - b^2 + c) = 2b^4. \quad (5)$$

Рассматривая уравнение (4) по  $(\text{mod } 4)$ , заключаем, что  $a \equiv 1 \pmod{2}$ ,  $b \equiv 0 \pmod{2}$ . Так как разность и произведение чисел  $a^2 - b^2 + c$ ,  $a^2 - b^2 - c$  четны, то четны и они сами.

Поскольку  $2(a^2 - b^2)$ , делясь на 2, не делится на 4, то из (5) следует, что  $a^2 - b^2 - c = \pm 2u^4$ ,  $a^2 - b^2 + c = \pm 16v^4$ , где  $b = 2uv$ ,  $(u, v)=1$ . Действительно, если не-

четное простое число  $p$  делит  $a^2 - b^2 \pm c$ , то  $p$  делит  $a^2 - b^2$ . причем из равенства (5) вытекает, что  $p$  делит  $b$ . Следовательно,  $p$  делит  $(a, b) = 1$ , что невозможно. Таким образом,  $a^2 - b^2 = \pm(u^4 + 8v^4)$ ,  $a^2 = \pm(u^4 \pm 4u^2v^2 + 8v^4)$ . Так как  $-(u^4 - 4u^2v^2 + 8v^4) < 0$ , то  $a^2 = u^4 + 4u^2v^2 + 8v^4$ .

Поскольку  $a \equiv 1 \pmod{2}$ , то  $u \equiv 1 \pmod{2}$ , ибо  $u^2 \equiv a^2 \equiv 1 \pmod{4}$ . Ввиду  $u \equiv 1 \pmod{2}$ ,  $(u, v) = 1$  имеем  $(u^2 + 2v^2, 2v^2) = 1$ . Таким образом,  $u^2 + 2v^2, 2v^2, a$  образуют примитивную пифагорову тройку. Следовательно,  $u^2 + 2v^2 = q^2 - r^2$ ,  $2v^2 = qr$ , где  $(q, r) = 1$ ,  $q \equiv 1 \pmod{2}$ ,  $r \equiv 0 \pmod{2}$ . Так как  $qr = v^2$ ,  $(q, r) = 1$ , то  $q = g^2$ ,  $r = h^2$ ,  $u^2 = g^4 - 2g^2h^2 - h^4$ , причем  $|b| > |h|$ , и мы оказываемся в рамках применения бесконечного спуска.

Аналогично показывается, что уравнение  $-a^4 - 2a^2b^2 + b^4 = c^2$  имеет решение лишь при  $a = 0$ . Итак,  $a = 0$ ,  $m = 0$ ,  $z = 0$ ,  $x = t$ ,  $y = 0$ , т. е.  $E_t(\mathbf{Q}) = \{O, (t, 0)\} \cong \mathbb{Z}/2\mathbb{Z}$ , что и требовалось доказать.

Можно привести ряд других семейств эллиптических кривых, для которых указанная процедура позволяет полностью описать их группы рациональных точек. Так, например, справедлива следующая

**Теорема 2.** Пусть задано семейство эллиптических кривых  $\{E_t\}_{t \in \mathbb{Q}}$ , где  $E_t: y^2 = x^3 - (6t - 5)x^2 + (6t^2 - 10t + 2)x - t(t - 2)(2t - 1)$ .

Тогда для любого рационального значения  $t$  имеет место следующий изоморфизм  $E_t(\mathbf{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ , причем

$$E_t(\mathbf{Q}) = \left\{ O, (t, 0), (t - 2, 0), \left(t - \frac{1}{2}, 0\right), (t + 1, \pm 3), (t - 1, \pm 1) \right\}.$$

1. Husemoller D. Elliptic curves. New York, 1986.
2. Silverman I. The arithmetic of elliptic curves. New York, 1985.
3. Stoll M. / J. reine angew. Math. 1998. **501**. S. 171.

Поступила в редакцию 20.11.2000.

*Дмитрий Федорович Базылев* – аспирант Института математики НАН Беларуси. Научный руководитель – доктор физико-математических наук, профессор кафедры геометрии, топологии и методики преподавания математики В.И. Янчевский.

УДК 517.977

Л.И. ЛАВРИНОВИЧ

## К МЕТОДАМ ГАРАНТИРОВАННОЙ ОПТИМИЗАЦИИ СИСТЕМ УПРАВЛЕНИЯ

The method of construction of extreme closable program controls for a problem of guaranteed optimization of dynamic systems based on external approximation of closure sets of is described. It is shown, that with increase of number of vectors of approximation the extreme control converges to optimal closable control.

1. Пусть  $\bar{t} = [t_*, t^*]$ ,  $h = (t^* - t_*)/N$ ,  $T_h = \{t_*, t_* + h, \dots, t^* - h\}$ . Функция  $u(t)$ ,  $t \in T_h$ , – дискретное управление, если  $u(t) = u(t_* + kh)$ ,  $t \in [t_* + kh, t_* + (k+1)h[$ ,  $k = 0, N-1$ .

В классе дискретных управлений рассмотрим задачу

$$c'x(t^*) \rightarrow \max, \dot{x} = A(t)x + b(t)u + w(t), x(t_*) = x_0, u(t) \in U = \{u \in R : |u| \leq 1\},$$