Math-Net.Ru

Общероссийский математический портал

В. А. Демьяненко, Эллиптические функции и кривая Ферма, *Матем. заметки*, 1996, том 60, выпуск 4, 606–608

DOI: <https://doi.org/10.4213/mzm1869>

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: 35.174.16.151

26 апреля 2023 г., 18:34:05

ЭЛЛИПТИЧЕСКИЕ ФУНКЦИИ И КРИВАЯ ФЕРМА

В. А. Демьяненко

Пусть $\mathbb{k}$ – алгебраическое числовое поле, $\mathcal{F}$ – кривая $y^2 = x^3 + rx + s$, определенная над $\mathbb{k}$, $4r^3 + 27s^2 \neq 0$, $\{\mathcal{C}_{m,1}(\mathcal{F}), \mathcal{C}_{m,2}(\mathcal{F})\}$ – базис всех точек порядка m на $\mathcal{F}$ и

$$\begin{aligned}\alpha_1 \mathcal{C}_{m,1}(\mathcal{F}) + \alpha_2 \mathcal{C}_{m,2}(\mathcal{F}) &= \{x_{\alpha_1/m, \alpha_2/m}, y_{\alpha_1/m, \alpha_2/m}\} \\ &= \{x(\alpha/m), y(\alpha/m)\}.\end{aligned}$$

Цель настоящей заметки – доказательство следующих теорем.

ТЕОРЕМА 1. Если $\mathcal{C}_{2^5,1}(\mathcal{F}) \in \mathbb{k}$, то кривая

$$Y^2 = X^3 - X \quad (1)$$

над полем $\mathbb{k}$ имеет точки

$$\begin{aligned}X &= \frac{b_{1/8,j}}{b_{1/8,1}} + \frac{b_{1/8,k}}{b_{1/8,k}}, \quad Y = (X-1) \frac{y'_{1/8,0} b_{1/16,1}}{y'_{1/16,0} b_{1/8,1}}, \quad \{j, k\} = \{2, 3\}, \{3, 2\}, \\ b_{1/2^t,i} &= (x'_{1/2^t,0} - \rho'_i)^2 - (\rho'_i - \rho'_j)(\rho'_i - \rho'_k), \\ t &= 3, 4, \quad i, j, k \in \{1, 2, 3\}, \quad i \neq j \neq k, \\ x'_{1/2^t,0} &= x_{1/2^{t+1},0} + x_{1/2^{t+1}+1/2,0} - x_{1/2,0}, \\ y'_{1/2^t,0} &= y_{1/2^{t+1},0} + y_{1/2^{t+1}+1/2,0}, \\ \rho'_1 &= 2x_{1/4,0} - x_{1/2,0}, \quad \rho'_2 = -2x_{1/2,0}, \quad \rho'_3 = 3x_{1/2,0} - 2x_{1/4,0}.\end{aligned} \quad (2)$$

ТЕОРЕМА 2. Если $\mathcal{C}_{3^3,1}(\mathcal{F}) \in \mathbb{k}$, то кривая

$$\mathcal{H} : x^3 + y^3 = 1 \quad (3)$$

над полем $\mathbb{k}(\sqrt{-3})$ имеет точки

$$\begin{aligned}x &= \frac{1}{2} \sqrt[3]{\frac{3r_{1/3} + 9x'^2_{1/3,0}}{x'^2_{1/3,0}}}, \quad y = -\frac{1}{2} \sqrt[3]{\frac{3r_{1/3} + x'^2_{1/3,0}}{x'^2_{1/3,0}}}, \\ \sqrt[3]{\frac{3r_{1/3} + x'^2_{1/3,0}}{x'^2_{1/3,0}}} &= \frac{1}{2} x'^{-1}_{1/3,0} \sum_{t=0}^2 \varepsilon^{-t}(3) x'_{t/3,1/3}, \\ \sqrt[3]{\frac{3r_{1/3} + 9x'^2_{1/3,0}}{x'^2_{1/3,0}}} &= \frac{1}{6} x'^{-1}_{1/3,0} \sum_{\alpha, \beta=0}^2 \varepsilon^{-\beta}(3) x'_{(3\alpha+1)/9, \beta/3},\end{aligned}$$

$$\begin{aligned}
 r_{1/3} &= -9r - 30x_{1/3,0}^2, & \varepsilon(3) &= e^{2\pi i/3}, \\
 x'_{1/9,0} &= \sum_{\gamma=0}^2 x_{1/27+\gamma/3,0} - 2x_{1/3,0}, \\
 y'_{1/9,0} &= \sum_{\gamma=0}^2 y_{1/27+\gamma/3,0}, & x'_{0,1/3} &= -3x_{1/3,0}, \\
 y'_{0,1/3} &= \sqrt{-3}y_{1/3,0} \frac{3r + x_{1/3,0}^2}{r + 3x_{1/3,0}^2}.
 \end{aligned} \tag{4}$$

Пусть $\varepsilon(n) = e^{2\pi i/n}$. По гипотезе Мазура [1], [2], если k -ранг кривой $\mathcal{F}$ равен r , то и $k(\varepsilon(n))$ -ранг $\mathcal{F}$ равен r .

По аналогии с гипотезой Мазура, на наш взгляд, справедлива следующая

ГИПОТЕЗА. Если $\mathcal{F} \in \mathbb{K}$ и порядок кручения $\mathcal{F}$ над $\mathbb{K}$ равен t , то и над полем $\mathbb{K}(\varepsilon(t))$ порядок кручения $\mathcal{F}$ равен t .

Например, в силу (2), (4) и [1], [2] имеем

ТЕОРЕМА 3. Пусть $\mathbb{Q}$ – поле рациональных чисел. Если $\mathcal{C}_{2^\alpha,1}(\mathcal{F}) \in \mathbb{Q}(\varepsilon(2^t))$ (t – произвольное), то $\alpha \leq 4$.

ТЕОРЕМА 4. Если $\mathcal{C}_{3^\beta,1}(\mathcal{F}) \in \mathbb{Q}(\varepsilon(3^t))$ (t – произвольное), то $\beta \leq 2$.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 1. Согласно [3] при $\mathcal{C}_{2^5,1}(\mathcal{F}) \in \mathbb{K}$ на кривой

$$\begin{aligned}
 \mathcal{F}' : y'^2 &= x'^3 r_{1/2} x' + s_{1/2}, \\
 r_{1/2} &= -4r - 15x_{1/2,0}^2, & s_{1/2} &= -13s - 21rx_{1/2,0} - 35x_{1/2,0}^3, \\
 \mathcal{C}_{2,1}(\mathcal{F}) &= \{x_{1/2,0}, 0\}, & x_{1/2,0}^3 + rx_{1/2,0} + s &= 0,
 \end{aligned} \tag{5}$$

имеются точки

$$\begin{aligned}
 \mathcal{C}_{2^4,1}(\mathcal{F}') &= \{x'_{1/16,0}, y'_{1/16,0}\} \\
 &= \{x_{1/32,0} + x_{1/32+1/2,0} - x_{1/2,0}, y_{1/32,0} + y_{1/32+1/2,0}\}, \\
 \mathcal{C}_{2,2}(\mathcal{F}') &= \{x'_{0,1/2}, y'_{0,1/2}\} = \{-2x_{1/2,0}, 0\}.
 \end{aligned} \tag{6}$$

Далее, пусть P' – произвольная точка на $\mathcal{F}'$ и $tP' = \{x'_t, y'_t\}$. Так как

$$2y'_t \sqrt{x'_t - \rho'_1} = (x'_t - \rho'_1)^2 - r_{1/2} - 3\rho'^2_{1/2}, \quad \rho'_1 = 2x_{1/4,0} - x_{1/2,0}, \tag{7}$$

то в силу (7) кривая $T: v^2 = u^4 + au^2 + b$, $a = 3\rho'_{1/2}$, $b = r_{1/2} + 3\rho'^2_{1/2}$, $\rho'^3_{1/2} + r_{1/2}\rho'_{1/2} + s_{1/2} = 0$, имеет точки $tQ = \{u_t, v_t\}$, $u_t = \pm \sqrt{x'_t - \rho'_1}$, $v_t = y'_t/u_t$, для которых аналогично (7) также имеем

$$\pm u_{2t} = \frac{u_t^4 - b}{2u_t v_t}, \quad v_{2t} = \frac{v_t^4 - (a^2 - 4b)u_t^4}{4u_t^2 v_t^2}. \tag{8}$$

Из (8) получаем

$$\left(\frac{v_t}{u_t}\right)^2 = \pm 2v_{2t} + a + 2u_{2t}^2, \quad u_t^2 = u_{2t}^2 \pm v_{2t} \pm u_t \left(\frac{v_t}{u_t}\right). \tag{9}$$

Полагая в (9) $t = 2, 4, \dots$ и учитывая (7), выводим

$$Y^2 = X^3 - X,$$

$$X = \frac{(x'_{1/8,0} - \rho'_2)^2 - (\rho'_2 - \rho'_1)(\rho'_2 - \rho'_3)}{(x'_{1/8,0} - \rho'_1)^2 - (\rho'_1 - \rho'_2)(\rho'_1 - \rho'_3)} + \frac{(x'_{1/8,0} - \rho'_2)^2 - (\rho'_2 - \rho'_1)(\rho'_2 - \rho'_3)}{(x'_{1/8,0} - \rho'_3)^2 - (\rho'_3 - \rho'_1)(\rho'_3 - \rho'_2)},$$

$$Y = \frac{(X-1)y'_{1/8,0}\{x'_{1/16,0} - \rho'_1\}^2 - (\rho'_1 - \rho'_2)(\rho'_1 - \rho'_3)}{y'_{1/16,0}\{(x'_{1/8,0} - \rho'_1)^2 - (\rho'_1 - \rho'_2)(\rho'_1 - \rho'_3)\}} \quad (10)$$

(6) и (10) дают (2). Теорема 1 доказана.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 2. Ввиду [3] при $\mathcal{C}_{3,1}(\mathcal{F}) \in \mathbb{K}$ на кривой

$$\mathcal{F}' : y'^2 = x'^3 + r_{1/3}x' + s_{1/3}, \quad r_{1/3} = -9r - 30x_{1/3,0}^2, \quad (11)$$

$$s_{1/3} = -27s - 42rx_{1/3,0} - 70x_{1/3,0}^3,$$

расположены точки

$$\mathcal{C}_{3,1}(\mathcal{F}') = \{x'_{1/9,0}, y'_{1/9,0}\}, \quad x'_{1/9,0} = \sum_{\gamma=0}^2 x_{1/27+\gamma/3,0} - 2x_{1/3,0},$$

$$y'_{1/9,0} = \sum_{\gamma=0}^2 y_{1/27+\gamma/3,0}, \quad \mathcal{C}_{3,2}(\mathcal{F}') = \{x'_{0,1/3}, y'_{0,1/3}\}, \quad (12)$$

$$x'_{0,1/3} = -3x_{1/3,0}, \quad y'_{0,1/3} = \sqrt{-3}y_{1/3,0} \frac{3r + x_{1/3,0}^2}{r + 3x_{1/3,0}^2}.$$

Далее, согласно [4] $u^3 - v^3 = 1$,

$$u = \frac{1}{2} \sqrt[3]{\frac{3r_{1/3} + 9x_{1/3,0}'^2}{x_{1/3,0}'^2}}, \quad v = \frac{1}{2} \sqrt[3]{\frac{3r_{1/3} + x_{1/3,0}'^2}{x_{1/3,0}'^2}},$$

$$\sqrt[3]{\frac{3r_{1/3} + x_{1/3,0}'^2}{x_{1/3,0}'^2}} = \frac{1}{2} x_{1/3,0}'^{-1} \sum_{t=0}^2 \varepsilon^{-t} (3) x_{t/3,1/3}', \quad (13)$$

$$\sqrt[3]{\frac{3r_{1/3} + 9x_{1/3,0}'^2}{x_{1/3,0}'^2}} = \frac{1}{6} x_{1/3,0}'^{-1} \sum_{\alpha, \beta=0}^2 \varepsilon^{-\beta} (3) x_{(3\alpha+1)/9, \beta/3}'.$$

Из (11)–(13) следуют соотношения (4). Теорема 2 доказана.

Институт математики и механики
Уральского отделения РАН

Поступило
06.02.96

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Башмаков М. И., Кириллов А. С. // Записки научн. семин. ЛОМИ. 1976. Т. 57. С. 5–7.
2. Башмаков М. И., Аль-Надер Н. Ж. // Матем. сб. 1973. Т. 90. № 1. С. 117–130.
3. Демьяненко В. А. // Тр. ИММ. 1992. Т. 1. С. 13–19.
4. Демьяненко В. А. // Матем. заметки. 1985. Т. 37. С. 99–102.