Общероссийский математический портал

В. А. Демьяненко, О структуре эллиптических полей. II, *Изв. РАН. Сер. матем.*, 1998, том 62, выпуск 1, 3–20

DOI: <https://doi.org/10.4213/im181>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.198.64.247

26 апреля 2023 г., 18:36:03

УДК 513.6

В. А. Демьяненко

О структуре эллиптических полей. II

Изучается кручение эллиптических и якобиевых кривых над круговыми полями.

Библиография: 10 наименований.

Пусть k – алгебраическое числовое поле, F и G – кривые $y^2 = x^3 + rx + s$ и $v^2 = u^4 + au^2 + b$, определенные над k , r, s, a, b целые, $D = -4r^3 - 27s^2$, $d = b^2(a^2 - 4b)$, $dD \neq 0$, $\{O_{m,1}, O_{m,2}\}$, $\{o_{m,1}, o_{m,2}\}$ – соответственно базисы всех точек порядка m (m произвольное натуральное) на F и G , $k(P_1, P_2, \dots)$ – поле, полученное присоединением к k координат точек $P_1, P_2, \dots$,

$$\alpha_1 O_{m,1} + \alpha_2 O_{m,2} = \{x_{\alpha_1/m, \alpha_2/m}, y_{\alpha_1/m, \alpha_2/m}\} = \{x(\alpha/m), y(\alpha/m)\},$$

$$\alpha_1 o_{m,1} + \alpha_2 o_{m,2} = \{u_{\alpha_1/m, \alpha_2/m}, v_{\alpha_1/m, \alpha_2/m}\} = \{u(\alpha/m), v(\alpha/m)\}$$

и $\varepsilon(m) = e^{2\pi i/m}$.

Цель настоящей работы – доказательство двух следующих теорем.

ТЕОРЕМА 1. Пусть Q – поле рациональных чисел и $m = p^t$, где p – простое и t – натуральное числа. Если $O_{m,1}, O_{m,2} \in Q(\varepsilon(p^l))$ (l произвольное целое рациональное) и $k = Q(\varepsilon(p^t))$, то $m \leq 5$. В случаях $m = 2, 3, 4, 5$ имеем:

$m = 2$:

$$-r = c^2 + cd + d^2, \quad s = cd(c + d),$$

$$O_{2,1} = \{x_{1/2,0}, y_{1/2,0}\} = \{c, 0\}, \quad O_{2,2} = \{x_{0,1/2}, y_{0,1/2}\} = \{d, 0\};$$

$m = 3$:

$$r = 48d(c^3 - d^3), \quad s = 16(c^6 - 20c^3d^3 - 8d^6),$$

$$O_{3,1} = \{x_{1/3,0}, y_{1/3,0}\} = \{12d^2, 4(c^3 + 8d^3)\},$$

$$O_{3,2} = \{x_{0,1/3}, y_{0,1/3}\} = \{-4(c - d)^2, 4\sqrt{-3}c(c^2 - 2cd + 4d^2)\};$$

$m = 4$:

$$-r = 9(c^2 + cd + d^2)\rho^4, \quad s = 27cd(c + d)\rho^6,$$

$$c = \alpha^4 + 6\alpha^2\beta^2 + \beta^4, \quad d = \alpha^4 - 6\alpha^2\beta^2 + \beta^4,$$

$$O_{4,1} = \{x_{1/4,0}, y_{1/4,0}\} = \{3(\alpha^4 + 6\alpha^3\beta + 6\alpha^2\beta^2 + 6\alpha\beta^3 + \beta^4)\rho^2,$$

$$54\alpha\beta(\alpha + \beta)^2(\alpha^2 + \beta^2)\rho^3\},$$

$$O_{4,2} = \{x_{0,1/4}, y_{0,1/4}\} = \{3(\alpha^4 + 6i\alpha^3\beta - 6\alpha^2\beta^2 - 6i\alpha\beta^3 + \beta^4)\rho^2,$$

$$54i\alpha\beta(\alpha + \beta i)^2(\alpha^2 - \beta^2)\rho^3\}, \quad i^2 = -1; \quad (1)$$

$m = 5$:

$$\begin{aligned}
-r &= 27(c^4 + 12c^3d + 14c^2d^2 - 12cd^3 + d^4)\rho^4, \\
s &= 54(c^6 + 18c^5d + 75c^4d^2 + 75c^2d^4 - 18cd^5 + d^6)\rho^6, \\
c &= \alpha^5 + (\varepsilon + \varepsilon^{-1})^5\beta^5, \quad d = (\varepsilon + \varepsilon^{-1})^5\alpha^5 + \beta^5, \quad \varepsilon = \varepsilon(5), \\
O_{5,1} &= \{x_{1/5,0}, y_{1/5,0}\} = \{3(c^2 + 6cd + d^2)\rho^2, 108cd^2\rho^3\}, \\
x_{\gamma/5,1/5} &= \sum_{i=0}^4 a_i \varepsilon^{\gamma^i(5)} L^i, \quad L = \sqrt[5]{(2c + (11 - 5\sqrt{5})d)/(2c + (11 + 5\sqrt{5})d)}, \\
2y_{1/5,0}y_{0,1/5} &= -x_{1/5,1/5}(x_{1/5,0} - x_{0,1/5})^2 \\
&\quad + (x_{1/5,0} + x_{0,1/5})(r + x_{1/5,0}x_{0,1/5}) + 2s,
\end{aligned}$$

где $\rho, c, d, \alpha, \beta, a_i, L \in Q(\varepsilon(p^l))$.

ТЕОРЕМА 2. В обозначениях предыдущей теоремы $m \leq 3$ при $k = Q(\varepsilon(p^t))$ и $o_{m,1}, o_{m,2} \in Q(\varepsilon(p^l))$. Для случаев $m = 2, 3$ имеем:

$m = 2$:

$$\begin{aligned}
-a &= c^2 + d^2, \quad b = (c^2 - d^2)^2, \\
O_{2,1} &= \{u_{1/2,0}, v_{1/2,0}\} = \{0, c^2 - d^2\}, \quad O_{2,2} = \{u_{0,1/2}, v_{0,1/2}\} = \{c + d, 0\};
\end{aligned}$$

$m = 3$:

$$\begin{aligned}
-a &= 3(c^6 + 2\sqrt{-3}c^5d - 5c^4d^2 - 5c^2d^4 - 2\sqrt{-3}cd^5 + d^6)\rho^2, \\
b &= 16\sqrt{-3}c^3d^3(c^2 + \sqrt{-3}cd - d^2)^3\rho^4, \\
O_{3,1} &= \{u_{1/3,0}, v_{1/3,0}\} \\
&= \{2c(c^2 + \sqrt{-3}cd - d^2)\rho, 2c(c^2 + \sqrt{-3}cd - d^2)(c + \sqrt{-3}d)(c^2 - d^2)\rho^2\}, \\
O_{3,2} &= \{u_{0,1/3}, v_{0,1/3}\} \\
&= \{2d(c^2 + \sqrt{-3}cd - d^2)\rho, 2d(c^2 + \sqrt{-3}cd - d^2)(d - \sqrt{-3}c)(c^2 - d^2)\rho^2\},
\end{aligned} \tag{2}$$

где $c, d, \rho \in Q(\varepsilon(p^l))$.

ЛЕММА 1. Имеем

$$\begin{aligned}
k(O_{m,1}, O_{m,2}) &= k(O_{m,2}, \varepsilon(m), \sqrt[m]{S}), \\
S &= \prod_{t=0}^{m-1} f(y_{1/m,t/m}) / \prod_{l=1}^{m-1} f(y_{0,l/m}), \\
f(y_{1/m,t/m}) &= 4y_{1/m,t/m}^2 \prod_{c=2}^{m-2} (x_{1/m,t/m} - x_{c/m,ct/m}), \\
f(y_{0,l/m}) &= 4y_{0,l/m}^2 \prod_{\substack{c=1 \\ c \neq l, m-l}}^{m-1} (x_{0,l/m} - x_{0,c/m})
\end{aligned} \tag{3}$$

(см. [1, с. 730]).

Заметим, что на основании той же работы [1] при нечетных m имеем

$$k(O_{m,1}, O_{m,2}) = k(O_{m,2}, \varepsilon(m), \sqrt[m]{T_l}),$$

$$T_l = \prod_{a=1}^{q-1} \left\{ \prod_{t=0}^{m-1} y_{2^a l/m, 2^a t/m} / \prod_{t=1}^{m-1} y_{0, 2^a t/m} \right\}^{2^{-2a}}, \quad (4)$$

где $l \in \{1, 2, \dots, m-1\}$, $(l, m) = 1$, $2^{2q} \equiv 1(m)$.

ЛЕММА 2. Если $P = \{x_1, y_1\}$ – произвольная точка на F и $tP = \{x_t, y_t\}$, то на кривой

$$F': y'^2 = x'^3 + r_{(\alpha/m)} x' + s_{(\alpha/m)},$$

$$r_{(\alpha/m)} = r - 5 \sum_{\delta=1}^{m-1} (r + 3x_{0,\delta(\alpha/m)}^2), \quad (5)$$

$$s_{(\alpha/m)} = s - 7 \sum_{\delta=1}^{m-1} (2s + 3rx_{0,\delta(\alpha/m)} + 5x_{0,\delta(\alpha/m)}^3),$$

расположены точки

$$tP' = \{x'_{t,(\alpha/m)}, y'_{t,(\alpha/m)}\},$$

где

$$x'_{t,(\alpha/m)} = \sum_{\gamma=0}^{m-1} x_{t,\gamma(\alpha/m)} - \sum_{\delta=1}^{m-1} x_{0,\delta(\alpha/m)},$$

$$y'_{t,(\alpha/m)} = \sum_{\gamma=0}^{m-1} y_{t,\gamma(\alpha/m)} \quad (6)$$

(см. [2]).

В силу [3] при нечетных m имеем

$$y'_{t,(\alpha/m)} = \prod_{\gamma=0}^{m-1} y_{t,\gamma(\alpha/m)} / \prod_{\delta=1}^{m-1} y_{0,\delta(\alpha/m)}. \quad (7)$$

ЛЕММА 3. Если порядок точки $\alpha_1 O_{m,1} + \alpha_2 O_{m,2} = \{x_{(\alpha/m)}, y_{(\alpha/m)}\}$ больше 2, то

$$\varepsilon_{(\alpha/m)} y_{(\alpha/m)} = c_0^3 \sigma_0 T_{(\alpha/m)}^{-3+4(1-e)} \prod_{i,j=0}^{m-1} c_{i,j}^{(\alpha_1 i + \alpha_2 j)}, \quad (8)$$

$$D = c_0^{12} \sigma_0^4 \prod_{i,j=0}^{m-1} c_{i,j}^m,$$

$r \equiv 0(c_0^4)$, $s \equiv 0(c_0^6)$, $\varepsilon_{(\alpha/m)}$ – единицы, a и $(\alpha_1 i + \alpha_2 j)$ – соответственно абсолютные наименьшие вычеты числа m по $\bmod 2$ и числа $(\alpha_1 i + \alpha_2 j)$ по $\bmod m$, $(i, j, m) = 1$, $c_0, \sigma_0, c_{i,j}, T_{(\alpha/m)}$ – целые числа поля $k'(O_{m,1}, O_{m,2})$, в котором все идеалы поля $k(O_{m,1}, O_{m,2})$ главные, $4 \equiv 0(\sigma_0)$, $c_{i,j}$ попарно взаимно просты, $T_{(\alpha/m)} = 1$ при $m/(\alpha_1, \alpha_2, m) \neq p^q, 2p^q$ (p простое нечетное), $m \equiv 0 \pmod{T_{(\alpha/m)}}$ при $m/(\alpha_1, \alpha_2, m) = p^q, 2p^q$, причем в случае $T_{(\alpha/m)}$, $T_{(\alpha'/m)} \equiv 0(q)$, $(\alpha'_1 \alpha_2 - \alpha'_2 \alpha_1, m) = 1$ для любых (α/m) имеем $T_{(\alpha/m)} \equiv 0(q)$.

Доказательство леммы 3 аналогично доказательству леммы 10 из [4].

ЛЕММА 4. Если $O_{m,1}, O_{m,2}$ – базис группы всех точек порядка m на F , то $O'_{m,1} = (O_{m,2}, O_{m,1}) = \{x'_{1/m,0}, y'_{1/m,0}\}$, $O'_{m,2} = (O_{m^2,1}, O_{m,1}) = \{x'_{0,1/m}, y'_{0,1/m}\}$ – базис группы всех точек порядка m на F' , где

$$\begin{aligned} x'_{1/m,0} &= \sum_{\gamma=0}^{m-1} x_{\gamma/m,1/m} - \sum_{\delta=1}^{m-1} x_{\delta/m,0}, \\ y'_{1/m,0} &= \sum_{\gamma=0}^{m-1} y_{\gamma/m,1/m} = \prod_{\gamma=0}^{m-1} y_{\gamma/m,1/m} / \prod_{\delta=1}^{m-1} y_{\delta/m,0}, \quad m \not\equiv 0(2), \\ x'_{0,1/m} &= \sum_{\gamma=0}^{m-1} x_{1/m^2+\gamma/m,0} - \sum_{\delta=1}^{m-1} x_{\delta/m,0}, \\ y'_{0,1/m} &= \sum_{\gamma=0}^{m-1} y_{1/m^2+\gamma/m,0} = \prod_{\gamma=0}^{m-1} y_{1/m^2+\gamma/m,0} / \prod_{\delta=1}^{m-1} y_{\delta/m,0}, \quad m \not\equiv 0(2). \end{aligned} \tag{9}$$

ЛЕММА 5. Пусть

$$s_i = \sum_{\delta_1, \dots, \delta_i} x_{\delta_1/m,0} \dots x_{\delta_i/m,0}$$

– симметрические функции от координат точек $\delta_i O_{m,1}$, $\delta_i \neq \delta_j$, $\delta_i = 1, 2, \dots, m-1$. Координаты точек $tO'_{m,1} = \{x'_{t/m,0}, y'_{t/m,0}\}$, $t = 1, 2, \dots, m-1$, можно представить в виде

$$\begin{aligned} x'_{t/m,0} &= \sum_{i=0}^{[m/2]-1} c_i (\varepsilon^t - \varepsilon^{-t})^{2i-2}, \\ y'_{t/m,0} &= \sum_{i=0}^{[m/2]-1} d_i (\varepsilon^t - \varepsilon^{-t})^{2i-3}, \quad \varepsilon = \varepsilon(m), \end{aligned} \tag{10}$$

где $t = 1, 2, \dots, m-1$, c_i, d_i – целые из $k(s_i)$.

(Лемма 4 есть лемма 7' в [5], а лемма 5 – с небольшими уточнениями – лемма 10' из той же работы [5].)

Аналогично леммам 1–5 для кривой G справедливы следующие леммы.

ЛЕММА 1'. Имеем

$$\begin{aligned} k(o_{m,1}, o_{m,2}) &= k(o_{m,2}, \varepsilon(m), \sqrt[m]{L}), \\ L &= \prod_{t=0}^{m-1} g(u_{1/m,t/m}) / \prod_{l=1}^{m-1} g(u_{0,l/m}), \\ g(u_{0,l/m}) &= 4u_{0,l/m}^2 v_{0,l/m}^2 \prod_{\substack{c=1 \\ c \neq l, m-l}}^{m-1} (u_{0,l/m}^2 - u_{0,c/m}^2), \\ g(u_{1/m,t/m}) &= 4u_{1/m,t/m}^2 v_{1/m,t/m}^2 \prod_{c=2}^{m-2} (u_{1/m,t/m}^2 - u_{c/m,ct/m}^2). \end{aligned} \tag{11}$$

При нечетном m (11) можно представить в виде

$$k(o_{m,1}, o_{m,2}) = k(o_{m,2}, \varepsilon(m), \sqrt[m]{M_l}),$$

$$M_l = \prod_{a=1}^{q-1} \left\{ \prod_{t=0}^{m-1} u_{2^a l/m, 2^a t/m} v_{2^a l/m, 2^a t/m} / \prod_{t=1}^{m-1} u_{0, 2^a t/m} v_{0, 2^a t/m} \right\}^{2^{-2a}}, \quad (12)$$

где $l = 1, 2, \dots, m-1$, $(l, m) = 1$, $2^{2q} \equiv 1(m)$.

ЛЕММА 2'. Если $Q = \{u_1, v_1\}$ – произвольная точка на G и $tQ = \{u_t, v_t\}$, то на кривой

$$G': v'^2 = u'^4 + a_{(\alpha/m)} u'^2 + b_{(\alpha/m)},$$

$$a_{(\alpha/m)} = a + 3 \sum_{\gamma=0}^{m-1} u_{1/2m+\gamma/m,0}^2 - 3 \sum_{\delta=1}^{m-1} u_{\delta/m,0}^2, \quad (13)$$

$$b_{(\alpha/m)} = b + (a_{(\alpha/m)}^2 - a^2)/3 - 5 \sum_{\delta=1}^{m-1} (b - 2a u_{\delta/m,0}^2 + 3u_{\delta/m,0}^4),$$

расположены точки $tQ' = \{u'_{t,(\alpha/m)}, v'_{t,(\alpha/m)}\}$, где

$$u'_{t,(\alpha/m)} = \sum_{\gamma=0}^{m-1} u_{t,\gamma(\alpha/m)},$$

$$v'_{t,(\alpha/m)} = \sum_{\gamma=0}^{m-1} u_{t,\gamma(\alpha/m)} \sum_{\gamma=0}^{m-1} v_{t,\gamma(\alpha/m)} / u_{t,\gamma(\alpha/m)}. \quad (14)$$

При нечетном m (14) можно представить в виде

$$a_{(\alpha/m)} = ma + 2 \sum_{\delta=1}^{m-1} b/u_{\delta(\alpha/m)}^2 - (a^2 - 4b) \sum_{\delta=1}^{m-1} u_{\delta(\alpha/m)}^2 / v_{\delta(\alpha/m)}^2,$$

$$b_{(\alpha/m)} = b^m / \prod_{\delta=1}^{m-1} u_{\delta(\alpha/m)}^4, \quad (15)$$

$$u'_{t,(\alpha/m)} = \prod_{\gamma=0}^{m-1} u_{t,\gamma(\alpha/m)} / \prod_{\delta=1}^{m-1} u_{\delta(\alpha/m)},$$

$$v'_{t,(\alpha/m)} = \prod_{\gamma=0}^{m-1} v_{t,\gamma(\alpha/m)} / \prod_{\delta=1}^{m-1} v_{\delta(\alpha/m)}.$$

ЛЕММА 3'. Если порядок точки $\alpha_1 o_{m,1} + \alpha_2 o_{m,2} = \{u_{(\alpha/m)}, v_{(\alpha/m)}\}$ больше 2, то

$$\begin{aligned} u_{(\alpha/m)} &= \varepsilon_{(\alpha/m)} c_0 \sigma_0 T_{(\alpha/m)}^{-1+2(1-e)} \prod_{i,j=0}^{m-1} a_{i,j}^{(\alpha_1 i + \alpha_2 j)}, \\ v_{(\alpha/m)} / u_{(\alpha/m)} &= \varepsilon'_{(\alpha/m)} c_0 \sigma'_0 T_{(\alpha/m)}^{-1} \prod_{i,j=0}^{m-1} b_{i,j}^{(\alpha_1 i + \alpha_2 j)}, \\ b &= c_0^4 \sigma_0^4 \prod_{i,j=0}^{m-1} a_{i,j}^m, \quad a^2 - 4b = c_0^4 \sigma_0'^4 \prod_{i,j=0}^{m-1} b_{i,j}^m, \end{aligned} \quad (16)$$

где $\varepsilon_{(\alpha/m)}$, $\varepsilon'_{(\alpha/m)}$ – единицы, $(\sigma_0, \sigma'_0) = 1$, а e , $(\alpha_1 i + \alpha_2 j)$, σ_0 , σ'_0 , $a_{i,j}$, $b_{i,j}$, $T_{(\alpha/m)}$ удовлетворяют условиям леммы 3.

ЛЕММА 4'. Если $o_{m,1}$, $o_{m,2}$ – базис группы всех точек порядка m на G , то $o'_{m,1} = (o_{m,2}, o_{m,1}) = \{u'_{1/m,0}, v'_{1/m,0}\}$, $o'_{m,2} = (o_{m^2,1}, o_{m,1}) = \{u'_{0,1/m}, v'_{0,1/m}\}$ – базис группы всех точек порядка m на G' , где

$$\begin{aligned} u'_{1/m,0} &= \sum_{\gamma=0}^{m-1} u_{\gamma/m,1/m}, \\ v'_{1/m,0} &= \sum_{\gamma=0}^{m-1} v_{\gamma/m,1/m} / u_{\gamma/m,1/m} \sum_{\gamma=0}^{m-1} u_{\gamma/m,1/m}, \\ u'_{0,1/m} &= \sum_{\gamma=0}^{m-1} u_{1/m^2+\gamma/m,0}, \\ v'_{0,1/m} &= \sum_{\gamma=0}^{m-1} v_{1/m^2+\gamma/m,0} / u_{1/m^2+\gamma/m,0} \sum_{\gamma=0}^{m-1} u_{1/m^2+\gamma/m,0}. \end{aligned} \quad (17)$$

При нечетном m (17) можно переписать в виде

$$\begin{aligned} u'_{1/m,0} &= \prod_{\gamma=0}^{m-1} u_{\gamma/m,1/m} / \prod_{\delta=1}^{m-1} u_{\delta/m,0}, \\ v'_{1/m,0} &= \prod_{\gamma=0}^{m-1} v_{\gamma/m,1/m} / \prod_{\delta=1}^{m-1} v_{\delta/m,0}, \\ u'_{0,1/m} &= \prod_{\gamma=0}^{m-1} u_{1/m^2+\gamma/m,0} / \prod_{\delta=1}^{m-1} u_{\delta/m,0}, \\ v'_{0,1/m} &= \prod_{\gamma=0}^{m-1} v_{1/m^2+\gamma/m,0} / \prod_{\delta=1}^{m-1} v_{\delta/m,0}. \end{aligned} \quad (18)$$

ЛЕММА 5'. Координаты точек $to'_{m,1} = \{u'_{t/m,0}, v'_{t/m,0}\}$, $t = 1, 2, \dots, m-1$, можно представить в виде

$$\begin{aligned} u'_{t/m,0} &= \sum_{i=0}^{[m/2]-1} a_i (\varepsilon^t - \varepsilon^{-t})^{2i-1}, \\ v'_{t/m,0} &= \sum_{i=0}^{[m/2]-1} b_i (\varepsilon^t - \varepsilon^{-t})^{2i-2}, \quad \varepsilon = \varepsilon(m), \end{aligned} \quad (19)$$

где a_i, b_i – целые числа из $k(s_i)$, $s_i = \sum_{\delta_1, \dots, \delta_i} u_{\delta_1/m,0} \dots u_{\delta_i/m,0}$ – симметрические функции от координат точек $\delta_i o_{m,1}$, $\delta_i = 1, 2, \dots, m-1$.

Прежде всего заметим, что если $k = k(O_{2^\alpha,1}, O_{2,2}) = Q(\varepsilon(2^l))$, l произвольное, то в силу

$$\begin{aligned} H: Y^2 &= X^3 - X, \\ X &= b_{1/8,j}/b_{1/8,1} + b_{1/8,j}/b_{1/8,k}, \\ Y &= y_{1/8,0}(X-1)b_{1/16,1}/y_{1/16,0}b_{1/8,1}, \\ \{j, k\} &= \{2, 3\}, \{3, 2\}, \\ b_{1/2^t,i} &= (x_{1/2^t,0} - \rho_i)^2 - (\rho_i - \rho_j)(\rho_i - \rho_k), \end{aligned} \quad (20)$$

где $i, j, k \in \{1, 2, 3\}$, $i \neq j \neq k$, $\rho^3 + r\rho + s = 0$, и работы [6] выводим: $\alpha \leq 3$. С другой стороны, при $k = k(O_{2^\alpha,1}, O_{8,2}) = Q(\varepsilon(2^l))$, l произвольное, из

$$\begin{aligned} T: X^4 + Y^4 &= Z^2, \\ X &= 3\rho_k, \quad Z = \rho_i^2 + \rho_j^2 - 8\rho_k^2 - 6\rho_i\rho_j, \\ Y &= [(x_{1/8,0} - \rho_i)^2 - (\rho_i - \rho_j)(\rho_i - \rho_k)] \\ &\quad \times [(x_{1/8,0} - \rho_j)^2 - (\rho_j - \rho_i)(\rho_j - \rho_k)]/2y_{1/8,0}y_{0,1/8}, \\ \{x_{1/2,0}, y_{1/2,0}\} &= \{\rho_i, 0\}, \quad \{x_{0,1/2}, y_{0,1/2}\} = \{\rho_j, 0\}, \quad i \neq j \neq k \in \{1, 2, 3\}, \end{aligned} \quad (21)$$

и работы [6] выводим: $\alpha \leq 2$. В случаях $\alpha = 1, 2$ непосредственным вычислением находим:

$m = 2$:

$$\begin{aligned} -r &= c^2 + cd + d^2, \quad s = cd(c + d), \\ O_{2,1} &= \{x_{1/2,0}, y_{1/2,0}\} = \{c, 0\}, \quad O_{2,2} = \{x_{0,1/2}, y_{0,1/2}\} = \{d, 0\}; \end{aligned}$$

$m = 4$:

$$\begin{aligned} -r &= 9(c^2 + cd + d^2)\rho^4, \quad s = 27cd(c + d)\rho^6, \\ c &= \alpha^4 + 6\alpha^2\beta^2 + \beta^4, \quad d = \alpha^4 - 6\alpha^2\beta^2 + \beta^4, \\ O_{4,1} &= \{x_{1/4,0}, y_{1/4,0}\} = \{3(\alpha^4 + 6\alpha^3\beta + 6\alpha^2\beta^2 + 6\alpha\beta^3 + \beta^4)\rho^2, \\ &\quad 54\alpha\beta(\alpha + \beta)^2(\alpha^2 + \beta^2)\rho^3\}, \\ O_{4,2} &= \{x_{0,1/4}, y_{0,1/4}\} = \{3(\alpha^4 + 6i\alpha^3\beta - 6\alpha^2\beta^2 - 6i\alpha\beta^3 + \beta^4)\rho^2, \\ &\quad 54i\alpha\beta(\alpha + \beta i)^2(\alpha^2 - \beta^2)\rho^3\}, \quad i^2 = -1, \end{aligned} \quad (22)$$

где $\rho, c, d, \alpha, \beta \in Q(\varepsilon(2^l))$.

Если же $k = k(O_{3\beta,1}, O_{3,2}) = Q(\varepsilon(3^l))$, l произвольное, то согласно [7]

$$\begin{aligned} H : x^3 + y^3 &= 1, \\ 2x &= \sqrt[3]{(3r + 9x_{1/3,0}^2)/x_{1/3,0}^2}, \quad 2y = -\sqrt[3]{(3r + x_{1/3,0}^2)/x_{1/3,0}^2}, \\ 2\sqrt[3]{(3r + x_{1/3,0}^2)/x_{1/3,0}^2} &= x_{1/3,0}^{-1} \sum_{t=0}^2 \varepsilon^{-t}(3)x_{t/3,1/3}, \\ 6\sqrt[3]{(3r + 9x_{1/3,0}^2)/x_{1/3,0}^2} &= x_{1/3,0}^{-1} \sum_{\alpha,\beta=0}^2 \varepsilon^{-\beta}(3)x_{1/9+\alpha/3,\beta/3}, \end{aligned} \quad (23)$$

что с учетом [8] дает $\beta \leq 1$. При $k = k(O_{3,1}, O_{3,2}) = Q(\varepsilon(3^l))$ имеем:

$m = 3$:

$$\begin{aligned} r &= 48d(c^3 - d^3), \quad s = 16(c^6 - 20c^3d^3 - 8d^6), \\ O_{3,1} &= \{x_{1/3,0}, y_{1/3,0}\} = \{12d^2, 4(c^3 + 8d^3)\}, \\ O_{3,2} &= \{x_{0,1/3}, y_{0,1/3}\} = \{-4(c-d)^2, 4\sqrt{-3}c(c^2 - 2cd + 4d^2)\}. \end{aligned} \quad (24)$$

Очевидно, $k(o_{m,1}, o_{m,2}) = k(O_{2m,1}, O_{m,2})$. Поэтому при $p = 2, 3$ из (20)–(24) и $k(O_{2m,1}, O_{m,2}) = Q(\varepsilon(p^l))$ следует, что $m = 2, 3, 4$. При $m = 4$ имеем

$$\begin{aligned} T : X^4 + Y^4 &= Z^2, \\ X &= 3\rho_1, \quad Z = (\rho_2 - \rho_3)^2 - 4(\rho_1 - \rho_2)(\rho_1 - \rho_3), \\ Y &= y_{0,1/4}\{(x_{1/8,0} - \rho_1)^2 - (\rho_1 - \rho_2)(\rho_1 - \rho_3)\}/y_{1/8,0}(x_{0,1/4} - \rho_1), \\ \{x_{1/2,0}, y_{1/2,0}\} &= \{\rho_1, 0\}, \quad \{x_{0,1/2}, y_{0,1/2}\} = \{\rho_2, 0\}, \quad \rho_i^3 + r\rho_i + s = 0, \end{aligned} \quad (25)$$

что в силу [6] невозможно. Для случаев $m = 2, 3$ легко находим:

$m = 2$:

$$\begin{aligned} -a &= c^2 + d^2, \quad b = (c^2 - d^2)^2, \\ O_{2,1} &= \{u_{1/2,0}, v_{1/2,0}\} = \{0, c^2 - d^2\}, \\ O_{2,2} &= \{u_{0,1/2}, v_{0,1/2}\} = \{c + d, 0\}; \end{aligned}$$

$m = 3$:

$$\begin{aligned} -a &= 3(c^6 + 2\sqrt{-3}c^5d - 5c^4d^2 - 5c^2d^4 - 2\sqrt{-3}cd^5 + d^6)\rho^2, \\ b &= 16\sqrt{-3}c^3d^3(c^2 + \sqrt{-3}cd - d^2)^3\rho^4, \\ O_{3,1} &= \{u_{1/3,0}, v_{1/3,0}\} = \left\{2c(c^2 + \sqrt{-3}cd - d^2)\rho, \right. \\ &\quad \left. 2c(c^2 + \sqrt{-3}cd - d^2)(c + \sqrt{-3}d)(c^2 - d^2)\rho^2\right\}, \\ O_{3,2} &= \{u_{0,1/3}, v_{0,1/3}\} = \left\{2d(c^2 + \sqrt{-3}cd - d^2)\rho, \right. \\ &\quad \left. 2d(c^2 + \sqrt{-3}cd - d^2)(d - \sqrt{-3}c)(c^2 - d^2)\rho^2\right\}. \end{aligned} \quad (26)$$

Таким образом, при $p = 2, 3$, ввиду (20)–(26), теоремы 1 и 2 доказаны.

Так как $1 - \varepsilon(p^l)$ – простой дивизор поля $Q(\varepsilon(p^l))$, то из лемм 3, 3' получаем следующие леммы.

ЛЕММА 6. Если $p > 5$, $k = Q(\varepsilon(p^l))$, l произвольное, то для кривой F имеем $r = (1 - \varepsilon(p^l))^{4q}r'$, $s = (1 - \varepsilon(p^l))^{6q}s'$, q целое рациональное, r' , s' целые, принадлежащие $Q(\varepsilon(p^l))$, и $(r', s', 1 - \varepsilon(p^l)) = 1$.

ЛЕММА 6'. Если $p > 3$, $k = Q(\varepsilon(p^l))$, l произвольное, то для кривой G имеем $a = (1 - \varepsilon(p^l))^{2q}a'$, $b = (1 - \varepsilon(p^l))^{4q}b'$, q целое рациональное, a' , b' целые, принадлежащие $Q(\varepsilon(p^l))$, и $(a', b', 1 - \varepsilon(p^l)) = 1$.

ЛЕММА 7. Пусть P_1, P_2 — произвольные, O_m — примитивная порядка m точки на F , $P_1 + \alpha O_m = \{x_{1,\alpha/m}, y_{1,\alpha/m}\}$, $P_2 + \alpha O_m = \{x'_{1,\alpha/m}, y'_{1,\alpha/m}\}$. Суммы

$$\sum_{\delta_1, \dots, \delta_i} x_{0,\delta_1/m} \dots x_{0,\delta_i/m},$$

$$\sum_{\gamma_1, \dots, \gamma_i} x_{1,\gamma_1/m} \dots x_{1,\gamma_i/m}, \quad \sum_{\gamma_1, \dots, \gamma_i} x'_{1,\gamma_1/m} \dots x'_{1,\gamma_i/m},$$

где $\delta_1, \dots, \delta_i; \gamma_1, \dots, \gamma_i$ пробегают все возможные наборы различных чисел из множеств $\{1, 2, \dots, m-1\}$, $\{0, 1, \dots, m-1\}$, обозначим соответственно через $C_i, B_{i,1}, B'_{i,1}$. Тогда

$$(B_{i,1} - B'_{i,1})/(B_{1,1} - B'_{1,1}) = C_{i-1}, \quad i = 1, 2, \dots, m. \quad (27)$$

ЛЕММА 7'. Пусть Q_1, Q_2 — произвольные, o_m — примитивная порядка m точки на G , $Q_1 + \alpha o_m = \{u_{1,\alpha/m}, v_{1,\alpha/m}\}$, $Q_2 + \alpha o_m = \{u'_{1,\alpha/m}, v'_{1,\alpha/m}\}$. Суммы

$$\sum_{\delta_1, \dots, \delta_i} u_{0,\delta_1/m} \dots u_{0,\delta_i/m},$$

$$\sum_{\gamma_1, \dots, \gamma_i} u_{1,\gamma_1/m} \dots u_{1,\gamma_i/m}, \quad \sum_{\gamma_1, \dots, \gamma_i} u'_{1,\gamma_1/m} \dots u'_{1,\gamma_i/m},$$

где $\delta_1, \dots, \delta_i; \gamma_1, \dots, \gamma_i$ пробегают все возможные наборы различных чисел из множеств $\{1, 2, \dots, m-1\}$, $\{0, 1, \dots, m-1\}$, обозначим соответственно через $c_i, b_{i,1}, b'_{i,1}$. Тогда

$$(b_{i,1} - b'_{i,1})/(b_{1,1} - b'_{1,1}) = c_{i-1}, \quad i = 1, 2, \dots, m \quad (28)$$

(см. [5, леммы 9 и 9']).

В дальнейшем будем полагать $m = p^t$, где p — простое ≥ 5 , и обозначать простой главный идеал поля $Q(\varepsilon(p^c))$ $1 - \varepsilon(p^c)$ через q_c .

ПРЕДЛОЖЕНИЕ 1. Если коэффициенты a, b кривой G принадлежат $Q(\varepsilon(m))$ и $o_{(\alpha/m)} \in Q(\varepsilon(p^l))$, l произвольное, то $a = q_t^{2\alpha} a'$, $b = q_t^{4\alpha} b'$, α целое рациональное не меньше 0, a', b' целые, принадлежащие $Q(\varepsilon(m))$, $(a', b', q_t) = 1$, и $o_{(\alpha/m)} \in Q(\varepsilon(m))$,

$$\begin{aligned} u_{(\alpha/m)} &= q_t^\alpha \bar{u}_{(\alpha/m)}, & v_{(\alpha/m)} &= q_t^{2\alpha} \bar{v}_{(\alpha/m)}, \\ \bar{u}_{i/m,0} &= q_t^{-c} a_{i/m,0}, & \bar{v}_{i/m,0} &= q_t^{-2c} b_{i/m,0}, & c &= (i, m), \end{aligned}$$

$a_{i/m,0}, b_{i/m,0}$ целые, принадлежащие $Q(\varepsilon(m))$, $(a_{i/m,0} b_{i/m,0}, q_t) = 1$, для остальных же значений (α/m) $\bar{u}_{(\alpha/m)}, \bar{v}_{(\alpha/m)}$ целые, принадлежащие $Q(\varepsilon(m))$.

ДОКАЗАТЕЛЬСТВО. При $a, b, o_{(\alpha/m)} \in Q(\varepsilon(p^l))$, p простое, большее 3, l произвольное, по лемме 6 $a = q_l^{2q} a'$, $b = q_l^{4q} b'$, $q \geq 0$ целое рациональное, a', b' целые, принадлежащие $Q(\varepsilon(p^l))$, и $(a', b', q_l) = 1$. Поэтому, если $a, b \in Q(\varepsilon(m))$, в случае $(a', q_l) = 1$ имеем $q_l^{2q} a' = q_t^\alpha a''$, a'' целое, $(a' a'', q_l) = 1$, $q_t = q_l^d$, $d = p^{l-t}$, $\alpha p^{l-t} = 2q$, $\alpha \equiv 0(2)$, $q \equiv 0(p^{l-t})$. Если же $(b', q_l) = 1$, аналогично получаем $q_l^{4q} b' = q_t^\beta b''$, $(b' b'', q_l) = 1$, $4q = p^{l-t} \beta$, $\beta \equiv 0(4)$, $q \equiv 0(p^{l-t})$. Таким образом,

$$\begin{aligned} a &= q_t^{2q} a', & b &= q_t^{4q} b', \\ u_{(\alpha/m)} &= q_t^q \bar{u}_{(\alpha/m)}, & v_{(\alpha/m)} &= q_t^{2q} \bar{v}_{(\alpha/m)}, \end{aligned}$$

a', b' целые, принадлежащие $Q(\varepsilon(m))$, $(a', b', q_t) = 1$, и $\bar{u}_{(\alpha/m)}, \bar{v}_{(\alpha/m)} \in Q(\varepsilon(p^l))$, вследствие чего, не нарушая общности, можно считать $(a, b, q_t) = 1$, a, b целые, принадлежащие $Q(\varepsilon(m))$.

Далее обозначим q – показатель числа c – через $\nu_q(c)$. Так как уравнения, которым удовлетворяют координаты $u_{(\alpha/p^t)}, v_{(\alpha/p^t)}/u_{(\alpha/p^t)}$ всех примитивных точек порядка p^t , имеют вид

$$\begin{aligned} F_{(\alpha/p^t)} &= \sum_{i=0}^{p^{2t-2}(p^2-1)/2} a_i u_{(\alpha/p^t)}^{p^{2t-2}(p^2-1)-2i} = 0, \\ a_0 &= p, & a_{p^{2t-2}(p^2-1)/2} &= (-1)^{(p-1)/2} b p^{2t-2}(p^2-1)/4, \\ \bar{F}_{(\alpha/p^t)} &= \sum_{i=0}^{p^{2t-2}(p^2-1)/2} b_i (v_{(\alpha/p^t)}/u_{(\alpha/p^t)})^{p^{2t-2}(p^2-1)-2i} = 0, \\ b_0 &= p, & b_{p^{2t-2}(p^2-1)/2} &= (-1)^{(p-1)/2} (a^2 - 4b) p^{2t-2}(p^2-1)/4, \\ \partial F_{(\alpha/p^t)}/\partial u_{(\alpha/p^t)}, \partial \bar{F}_{(\alpha/p^t)}/\partial (v_{(\alpha/p^t)}/u_{(\alpha/p^t)}) &\equiv 0(p), \\ u_{p^c(\alpha/p^t)} &= U_{p^c(\alpha/p^t)}/W_{p^c(\alpha/p^t)} = \sum_{i=0}^{(p^{2c}-1)/2} c_i u_{(\alpha/p^t)}^{p^{2c}-2i} \bigg/ \sum_{i=0}^{(p^{2c}-1)/2} d_i u_{(\alpha/p^t)}^{p^{2c}-1-2i}, \\ \partial W_{p^c(\alpha/p^t)}/\partial u_{(\alpha/p^t)} &\equiv 0(p^c), \end{aligned} \tag{29}$$

$c_0 = 1$, c_i , d_i – многочлены от a , b с целыми рациональными коэффициентами, a_i , b_i – многочлены с целыми рациональными коэффициентами соответственно от переменных a , b и $-2a$, $a^2 - 4b$, то из $(a, b, q_l) = 1$ и (29) следует

$$\begin{aligned} \max_{(\alpha/p^t), (\alpha_1, \alpha_2, p)=1} \{-\nu_{q_l}(u_{(\alpha/p^t)})\} &= \alpha > 0, \\ \min_{(\alpha/p^t), (\alpha_1, \alpha_2, p)=1} \{-\nu_{q_l}(u_{(\alpha/p^t)})\} &= \beta. \end{aligned}$$

Если $\alpha = \beta$, то из тех же соотношений (29) имеем

$$p^{2t-2}(p^2 - 1)\alpha = p^{l-1}(p - 1), \quad p^{l+1-2t} \equiv 0(p + 1),$$

что невозможно.

Предположим теперь, что $\beta > 0$. Имеем

$$\begin{aligned} u_{\alpha \pm \beta} &= (u_{\alpha}v_{\beta} \mp u_{\beta}v_{\alpha})/(u_{\beta}^2 - u_{\alpha}^2), \\ u_{\alpha}u_{\beta} &= (u_{\alpha}^2u_{\beta}^2 - b)/(u_{\beta}^2 - u_{\alpha}^2), \quad q_l = q, \\ -\nu_q(u_{(\alpha/m)}) &= \min\{-\nu_q(u_{\alpha_1/m,0}), -\nu_q(u_{0,\alpha_2/m})\}, \end{aligned} \tag{30}$$

$$(\alpha/m) = p^c(a/m), \quad a_1, a_2 \text{ целые}, \quad (a_1, a_2, p) = 1,$$

$$-\nu_q(u_{(a/p^{t-c})}) \geq -p^c \nu_q(u_{(a/p^t)}).$$

Из (30) получаем

$$\begin{aligned} (\alpha_1, \alpha_2, p) &= 1, \quad \alpha = -\nu_q(u_{1/m,0}), \\ \beta &= -\nu_q(u_{\alpha_1/m, \alpha_2/m}) = \min\{-\nu_q(u_{\alpha_1/m,0}), -\nu_q(u_{0,\alpha_2/m})\} \\ &\geq \min\{\alpha, -p^c \nu_q(u_{0,\alpha_2/m})\}, \\ \alpha_2 &= p^c a, \quad (a, p) = 1, \quad c = 0, \quad (\alpha_2, p) = 1. \end{aligned} \tag{31}$$

Согласно (31) базис всех примитивных точек $o_{(\alpha/m)}$ можно выбрать следующим образом: $\{o_{m,1}, o_{m,2}\}$, $-\nu_q(u_{1/m,0}) = \alpha$, $-\nu_q(u_{0,1/m}) = \beta$. Ни при каких значениях c

$$\nu_q(u_{0,c/m}) \neq \nu_q(u_{1/m,0}).$$

Действительно,

$$\begin{aligned}
\prod_{\alpha_1, \alpha_2} u_{\alpha_1/p^i, 1/p^t + \alpha_2/p^i} &= (-1)^{(p-1)/2} b^{(p^{2i}-1)/4} u_{0,1/p^{t-i}}, \\
\prod_{\alpha_1, \alpha_2} (v_{\alpha_1/p^i, 1/p^t + \alpha_2/p^i} / u_{\alpha_1/p^i, 1/p^t + \alpha_2/p^i}) \\
&= (-1)^{(p-1)/2} (a^2 - 4b)^{(p^{2i}-1)/4} (v_{0,1/p^{t-i}} / u_{0,1/p^{t-i}}), \\
0 \leq i \leq c \leq t, \\
-\nu_q(u_{(\alpha/p^{t-i})}) &\geq -p^i \nu_q(u_{(\alpha/p^t)}), \\
-\nu_q(u_{\alpha_1/p^i, 1/p^t + \alpha_2/p^i}) &= \min\{-\nu_q(u_{\alpha_1/p^i, 0}), -\nu_q(u_{0,1/p^t}), -\nu_q(u_{0,\alpha_2/p^i})\} \\
&= -\nu_q(u_{0,1/p^t}) = \beta, \\
-\sum_{\alpha_1, \alpha_2} \nu_q(u_{\alpha_1/p^i, 1/p^t + \alpha_2/p^i}) &= -\nu_q(u_{0,1/p^{t-i}}), \\
-\nu_q(u_{0,1/p^{t-i}}) &= p^{2i}\beta, \quad -\nu_q(u_{0,1/p^{t-c}}) = \alpha = p^{2c}\beta, \\
\nu_q(p) = p^{l-1}(p-1) &= \sum_{\alpha_1, \alpha_2} -\nu_q(u_{(\alpha/p^t)}) = p^{2t-2+c}(p^2-1)\beta.
\end{aligned} \tag{32}$$

Но (32) невозможно. Далее, так как $a, b \in Q(\varepsilon(m))$, $-\nu_q(u_{0,c/m}) \neq -\nu_q(u_{1/m,0}) = \alpha > 0$, то уравнение $F_m(u) = 0$, которому удовлетворяют координаты всех примитивных точек порядка m , над полем $Q(\varepsilon(m))$ распадается на два множителя:

$$\begin{aligned}
F_m(u) &= F_{m,1}(u) \cdot F_{m,2}(u) = 0, \\
F_{m,1}(u) &= \prod_{\substack{\alpha=1 \\ (\alpha,p)=1}}^{m-1} (u - u_{\alpha/m,0}) = \sum_{i=0}^{m-1} s_i u^{m-1-i}, \\
s_0 &= 1, \quad (-1)^i s_i = \sum_{\delta_1, \dots, \delta_i} u_{\delta_1/m,0} \dots u_{\delta_i/m,0} \in Q(\varepsilon(m)).
\end{aligned} \tag{33}$$

На основании же лемм 1', 5' и (33) имеем

$$\begin{aligned}
m &= p^t, \quad n(d) = p^d, \\
W_{(\alpha/m)} &= m \left\{ \sum_{i=0}^{m-1} s_i u^{m-1-i} \right\} \prod_{d=1}^t \prod_{\alpha=1}^{n(d)-1} \left\{ \sum_{i=0}^m s_{i,n(d),\alpha} u^{m-i} \right\}, \\
(-1)^i s_i &= \sum_{\delta_1, \dots, \delta_i} u_{\delta_1/m,0} \dots u_{\delta_i/m,0}, \quad s_0 = s_{0,n(d),\alpha} = 1, \\
(-1)^i s_{i,n(d),\alpha} &= \sum_{\gamma_1, \dots, \gamma_i} u_{\gamma_1/m,\alpha/n(d)} \dots u_{\gamma_i/m,\alpha/n(d)},
\end{aligned}$$

$$\begin{aligned}
W'_{(\alpha/m)} &= m \left\{ \sum_{i=0}^{m-1} s'_i u'^{m-1-i} \right\} \prod_{d=1}^t \prod_{\alpha=1}^{n(d)-1} \left\{ \sum_{i=0}^m s_{i,n(d),\alpha} u'^{m-i} \right\}, \\
(-1)^i s'_i &= \sum_{\delta_1, \dots, \delta_i} u'_{\delta_1/m,0} \dots u'_{\delta_i/m,0}, \quad s'_0 = s'_{0,n(d),\alpha} = 1, \\
(-1)^i s'_{i,n(d),\alpha} &= \sum_{\gamma_1, \dots, \gamma_i} u'_{\gamma_1/m,\alpha/n(d)} \dots u'_{\gamma_i/m,\alpha/n(d)}, \\
-s_{1,m,\alpha} &= \sum_{\gamma=0}^m u'_{\gamma/m,1/m} = \sum_{\gamma_1, \gamma_2=0}^m u_{1/m^2+\gamma_1/m, \gamma_2/m} = m u_{1/m,0} \in Q(\varepsilon(m)), \\
to_{m,1} &= \{u_{t/m,0}, v_{t/m,0}\} \in Q(\varepsilon(m)), \quad t = 1, 2, \dots, m-1, \\
\sqrt[m]{L} &= L_1, \quad L_1 \in Q(\varepsilon(p^l)), \quad L \in Q(\varepsilon(m) + \varepsilon^{-1}(m), s_i), \\
L_1 &\in Q(\varepsilon(m)), \quad \{u_{(\alpha/m)}, v_{(\alpha/m)}\} \in Q(\varepsilon(m)), \\
-\sum_{\delta=1}^{m-1} \nu_q(u_{\delta/m,0}) &= \nu_q(m), \quad -\sum_{(\alpha/m)} \nu_q(u_{(\alpha/m)}) = \nu_q(m). \quad (34)
\end{aligned}$$

Таким образом, $\beta \leq 0$, $u_{(\alpha/m)}, v_{(\alpha/m)} \in Q(\varepsilon(m))$, $(a, b, q_t) = 1$, $\bar{u}_{i/m,0} = q_t^{-c} a_{i/m,0}$, $\bar{v}_{i/m,0} = q_t^{-2c} b_{i/m,0}$, $c = (i, m)$, $a_{i/m,0}, b_{i/m,0}$ целые, принадлежащие $Q(\varepsilon(m))$, $(a_{i/m,0} b_{i/m,0}, q_t) = 1$, а для всех остальных значений (α/m) $\bar{u}_{(\alpha/m)}, \bar{v}_{(\alpha/m)}$ целые, принадлежащие $Q(\varepsilon(m))$. Предложение 1 доказано.

Аналогичным образом доказывается

ПРЕДЛОЖЕНИЕ 2. Если коэффициенты кривой F $r, s \in Q(\varepsilon(m))$ и $p > 5$, $O_{(\alpha/m)} \in Q(\varepsilon(p^l))$, l произвольное, то $r = q_t^{4\alpha} r'$, $s = q_t^{6\alpha} s'$, $\alpha \geq 0$ целое рациональное, r', s' целые, принадлежащие $Q(\varepsilon(m))$, $(r', s', q_t) = 1$, и $o_{(\alpha/m)} \in Q(\varepsilon(m))$, $x_{(\alpha/m)} = q_t^{2\alpha} \bar{x}_{(\alpha/m)}$, $y_{(\alpha/m)} = q_t^{3\alpha} \bar{y}_{(\alpha/m)}$, $\bar{x}_{i/m,0} = q_t^{-2c} c_{i/m,0}$, $\bar{y}_{i/m,0} = q_t^{-3c} d_{i/m,0}$, $c = (i, m)$, $c_{i/m,0}, d_{i/m,0}$ целые, принадлежащие $Q(\varepsilon(m))$, $(c_{i/m,0} d_{i/m,0}, q_t) = 1$, для остальных же значений (α/m) $\bar{x}_{(\alpha/m)}, \bar{y}_{(\alpha/m)}$ целые, принадлежащие $Q(\varepsilon(m))$.

ПРЕДЛОЖЕНИЕ 3. Если у кривой G $a, b \in Q(\varepsilon(m))$, $d/q_t^{12\alpha} = d_1$, $(d_1, p) = 1$ и $o_{(\alpha/m)} \in Q(\varepsilon(p^l))$, l произвольное, то $m \leq 5$.

ДОКАЗАТЕЛЬСТВО. Утверждение следует из предложения 1 при $a, b \in Q(\varepsilon(p^t))$ и $o_{(\alpha/p^t)} \in Q(\varepsilon(p^t))$. Дальнейшее доказательство с учетом леммы 7' и с заменой p на p^t следует из [9, предложение 1].

ПРЕДЛОЖЕНИЕ 4. Если у кривой F $r, s \in Q(\varepsilon(p^t))$, $D_1 = D/q_t^{12\alpha}$, $(D_1, p) = 1$ и $o_{(\alpha/p^t)} \in Q(\varepsilon(p^l))$, l произвольное, то $p^t \leq 7$.

ДОКАЗАТЕЛЬСТВО. Утверждение следует из предложения 2 при $r, s \in Q(\varepsilon(p^t))$ и $o_{(\alpha/p^t)} \in Q(\varepsilon(p^t))$. Дальнейшее доказательство с учетом леммы 7 настоящей работы, леммы 9 из [9] и с заменой p на p^t следует из [9, предложение 2].

ПРЕДЛОЖЕНИЕ 5. Если для кривой G $a, b \in Q(\varepsilon(p^t))$, $(d/q_t^{12\alpha}, p) \neq 1$ и $o_{(\alpha/p^t)} \in Q(\varepsilon(p^l))$, l произвольное, то $p^t \leq 5$.

ДОКАЗАТЕЛЬСТВО. Утверждение следует из предложения 1 при $a, b \in Q(\varepsilon(p^t))$ и $o_{(\alpha/p^t)} \in Q(\varepsilon(p^t))$. Далее, для упрощения записи формул введем обозначения: $p^t = m$, $1 - \varepsilon(p^t) = q_t$, $W_m(u) = 0$ – уравнение, которому удовлетворяют координаты всех точек порядка m . По условию $p \geq 5$, $(a, b, q_t) = 1$, $\nu_q(d) = \nu_q(b^2(a^2 - 4b)) > 0$; не нарушая общности, можно считать $\nu_q(b) > 0$. Тогда на основании (16) $\nu_{q_t}(b) = mc$, c натуральное, а в силу (29) и [10, с. 56]

$$\begin{aligned} \partial W_m(u)/\partial u &\equiv 0(m), \\ W_m(u) &\equiv u^{m^2-m} \{(v/u + \sqrt{a})^m - (v/u - \sqrt{a})^m\}(b), \end{aligned} \quad (35)$$

$$\begin{aligned} (\varepsilon^t - \varepsilon^{-t})^2 u_{t/m,0}^2 &\equiv 4a(q_t^{mc}), \quad \varepsilon = \varepsilon(m), \quad t = 1, 2, \dots, (m-1)/2, \\ (\varepsilon^t - \varepsilon^{-t})^2 v_{t/m,0}^2 / u_{t/m,0}^2 &\equiv (\varepsilon^t + \varepsilon^{-t})^2 a(q_t^{mc}). \end{aligned} \quad (36)$$

Согласно (16) и предложению 1 имеем

$$\begin{aligned} \nu_{q_t}(u_{i/m,0}) &= -(i, m), \quad \nu_{q_t}(v_{i/m,0}) = -2(i, m), \\ \nu_{q_t}(u_{0,l/m}) &= lc, \quad \nu_{q_t}(v_{0,l/m}) = lc, \quad l = 1, 2, \dots, (m-1)/2. \end{aligned} \quad (37)$$

Пусть

$$\beta_k = \prod_{d=1}^{(p-1)/2} \prod_{\gamma=0}^{p^k-1} (u_{0,d/p^{k+1}+\gamma/p^k} v_{0,d/p^{k+1}+\gamma/p^k})^{1/d^2} = \alpha_k^p, \quad k = 0, 1, 2, \dots$$

Тогда $\beta_k = f_k(u_{0,1/p}, v_{0,1/p}, \alpha_0, \alpha_1, \dots, \alpha_{k-1})$ – рациональные функции от $u_{0,1/p}, v_{0,1/p}, \alpha_0, \alpha_1, \dots, \alpha_{k-1}$ (см. [1]). При $M = p^k$, $G_{(\alpha/M)}: v'^2 = u'^4 + a_{(\alpha/M)} u'^2 + b_{(\alpha/M)}$, $(\alpha/M) = \{0, 1/p^k\}$, по лемме 3' имеем $\nu_{q_1}(b) = pc$, а на основании формул (15) $\nu_{q_1}(b_{(\alpha/M)}) = \nu_{q_1}(b)/p^k$. Согласно лемме 4' $\{o'_{p,1}, o'_{p,2}\}$ – базис всех точек порядка p на кривой $o_{(\alpha/M)}$, причем

$$o'_{p,1} = \{u'_{1/p,0}, v'_{1/p,0}\}, \quad o'_{p,2} = \{u'_{0,1/p}, v'_{0,1/p}\},$$

где

$$\begin{aligned} u'_{t/p,0} &= \prod_{\gamma=0}^{M-1} u_{t/p,\gamma/M} \Big/ \prod_{\delta=1}^{p-1} u_{0,\delta/M}, \\ v'_{t/p,0} &= \prod_{\gamma=0}^{M-1} v_{t/p,\gamma/M} \Big/ \prod_{\delta=1}^{M-1} v_{0,\delta/M}, \\ u'_{0,t/p} &= \prod_{\gamma=0}^{M-1} u_{0,t/p^{k+1}+\gamma/M} \Big/ \prod_{\delta=1}^{M-1} u_{0,\delta/M}, \\ v'_{0,t/p} &= \prod_{\gamma=0}^{M-1} v_{0,t/p^{k+1}+\gamma/M} \Big/ \prod_{\delta=1}^{M-1} v_{0,\delta/M}, \end{aligned} \quad (38)$$

$a_{(\alpha/M)}, b_{(\alpha/M)}$ целые, $(a_{(\alpha/M)}, b_{(\alpha/M)}, p) = 1$, $\nu_{q_1}(u'_{t/p,0}) = -1$, $\nu_{q_1}(v'_{t/p,0}) = -2$, $\nu_{q_1}(u'_{0,t/p}) = t\nu_{q_1}(b)/p^{k+1}$, $\nu_{q_1}(v'_{0,t/p}) = t\nu_{q_1}(b)/p^{k+1}$, $t = 1, 2, \dots, (p-1)/2$.

Уравнение, которому удовлетворяют все точки порядка p изогенной кривой $G_{(\alpha/M)}$, можно представить в виде

$$\begin{aligned} F'_{(\alpha/p)} &= F'_{(\alpha/p),1} \prod_{j=1}^{(p-1)/2} G'_{(\alpha/p),j} = 0, \\ F'_{(\alpha/p),1} &= \sum_{i=1}^{(p-1)/2} s'_i (u'^2)^{(p-1)/2-i}, \\ (-1)^i s'_i &= \sum_{\delta_1, \dots, \delta_i} u \delta_{1/p,0} \dots u \delta_{i/p,0}, \quad \delta_1, \dots, \delta_i \in \{1, 2, \dots, (p-1)/2\}, \\ G'_{(\alpha/p),j} &= \sum_{i=0}^{p-1} s'_{i,j} u'^{p-i}, \\ (-1)^i s'_{i,j} &= \sum_{\gamma_1, \dots, \gamma_i} u'_{j/p, \gamma_1/p} \dots u'_{j/p, \gamma_i/p}, \quad \gamma_1, \dots, \gamma_i \in \{0, 1, \dots, p-1\} \\ s'_{i,j} &\in Q(\varepsilon(p) + \varepsilon^{-1}(p), s'_1, \dots, s'_{(p-1)/2}). \end{aligned} \quad (39)$$

По лемме 1' корни уравнений (39) $G'_{(\alpha/p),j} = 0 \{u'_{j/p,0}, u'_{j/p,1}, \dots, u'_{j/p,(p-1)/p}\}$ принадлежат полю

$$Q(\varepsilon(p) + \varepsilon^{-1}(p), s'_1, \dots, s'_{(p-1)/2}, \sqrt[p]{M}),$$

где

$$M = \prod_{d=1}^{(p-1)/2} \left\{ \prod_{\gamma=0}^{p-1} u'_{d/p, \gamma/p} v'_{d/p, \gamma/p} / \prod_{\delta=1}^{p-1} u'_{0, \delta/p} v'_{0, \delta/p} \right\}^{1/d^2}.$$

Так как $\nu_{q_1}(u'_{j/p,0}) = -1$ и $\nu_{q_1}(u'_{j/p, \gamma/p}) > 0$ (при $\gamma \neq 0$), то

$$M = L^p, \quad L \in Q(\varepsilon(p) + \varepsilon^{-1}(p), s'_1, \dots, s'_{(p-1)/2}). \quad (40)$$

Представляя M в виде $A^2 B$, где

$$\begin{aligned} A &= \prod_{d=1}^{(p-1)/2} \left\{ \prod_{\gamma=0}^{p-1} u'_{d/p, \gamma/p} / \prod_{\delta=1}^{p-1} u'_{0, \delta/p} \right\}^{1/d^2}, \\ B &= \prod_{d=1}^{(p-1)/2} \left\{ \prod_{\gamma=0}^{p-1} (v'_{d/p, \gamma/p} / u'_{d/p, \gamma/p}) / \prod_{\delta=1}^{p-1} (v'_{0, \delta/p} / u'_{0, \delta/p}) \right\}^{1/d^2}, \end{aligned}$$

и учитывая, что на якобиевой кривой между координатами точек u , v имеются соотношения

$$\begin{aligned} u_{\alpha-\beta} u_{\alpha+\beta} &= (u_{\alpha}^2 u_{\beta}^2 - b) / (u_{\alpha}^2 - u_{\beta}^2), \\ (v_{\alpha-\beta} / u_{\alpha-\beta}) (v_{\alpha+\beta} / u_{\alpha+\beta}) &= (v_{\alpha}^2 v_{\beta}^2 / u_{\alpha}^2 u_{\beta}^2 - a^2 + 4b) / (v_{\alpha}^2 / u_{\alpha}^2 - v_{\beta}^2 / u_{\beta}^2), \end{aligned}$$

для A и B с использованием (38) последовательно получаем

$$\begin{aligned}
& \prod_{\gamma=0}^{p-1} u'_{1/p, \gamma/p} / \prod_{\delta=1}^{p-1} u'_{0, \delta/p} \\
&= u'_{1/p, 0} \prod_{\delta=1}^{(p-1)/2} (u'^2_{1/p, 0} u'^2_{0, \delta/p} - b_{(\alpha/M)}) / \prod_{\delta=1}^{(p-1)/2} (u'^2_{1/p, 0} - u'^2_{0, \delta/p}) u'^2_{0, \delta/p} \\
&= u'_{1/p, 0} \prod_{\delta=1}^{(p-1)/2} (1 - b_{(\alpha/M)} u'^{-2}_{1/p, 0} u'^{-2}_{0, \delta/p}) / (1 - u'^2_{0, \delta/p} u'^{-2}_{1/p, 0}) \\
&\equiv u'_{1/p, 0} (1 - b_{(\alpha/M)} u'^{-2}_{1/p, 0} u'^{-2}_{0, (M-1)/2M} + u'^2_{0, 1/p} u'^{-2}_{1/p, 0}) (q_1^{2+a+d(2+b)}),
\end{aligned}$$

a, b целые рациональные, $a, b \geq 0$, $a + b > 0$, $d = c/p^k$,

$$\begin{aligned}
A &\equiv \prod_{d=1}^{(p-1)/2} u'^{1/d^2}_{d/p, 0} \\
&\times \prod_{d=1}^{(p-1)/2} (1 - b_{(\alpha/M)} u'^{-2}_{d/p, 0} u'^{-2}_{0, (M-1)/2M} + u'^{-2}_{d/p, 0} u'^2_{0, 1/p})^{1/d^2} (q_1^{2+a+d(2+b)}), \\
B &\equiv \prod_{d=1}^{(p-1)/2} (v'_{d/p, 0} / u'_{d/p, 0})^{1/d^2} \\
&\times \prod_{d=1}^{(p-1)/2} (1 + b_{(\alpha/M)} u'^{-2}_{1/p, 0} u'^{-2}_{0, (M-1)/2M} + u'^{-2}_{1/p, 0} u'^2_{0, 1/p}) (q_1^{2+a+d(2+b)}).
\end{aligned}$$

Следовательно,

$$M \equiv \prod_{d=1}^{(p-1)/2} (u'_{d/p, 0} v'_{d/p, 0})^{1/d^2} \prod_{d=1}^{(p-1)/2} (1 + 4u'^{-2}_{d/p, 0} u'^2_{0, 1/p})^{1/d^2} (q_1^{2+a+d(2+b)}), \quad (41)$$

$a, b \geq 0$ целые рациональные, $a + b > 0$, $d = c/p^k$.

Пусть $(1/q)$, $q = 1, 2, \dots, (p-1)/2$, – абсолютные наименьшие вычеты чисел $1/q$ по $\text{mod } p$; тогда для (40)

$$\begin{aligned}
M &= M_1 M_2^p, \quad M_2 \in Q(\varepsilon(p) + \varepsilon^{-1}(p), s'_1, \dots, s'_{(p-1)/2}), \\
M_1 &\equiv \prod_{d=1}^{(p-1)/2} (u'_{(1/d)/p, 0} v'_{(1/d)/p, 0})^{d^2} \\
&\times \prod_{d=1}^{(p-1)/2} (1 + 4u'^{-2}_{(1/d)/p, 0} u'^2_{0, 1/p})^{d^2} (q_1^{2+a+d(2+b)}).
\end{aligned} \quad (42)$$

Если обозначить уравнение, которому удовлетворяют все точки порядка p изогенной кривой $G_{(\alpha/M)}$, через $W_p(u') = 0$, то, как в (35) и (36),

$$\begin{aligned} W_p(u') &\equiv u'^{p^2-p} \{ (v'/u' + \sqrt{a_{(\alpha/M)}})^p - (v'/u' - \sqrt{a_{(\alpha/M)}})^p \} (b_{(\alpha/M)}), \\ (\varepsilon^t - \varepsilon^{-t})^2 u'_{t/p,0} &\equiv 4a_{(\alpha/M)} (q_t^{mc/p^k}), \quad \varepsilon = \varepsilon(p), \\ (\varepsilon^t - \varepsilon^{-t})^2 v'_{t/p,0} / u'_{t/p,0} &\equiv (\varepsilon^t + \varepsilon^{-t})^2 a_{(\alpha/M)} (q_t^{mc/p^k}). \end{aligned} \quad (43)$$

Из (42) и (43) имеем

$$\begin{aligned} \prod_{d=1}^{(p-1)/2} (u'_{(1/d)/p,0} v'_{(1/d)/p,0})^{2d^2} &\equiv L_1^p(b_{(\alpha/M)}), \\ \prod_{d=1}^{(p-1)/2} (u'_{(1/d)/p,0} v'_{(1/d)/p,0})^{2d^2} &= L_1^p(1 + N_1) = L_1^p(1 + b_{(\alpha/M)} u'_{1/p,0}^{-4} L_2'), \\ \nu_{q_1}(L_2') &\geq 0, \quad \nu_{q_1}(N_1) \geq 4 + pd, \\ \prod_{d=1}^{(p-1)/2} (1 + 4u'_{0,1/p} u'^{-2}_{(1/d)/p,0})^{2d^2} &\equiv 1 + 8u'_{0,1/p} \sum_{d=1}^{(p-1)/2} d^2 u'^{-2}_{(1/d)/p,0} (q_1^{2+a+(2+b)d}). \end{aligned} \quad (44)$$

Из (43) и (44) следует

$$\nu_{q_1} \left(8u'_{0,1/p} \sum_{d=1}^{(p-1)/2} d^2 u'^{-2}_{(1/d)/p,0} \right) = 2 + 2d.$$

Так как $4 + pd > 2 + 2d$, то $M_1 = 1 + N = (L^2/L_1)^p = L_2^p$, $\nu_q(M-1) = 2 + 2d = \nu_{q_1}(L_2^p - 1)$,

$$L^2 \in Q(\varepsilon(p) + \varepsilon^{-1}(p), s'_1, \dots, s'_{(p-1)/2}). \quad (45)$$

Подберем k таким, чтобы $d = c/p^k < 1$. Тогда из (45) получаем

$$2 + 2d = 2 + 2c/p^k = pd\alpha = c\alpha/p^{k-1},$$

α натуральное, $c \equiv 0(p^k)$, что при фиксированном $c > 0$ и произвольном k невозможно. Следовательно, $p^t \leq 5$. Предложение 5 доказано.

Аналогичным образом, т.е. с использованием предложения 2 и лемм 1–5, доказывается

ПРЕДЛОЖЕНИЕ 6. Если для кривой F $r, s \in Q(\varepsilon(m))$, $(D/q_t^{12\alpha}, p) \neq 1$ и $O_{(\alpha/m)} \in Q(\varepsilon(p^l))$, l произвольное, то $m \leq 7$.

Невозможность, наконец, случаев $\{o_{5,1}, o_{5,2}\} \in Q(\varepsilon(5))$ (для кривой G) и $\{O_{7,1}, O_{7,2}\} \in Q(\varepsilon(7))$ (для кривой F) приведена в предложениях 1, 2 статьи [9]. Для последнего же случая $\{O_{5,1}, O_{5,2}\} \in Q(\varepsilon(5))$ (для кривой F) непосредственным вычислением получаем

$m = 5$:

$$\begin{aligned}
 -r &= 27(c^4 + 12c^3d + 14c^2d^2 - 12cd^3 + d^4)\rho^4, \\
 s &= 54(c^6 + 18c^5d + 75c^4d^2 + 75c^2d^4 - 18cd^5 + d^6)\rho^6, \\
 c &= \alpha^5 + (\varepsilon + \varepsilon^{-1})^5\beta^5, \quad d = (\varepsilon + \varepsilon^{-1})^5\alpha^5 + \beta^5, \quad \varepsilon = \varepsilon(5), \\
 O_{5,1} &= \{x_{1/5,0}, y_{1/5,0}\} = \{3(c^2 + 6cd + d^2)\rho^2, 108cd^2\rho^3\}, \\
 x_{\gamma/5,1/5} &= \sum_{i=0}^4 a_i \varepsilon^{\gamma^i} L^i, \quad \gamma = 0, 1, 2, 3, 4, \quad \varepsilon = \varepsilon(5), \\
 L &= \sqrt[5]{(2c + (11 - 5\sqrt{5})d) / (2c + (11 + 5\sqrt{5})d)}, \\
 2y_{1/5,0}y_{0,1/5} &= -x_{1/5,1/5}(x_{1/5,0} - x_{0,1/5})^2 \\
 &\quad + (x_{1/5,0} + x_{0,1/5})(r + x_{1/5,0}x_{0,1/5}) + 2s, \\
 \rho, \alpha, \beta, a_i, L &\in Q(\varepsilon(p^l)).
 \end{aligned} \tag{46}$$

Из (22), (24), (46) и предложений 1–6 следует справедливость теорем 1 и 2.

Список литературы

1. Демьяненко В. А. О структуре эллиптических полей. I // Изв. АН СССР. Сер. матем. 1985. Т. 49. №4. С. 719–730.
2. Демьяненко В. А. Явное описание изогении эллиптических кривых // Тр. ИММ УрО РАН. 1992. Т. 1. С. 13–19.
3. Демьяненко В. А. О структуре групп точек кручения на производных кривых // Исследования по теории групп. Свердловск, 1984. С. 51–60.
4. Демьяненко В. А. Кручение эллиптических кривых // Изв. АН СССР. Сер. матем. 1971. Т. 35. №2. С. 280–307.
5. Демьяненко В. А. О точных оценках порядков кручения точек кривых первого рода // Зап. научн. сем. ЛОМИ. 1986. Т. 151. С. 57–65.
6. Башмаков М. И., Кириллов А. С. Рациональные точки на одной модулярной кривой в круговом 2-расширении // Зап. научн. сем. ЛОМИ. 1976. Т. 57. С. 5–7.
7. Демьяненко В. А. О делении эллиптических функций // Матем. заметки. 1985. Т. 37. №1. С. 99–102.
8. Башмаков М. И., Аль-Надер Н. Ж. Поведение кривой в круговом Γ -расширении // Матем. сб. 1973. Т. 90. №1. С. 117–130.
9. Демьяненко В. А. Эллиптические функции и уравнение Ферма // Матем. сб. 1992. Т. 183. №9. С. 15–28.
10. Демьяненко В. А. Кручение эллиптических кривых // Актуальные проблемы аналит. теории чисел. Минск: Наука и техника, 1974. С. 49–80.

Поступило в редакцию
16.V.1996