Remarks. At each stage of the construction, we have to solve a congruence

$$g(n) \equiv l \bmod N$$

where N is the lowest common multiple of the integers not exceeding n. We may select at least one of the first two solutions of this congruence, so that

$$g(n) \ll e^{An}$$

for some fixed A. But this is not good enough for condition (iii).

Condition (i) is easily arranged by setting $g(1) = 1$.

Condition (ii) is more difficult. Nothing in the construction implies that the numbers $g(0), g(1), g(2), \ldots, g(p-1)$ are well distributed mod p, in fact $B(p)$ could be p. We can make g satisfy (ii) by selecting $g(n)$ to satisfy congruences to moduli $p > n$, but so far as I can see at the expense of dropping condition (iii). Suppose that for $n < p \leqslant t(n)$ (some increasing function of n) we set

$$g(n) \equiv t_p(n) \bmod p$$

where $t_p(n)$ is one of the most deficient residue classes mod p so far. Then for all p,

$$B(p) \leqslant t^{-1}(p)$$

that is, the number of n for which $g(n)$ is not corrected mod p. Roughly we want

$$t^{-1}(p) \ll \frac{p}{(\log\log p)^{\alpha}}$$

for some $\alpha > 2$, so that we shall satisfy conditions (i) and (ii) if for example

$$t(n) = n(\log\log n)^{\alpha}.$$

This however, could make $\log(1+|g(n)|)$ too large. The conclusion is that there are infinitely many pseudo-polynomials satisfying the first two conditions, which are not polynomials.

I do not know of any number-theoretic function which presents itself naturally and is a pseudo-polynomial. The chances are that it would satisfy our conditions, and this is one way that the problem could be solved.

Reference

[1] R. R. Hall, *On the probability that n and f(n) are relatively prime*, Acta Arith. 17 (1970), pp. 169–183.

Received on 14. 4. 1970 (81)

ACTA ARITHMETICA
XIX (1971)

О точках конечного порядка эллиптических кривых

В. А. Демьяненко (Свердловск)

Пусть T — кривая первого рода $y^2 = x^4 + ax^2 + b$, определенная над полем рациональных чисел; P — произвольная точка на T; O_m — рациональная точка на T конечного порядка m; $v_q(c) - q$ — показатель числа c; $[t]$ — целая часть числа t; $\{t\}$ — расстояние от t до ближайшего целого числа.

Целью настоящей работы является доказательство следующей теоремы:

Если $m = p^2$, где p — простое > 3, то на кривой $z^p - t^p = 1$, $z^p + t^p = r^p$ $(zt \neq 0)$ лежит не менее $C^2_{(p-1)/2}$ рациональных точек.

Предварительно докажем несколько лемм.

Лемма I. *Координаты точек $kP = \{x_k, y_k\}$ $(k = 1, 2, \ldots)$ можно вычислять по следующим рекуррентным соотношениям:*

$$(1)\quad \begin{cases} x_k = u_k/w_k,\ y_k = v_k/w_k^2,\ u_1 = x_1,\ v_1 = y_1, \quad w_1 = 1; \\ u_k = u_{k/2}^4 - bw_{k/2}^4,\ v_k = v_{k/2}^4 - (a^2-4b)u_{k/2}^4 w_{k/2}^4,\ w_k = 2u_{k/2}v_{k/2}w_{k/2} \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{при } k \equiv 0 \pmod 2 \\ u \\ u_k u_1 = u_{\frac{k-1}{2}}^2 u_{\frac{k+1}{2}}^2 - bw_{\frac{k-1}{2}}^2 w_{\frac{k+1}{2}}^2,\ w_k w_1 = u_{\frac{k-1}{2}}^2 w_{\frac{k+1}{2}}^2 - u_{\frac{k+1}{2}}^2 w_{\frac{k-1}{2}}^2, \\ v_k v_1 = v_{\frac{k-1}{2}}^2 v_{\frac{k+1}{2}}^2 - (a^2-4b)u_{\frac{k-1}{2}}^2 u_{\frac{k+1}{2}}^2 w_{\frac{k-1}{2}}^2 w_{\frac{k+1}{2}}^2 \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{при } k \not\equiv 0 \pmod 2. \end{cases}$$

Доказательство. Согласно формулам сложения и вычитания точек на кривой T, имеем:

$$x_k = \frac{x_{k/2}^4 - b}{2x_{k/2}y_{k/2}}, \qquad y_k = \frac{y_{k/2}^4 - (a^2-4b)x_{k/2}^4}{4x_{k/2}^2 y_{k/2}^2}$$

при $k \equiv 0 \pmod 2$ и

$$x_{\frac{k+1}{2}\pm\frac{k-1}{2}} = \frac{x_{\frac{k+1}{2}} y_{\frac{k-1}{2}} \mp x_{\frac{k-1}{2}} y_{\frac{k+1}{2}}}{x^2_{\frac{k-1}{2}} - x^2_{\frac{k+1}{2}}},$$

(2)

$$y_{\frac{k+1}{2}\pm\frac{k-1}{2}} = \frac{y_{\frac{k-1}{2}} y_{\frac{k+1}{2}} (x^2_{\frac{k-1}{2}} + x^2_{\frac{k+1}{2}}) \mp x_{\frac{k-1}{2}} x_{\frac{k+1}{2}} (2x^2_{\frac{k-1}{2}} x^2_{\frac{k+1}{2}} + ax^2_{\frac{k-1}{2}} + ax^2_{\frac{k+1}{2}} + 2b)}{(x^2_{\frac{k-1}{2}} - x^2_{\frac{k+1}{2}})^2}.$$

Так как при любом s $x_s = u_s/w_s$, $y_s = v_s/w_s^2$, то

$$\frac{u_k}{w_k} = \frac{u^4_{k/2} - bw^4_{k/2}}{2u_{k/2}v_{k/2}w_{k/2}}, \qquad \frac{v_k}{w_k^2} = \frac{v^4_{k/2} - (a^2-4b)u^4_{k/2}w^4_{k/2}}{4u^2_{k/2}v^2_{k/2}w^2_{k/2}} \tag{3}$$

при $k \equiv 0 \pmod 2$ и

$$\frac{u_{\frac{k+1}{2}\pm\frac{k-1}{2}}}{w_{\frac{k+1}{2}\pm\frac{k-1}{2}}} = \frac{u_{\frac{k+1}{2}} w_{\frac{k+1}{2}} v_{\frac{k-1}{2}} \mp u_{\frac{k-1}{2}} w_{\frac{k-1}{2}} v_{\frac{k+1}{2}}}{u^2_{\frac{k-1}{2}} w^2_{\frac{k+1}{2}} - u^2_{\frac{k+1}{2}} w^2_{\frac{k-1}{2}}}, \tag{4}$$

$$\frac{v_{\frac{k+1}{2}\pm\frac{k-1}{2}}}{w^2_{\frac{k+1}{2}\pm\frac{k-1}{2}}} = \frac{v_{\frac{k-1}{2}} v_{\frac{k+1}{2}} (u^2_{\frac{k-1}{2}} w^2_{\frac{k+1}{2}} + u^2_{\frac{k+1}{2}} w^2_{\frac{k-1}{2}})}{(u^2_{\frac{k-1}{2}} w^2_{\frac{k+1}{2}} - u^2_{\frac{k+1}{2}} w^2_{\frac{k-1}{2}})^2} \mp$$

$$\mp \frac{u_{\frac{k-1}{2}} u_{\frac{k+1}{2}} w_{\frac{k-1}{2}} w_{\frac{k+1}{2}} (2u^2_{\frac{k-1}{2}} u^2_{\frac{k+1}{2}} + au^2_{\frac{k-1}{2}} w^2_{\frac{k+1}{2}} + au^2_{\frac{k+1}{2}} w^2_{\frac{k-1}{2}} + 2bw^2_{\frac{k-1}{2}} w^2_{\frac{k+1}{2}})}{(u^2_{\frac{k-1}{2}} w^2_{\frac{k+1}{2}} - u^2_{\frac{k+1}{2}} w^2_{\frac{k-1}{2}})^2}. \tag{5}$$

Перемножая (4) и (5), получим:

$$\frac{u_k u_1}{w_k w_1} = \frac{u^2_{\frac{k-1}{2}} u^2_{\frac{k+1}{2}} - bw^2_{\frac{k-1}{2}} w^2_{\frac{k+1}{2}}}{u^2_{\frac{k-1}{2}} w^2_{\frac{k+1}{2}} - u^2_{\frac{k+1}{2}} w^2_{\frac{k-1}{2}}},$$

$$\frac{v_k v_1}{w_k^2 w_1^2} = \frac{v^2_{\frac{k-1}{2}} v^2_{\frac{k+1}{2}} - (a^2-4b) u^2_{\frac{k-1}{2}} u^2_{\frac{k+1}{2}} w^2_{\frac{k-1}{2}} w^2_{\frac{k+1}{2}}}{(u^2_{\frac{k-1}{2}} w^2_{\frac{k+1}{2}} - u^2_{\frac{k+1}{2}} w^2_{\frac{k-1}{2}})^2}. \tag{6}$$

Следовательно, приравнивая числители и знаменатели обеих частей в выражениях (3) и (6), мы получим соотношения (1).

Лемма 2. *Если* $t \not\equiv 0 \pmod 2$, *то*

$$u_t = u_1 A_t, \quad v_t = v_1 B_t, \quad w_t = w_1 C_t,$$

$$A_t = \sum_{\substack{i,j,k=0 \\ i+j+k=\frac{t^2-1}{4}}}^{\frac{t^2-1}{4}} a_{i,j,k} \alpha^i \beta^j \gamma^k, \qquad B_t = \sum_{\substack{i,j,k=0 \\ i+j+k=\frac{t^2-1}{2}}}^{\frac{t^2-1}{2}} b_{i,j,k} \alpha^i \beta^j \gamma^k,$$

$$C_t = \sum_{\substack{i,j,k=0 \\ i+j+k=\frac{t^2-1}{4}}}^{\frac{t^2-1}{4}} c_{i,j,k} \alpha^i \beta^j \gamma^k, \tag{7}$$

если же $t \equiv 0 \pmod 2$, *то*

$$u_t = A_t, \quad v_t = B_t, \quad w_t = u_1 v_1 w_1 C_t,$$

$$A_t = \sum_{\substack{i,j,k=0 \\ i+j+k=t^2/4}}^{t^2/4} a_{i,j,k} \alpha^i \beta^j \gamma^k, \qquad B_t = \sum_{\substack{i,j,k=0 \\ i+j+k=t^2/2}}^{t^2/2} b_{i,j,k} \alpha^i \beta^j \gamma^k,$$

$$C_t = \sum_{\substack{i,j,k=0 \\ i+j+k=t^2/4-1}}^{t^2/4-1} c_{i,j,k} \alpha^i \beta^j \gamma^k$$

где $a = u_1^4$, $\beta = au_1^2 w_1^2$, $\gamma = bw_1^4$ *и* $a_{i,j,k}$, $b_{i,j,k}$, $c_{i,j,k}$ — *целые рациональные числа, удовлетворяющие следующим условиям:*

1) $b_{i,j,k} = b_{k,j,i}$; $a_{i,j,k} = (-1)^{(t-1)/2} c_{k,j,i}$ *при* $t \not\equiv 0 \pmod 2$ *и* $a_{i,j,k} = (-1)^{t/2} a_{k,j,i}$, $c_{i,j,k} = (-1)^{t/2} c_{k,j,i}$ *при* $t \equiv 0 \pmod 2$;
2) $a_{[t^2/4],0,0} = b_{[t^2/2],0,0} = 1$, $a_{0,0,[t^2/4]} = (-1)^{(t-1)/2} t$ *при* $t \not\equiv 0 \pmod 2$, $c_{t^2/4-1,0,0} = t$ *при* $t \equiv 0 \pmod 2$;
3) $a_{i,j,0} = 0$ *при* $i < [t^2/4]$.

Доказательство. Доказательство проведем методом математической индукции. При $t = 1$ справедливость леммы очевидна. Предположим теперь, что лемма верна для всех $t < n$ и докажем, что в этом случае она справедлива и при $t = n$. На основании формул (1)

$$A_{4r} = A^4_{2r} - \alpha\gamma(\alpha+\beta+\gamma)^2 C^4_{2r}, \qquad C_{4r} = 2A_{2r}B_{2r}C_{2r},$$

$$B_{4r} = B^4_{2r} - (\beta^2 - 4\alpha\gamma)(\alpha+\beta+\gamma)^2 A^4_{2r} C^4_{2r};$$

$$A_{4r\pm1} = A^2_{2r}A^2_{2r\pm1} - \gamma(\alpha+\beta+\gamma)C^2_{2r}C^2_{2r\pm1}, \qquad C_{4r\pm1} = A^2_{2r}C^2_{2r\pm1} - A^2_{2r\pm1}C^2_{2r},$$

$$B_{4r\pm1} = B^2_{2r}B^2_{2r\pm1} - (\beta^2 - 4\alpha\gamma)(\alpha+\beta+\gamma)A^2_{2r}A^2_{2r\pm1}C^2_{2r}C^2_{2r\pm1}; \tag{8}$$

$$A_{4r+2} = \alpha A^4_{2r+1} - \gamma C^4_{2r+1}, \qquad C_{4r+2} = 2A_{2r+1}B_{2r+1}C_{2r+1},$$

$$B_{4r+2} = (\alpha+\beta+\gamma)^2 B^4_{2r+1} - (\beta^2 - 4\alpha\gamma)A^4_{2r+1}C^4_{2r+1}.$$

Поэтому

$$A_n = \sum_{\substack{i,j,k=0 \\ i+j+k=\frac{n^2-1}{4}}}^{\frac{n^2-1}{4}} a_{i,j,k}\alpha^i\beta^j\gamma^k, \qquad B_n = \sum_{\substack{i,j,k=0 \\ i+j+k=\frac{n^2-1}{2}}}^{\frac{n^2-1}{2}} b_{i,j,k}\alpha^i\beta^j\gamma^k,$$

$$C_n = \sum_{\substack{i,j,k=0 \\ i+j+k=\frac{n^2-1}{4}}}^{\frac{n^2-1}{4}} c_{i,j,k}\alpha^i\beta^j\gamma^k$$

при $n \not\equiv 0 \pmod 2$ и

$$A_n = \sum_{\substack{i,j,k=0 \\ i+j+k=n^2/4}}^{n^2/4} a_{i,j,k}\alpha^i\beta^j\gamma^k, \qquad B_n = \sum_{\substack{i,j,k=0 \\ i+j+k=n^2/2}}^{n^2/2} b_{i,j,k}\alpha^i\beta^j\gamma^k,$$

$$C_n = \sum_{\substack{i,j,k=0 \\ i+j+k=n^2/4-1}}^{n^2/4-1} c_{i,j,k}\alpha^i\beta^j\gamma^k$$

при $n \equiv 0 \pmod 2$, где $a_{i,j,k}$, $b_{i,j,k}$, $c_{i,j,k}$ — целые рациональные числа, причем $a_{[n^2/4],0,0} = b_{[n^2/2],0,0} = 1$. Далее, в силу предположения, при подстановке $(\alpha, \beta, \gamma) \to (\gamma, \beta, \alpha)$ (A_{2r}, B_{2r}, C_{2r}), $(A_{2r\pm1}, B_{2r\pm1}, C_{2r\pm1})$ переходят соответственно в $\big((-1)^r A_{2r}, B_{2r}, (-1)^r C_{2r}\big)$, $\big(\pm(-1)^r C_{2r\pm1}, B_{2r\pm1}, \pm(-1)^r A_{2r\pm1}\big)$, вследствие чего из формул (8) получаем:

$$(A_{4r}, B_{4r}, C_{4r}) \to (A_{4r}, B_{4r}, C_{4r}),$$

$$(A_{4r+2}, B_{4r+2}, C_{4r+2}) \to (-A_{4r+2}, B_{4r+2}, -C_{4r+2}),$$

$$(A_{4r\pm1}, B_{4r\pm1}, C_{4r\pm1}) \to (\pm C_{4r\pm1}, B_{4r\pm1}, A_{4r\pm1}).$$

Таким образом,

$$b_{i,j,k} = b_{k,j,i}; \quad a_{i,j,k} = (-1)^{(n-1)/2} c_{k,j,i} \quad (n \not\equiv 0 \pmod 2);$$

$$a_{i,j,k} = (-1)^{n/2} a_{k,j,i}, \quad c_{i,j,k} = (-1)^{n/2} c_{k,j,i} \quad (n \equiv 0 \pmod 2).$$

Из этих же формул выводим:

$$a_{0,0,[n^2/4]} = (-1)^{(n-1)/2} n \quad (n \not\equiv 0 \pmod 2), \quad c_{n^2/4-1,0,0} = n \quad (n \equiv 0 \pmod 2).$$

Наконец, условие $a_{i,j,0} = 0$ при $i < [n^2/4]$, $i+j = [n^2/4]$ с очевидностью вытекает из (8). Лемма доказана.

Следствие I. *u_k^4, v_k^2, есть примитивные многочлены от переменных u_1, w_1.*

Лемма 3. *Над кольцом $R[u_1, w_1]$ многочлены u_k^4, v_k^2, w_k^4 взаимно просты.*

Доказательство. Так как $\{u_1^4, v_1^2, w_1^4\} = \{u_1^4, u_1^4 + a u_1^2 w_1^2 + b w_1^4, w_1^4\}$, то при $k = 1$ справедливость леммы очевидна. Далее, учитывая что дискриминант кривой T отличен от 0 и многочлены u_k^4, v_k^2, примитивны, из формул (1) выводим: над кольцом $R[u_1, w_1]$

$$(u_{k/2}^4, v_{k/2}^2, w_{k/2}^4)^4 \equiv 0 \pmod{(u_k^4, v_k^2, w_k^4)} \tag{9}$$

при $k \equiv 0 \pmod 2$ и

$$(u_{\frac{k-1}{2}}^4, v_{\frac{k-1}{2}}^2, w_{\frac{k-1}{2}}^4)^2 (u_{\frac{k+1}{2}}^4, v_{\frac{k+1}{2}}^2, w_{\frac{k+1}{2}}^4)^2 \equiv 0 \pmod{(u_k^4, v_k^2, w_k^4)}$$

при $k \not\equiv 0 \pmod 2$. Применяя к сравнениям (9) метод математической индукции, мы и получаем утверждение леммы.

Лемма 4. *Для любых натуральных r и s*

$$u_{r+s}u_{r-s} = u_r^2 u_s^2 - b w_r^2 w_s^2, \qquad w_{r+s}w_{r-s} = u_s^2 w_r^2 - u_r^2 w_s^2,$$

$$v_{r+s}v_{r-s} = v_r^2 v_s^2 - (a^2 - 4b) u_r^2 u_s^2 w_r^2 w_s^2.$$

Доказательство. Так как

$$x_{r\pm s} = \frac{x_r y_s \mp x_s y_r}{x_s^2 - x_r^2},$$

$$y_{r\pm s} = \frac{y_r y_s (x_r^2 + x_s^2) \mp x_r x_s (2x_r^2 x_s^2 + a x_r^2 + a x_s^2 + 2b)}{(x_s^2 - x_r^2)^2},$$

$$x_r = u_r/w_r, \quad x_s = u_s/w_s, \quad x_{r\pm s} = u_{r\pm s}/w_{r\pm s},$$

$$y_r = v_r/w_r^2, \quad y_s = v_s/w_s^2, \quad y_{r\pm s} = v_{r\pm s}/w_{r\pm s}^2,$$

то

$$\frac{u_{r\pm s}}{w_{r\pm s}} = \frac{u_r w_r v_s \mp u_s w_s v_r}{u_s^2 w_r^2 - u_r^2 w_s^2},$$

$$\frac{v_{r\pm s}}{w_{r\pm s}^2} = \frac{v_r v_s (u_r^2 w_s^2 + u_s^2 w_r^2) \mp u_r u_s w_r w_s (2u_r^2 u_s^2 + a u_r^2 w_s^2 + a u_s^2 w_r^2 + 2b w_r^2 w_s^2)}{(u_s^2 w_r^2 - u_r^2 w_s^2)^2},$$

откуда

$$\frac{u_{r+s}u_{r-s}}{w_{r+s}w_{r-s}} = \frac{u_r^2 u_s^2 - b w_r^2 w_s^2}{u_s^2 w_r^2 - u_r^2 w_s^2}, \qquad \frac{v_{r+s}v_{r-s}}{w_{r+s}^2 w_{r-s}^2} = \frac{v_r^2 v_s^2 - (a^2 - 4b) u_r^2 u_s^2 w_r^2 w_s^2}{(u_s^2 w_r^2 - u_r^2 w_s^2)^2}.$$

Таким образом, должны выполняться следующие тождества

$$\frac{u_r^2 u_s^2 - b w_r^2 w_s^2}{u_{r+s}u_{r-s}} \equiv \frac{u_s^2 w_r^2 - u_r^2 w_s^2}{w_{r+s}w_{r-s}} \equiv \frac{f}{g}, \qquad \frac{v_r^2 v_s^2 - (a^2 - 4b) u_r^2 u_s^2 w_r^2 w_s^2}{v_{r+s}v_{r-s}} \equiv \frac{f^2}{g^2}, \tag{10}$$

где f, g — примитивные многочлены от переменных u_1, w_1, взаимно простые над кольцом $R[u_1, w_1]$. Из (10) и условия $b(a^2 - 4b) \neq 0$ вытекает

$$(u_r^4, v_r^2, w_r^4)(u_s^4, v_s^2, w_s^4) \equiv 0 \pmod f,$$

$$(u_{r+s}^4, v_{r+s}^2, w_{r+s}^4)(u_{r-s}^4, v_{r-s}^2, w_{r-s}^4) \equiv 0 \pmod g,$$

что, в силу леммы 3 и свойства 2) леммы 2 даёт: $f/g = 1$. Лемма доказана.

Следствие 2.

$$u_{r+s}w_{r-s} = u_r w_r v_s - u_s w_s v_r, \qquad u_{r-s}w_{r+s} = u_r w_r v_s + u_s w_s v_r.$$

Лемма 5. *Если* $O_m = \{u_1/w_1, v_1/w_1^2\}$, $m > 2$, *то при любом* q

$$\nu_q(b) \geqslant 2\nu_q(u_1/w_1).$$

Доказательство. Предположим, что $\nu_q(b) < 2\nu_q(u_1/w_1)$ и рассмотрим точку $2O_m = \{u_2/w_2, v_2/w_2^2\}$. Согласно следствию, вытекающему из известной теоремы Нагеля и Лутц, координаты точки $2O_m$ должны быть целыми числами (заметим, что целочисленность координат можно было бы доказать и способом указанным в работе [1]). Поэтому, учитывая что $u_2 = u_1^4 - bw_1^4$, $w_2 = 2u_1v_1w_1$, имеем:

$$(u_1^4 - bw_1^4)^2 \equiv 0 \pmod{u_1^2w_1^2(u_1^4 + au_1^2w_1^2 + bw_1^4)}. \tag{11}$$

Однако, $\nu_q(u_1^4 - bw_1^4)^2 = 2\nu_q(b) + 8\nu_q(w_1)$, $2\nu_q(b) + 8\nu_q(w_1) < \nu_q(u_1^2w_1^2(u_1^4 + au_1^2w_1^2 + bw_1^4))$. Следовательно, (11) невозможно. Лемма доказана.

Лемма 6. *Если кривая* T *имеет точку конечного порядка* $m > 2$, *то, не нарушая общности, можно считать* $(a, b) = 1$.

Доказательство. Пусть q такое, что $\nu_q(a)$, $\nu_q(b) > 0$. Обозначим $\nu_q(a)$, $\nu_q(b)$, $\nu_q(u_1/w_1)$ через α, β, γ. Если $\alpha + 2\gamma > \beta$ или 4γ, то $\beta = 4\gamma$. Действительно, случаи $\beta < 4\gamma$ и $\beta > 4\gamma$ невозможны в силу условий 2) леммы 2. Полагая $a = q^{2\gamma}a'$, $b = q^{4\gamma}b'$, $u_1/w_1 = q^\gamma u'$, $v_1/w_1^2 = q^{2\gamma}v'$, кривую T можно записать в виде $v'^2 = u'^4 + a'u'^2 + b'$, где $\nu_q(a', b') = 0$, откуда видно, что при $\alpha + 2\gamma > \beta$ или 4γ лемма справедлива. Если же $\alpha + 2\gamma \leqslant \beta$ или 4γ, то в силу тех же условий 2) $\alpha + 2\gamma \leqslant \min\{\beta, 4\gamma\}$. Далее, при нечётном α $\beta = \alpha + 2\gamma$ и $4\gamma > \alpha + 2\gamma = \beta$, что невозможно на основании условия 3) леммы 2. Следовательно, $\alpha = 2\alpha_1$. Положим $a = q^{2\alpha_1}a'$, $b = q^{4\alpha_1}b'$, $u_1/w_1 = q^{\alpha_1}u'$, $v_1/w_1^2 = q^{2\alpha_1}v'$. В этом случае кривую T можно записать в виде $v'^2 = u'^4 + a'u'^2 + b'$, где $\nu_q(a', b') = 0$. Лемма доказана.

Лемма 7. *Если* q *нечетное и* $\nu_q(b) > 0$, *то для любого натурального* $k < m$ *и* $\neq m/2$

$$\nu_q(u_k/w_k) = \{k\nu_q(u_1/w_1)/\nu_q(b)\}\nu_q(b) \qquad \text{где} \qquad kO_m = \{u_k/w_k, v_k/w_k^2\}.$$

Доказательство. Доказательство проведём методом математической индукции. Так как на основании леммы 5 $\frac{1}{2} \geqslant \nu_q(u_1/w_1)/\nu_q(b)$, то

$$\{\nu_q(u_1/w_1)/\nu_q(b)\}\nu_q(b) = \nu_q(u_1/w_1).$$

Таким образом, при $k = 1$ лемма верна. Предположим теперь, что лемма доказана при $k < n$ и покажем, что в этом случае она справедлива и при $k = n$. Рассмотрим раздельно следующие два случая: 1) $n \equiv 0 \pmod 2$, 2) $n \not\equiv 0 \pmod 2$.

1) $n \equiv 0 \pmod 2$. По формулам (1)

$$u_n = u_{n/2}^4 - bw_{n/2}^4, \qquad w_n = 2u_{n/2}v_{n/2}w_{n/2}.$$

Если $\nu_q(u_{n/2}/w_{n/2}) = \frac{1}{4}\nu_q(b)$, то имеем

$$\nu_q(b) \leqslant \nu_q(u_n) < \infty, \qquad \nu_q(w_n) = \tfrac{1}{2}\nu_q(b), \qquad \nu_q(b) \leqslant 2\nu_q(u_n/w_n) < \infty.$$

С другой стороны, по лемме 5 $\nu_q(b) \geqslant 2\nu_q(u_n/w_n)$, следовательно,

$$\nu_q(u_n/w_n) = \tfrac{1}{2}\nu_q(b).$$

По предположению $\nu_q(u_{n/2}/w_{n/2}) = \frac{1}{4}\nu_q(b) = \{n\nu_q(u_1/w_1)/2\nu_q(b)\}\nu_q(b)$, то есть $n\nu_q(u_1/w_1)/2\nu_q(b) = \pm\frac{1}{4} + r$, где r целое число, что даёт $\pm\frac{1}{2} + 2r = n\nu_q(u_1/w_1)/\nu_q(b)$,

$$\{n\nu_q(u_1/w_1)/\nu_q(b)\}\nu_q(b) = \tfrac{1}{2}\nu_q(b) = \nu_q(u_n/w_n).$$

Если же $\nu_q(u_{n/2}/w_{n/2}) \neq \frac{1}{4}\nu_q(b)$, то, в силу нечетности q

$$\nu_q(u_n/w_n) = -2\nu_q(u_{n/2}/w_{n/2}) + \min\{4\nu_q(u_{n/2}/w_{n/2}), \nu_q(b)\}.$$

Отсюда легко заключить, что в случае $4\nu_q(u_{n/2}/w_{n/2}) < \nu_q(b)$

$$\nu_q(u_n/w_n) = 2\nu_q(u_{n/2}/w_{n/2}) = 2\{n\nu_q(u_1/w_1)/2\nu_q(b)\}\nu_q(b) = \{n\nu_q(u_1/w_1)/\nu_q(b)\}\nu_q(b),$$

а в случае $\nu_q(b) < 4\nu_q(u_{n/2}/w_{n/2})$

$$\nu_q(u_n/w_n) = \nu_q(b) - 2\nu_q(u_{n/2}/w_{n/2}) = \nu_q(b) - 2\{n\nu_q(u_1/w_1)/2\nu_q(b)\}\nu_q(b) = \{n\nu_q(u_1/w_1)/\nu_q(b)\}\nu_q(b),$$

то есть опять таки

$$\nu_q(u_n/w_n) = \{n\nu_q(u_1/w_1)/\nu_q(b)\}\nu_q(b).$$

2) $n \not\equiv 0 \pmod 2$. По формулам (1)

$$u_n u_1 = u_{\frac{n+1}{2}}^2 u_{\frac{n-1}{2}}^2 - bw_{\frac{n+1}{2}}^2 w_{\frac{n-1}{2}}^2, \qquad w_n w_1 = u_{\frac{n-1}{2}}^2 w_{\frac{n+1}{2}}^2 - u_{\frac{n+1}{2}}^2 w_{\frac{n-1}{2}}^2.$$

а) $\nu_q(u_{\frac{n+1}{2}}/w_{\frac{n+1}{2}}) = \nu_q(u_{\frac{n-1}{2}}/w_{\frac{n-1}{2}})$. По условию

$$\nu_q(u_{\frac{n+1}{2}}/w_{\frac{n+1}{2}}) = \{(n+1)\nu_q(u_1/w_1)/2\nu_q(b)\}\nu_q(b),$$

$$\nu_q(u_{\frac{n-1}{2}}/w_{\frac{n-1}{2}}) = \{(n-1)\nu_q(u_1/w_1)/2\nu_q(b)\}\nu_q(b);$$

пусть

$$(n+1)v_q(u_1/w_1)/2v_q(b) = \alpha+r, \quad (n-1)v_q(u_1/w_1)/2v_q(b) = \pm\alpha+s,$$

где r, s — целые числа, $\alpha \leqslant \frac{1}{2}$. Так как $v_q(u_1/w_1)/v_q(b) \leqslant \frac{1}{2}$, то

$$(n-1)v_q(u_1/w_1)/2v_q(b) = -\alpha+s,$$
$$2v_q(u_{\frac{n+1}{2}}/w_{\frac{n+1}{2}})+2v_q(u_{\frac{n-1}{2}}/w_{\frac{n-1}{2}}) \neq v_q(b).$$

Действительно, если $2v_q(u_{\frac{n+1}{2}}/w_{\frac{n+1}{2}})+2v_q(u_{\frac{n-1}{2}}/w_{\frac{n-1}{2}}) = v_q(b)$, то $(r+s)/n-\frac{1}{2}$ должно быть целым числом, что в силу нечетности n невозможно. Следовательно,

$$0 \leqslant v_q(u_n/w_n)/v_q(b) \leqslant \min\{1, 4|\alpha|\}-\min\{1, 4|\alpha|\} = 0,$$

откуда

$$v_q(u_n/w_n) = 0.$$

Но $nv_q(u_1/w_1)/v_q(b) = r+s$, поэтому

$$\{nv_q(u_1/w_1)/v_q(b)\}v_q(b) = 0 = v_q(u_n/w_n).$$

b) $2v_q(u_{\frac{n+1}{2}}/w_{\frac{n+1}{2}})+2v_q(u_{\frac{n-1}{2}}/w_{\frac{n-1}{2}}) = v_q(b)$. Как и в предыдущем случае, положим

$$(n+1)v_q(u_1/w_1)/2v_q(b) = \alpha+r, \quad (n-1)v_q(u_1/w_1)/2v_q(b) = \beta+s,$$

где $|\alpha|, |\beta| \leqslant \frac{1}{2}$, r, s — целые числа. На основании предыдущего $|\alpha| \neq |\beta|$, поэтому

$$\infty > v_q(u_n/w_n) \geqslant (1-2\min\{|\alpha|, |\beta|\})v_q(b) > \tfrac{1}{2}v_q(b),$$

что противоречит лемме 5.

c) $v_q(u_{\frac{n+1}{2}}/w_{\frac{n+1}{2}}) \neq v_q(u_{\frac{n-1}{2}}/w_{\frac{n-1}{2}})$,

$$2v_q(u_{\frac{n+1}{2}}/w_{\frac{n+1}{2}})+2v_q(u_{\frac{n-1}{2}}/w_{\frac{n-1}{2}}) \neq v_q(b).$$

$$v_q(u_n/w_n)+v_q(u_1/w_1) = \min\{2v_q(u_{\frac{n+1}{2}}/w_{\frac{n+1}{2}})+2v_q(u_{\frac{n-1}{2}}/w_{\frac{n-1}{2}}), v_q(b)\}-$$
$$-2\min\{v_q(u_{\frac{n+1}{2}}/w_{\frac{n+1}{2}}), v_q(u_{\frac{n-1}{2}}/w_{\frac{n-1}{2}})\}.$$

Обозначим $v_q(u_{\frac{n+1}{2}}/w_{\frac{n+1}{2}})/v_q(b)$, $v_q(u_{\frac{n-1}{2}}/w_{\frac{n-1}{2}})/v_q(b)$ через α и β. Если $2\alpha+2\beta < 1$, то $\alpha > \beta$, поэтому $v_q(u_n/w_n)+v_q(u_1/w_1) = 2\max\{\alpha, \beta\} = 2\alpha$, откуда опять таки получаем

$$v_q(u_n/w_n) = \{nv_q(u_1/w_1)/v_q(b)\}v_q(b).$$

Лемма 8. *Если q — нечетное такое, что $v_q(b) > 0$, то*

$$mv_q(u_1/w_1) \equiv 0 \pmod{v_q(b)}.$$

Доказательство. По определению точки конечного порядка для любых чисел n и q

$$v_q(u_n/w_n) = v_q(u_{m-n}/w_{m-n}),$$

поэтому при $q \neq 2$ и $0 < n < m$

$$\{nv_q(u_1/w_1)/v_q(b)\} = \{(m-n)v_q(u_1/w_1)/v_q(b)\},$$

откуда и получаем $mv_q(u_1/w_1) \equiv 0 \pmod{v_q(b)}$.

Следствие 3. *Если $kO_m = \{u_k/w_k, v_k/w_k^2\}$, $0 < k < m$, $k \neq m/2$, то*

$$\pm u_k/w_k = 2^{\varphi(k)} \prod_{\substack{d_i>1 \\ (d_i,j)=1}} \prod_{j=1}^{[d_i/2]} a_j^{\{kj/d_i\}d_i},$$

где d_i пробегает делители числа m и $\varphi(k)$ есть некоторое целое число, зависящее от k.

Следствие 4. *Если $kO_m = \{u_k/w_k, v_k/w_k^2\}$, то*

$$v_k/u_kw_k = \pm 2^{\psi(k)} \prod_{d_i>1} \prod_{j=1}^{[d_i/2]} b_j^{\{kj/d_i\}d_i}, \quad 0 < k < m, k \neq m/2,$$

где d_i пробегает делители числа m и $\psi(k)$ есть некоторое целое число, зависящее от k.

Действительно, точка $\{u_k/w_k, v_k/w_k^2\}$ кривой T порождает точку

$$\{u_k'/w_k', v_k'/w_k'^2\} = \{v_k/u_kw_k, (u_k^4-bw_k^4)/u_k^2w_k^2\}$$

кривой T_1: $y'^2 = x'^4-2ax'^2+a^2-4b$.

Лемма 9. *Если $m \geqslant 5$, то, не нарушая общности, можно считать, что выполняются следующие условия:*

1) $v_2(u_k/w_k) > 1$, $v_2(b) > 4$;

2) $v_2(u_k/w_k)-1 = \{k(v_2(u_1/w_1)-1)/(v_2(b)-4)\}(v_2(b)-4)$, *где* $0 < k < m$, $k \neq m/2$.

Доказательства условий 1) и 2) соответственно аналогичны доказательствам лемм 5 и 7.

Следствие 5. *Если $m \geqslant 5$, то u_k/w_k, v_k/u_kw_k $(0 < k < m$, $k \neq m/2)$ можно представить в виде*

$$u_k/w_k = \pm 2 \prod_{\substack{d_i>1 \\ (d_i,j)=1}} \prod_{j=1}^{[d_i/2]} a_j^{\{kj/d_i\}d_i}, \qquad m \equiv 0 \pmod{d_i},$$
$$v_k/u_kw_k = \pm \prod_{\substack{d_i>1 \\ (d_i,j)=1}} \prod_{j=1}^{[d_i/2]} b_j^{\{kj/d_i\}d_i},$$

где a_j, b_j — целые рациональные взаимно простые числа.

Доказательство теоремы. Рассмотрим точки tpO_{p^2} $(t = 1, 2, \ldots, (p-1)/2)$. На основании следствия 5

$$u_{tp}/w_{tp} = \pm 2 \prod_{j=1}^{(p-1)/2} (a_j^p)^{(tj/p)p} = \pm 2A_t^p,$$

$$v_{tp}/u_{tp}w_{tp} = \pm \prod_{j=1}^{(p-1)/2} (b_j^p)^{(tj/p)p} = \pm B_t^p$$

$(t = 1, 2, \ldots, (p-1)/2)$.

В силу же следствия 2

$$\frac{2u_{sp}w_{sp}v_{rp}}{w_{p(s+r)}w_{p(s-r)}} = \frac{u_{p(s+r)}}{w_{p(s+r)}} + \frac{u_{p(s-r)}}{w_{p(s-r)}},$$

$$\frac{2u_{rp}w_{rp}v_{sp}}{w_{p(s+r)}w_{p(s-r)}} = \frac{u_{p(s-r)}}{w_{p(s-r)}} - \frac{u_{p(s+r)}}{w_{p(s+r)}}$$

$(r, s = 1, 2, \ldots, (p-1)/2, r \neq s)$.

Так как

$$u_{sp}w_{sp}v_{rp}/u_{rp}w_{rp}v_{sp} = (v_{rp}/u_{rp}w_{rp})/(v_{sp}/u_{sp}w_{sp}),$$

то

$$A_{s+r}^p + A_{s-r}^p = C_{s,r}^p, \qquad A_{s-r}^p - A_{s+r}^p = D_{s,r}^p,$$

откуда, вводя новые обозначения,

$$z_i^p - t_i^p = 1, \qquad z_i^p + t_i^p = r_i^p \qquad (i = 1, 2, \ldots, C_{(p-1)/2}^2). \tag{12}$$

Полученные точки кривой (12) должны быть различны, так как в противном случае точка pO_{p^2} имела бы порядок меньший p. Далее, так как род кривой T больше 0, то координаты точек ptO_{p^2} $(t = 1, 2, \ldots, (p-1)/2)$ отличны от 0. Теорема доказана.

В заключение считаю своим приятным долгом выразить благодарность И. Р. Шафаревичу за ряд ценных замечаний, касающихся этой работы.

Литература

[1] В. А. Демьяненко, *О точках конечного порядка эллиптических кривых*, Изв. АН СССР, сер. матем., 31 (6) (1967), стр. 1327–1340.

Получено 20. 5. 1970

ACTA ARITHMETICA
XIX (1971)

A note on the paper "Reducibility of lacunary polynomials I"

by

A. Schinzel and J. Wójcik (Warszawa)

In the paper [1] mentioned in the title the first writer has left a gap in the proof of Lemma 1. The aim of this note is to fill this gap by proving a property of normal number fields which may be of independent interest.

Let Ω be a number field of degree $|\Omega|$, $\alpha \in \Omega$, $\alpha \neq 0$. We denote by ζ_q a primitive qth root of unity and set following [1]

$$e(\alpha, \Omega) = \begin{cases} 0 \text{ if } \alpha = \zeta_q \text{ for some } q, \\ \text{maximal } e \text{ such that } \alpha = \zeta_q \beta^e \text{ with suitable } q \text{ and} \\ \qquad \beta \in \Omega, \text{ otherwise.} \end{cases}$$

It is asserted in Lemma 1 of [1] that if $\alpha \neq 0, f(\alpha) = 0$, where $f(x) = \sum_{i=0}^{m} a_i x^i$ is a polynomial with integral coefficients and $\|f\| = \sum_{i=0}^{m} a_i^2$, then

$$e(\alpha, \Omega) \leqslant \tfrac{5}{2}|\Omega| \log \|f\|. \tag{1}$$

The proof for α not being an integer is correct. The proof for α being an integer is based on the following refinement of a result of Cassels ([1], p. 159).

If an algebraic integer β of degree n is not conjugate to β^{-1} then

$$\overline{|\beta|} > 1 + \frac{1}{5n-1}, \tag{2}$$

where $\overline{|\beta|}$ is the maximal absolute value of the conjugates of β.

If α is an integer and $\alpha = \zeta_q \beta^e$ then β is also an integer $(e > 0)$. However it does not follow that if α is not conjugate to α^{-1} then β is not conjugate to β^{-1}. The example

$$\alpha = -1 - \sqrt{2} = \zeta_4 \left(\zeta_8 \sqrt{1+\sqrt{2}}\right)^2 = \zeta_4 \beta^2$$

shows that even for all i $\zeta_q^i \beta$ may be conjugate to $\zeta_q^{-i} \beta^{-1}$.