V. A. Dem'yanenko, On one property of elliptic curves, *Zap. Nauchn. Sem. LOMI*, 1981, Volume 106, 70–75

В.А.Демьяненко

ОБ ОДНОМ СВОЙСТВЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Пусть Γ – уравнение кривой Вейерштрасса

$$y^2 = 4x^3 - rx - s .$$

Цель настоящей заметки – доказательство следующего свойства точек кручения на Γ .

ТЕОРЕМА. Если $\mathcal{O}_p$, $\mathcal{O}'_p$ – базис группы всех точек порядка p на Γ (p – простое) и $\alpha\mathcal{O}_p + \beta\mathcal{O}'_p = \{x_{\alpha,\beta}, y_{\alpha,\beta}\}$, то

$$\prod_{i=1}^{[p/2]} \left\{ \prod_{j=0}^{p-1} y_{(1/i),j} \Big/ \prod_{j=1}^{[p/2]} y_{0,j}^2 \right\}^{i^2} = \mathcal{Z}^p , \qquad (I)$$

где $\mathcal{Z}$ – рациональная функция от $x_{1,0}$, $y_{1,0}$, $x_{0,1}$, $y_{0,1}$, r , s .

Так как при $p=2$ $y_{\alpha,\beta} = 0$, то достаточно ограничиться рассмотрением формулы (I) при $p \geqslant 3$. Для ясности рассуждений предварительно рассмотрим наиболее простые частные случаи. Пусть $p=3$ или $p=5$. Положим

при $p=3$:

$$y_{1,0} = \theta_{1,0}\theta_{1,1}\theta_{1,2}, \quad y_{1,1} = \theta_{1,0}\theta_{1,1}\theta_{0,1},$$
$$y_{1,2} = \theta_{1,0}\theta_{1,2}\theta_{0,1}, \quad y_{0,1} = \theta_{1,1}\theta_{1,2}\theta_{0,1}$$

при $p=5$:

$$\begin{aligned}
y_{1,0} &= (\theta_{1,0}\theta_{1,1}\theta_{1,2}\theta_{1,3}\theta_{1,4})(\theta_{2,0}\theta_{2,1}\theta_{2,2}\theta_{2,3}\theta_{2,4})^2,\\
y_{1,1} &= (\theta_{1,0}\theta_{0,1}\theta_{1,3}\theta_{2,2}\theta_{2,4})(\theta_{2,0}\theta_{0,2}\theta_{1,1}\theta_{1,2}\theta_{2,1})^2,\\
y_{1,2} &= (\theta_{1,0}\theta_{1,4}\theta_{0,2}\theta_{2,1}\theta_{2,2})(\theta_{2,0}\theta_{0,1}\theta_{1,1}\theta_{1,3}\theta_{2,3})^2,\\
y_{1,3} &= (\theta_{1,0}\theta_{1,1}\theta_{0,2}\theta_{2,3}\theta_{2,4})(\theta_{2,0}\theta_{0,1}\theta_{1,2}\theta_{1,4}\theta_{2,2})^2,\\
y_{1,4} &= (\theta_{1,0}\theta_{0,1}\theta_{1,2}\theta_{2,1}\theta_{2,3})(\theta_{2,0}\theta_{0,2}\theta_{1,3}\theta_{1,4}\theta_{2,4})^2,\\
y_{0,1} &= (\theta_{0,1}\theta_{1,1}\theta_{2,1}\theta_{2,4}\theta_{1,4})(\theta_{0,2}\theta_{1,2}\theta_{2,2}\theta_{1,3}\theta_{2,3})^2,
\end{aligned} \qquad (2)$$

$$y_{2,0} = (\beta_{1,0}\beta_{1,1}\beta_{1,2}\beta_{1,3}\beta_{1,4})^2 (\beta_{2,0}\beta_{2,1}\beta_{2,2}\beta_{2,3}\beta_{2,4}),$$

$$y_{2,1} = (\beta_{1,0}\beta_{1,1}\beta_{0,2}\beta_{2,3}\beta_{2,4})^2 (\beta_{2,0}\beta_{0,1}\beta_{1,2}\beta_{1,4}\beta_{2,2}),$$

$$y_{2,2} = (\beta_{1,0}\beta_{0,1}\beta_{1,3}\beta_{2,2}\beta_{2,4})^2 (\beta_{2,0}\beta_{0,2}\beta_{1,1}\beta_{1,2}\beta_{2,1}),$$

$$y_{2,3} = (\beta_{1,0}\beta_{0,1}\beta_{1,2}\beta_{2,1}\beta_{2,3})^2 (\beta_{2,0}\beta_{0,2}\beta_{1,3}\beta_{1,4}\beta_{2,4}),$$

$$y_{2,4} = (\beta_{1,0}\beta_{1,4}\beta_{0,2}\beta_{2,1}\beta_{2,2})^2 (\beta_{2,0}\beta_{0,1}\beta_{1,1}\beta_{1,3}\beta_{2,3}),$$

$$y_{0,2} = (\beta_{0,1}\beta_{1,1}\beta_{2,1}\beta_{2,4}\beta_{1,4})^2 (\beta_{0,2}\beta_{1,2}\beta_{2,2}\beta_{1,3}\beta_{2,3}).$$

Система (2) разрешима относительно $\beta_{i,j}$. Действительно, достаточно взять

при $p=3$:

$$\beta_{1,0} = (y_{1,0}y_{1,1}y_{1,2}y_{0,1}^{-2})^{1/3}, \quad \beta_{1,1} = (y_{1,0}y_{1,1}y_{1,2}^{-2}y_{0,1})^{1/3},$$
$$\beta_{1,2} = (y_{1,0}y_{1,1}^{-2}y_{1,2}y_{0,1})^{1/3}, \quad \beta_{0,1} = (y_{1,0}^{-2}y_{1,1}y_{1,2}y_{0,1})^{1/3},$$

при $p=5$:

$$\frac{\beta_{2,0}}{\beta_{1,0}} = \left(\frac{y_{1,0}y_{1,1}y_{1,2}y_{1,3}y_{1,4}}{y_{2,0}y_{2,1}y_{2,2}y_{2,3}y_{2,4}}\right)^{1/5}, \quad \frac{\beta_{2,2}}{\beta_{1,1}} = \left(\frac{y_{1,0}y_{0,1}y_{1,3}y_{2,2}y_{2,4}}{y_{2,0}y_{0,2}y_{2,1}y_{1,1}y_{1,2}}\right)^{1/5},$$

$$\frac{\beta_{2,4}}{\beta_{1,2}} = \left(\frac{y_{1,0}y_{1,4}y_{2,2}y_{0,2}y_{2,1}}{y_{2,0}y_{2,3}y_{1,1}y_{0,1}y_{1,3}}\right)^{1/5}, \quad \frac{\beta_{2,1}}{\beta_{1,3}} = \left(\frac{y_{1,0}y_{2,4}y_{0,2}y_{2,3}y_{1,1}}{y_{2,0}y_{1,2}y_{0,1}y_{1,4}y_{2,2}}\right)^{1/5},$$

$$\frac{\beta_{2,3}}{\beta_{1,4}} = \left(\frac{y_{1,0}y_{2,1}y_{2,3}y_{1,2}y_{0,1}}{y_{2,0}y_{1,3}y_{1,4}y_{2,4}y_{0,2}}\right)^{1/5}, \quad \frac{\beta_{0,2}}{\beta_{0,1}} = \left(\frac{y_{0,1}y_{1,1}y_{2,1}y_{2,4}y_{1,4}}{y_{0,2}y_{1,2}y_{2,2}y_{2,3}y_{1,3}}\right)^{1/5},$$

$$(\beta_{1,0}/\beta_{0,1})^2 = (y_{1,0}y_{2,0}/y_{0,1}y_{0,2})^{1/3}(y_{2,0}y_{0,1}y_{2,1}^2y_{2,4}^2/y_{1,0}y_{0,2}y_{1,2}^2y_{1,3}^2)^{1/5},$$

$$(\beta_{1,1}/\beta_{0,1})^2 = (y_{1,0}y_{2,0}/y_{1,4}y_{2,3})^{1/3}(y_{2,0}y_{1,4}y_{1,1}^2y_{2,1}^2/y_{1,0}y_{2,3}y_{1,3}^2y_{2,2}^2)^{1/5},$$

$$(\beta_{1,2}/\beta_{0,1})^2 = (y_{1,0}y_{2,0}/y_{1,2}y_{2,4})^{1/3}(y_{2,0}y_{2,4}y_{0,1}^2y_{1,1}^2/y_{1,0}y_{1,2}y_{0,2}^2y_{2,2}^2)^{1/5},$$

$$\left(\varepsilon_{1,3}/\varepsilon_{0,1}\right)^2=\left(y_{1,0}y_{2,0}/y_{1,3}y_{2,1}\right)^{1/3}\left(y_{2,0}y_{2,1}y_{0,1}^2y_{1,4}^2/y_{1,0}y_{1,3}y_{0,2}^2y_{2,3}^2\right)^{1/5},$$

$$\left(\varepsilon_{1,4}/\varepsilon_{0,1}\right)^2=\left(y_{1,0}y_{2,0}/y_{1,1}y_{2,2}\right)^{1/3}\left(y_{2,0}y_{1,1}y_{1,4}^2y_{2,4}^2/y_{1,0}y_{2,2}y_{1,2}^2y_{2,3}^2\right)^{1/5},$$

$$\left(\frac{\varepsilon_{1,0}}{\varepsilon_{0,1}}\cdot\frac{\varepsilon_{1,1}}{\varepsilon_{0,1}}\cdot\frac{\varepsilon_{1,2}}{\varepsilon_{0,1}}\cdot\frac{\varepsilon_{1,3}}{\varepsilon_{0,1}}\cdot\frac{\varepsilon_{1,4}}{\varepsilon_{0,1}}\right)^3\left(\frac{\varepsilon_{2,0}}{\varepsilon_{1,0}}\,\frac{\varepsilon_{2,1}}{\varepsilon_{1,3}}\,\frac{\varepsilon_{2,2}}{\varepsilon_{1,1}}\,\frac{\varepsilon_{2,3}}{\varepsilon_{1,4}}\,\frac{\varepsilon_{2,4}}{\varepsilon_{1,2}}\right)^2\varepsilon_{0,1}^{15}=y_{1,0}$$

с одними и теми же значениями радикалов $y_{i,j}^{1/a_{i,j}}$ для $\varepsilon_{i,j}$, чтобы выполнялись соотношения (2).

Пусть $\nu_{\varepsilon_{i,j}}(y_{\alpha,\beta})=\psi(i,j,\alpha,\beta)$, где $\nu_q(c)$ – q – показатель числа c. Например, $\psi(1,0,\alpha,0)=\alpha$. Введем функцию

$$\left(x_{\alpha,\beta}-x_{\gamma,\delta}\right)\Big/\left(y_{\alpha,\beta},y_{\gamma,\delta}\right)=\varepsilon_{\alpha,\beta;\,\gamma,\delta}\,, \tag{3}$$

где

$$\left(y_{\alpha,\beta},y_{\gamma,\delta}\right)=\prod_{i,j}\varepsilon_{i,j}^{\min\{\psi(i,j,\alpha,\beta);\psi(i,j,\gamma,\delta)\}}$$

Нетрудно установить, что

$$2\min\left\{\psi(i,j,\alpha,\beta),\,\psi(i,j,\gamma,\delta)\right\}+\min\left\{\psi(i,j,\alpha+\gamma,\beta+\delta),\right.$$
$$\left.\psi(i,j,\alpha-\gamma,\beta-\delta)\right\}=\psi(i,j,\alpha,\beta)+\psi(i,j,\gamma,\delta),$$

поэтому

$$\left(y_{\alpha,\beta},y_{\gamma,\delta}\right)^2\left(y_{\alpha+\gamma,\beta+\delta},\,y_{\alpha-\gamma,\beta-\delta}\right)=y_{\alpha,\beta}y_{\gamma,\delta}\,.$$

С другой стороны, в силу формул сложения эллиптических функций

$$\left(x_{\alpha,\beta}-x_{\gamma,\delta}\right)^2\left(x_{\alpha+\gamma,\beta+\delta}-x_{\alpha-\gamma,\beta-\delta}\right)=y_{\alpha,\beta}\,y_{\gamma,\delta}\,.$$

В результате этого из (3) получаем

$$\varepsilon_{\alpha+\gamma,\beta+\delta;\,\alpha-\gamma,\beta-\delta}\,\varepsilon^2_{\alpha,\beta;\,\gamma,\delta}=1\,. \tag{4}$$

Производя в (4) подстановку $\left\{\alpha,\beta;\,\gamma,\delta\right\}\to\left\{\alpha+\gamma,\beta+\delta;\,\alpha-\gamma,\beta-\delta\right\}$, выводим

$$\varepsilon^2_{\alpha+\gamma,\beta+\delta;\,\alpha-\gamma,\beta-\delta}\,\varepsilon_{2\alpha,2\beta;\,2\gamma,2\delta}=1\,.$$

Следовательно, $\varepsilon_{2\alpha,2\beta;\,2\gamma,2\delta}=\varepsilon^4_{\alpha,\beta;\,\gamma,\delta}$, $\varepsilon_{2^t\alpha,2^t\beta;\,2^t\gamma,2^t\delta}=$

$=\varepsilon_{\alpha,\beta;\gamma,\delta}^{2^{2t}}$ $(t=1,2,\ldots)$. Пусть $t=1,2$, тогда $2\equiv -1 \pmod 3$, $2^2\equiv -1 \pmod 5$ и $x_{2^t\alpha,2^t\beta}=x_{\alpha,\beta}$, $x_{2^t\gamma,2^t\delta}=x_{\gamma,\delta}$, $y_{2^t\alpha,2^t\beta}\,y_{2^t\gamma,2^t\delta}=y_{\alpha\beta}y_{\gamma,\delta}$, $\varepsilon_{2^t\alpha,2^t\beta;\,2^t\gamma,2^t\delta}=\varepsilon_{\alpha,\beta;\,\gamma,\delta}=\varepsilon_{\alpha,\beta,\gamma,\delta}^{2^{2t}}$, так что $\varepsilon_{\alpha,\beta,\gamma,\delta}$ есть циклическая единица, степень которой является делителем 3 при $p=3$ и делителем 15 при $p=5$. Из (2) выводим

$$y_{1,0}\,y_{1,1}\,y_{1,2}\Big/y_{0,1}^2=\Big[y_{1,2}\Big/(y_{0,1},y_{1,2})\Big]^3,$$

$$y_{1,0}\,y_{1,1}\,y_{1,2}\Big/y_{0,1}^2=\Big[\varepsilon\,y_{1,2}\Big/(x_{1,2}-x_{0,1})\Big]^3,$$

$$\frac{y_{1,0}\,y_{1,1}\,y_{1,2}\,y_{1,3}\,y_{1,4}}{(y_{0,1}\,y_{0,2})^2}\left[\frac{y_{(1/2),0}\,y_{(1/2),1}\,y_{(1/2),2}\,y_{(1/2),3}\,y_{(1/2),4}}{(y_{0,1}\,y_{0,2})^2}\right]^{2^2}=$$

$$=\left\{\prod_{i=0}^{4}(y_{1,0},y_{1,i})(y_{1,0},y_{2,i})^2\Big/\big(y_{1,0}\,(y_{1,0}\,y_{2,0})\big)^6\right\}^{15},$$

$$\prod_{i=0}^{4}y_{1,i}\,y_{2,i}^4\Big/(y_{0,1}\,y_{0,2})^{10}=$$

$$=\left\{\varepsilon\prod_{i=1}^{4}(x_{1,0}-x_{1,i})(x_{1,0}-x_{2,i})^2\Big/y_{1,0}^5(x_{1,0}-x_{2,0})^4\right\}^{15}.$$

Так как циклическая единица порядка m $2^{2t}-1\equiv 0 \pmod m$ принадлежит полю $Q(\varepsilon)$, $\varepsilon^{2^{2t}}=1$, то

$$y_{1,0}\,y_{1,1}\,y_{1,2}\Big/y_{0,1}^2=\mathcal{L}^3\quad(p=3)$$

$$\left\{\prod_{i=0}^{4}y_{1,i}\Big/\prod_{i=1}^{2}y_{0,i}^2\right\}\left\{\prod_{i=0}^{4}y_{2,i}\Big/\prod_{i=1}^{2}y_{0,i}^2\right\}^4=\mathcal{L}^5\quad(p=5),$$

где $\mathcal{L}$ = рациональная функция от $x_{1,0}$, $y_{1,0}$, $x_{0,1}$, $y_{0,1}$, z, s .

Рассмотрим теперь общий случай.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ. Пусть

$$y_{\alpha,\beta}=\prod_{i=0}^{\frac{p-1}{2}}\prod_{j=0}^{p-1}\vartheta_{i,j}^{(\alpha i+\beta j)}\qquad\left(\alpha=0,1,\ldots,\frac{p-1}{2};\ \beta=0,1,\ldots,p-1\right).\quad(5)$$

$(\alpha i+\beta j)$ – абсолютный наименьший вычет числа $\alpha i+\beta j$ по $\bmod p$;

$(i_1, j_1) \neq (0,0), (\pm i_2, j_2) \pmod p$, где одновременно берутся верхние или нижние знаки. Как было показано в работе [I] , если $\alpha O_p + \beta O'_p = \{x_{\alpha,\beta} y_{\alpha,\beta}\}$, то

$$(y_{\alpha,\beta}) = q_{\alpha,\beta} \prod_{i=0}^{\frac{p-1}{2}} \prod_{j=0}^{p-1} (a_{ij})^{(\alpha i + \beta j)},$$

где $q_{\alpha,\beta}$ состоит из делителей числа p , (a_{ij}) - целые попарно взаимно простые дивизоры. Вследствие этого, $\det \|(\alpha i + \beta j)\| \neq 0$, так как в противном случае $(a_{i,j})$ не обязательно были бы взаимно простыми. Число уравнений в системе (5) равно числу переменных $\beta_{i,j}$, $\det \|(\alpha i + \beta j)\|$, как было отмечено выше, отличен от 0 . Следовательно, она разрешима относительно $\beta_{i,j}$.

Введем следующие функции

$$\partial i f (y_{i,0}) = \prod_{j=1}^{\frac{p-1}{2}} (y_{i,0}, y_{j,0}) =$$

$$= \varepsilon_i y_{i,0} \prod_{\substack{j=1 \\ j \neq i}}^{\frac{p-1}{2}} (x_{i,0} - x_{j,0}), \qquad \left(i = 1,2,\ldots, \frac{p-1}{2}\right)$$

$$\partial i f' (y_{i,0}) = \prod_{j=0}^{p-1} (y_{i,0}, y_{i,j}) =$$

$$= \varepsilon'_i y_{i,0} \prod_{j=1}^{p-1} (x_{i,0} - x_{i,j}), \qquad \left(i = 1,2,\ldots, \frac{p-1}{2}\right)$$

$$\prod_{j=0}^{p-1} y_{(1/i),j} \Big/ \left(\prod_{j=1}^{\frac{p-1}{2}} y_{0,j}\right)^2 = M_i$$

Нетрудно установить справедливость следующих соотношений

$$\frac{\partial i f' (y_{(1/i),0})}{\partial i f^2 (y_{(1/i),0})} = \prod_{s=1}^{\frac{p-1}{2}} \beta_{(is),0}^{s^2}, \qquad \left(i = 1,2,\ldots, \frac{p-1}{2}\right)$$

$$M_i = \left(\prod_{s=1}^{\frac{p-1}{2}} \beta_{(is),0}^{s} \right)^p$$

$$\prod_{i=1}^{\frac{p-1}{2}} M_i^{i^2} = \left\{ \prod_{i=1}^{\frac{p-1}{2}} \left[\partial_i f'\left(y_{(1/i),0}\right) \Big/ \partial_i f^2\left(y_{(1/i),0}\right) \right]^i \right\}^p .$$

Следовательно, $\prod_{i=1}^{[p/2]} \left\{ \prod_{j=0}^{p-1} y_{(1/i),j} \Big/ \prod_{j=1}^{[p/2]} y_{0,j}^2 \right\}^{i^2} = \mathcal{Z}^p$, где $\mathcal{Z}$ - рациональная функция от $x_{1,0}$, $y_{1,0}$, $x_{0,1}$, $y_{0,1}$, r , s .

Теорема доказана.

Так как базисные точки можно выбирать произвольным образом, то из (I) с помощью подстановок $\{1,0;\ 0,1\} \longrightarrow \{\alpha,\beta;\ \gamma,\delta\}$ $(\alpha\delta - \beta\gamma \not\equiv 0 \pmod p)$ можно получить ряд других аналогичных соотношений.

Литература

I. Демьяненко В.А. О кручении эллиптических кривых. - Изв.АН СССР, Сер.мат., 1971, т.35, № 2, с.281-307.