

О ТОЧНЫХ ОЦЕНКАХ ПОРЯДКОВ КРУЧЕНИЯ ТОЧЕК КРИВЫХ
ПЕРВОГО РОДА

Пусть κ - алгебраическое числовое поле степени n относительно поля рациональных чисел \mathbb{Q} , \mathcal{F} и \mathcal{G} - соответственно кривые $y^2 = x^3 + rx + s$ и $v^2 = u^4 + au^2 + b$, определенные над κ ; r, s, a, b - целые числа, $4r^3 + 27s^2 = D$, $b^2(a^2 - 4b) = d$, $Dd \neq 0$.

Пусть $\kappa(P_1, P_2, \dots)$ - поле, полученное присоединением к полю κ координат точек P_1, P_2, \dots ; O_m, O'_m и o_m, o'_m - базисы групп всех точек порядка m на \mathcal{F} и \mathcal{G} , $\alpha_1 O_m + \alpha_2 O'_m =$

$$\{x_{\alpha_1/m, \alpha_2/m}, y_{\alpha_1/m, \alpha_2/m}\} = \{x_{(\alpha/m)}, y_{(\alpha/m)}\}, \alpha_1 O_m + \alpha_2 O'_m =$$

$$\{u_{\alpha_1/m, \alpha_2/m}, v_{\alpha_1/m, \alpha_2/m}\} = \{u_{(\alpha/m)}, v_{(\alpha/m)}\}, \kappa'(P_1, P_2, \dots) -$$

минимальное поле, в котором все дивизоры из $\kappa(P_1, P_2, \dots)$ - главные.

Известно [1], что всякая плоская кривая рода 1, определенная над κ и имеющая κ -рациональную точку, может быть приведена над этим полем к виду кривой \mathcal{F} .

В настоящей статье приводится схема доказательства следующего утверждения.

ТЕОРЕМА. Пусть p - простое число, большее 3. Если $\kappa(O_{p^t}) = \kappa$, то $\varphi(p^t) = p^{t-1}(p-1) \leq 6n$, если же $\kappa(O_{p^t}) = \kappa$, то $\varphi(p^t) \leq 4n$.

Предварительно будем изучать кручение на якобиевой кривой, так как формулы сложения точек на \mathcal{G} более просты по конструкции, а затем уже с помощью одного дополнительного соображения получим аналогичные результаты и для кривой \mathcal{F} .

Для удобства записи формул элементы поля $\kappa(P_1, P_2, \dots)$ будем обозначать рукописными буквами, а элементы поля $\kappa'(P_1, P_2, \dots)$, соответствующие с точностью до ассоциированности дивизорам из $\kappa(P_1, P_2, \dots)$, - печатными.

Прежде всего заметим, что u, v, w , связанные между собой соотношениями $u/w = u$, $v/w^2 = v$, где $v^2 = u^4 + au^2 + b$, определяют одну и ту же точку $P = \{u, v\}$. Поэтому решениям $\{u, v, w\} = \{\pm 1, \pm 1, 0\}$ уравнения $v^2 = u^4 + au^2 w^2 + b$

\mathcal{W}^4 соответствуют две бесконечно удаленные точки $O = \{1:0, 1:0^2\}$, $O' = \{1:0, -1:0^2\}$. Примем за нуль произвольной аддитивной группы точек на \mathcal{Y} бесконечно удаленную точку O . В этом случае, если $t\mathcal{P} = \{u_t, v_t\}$, то $-t\mathcal{P} = \{-u_t, v_t\}$.

ЛЕММА 1. Если $\{u_{(\alpha/m)}, v_{(\alpha/m)}\}$ - примитивная κ - точка порядка m на \mathcal{Y} , то при $\varphi(m) > n$ $u_{(\alpha/m)}, v_{(\alpha/m)}$ - целые.

ЛЕММА 2. Если $\{u_{(\alpha/m)}, v_{(\alpha/m)}\}$ - примитивная κ - точка порядка m , то при $\varphi(m) > 4n$

$$u_{(\alpha/m)} = qU_{(\alpha/m)}, \quad v_{(\alpha/m)} = q^2V_{(\alpha/m)}, \quad a = q^2a, \quad b = q^4b, \quad (1)$$

где $a, b, q, U_{(\alpha/m)}, V_{(\alpha/m)}$ - целые числа и $(a, b) = 1$.

Пусть $m = p^t$, где p - простое нечетное число и

$$W_{p^t}(u) = \sum_{i=0}^{p^{2t-2}(p^2-1)} b_i u^{p^{2t-2}(p^2-1)-i} = 0 \quad (2)$$

есть уравнение, которому удовлетворяют координаты u всех примитивных точек порядка p^t кривой \mathcal{Y} .

ЛЕММА 3. b_i, b'_i - многочлены от переменных a, b с целыми рациональными коэффициентами, причем

$$b_i \equiv b_{\varphi(p^t)} \cdot b'_i \pmod{p} \quad i = 0, 1, \dots, p^{2t-2}(p^2-1)-1. \quad (3)$$

ЛЕММА 4. Для любого натурального числа $t < m/2$

$$u_{t/m,0} = \varepsilon_t P_0 \sigma_0 T_{(m,t)}^{(-1)} \prod_{d_i \parallel m} \prod_{j=1}^{[d_i/2]} A_{d_i,j}^{\{t_j/d_i\} d_i},$$

$$v_{t/m,0} / u_{t/m,0} = \varepsilon'_t P'_0 \sigma'_0 T_{(m,t)}^{-1} \prod_{d_i \parallel m} \prod_{j=1}^{[d_i/2]} B_{d_i,j}^{\{t_j/d_i\} d_i}, \quad (4)$$

$$b = \sigma_0^4 P_0^4 \prod_{d_i \parallel m} \prod_{j=1}^{[d_i/2]} A_{d_i,j}^{d_i} \cdot c,$$

$$a^2 - 4b = \sigma_0^4 P_0^4 \prod_{d_i \parallel m} \prod_{j=1}^{[d_i/2]} B_{d_i,j}^{d_i} \cdot d,$$

где $\{c\}$ - расстояние от c до ближайшего целого числа, $\varepsilon_t, \varepsilon'_t, \dots$,
 d - целые числа из $\kappa'(O_m)$, $1 \equiv 0 \pmod{\varepsilon_t \varepsilon'_t}$, $4 \equiv 0 \pmod{\sigma_0^2 \sigma_0'}$,
 $A_{d_i, j}, B_{d_i, j}, c, d$ попарно взаимно просты, $m \equiv 0 \pmod{T_{(m, t)}}$,
 $T_{(m, t)} = 1$ в случае $m/(m, t) \neq p^2, 2p^2$ (p - простое число).

ЛЕММА 5. Для любых целых рациональных чисел α_1 и α_2 ,
 при которых порядок точки $\{u_{(\alpha/m)}, v_{(\alpha/m)}\}$ отличен от 2,

$$u_{(\alpha/m)} = \varepsilon_{(\alpha/m)} P_0 \sigma_0 T_{(\alpha_1, \alpha_2, m), \alpha_1/\alpha_2}^{(-1) \frac{m/d_2, \alpha_2, m}{m}} \prod_{i=0}^{[m/2]} \prod_{j=0}^{m-1} A_{i, j}^{\left\{ \frac{\alpha_1 i + \alpha_2 j}{m} \right\} m},$$

$$v_{(\alpha/m)} / u_{(\alpha/m)} = \varepsilon'_{(\alpha/m)} P_0 \sigma_0' T_{(\alpha_1, \alpha_2, m), \alpha_1/\alpha_2}^{-1} \prod_{i=0}^{[m/2]} \prod_{j=0}^{m-1} B_{i, j}^{\left\{ \frac{\alpha_1 i + \alpha_2 j}{m} \right\} m}, \quad (5)$$

$$b = \sigma_0^4 P_0^4 \prod_{i=0}^{[m/2]} \prod_{j=0}^{m-1} A_{i, j}^m,$$

$$a^2 - 4b = \sigma_0'^4 P_0^4 \prod_{i=0}^{[m/2]} \prod_{j=0}^{m-1} B_{i, j}^m,$$

где (a, b, c) - н.о.д. чисел a, b, c ; $a, \varepsilon_{(\alpha/m)}, \dots, B_{i, j}$
 удовлетворяют условиям, указанным в соотношениях (4).

ЛЕММА 6. Пусть $\alpha \mathcal{P} + \beta O_m = \{u_{\alpha, \beta/m}, v_{\alpha, \beta/m}\}$, где \mathcal{P} -
 произвольная, а O_m - примитивная нечетного порядка m точки на
 \mathcal{E}' . Тогда на кривой

$$\mathcal{E}' = (\mathcal{E}', O_m): v'^2 = u'^4 + a' u'^2 + b', \quad b' = b^m / \prod_{\delta=1}^{m-1} u_{0, \delta/m}^4,$$

$$a' = ma + 2 \sum_{\delta=1}^{m-1} b / u_{0, \delta/m}^2 - (a^2 - 4b) \sum_{\delta=1}^{m-1} u_{0, \delta/m}^2 / v_{0, \delta/m}^2$$

расположены точки $\mathcal{P}' = \alpha \mathcal{P}' = (\alpha \mathcal{P}, O_m) = \alpha(\mathcal{P}, O_m) = \{u'_\alpha, v'_\alpha\} =$

$$\left\{ \prod_{\gamma=0}^{m-1} u_{\alpha, \gamma/m} / \prod_{\delta=1}^{m-1} u_{0, \delta/m}, \prod_{\gamma=0}^{m-1} v_{\alpha, \gamma/m} / \prod_{\delta=1}^{m-1} v_{0, \delta/m} \right\}.$$

ЛЕММА 7. Если O_m, O'_m - базис группы всех точек поряд-
 ка m на \mathcal{E}' , то $(O'_m, O_m) = O_{m, 1}, (O_{m, 2}, O_m) = O'_{m, 1} (m O_m^2 = O_m)$;
 - базис группы всех точек порядка m на \mathcal{E}' .

ЛЕММА 8. $a_i = \sum_{\delta=1}^{m-1} u_{0, \delta/m}^{2i}$ ($i=2, 3, \dots$) удовлетворяют рекур-
 рентным соотношениям

$$\frac{(2i+3)(2i+5)}{6} a_{i+2} = -2a a_{i+1} - 3b a_i + \frac{1}{2} b^2 a_{i-2} +$$

$$\frac{1}{i-1} \sum_{j=1}^{i-1} \left\{ \frac{1}{2} (2j+1)(2i-2j+1) a_{j+1} a_{i-j+1} + 2j(2i-2j+1) a (-2a_{i+1} +$$

$$a_j a_{i-j+1}) + (2j-1)(2i-2j+1) b (a_{j-1} a_{i-j+1} - 2a_i) + 2j(i- \quad (6)$$

$$j)(a_j a_{i-j} - 2a_i) + 2(i-j)(2j-1) a b (a_{j-1} a_{i-j} - 2a_{i-1}) +$$

$$+ \frac{1}{2} (2j-1)(2i-2j-1) b^2 (a_{j-1} a_{i-j-1} - 2a_{i-2}) \Big\}.$$

ПРЕДЛОЖЕНИЕ I. Пусть p - простое число и 0 - примитивная K - точка. Если $p \neq 2, 3$ и $\varphi(p^t) > 4n$, то $d = b^2(a^2 - 4b)$, $(a, b) = 1$, $d^{p^{t-1}} \equiv 0 \pmod{p}$.

В основе доказательства предложения I лежит следующий факт. Если $p \equiv 0 \pmod{p}$, $(d, p) = 1$ и $a^{p^t} \equiv a$, $b^{p^t} \equiv b$,

$$U_{1/p^t, 0} \equiv U_{1/p^t, 0} \pmod{p}, \text{ то в уравнении (2) } b_i = b_i / q^i \equiv 0 \pmod{p}$$

$$(i=0, 1, \dots, p^{2t-2}(p^2-1)-1; i \neq \varphi(p^t)),$$

$(b_{\varphi(p^t)}, b_{p^{2t-2}(p^2-1)}, p) = 1$, что при $p \geq 5$ невозможно. Если же $p \equiv 0 \pmod{p}$, $(d, p) = 1$, $a^{p^t} \equiv a$, $b^{p^t} \equiv b$,

$$U_{1/p^t, 0} \equiv U_{1/p^t, 0} \pmod{p}, \text{ то } a_{\mu i} = a_{\mu i} / q^{2\mu i} \equiv 0 \pmod{p},$$

$\mu = (p^t - 1) / (p - 1)$, $i = 1, 2, \dots, c$, $c > 4$, что противоречит (6).

Пусть P_1, P_2 - произвольные, 0_m - примитивная нечетного порядка m , точки на \mathcal{U} и $P_1 + d0_m = \{u_{1, \alpha/m}, v_{1, \alpha/m}\}$, $P_2 + d0_m = \{u_{1, \alpha/m}, v_{1, \alpha/m}\}$. Суммы $\sum_{\delta_1, \dots, \delta_i} u_{1, \delta_1/m}^2 \dots u_{1, \delta_i/m}^2$, $\sum_{\gamma_1, \dots, \gamma_i} u_{1, \gamma_1/m}^2 \dots u_{1, \gamma_i/m}^2$, $\sum_{\delta_1, \dots, \delta_i} u_{1, \delta_1/m} \dots u_{1, \delta_i/m}$, $\sum_{\gamma_1, \dots, \gamma_i} u_{1, \gamma_1/m} \dots u_{1, \gamma_i/m}$, где $\delta_1, \dots, \delta_i; \gamma_1, \dots, \gamma_i$ пробегает все возможные наборы различных чисел из множеств $\{1, 2, \dots, m-1\}$, $\{0, 1, \dots, m-1\}$, обозначим соответственно через $c_i, b'_{i,1}, b'_{i,1}$.

ЛЕММА 9.

$$(b_{i,1} - b'_{i,1}) / (b_{i,1} - b'_{i,1}) = c_{i-1} \quad (i=1, 2, \dots, m-1) \quad (7)$$

ЛЕММА 10. Координаты точек $t0_{m,1} = \{u_{t/m,0}, v_{t/m,0}\}$ ($t=1, 2, \dots, m-1$) можно представить в виде

$$u_{t/m,0}' = \sum_{i=0}^{[m/2]} a_{0,i} (\varepsilon^t - \varepsilon^{-t})^{2i-1}, \quad v_{t/m,0}' = \sum_{i=0}^{[m/2]} b_{0,i} (\varepsilon^t - \varepsilon^{-t})^{2i-2} \quad (8)$$

$$(m,t) = (m,2) = 1, \quad \varepsilon = e^{2\pi i/m},$$

где $a_{0,i}, b_{0,i}$ - целые числа из $\kappa(O_m)$.

ЛЕММА II. Координаты точек $l_{0,m,1} + o_{m,1}$ кривой y' можно представить в виде

$$u_{l/m,1/m}' = \sum_{j=0}^{m-1} c_{0,j} \varepsilon^{lj} \alpha^j, \quad v_{l/m,1/m}' = \sum_{j=0}^{m-1} d_{0,j} \varepsilon^{lj} \alpha^j, \quad (9)$$

$$\alpha = \sqrt[m]{\beta}, \quad \beta = 2u_{1/m,0}' v_{1/m,0}' \prod_{t=2}^{m-2} (u_{1/m,0}' - u_{t/m,0}')$$

ЛЕММА I2. Если $\kappa(O_{r^t}) = \kappa$, $\varphi(r^t) > 4n$, то

$$\sum_{i=2}^{[m/2]} a_{0,i} (\varepsilon^t - \varepsilon^{-t})^{2i-1} \equiv 0 \pmod{(1-\varepsilon)^{2\ell}}, \quad \ell > 4. \quad (10)$$

Из (7)-(10) следует

ПРЕДЛОЖЕНИЕ 2. Пусть r - простое число и O_{r^t} - примитивная κ - точка. Если $r \neq 2, 3$, $d^{r^t-1} \equiv 0 \pmod{r}$, то $\varphi(r^t) \leq 4n$.

Примем за нуль произвольной аддитивной группы точек на \mathcal{F} бесконечно удаленную точку O . Тогда, если $tP = \{x_t, y_t\}$, то $-tP = \{x_t, -y_t\}$.

ЛЕММА I'. Если $\{x_{(d/m)}, y_{(d/m)}\}$ - примитивная κ - точка порядка m на \mathcal{F} , то при $\varphi(m) > n$ $x_{(d/m)}, y_{(d/m)}$ - целые числа.

ЛЕММА 2'. Если $\{x_{(d/m)}, y_{(d/m)}\}$ - примитивная κ - точка порядка m , то при $\varphi(m) > 6n$

$$x_{(d/m)} = Q^2 X_{(d/m)}, y_{(d/m)} = Q^3 Y_{(d/m)}, r = Q^4 r, s = Q^6 s, \quad (I')$$

где $r, s, X_{(d/m)}, Y_{(d/m)}$ - целые числа и $(r, s) = 1$.

Если $m = r^t$ (r - простое нечетное число), то уравнение, которому удовлетворяют координаты x всех примитивных точек порядка r^t , имеет вид

$$\sum_{i=0}^{\rho^{2t-2}(\rho^2-1)/2} c_i x^{\rho^{2t-2}(\rho^2-1)/2-i} = 0, \quad (2')$$

где c_i - многочлены от γ , S с целыми рациональными коэффициентами.

ЛЕММА 3'. c_i, c'_i - многочлены от γ, S с целыми рациональными коэффициентами, причем

$$c_i \equiv c_{\varphi(\rho^t)/2} c'_i \pmod{\rho}, \quad i=0,1,\dots,\rho^{2t-2}(\rho^2-1)/2-1. \quad (3')$$

ЛЕММА 4'. Для любого натурального числа $t < m/2$

$$y_{t/m,0} = \varepsilon_t c_0^3 L_0 T_{(m/t)}^{-3+4(1-e)} \prod_{d_i \parallel m} \prod_{j=1}^{[d_i/2]} C_{d_i,j}^{\{t_j/d_i\} d_i}, \quad (4')$$

$$D = c_0^{12} L_0^4 \prod_{d_i \parallel m} \prod_{j=1}^{[d_i/2]} C_{d_i,j}^{d_i} \cdot d, \quad ,$$

где $\{c\}$ - та же функция, что и в лемме 4, e - абсолютный наименьший вычет числа $m/(m,t)$ по $\text{mod } 2$; $\varepsilon_t, c_0, L_0, C_{d_i,j}, d$ - целые числа из $\kappa'(O_m)$, $1 \equiv 0 \pmod{\varepsilon_t}$, $4 \equiv 0 \pmod{L_0}$, $d_{i,j}, C_{d_i,j}, d$ попарно взаимно просты, $m \equiv 0 \pmod{T_{(m,t)}}$, $T_{(m,t)} = 1$ в случае $m/(m,t) \neq \rho^2, 2\rho^2$ (ρ - простое число).

ЛЕММА 5'. Для любых целых рациональных α_1 и α_2 , при которых порядок точки $\alpha_1 O_m + \alpha_2 O_m$ отличен от 2,

$$y_{(\alpha/m)} = \varepsilon_{(\alpha/m)} c_0^3 L_0 T_{(\alpha_1, \alpha_2, m)}^{-3+4(1-e)} \prod_{i=0}^{[m/2]} \prod_{j=0}^{m-1} C_{i,j}^{\{\frac{\alpha_1 i + \alpha_2 j}{m}\}}, \quad (5')$$

$$D = c_0^{12} L_0^4 \prod_{i=0}^{[m/2]} \prod_{j=0}^{m-1} C_{i,j}^m, \quad ,$$

где e - абсолютный наименьший вычет числа $m/(\alpha_1, \alpha_2, m)$ по $\text{mod } 2$, а целые из $\kappa'(O_m, O_m)$ $\varepsilon_{(\alpha/m)}, c_0, L_0, C_{i,j}$ удовлетворяют всем условиям, указанным в (4').

ЛЕММА 6'. Пусть $\alpha P + \beta O_m = \{x_{\alpha,\beta/m}, y_{\alpha,\beta/m}\}$, где P - произвольная, а O_m - примитивная нечетного порядка m точки на

\mathcal{F} . Тогда на кривой

$$\mathcal{F}' = (\mathcal{F}, O_m) : y'^2 = x'^3 + \tau'x' + s',$$

$$\tau' = \tau - 5 \sum_{\delta=1}^{m-1} (\tau + 3x_{0,\delta/m}^2), \quad s' = s - 7 \sum_{\delta=1}^{m-1} (2s + 3\tau x_{0,\delta/m} + 5x_{0,\delta/m}^3)$$

расположены точки $\mathcal{P}' = \alpha \mathcal{P}' = (\alpha \mathcal{P}, O_m) = \alpha(\mathcal{P}, O_m) = \{x'_\alpha, y'_\alpha\} =$
 $\left\{ \sum_{\gamma=0}^{m-1} x_{\alpha,\gamma/m} - \sum_{\delta=1}^{m-1} x_{0,\delta/m}, \prod_{\gamma=0}^{m-1} y_{\alpha,\gamma/m} / \prod_{\delta=1}^{m-1} y_{0,\delta/m} \right\}$.

ЛЕММА 7'. Если O_m, O'_m - базис группы всех точек порядка m на \mathcal{F} , то $(O'_m, O_m) = O_{m,1}, (O_{m,2}, O_m) = O_{m,1}'$,
 $(mO_{m,2} = O_m)$ - базис группы всех точек порядка m на \mathcal{F}' .

ЛЕММА 8'. $\mathcal{A}_i = \sum_{\delta=1}^{m-1} x_{0,\delta/m}^i$ ($i=2,3,\dots$) удовлетворяют рекуррентным соотношениям

$$\begin{aligned} \frac{(2i+3)(2i+5)}{6} \mathcal{A}_{i+2} &= -3\tau \mathcal{A}_i - 6s \mathcal{A}_{i-1} + \frac{1}{2} \tau^2 \mathcal{A}_{i-2} + \\ &+ \frac{1}{i-1} \sum_{j=1}^{m-1} \left\{ \frac{1}{2} (2j+1)(2i-2j+1) \mathcal{A}_{j+1} \mathcal{A}_{i-j+1} + (2j-1)(2i-2j+1) \tau (-2\mathcal{A}_i + \right. \\ &\left. \mathcal{A}_{j-1} \mathcal{A}_{i-j+1}) + (2j-2)(2i-2j+1) s (\mathcal{A}_{j-2} \mathcal{A}_{i-j+1} - 2\mathcal{A}_{i-1}) + \right. \\ &\left. + \frac{1}{2} (2j-1)(2i-2j-1) \tau^2 (\mathcal{A}_{j-1} \mathcal{A}_{i-j-1} - 2\mathcal{A}_{i-2}) + (2j-2)(2i-2j- \right. \\ &\left. - 1) \tau s (\mathcal{A}_{j-2} \mathcal{A}_{i-j-1} - 2\mathcal{A}_{i-3}) + (j-1)(2i-2j-2) s^2 (\mathcal{A}_{j-2} \mathcal{A}_{i-j-2} - \right. \\ &\left. - 2\mathcal{A}_{i-4}) \right\}, \quad \mathcal{A}_{-t} = 0 \quad (t > 0), \quad \mathcal{A}_0 = m-1. \end{aligned} \quad (6')$$

Пусть

$$\mathcal{Z}_m(x) = \sum_{i=0}^{[m/2]} c_i x^{[m/2]-i} = 0, \quad \mathcal{L}_m(y) = \sum_{i=0}^{[m/2]} d_i (y^2)^{[m/2]-i} = 0$$

- уравнения, которым удовлетворяют соответственно координаты

$$x_{h/m,0} \text{ и } y_{h/m,0} \quad (h=1,2,\dots).$$

ЛЕММА 8''

$$\sum_{i_1, \dots, i_4} \frac{([m/2] - i_4)!}{i_2! i_3! i_4!} z^{i_3} s^{i_4} d_{i_1} =$$

$$i_1 + i_2 + i_3 + i_4 = [m/2], \quad 3i_1 + 2i_3 + 3i_4 = T$$

$$= 2^e \sum_{j_1=0}^T \sum_{j_2=0}^{[j_1/2]} \sum_{j_3=0}^{[m/2]-j_1+j_2} \sum_{j_4=0}^{[j_1/2]-j_2} \sum_{j_5=0}^{j_4} (-2)^{-j_1-2j_2-j_4+2j_5} \quad (6'')$$

$$\cdot 3^{j_4-j_5} C_{[m/2]-j_1+j_2}^{j_3} C_{j_1-2j_2}^{2j_4} C_{j_4}^{j_5} C_{j_1-j_2} C_{j_2} C_{T-j_1-2j_3-2j_5}$$

$e=0$ при $j_1=2j_2$ и $e=1$ при $j_1 \neq 2j_2$.

ПРЕДЛОЖЕНИЕ 3. Пусть p - простое число и O_{p^t} - примитивная κ - точка на \mathcal{F} . Если $p \neq 2, 3$ и $\varphi(p^t) \geq 6n$, то $D = 4r^3 + 27s^2$, $(r, s) = 1$, $D^{p^t-1} \equiv 0 \pmod{p}$.

Доказательство предложения 3 по существу отличается от доказательства предложения I лишь использованием дополнительных соотношений (6').

Пусть P_1, P_2 - произвольные, O_m - примитивная нечетного порядка m точки на \mathcal{F} и $P_1 + \alpha O_m = \{x_{1,\alpha/m}, y_{1,\alpha/m}\}$, $P_2 + \alpha O_m = \{x_{2,\alpha/m}, y_{2,\alpha/m}\}$. Суммы $\sum_{\delta_1, \dots, \delta_i} x_{0,\delta_1/m} \dots x_{0,\delta_i/m}$, $\sum_{\delta_1, \dots, \delta_i} x_{1,\delta_1/m} \dots x_{1,\delta_i/m}$, где $\delta_1, \dots, \delta_i; \delta_1', \dots, \delta_i'$ пробегают все возможные наборы различных чисел из множеств $\{1, 2, \dots, m-1\}, \{0, 1, \dots, m-1\}$, обозначим соответственно через $C_i, B_{i,1}, B_{i,1}'$.

ЛЕММА 9''.

$$(B_{i,1} - B_{i,1}') / (B_{1,1} - B_{1,1}') = C_{i-1} \quad (7'')$$

$(i=1, 2, \dots, m)$

ЛЕММА 10''. Координаты точек $tO_{m,1} = \{x_{t/m,0}', y_{t/m,0}'\}$ ($t=1, 2, \dots, m-1$) можно представить в виде

$$x_{t/m,0}' = \sum_{i=0}^{[m/2]} A_{0,i} (\varepsilon^t - \varepsilon^{-t})^{2i-2}, \quad y_{t/m,0}' = \sum_{i=0}^{[m/2]} B_{0,i} (\varepsilon^t - \varepsilon^{-t})^{2i-3},$$

$$(m, t) = (m, 2) = 1, \varepsilon = e^{2\pi i/m}, A_{\alpha, i}, B_{\alpha, i} - \text{целые из } \kappa(O_m). \quad (8')$$

ЛЕММА II'. Координаты точек $\ell O_{m,1} + O'_{m,1}$ кривой F' можно представить в виде

$$x_{\ell/m, 1/m} = \sum_{j=0}^{m-1} C_{\alpha, j} \varepsilon^{\ell j} \eta^j, \quad y_{\ell/m, 1/m} = \sum_{j=0}^{m-1} D_{\alpha, j} \varepsilon^{\ell j} \eta^j, \quad (9')$$

$$\eta = \sqrt[m]{\xi}, \quad \xi = 2y_{1/m, 0} \prod_{t=2}^{[m/2]} (x_{1/m, 0} - x_{t/m, 0}).$$

ЛЕММА I2'. Если $\kappa(O_{p^t}) = \kappa$ и $\varphi(p^t) > 6n$, $D^{p^t-1} \equiv 0 \pmod{p}$, то

$$\sum_{i=2}^{[p^t/2]} B_{\alpha, i} (\varepsilon^t - \varepsilon^{-t})^{2i-3} \equiv 0 \pmod{(1-\varepsilon)^{2\ell}}, \quad \ell > 6. \quad (10')$$

Из лемм 7' - I2' следует.

ПРЕДЛОЖЕНИЕ 4. Пусть p - простое число и O_{p^t} - примитивная κ - точка. Если $p \neq 2, 3$, $D^{p^t-1} \equiv 0 \pmod{p}$, $\varphi(p^t) \leq 6n$.

Из предложений I-4 вытекает справедливость теоремы.

Заметим, что полученные оценки уже не являются улучшаемыми.

Например, при $n=1$ имеем

$$1) p=5. \quad v^2 = u^4 + \alpha u^2 + \beta, \quad \alpha = (t^2+1)(t^4-2t^3-6t^2+2t+1),$$

$$\beta = 16t^5(t^2+t-1), \quad O_5 = \{2t, 2t(t-1)(t+1)^2\}, \quad t \in \mathbb{Q}, \quad \varphi(p) = \varphi(5) = 4 = 4n.$$

$$2) p=7. \quad y^2 = x^3 + \gamma x + \delta, \quad -48\gamma = t^8 + 12t^7 + 42t^6 + 56t^5 + 35t^4 -$$

$$-14t^2 - 4t + 1, \quad 864\delta = t^{12} + 18t^{11} + 147t^{10} + 354t^9 + 570t^8 + 486t^7 +$$

$$273t^6 + 222t^5 + 174t^4 + 46t^3 - 15t^2 - 6t + 1, \quad O_7 = \{(t^4 + 6t^3 + 15t^2 + 10t + 1)/12, t(t+1)^3/2\}, \quad t \in \mathbb{Q}, \quad \varphi(p) = \varphi(7) = 6 = 6n.$$

Литература

I. Пуанкаре А. Избранные труды. М., 1972, т.2. 999 с.