В. А. Демьяненко, Об ограниченности кручения эллиптических кривых, *Матем. заметки*, 1972, том 12, выпуск 1, 53–58

МАТЕМАТИЧЕСКИЕ ЗАМЕТКИ

т. 12, № 1 (1972), 53—58

УДК 511

ОБ ОГРАНИЧЕННОСТИ КРУЧЕНИЯ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

В. А. Демьяненко

Указывается явная оценка, ограничивающая кручение эллиптических кривых над полем рациональных чисел.

Пусть Γ — эллиптическая кривая над полем рациональных чисел R, а Q_m — примитивная R-точка на ней порядка m, где m — простое или удвоенное простое число. Тогда если $m = 2p$, то $p \leqslant 509$, а в случае $m = p$ $p < 6144$. Библ. 2 назв.

В статье [1] приводится доказательство ограниченности кручения эллиптической кривой Γ: $y^2 = x^3 + rx + s$ над алгебраическим числовым полем. Однако явной оценки, ограничивающей кручение, в этой работе не дается.

Целью настоящей заметки является вывод соответствующей оценки, ограничивающей кручение кривой Γ над полем рациональных чисел R.

Пусть

$$\Gamma_i : v_i^2 = u_i^4 - 6\rho_i u_i^2 - 4r - 3\rho_i^2, \quad \rho_i^3 + r\rho_i + s = 0,$$

$i = 1, 2, 3$ есть кривые, связанные с кривой Γ посредством формул

$$u_i = \frac{y}{x - \rho_i}, \qquad v_i = x - \rho_i - \frac{r + 3\rho_i^2}{x - \rho_i}, \tag{1}$$

а O_m, как и в работе [1], является примитивной R-точкой на Γ порядка m, где m — простое или удвоенное простое число.

ТЕОРЕМА 1. *Если* $m = 2p$, *то* $p \leqslant 509$.

Доказательство. Прежде всего заметим, что если кривая Γ имеет R-точку O_{2p}, то по крайней мере

один из корней уравнения $\rho^3 + r\rho + s = 0$ принадлежит R. Обозначим корень $\rho_i \in R$ через ρ_1. Тогда кривая Γ_1 должна обладать над R точкой O'_p порядка p. Расширим поле R до такого поля K степени n, чтобы в последнем кривая Γ имела примитивные точки порядка $16p$. В этом случае, не нарушая общности, можно считать, что Γ имеет группу K-точек, образующими которой являются O''_{8p}, O'''_{8p}, удовлетворяющие равенству $4O''_{8p} = 4O'''_{8p}$, такие, что если обозначить координаты точек $q_1O''_{8p} + q_2O'''_{8p}$ через $\{x_{q_1,q_2},\ y_{q_1,q_2}\}$, то для $u_{4p,0}$, $u_{0,4p}$, определяемых по формулам (1), справедливы равенства $u_{4p,0} = u_{0,4p} = 0$. Согласно (36) и следствию 3 статьи [1] будем иметь

$$u_{\alpha,\beta} = \varepsilon_{\alpha,\beta} P_0 \prod_{i,j=1}^{4p} A_{i,j}^{\left\{\frac{\alpha i+\beta j}{8p}\right\} 8p} B_{i,j}^{\left\{\frac{\alpha i-\beta j}{8p}\right\} 8p}$$

(i, j — нечетные),

$$\frac{v_{\alpha,\beta}}{u_{\alpha,\beta}} = \varepsilon'_{\alpha,\beta} Q_0 \prod_{i,j=0}^{2p} C_{i,j}^{\left\{\frac{\alpha i+\beta j}{4p}\right\} 4p} D_{i,j}^{\left\{\frac{\alpha i-\beta j}{4p}\right\} 4p} \qquad (2)$$

(i, j — различной четности),

$$\frac{u_{4\alpha,\,4\beta}}{u_{4\gamma,\,4\delta}} = S^2, \qquad \frac{v_{4\alpha,\,4\beta}}{v_{4\gamma,\,4\delta}} = T^2 \qquad (S,\ T \in K),$$

если только порядки точек $\alpha O''_{8p} + \beta O'''_{8p}$, $\gamma O''_{8p} + \delta O'''_{8p}$ кратны 8 или превышают $8n \leqslant 8 \cdot 64 = 512$.

Таким образом, кривая

$$u^4 - 1 = v^2 \qquad (3)$$

имеет точки с координатами, принадлежащими полю K:

$$u = \sqrt{u_{4\alpha-4\gamma,\,4\beta-4\delta}/u_{4\alpha+4\gamma,\,4\beta+4\delta}},$$

$$v = \sqrt{v_{4\gamma,\,4\delta} u_{4\alpha,\,4\beta}/v_{4\alpha,\,4\beta} u_{4\gamma,\,4\delta}}\,(u_{4\alpha-4\gamma,\,4\beta-4\delta}/u_{4\alpha+4\gamma,\,4\beta+4\delta} - 1),$$

где α, β, γ, δ — произвольные целые рациональные числа, при которых порядки точек $\alpha O''_{8p} + \beta O'''_{8p}$, $\gamma O''_{8p} + \delta O'''_{8p}$, $(\alpha \pm \gamma)O''_{8p} + (\beta \pm \delta)O'''_{8p}$ кратны 8 или превышают 512. Предположим, что $p > 512$, и рассмотрим точки $P_i = \{u^{(i)}, v^{(i)}\}$ ($i = 1,2,\ldots,n$), $n \leqslant 64$, сопряженные с точкой (u, v). Координаты этих точек должны удовлетворять

равенствам

$$u^{(i)} = \sqrt{u_{\alpha_i-\gamma_i,\ \beta_i-\delta_i}/u_{\alpha_i+\gamma_i,\ \beta_i+\delta_i}},$$
$$v^{(i)} = \sqrt{v_{\gamma_i,\ \delta_i} u_{\alpha_i,\ \beta_i}/v_{\alpha_i,\ \beta_i} u_{\gamma_i,\ \delta_i}}\,(u_{\alpha_i-\gamma_i,\ \beta_i-\delta_i}/u_{\alpha_i+\gamma_i,\ \beta_i+\delta_i} - 1), \tag{4}$$

где u_{α_i,β_i}, u_{γ_i,δ_i}, v_{α_i,β_i}, v_{γ_i,δ_i}, $u_{\alpha_i\pm\beta_i,\gamma_i\pm\delta_i}$, $v_{\alpha_i\pm\beta_i,\gamma_i\pm\delta_i}$ в силу простоты $p > 512$ и отличия от 0 координат u, v удовлетворяют соотношениям (2). Складывая точки P_i, мы получим точку

$$P_+ = \sum_{i=1}^{n} P_i = \{u_+, v_+\} = \{w_+/s_+,\ t_+/s_+^2\}, \qquad (w_+, s_+, t_+) = 1,$$

координаты которой будут уже принадлежать полю R. Следовательно, точка P_+ будет или бесконечно удаленной или же порядок ее будет равен 2, что возможно лишь при $s_+t_+ = 0$. Далее, так как $p > 512$, то в силу леммы 12 статьи [1] при некоторых $A_{i_0,\ j_0}$, $B_{i_1,\ j_1}$

$$\nu_{A_{i_0,\ j_0}}(w_+),\ \nu_{B_{i_1,j_1}}(w_+) > 0,$$

где $\nu_q(c)$ — q-показатель числа c.

Поэтому

$$1 \equiv 0 \,(\mathrm{mod}\, A_{i_0,\ j_0} B_{i_1,\ j_1}). \tag{5}$$

Заметим еще, что если $P_i = \{u^{(i)}, v^{(i)}\}$ — система сопряженных точек, то и $tP_i = \{u_t^{(i)}, v_t^{(i)}\}$ также будет системой сопряженных точек. Вследствие этого из (5) и простоты p вытекает

$$1 \equiv 0 \left(\mathrm{mod} \prod_{i,\ j=1}^{4p} A_{i,\ j} B_{i,\ j}\right). \tag{6}$$

Рассмотрим теперь точки $4\alpha O''_{8p}$ и $4\gamma O''_{8p}$. С одной стороны, для этих точек $u_{4\alpha,0}$, $u_{4\gamma,0}$, $v_{4\alpha,0}$, $v_{4\gamma,0}$ должны быть целыми рациональными числами, а с другой —, так как $p > 512$, они удовлетворяют соотношениям (2). Таким образом, $u_{4\alpha,0} = \pm P_0$, $u_{4\gamma,0} = \pm P_0$. Но тогда из равенств (34)

работы [1] будем иметь

$$u_{4\alpha,\,0}+u_{4\gamma,\,0}=2\frac{u_{2\alpha+2\gamma,\,0}\,v_{2\alpha-2\gamma,\,0}}{u^2_{2\alpha-2\gamma,\,0}-u^2_{2\alpha+2\gamma,\,0}},$$

$$u_{4\alpha,\,0}-u_{4\gamma,\,0}=2\frac{u_{2\alpha-2\gamma,\,0}\,v_{2\alpha+2\gamma,\,0}}{u^2_{2\alpha-2\gamma,\,0}-u^2_{2\alpha+2\gamma,\,0}},$$

откуда

$$u_{2\alpha-2\gamma,\,0}u_{2\alpha+2\gamma,\,0}v_{2\alpha-2\gamma,\,0}v_{2\alpha+2\gamma,\,0}=0,$$

что, в силу отличия от 0 дискриминанта кривой Γ, невозможно. Наконец, учитывая, что числа 513, 512, 511, 510 — составные, получаем $p\leqslant 509$. Теорема доказана.

Следствие. *Если* $O_{2m}\in\Gamma$ *и* m *— составное, то при* $p>3$ $m\not\equiv 0\pmod{p^2}$.

Действительно, если бы $m\equiv 0\pmod{p^2}$, $p>3$, то на основании работы 2 и теоремы 1 мы бы имели: $p\leqslant 509$, $x^p+y^p=1$, $x,\ y\in R$, $xy\neq 0$, что, очевидно, невозможно.

ТЕОРЕМА 2. *Если* $m=p$, *то* $m<6144$.

Доказательство. Как и в предыдущей теореме, расширим поле R до поля K степени n с тем, чтобы в последнем кривая Γ имела примитивные точки порядка $16p$. Очевидно, $n\leqslant 256$. Далее, так как поле $R(\rho)$ нельзя считать уже заданным, то мы для каждого корня ρ_l уравнения $\rho^3+r\rho+s=0$ составляем по аналогии с (2) выражения

$$u_{\alpha,\,\beta,\,l}=\varepsilon_{\alpha,\,\beta,\,l}P_0\prod_{i,\,j=1}^{4p}A_{i,\,j,\,l}^{\left\{\frac{\alpha i+\beta j}{8p}\right\}8p}B_{i,\,j,\,l}^{\left\{\frac{\alpha i-\beta j}{8p}\right\}8p}$$

(i, j — нечетные),

$$\frac{v_{\alpha,\,\beta,\,l}}{u_{\alpha,\,\beta,\,l}}=\varepsilon'_{\alpha,\,\beta,\,l}Q_0\prod_{i,\,j=0}^{2p}C_{i,\,j,\,l}^{\left\{\frac{\alpha i+\beta j}{4p}\right\}4p}D_{i,\,j,\,l}^{\left\{\frac{\alpha i-\beta j}{4p}\right\}4p}\qquad(7)$$

(i, j — различной четности),

$$\frac{u_{4\alpha,\,4\beta,\,l}}{u_{4\gamma,\,4\delta,\,l}}=S^2,\qquad\frac{v_{4\alpha,\,4\beta,\,l}}{v_{4\gamma,\,4\delta,\,l}}=T^2\qquad(S,\ T\in K)$$

в предположении, что p превышает $3\cdot 8n\leqslant 6144$, и

определяем точки

$$P_{+,l} = \sum_{i=1}^{n} P_{i,l} \ (l = 1, 2, 3).$$

Нетрудно заметить, что точки $P_{+,l}$ являются сопряженными и координаты их принадлежат соответственно полям $R(\rho_l)$. Вследствие этого точка

$$P_{+,+} = \sum_{l=1}^{3} P_{+,l}$$

будет иметь координаты уже в поле R.

На основании [1]

$$4r + 3\rho_l^2 \equiv 0 \pmod{u^2_{\alpha,\beta,l}},$$
$$16(r + 3\rho_l^2) \equiv 0 \pmod{v^2_{\alpha,\beta,l}/u^2_{\alpha,\beta,l}},$$

поэтому, учитывая, что

$$\prod_{l=1}^{3}(4r + 3\rho_l^2) = \prod_{l=1}^{3}(r + 3\rho_l^2),$$

выводим: $A_{i,j,l}$, $B_{i,j,l}$, $C_{i,j,l}$, $D_{i,j,l}$ состоят из тех и только тех простых дивизоров, которые входят в $A_{i,j,1}$, $B_{i,j,1}$, $C_{i,j,1}$, $D_{i,j,1}$. Таким образом, при $p > 6144$ мы так же, как и в теореме 1, из (7) и последнего замечания получаем

$$1 \equiv 0 \left(\operatorname{mod} \prod_{i,j,l} A_{i,j,l} B_{i,j,l}\right). \tag{8}$$

Так как при $p > 6144$ $u_{8\alpha,0,l}$ — единица поля $R(\rho_l)$ и

$$u_{8\alpha,0,l} = \frac{y_{8\alpha,0}}{x_{8\alpha,0} - \rho_l},$$

то $\prod_{l=1}^{3} u_{8\alpha,0,l} = y^3_{8\alpha,0} \Big/ \prod_{l=1}^{3}(x_{8\alpha,0} - \rho_l) = y_{8\alpha,0}$ — есть единица поля R, т. е. $y_{8\alpha,0} = \pm 1$. Но кривая Г при $y = \pm 1$ может иметь не более 6 различных точек, что противоречит условию $p > 6144$. Учитывая, что 6145, 6144 — составные числа, окончательно имеем $p < 3 \cdot 2^{11} = 6144$. Теорема доказана.

В заключение заметим, что если кривую Г рассматривать не над полем рациональных чисел, а над алгебраическим числовым полем K степени n, то аналогично теоремам 1 и 2 из работы [1] можно было бы вывести следующее утверждение.

ТЕОРЕМА 3. *Пусть* r *— ранг кривой* (3) *над полем* K, m *— число целых* K*-точек кривой* $\varepsilon_0 = x^3 + rxy^2 + sy^3$, *где* ε_0 *— некоторая единица из* K, *а* O_p *— примитивная* K*-точка на* Γ *порядка* p. *Тогда* $p \leqslant 6144\ mn \cdot (r+1) + 1$.

Институт математики
и механики АН СССР

Поступило
16.III.1971

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] Демьяненко В. А., О кручении эллиптических кривых, Изв. АН СССР, Сер. матем., 35 (1971), 280—307.
[2] Демьяненко В. А., О точках кручения эллиптических кривых, Изв. АН СССР, Сер. матем., 34 (1970), 757—774.