ЧЕБЫШЕВСКИЙ СБОРНИК
Том 11 Выпуск 1 (2010)

Труды VII Международной конференции
Алгебра и теория чисел: современные проблемы и приложения,
посвященной памяти профессора Анатолия Алексеевича Карацубы

О НЕКОТОРЫХ СВОЙСТВАХ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ В ФОРМЕ ЯКОБИ

А. Ю. Нестеренко (г. Москва)
nesterenko_a_y@mail.ru

Пусть $p > 3$ простое число и $\lambda \not\equiv 0, 1 \pmod p$. Рассмотрим эллиптическую кривую, заданную в форме Якоби однородным сравнением

$$E_\lambda : \quad y^2 z \equiv x(x-z)(x-\lambda z) \pmod p. \tag{1}$$

Основным результатом предлагаемой работы является доказательство следующего результата.

Теорема 1. *Пусть значения $-1, \lambda, 1-\lambda$ являются квадратичными вычетами по модулю простого числа p. Тогда порядки групп точек эллиптических кривых*

$$E_\lambda, \quad E_{\frac{1}{\lambda}}, \quad E_{1-\lambda}, \quad E_{\frac{1}{1-\lambda}}, \quad E_{\frac{\lambda}{\lambda-1}}, \quad E_{\frac{\lambda-1}{\lambda}}, \tag{2}$$

совпадают.

Данный результат известен и его доказательство может быть найдено, например, в книге [2]. Метод доказательства основывается на вычислении в явном виде и сравнении j-инвариантов кривых из (2).

Предлагаемый нами подход к доказательству теоремы основан на других принципах. Мы показываем, что порядок группы точек эллиптической кривой (1) совпадает с порядком группы точек эллиптической кривой, заданной системой сравнений

$$S_\lambda := \quad \begin{cases} u_1^2 + u_2^2 \equiv 1 \pmod p, \\ \lambda u_1^2 + u_3^2 = 1 \pmod p, \end{cases} \tag{3}$$

где $\lambda \not\equiv 0, 1 \pmod p$. Далее мы предъявляем в явном виде элементарные изоморфизмы между кривыми

$$S_\lambda, \quad S_{\frac{1}{\lambda}}, \quad S_{1-\lambda}, \quad S_{\frac{1}{1-\lambda}}, \quad S_{\frac{\lambda}{\lambda-1}}, \quad S_{\frac{\lambda-1}{\lambda}}, \tag{4}$$

откуда следует, что порядки групп точек кривых (4) совпадают, из чего следует доказательство сформулированной теоремы 1.

Докажем следующее утверждение

Теорема 2. *Для порядков рассматриваемых групп эллиптических кривых S_λ и E_λ выполнено равенство $|S_\lambda| = |E_\lambda|$.*

Для доказательство теоремы 2 нам потребуются вспомогательные результаты.

Лемма 1. *Пусть p нечетное простое число, тогда выполнены следующие равенства*

$$\sum_{u=0}^{p-1} u^m \equiv \begin{cases} 0, & \text{если} \quad p-1 \not| \, m, \\ -1, & \text{если} \quad p-1 \mid m, \end{cases} \pmod p.$$

$$\sum_{u=0}^{p-1} \left(\frac{u^2+bu+c}{p} \right) = \begin{cases} -1, & \text{если} \quad p \not| d, \\ p-1, & \text{если} \quad p|d, \end{cases}$$

где $d = b^2 - 4c$ — дискриминант многочлена $u^2 + bu + c$.

Доказательство. См. [4], гл. II, §10, п.4, утверждение III. □

Лемма 2. *Пусть m натуральное, λ отличное от нуля и единицы целое число. Тогда у многочленов $(x-1)^m(x-\lambda)^m$ и $(1-x)^m(1-\lambda x)^m$ коэффициенты при x^m совпадают и равны*

$$D_m(\lambda) = (-1)^m \sum_{k=0}^{m} (C_k^m)^2 \, \lambda^k, \tag{5}$$

где $C_k^m = \dfrac{m!}{k!(m-k)!}$ — биномиальный коэффициент.

Доказательство. Из равенств

$$(x-1)^m(x-\lambda)^m = \left(\sum_{i=0}^{m} (-1)^{m-i} C_i^m x^i \right) \left(\sum_{j=0}^{m} (-1)^{m-j} C_j^m \lambda^{m-j} x^j \right) = \sum_{k=0}^{2m} \sum_{i+j=k} (-1)^{2m-k} C_i^m C_j^m \lambda^{m-j} x^k,$$

следует, с учетом равенства $C_i^m = C_{m-i}^m$, что коэффициент при x^m многочлена $(x-1)^m(x-\lambda)^m$ равен

$$\sum_{i+j=m} (-1)^m C_i^m C_j^m \lambda^{m-j} = (-1)^m \sum_{i=0}^{m} (C_i^m)^2 \lambda^i = D_m(\lambda).$$

Аналогично, из равенств

$$(1-x)^m(1-\lambda x)^m = (x-1)^m(\lambda x-1)^m = \left(\sum_{i=0}^{m}(-1)^{m-i}C_i^m x^i\right)\left(\sum_{j=0}^{m}(-1)^{m-j}C_j^m\lambda^j x^j\right) = \sum_{k=0}^{2m}\sum_{i+j=k}(-1)^{2m-k}C_i^m C_j^m\lambda^j x^k,$$

получаем, что коэффициент многочлена $(1-x)^m(1-\lambda x)^m$ равен $D_m(\lambda)$. □

Теорема 3 (**Хассе**). *Пусть $p>3$ простое число и $f(x)$ многочлен третьей степени, не имеющий кратных кратных корней по модулю p. Тогда порядок группы точек эллиптической кривой $E: y^2 \equiv f(x) \pmod p$ удовлетворяет неравенству*

$$|E| = p+1+t, \quad \text{где} \quad |t| < 2\sqrt{p}.$$

Доказательство. См. [4], гл. II, §10, п.6. или [1], глава 10. □

Очевидным следствием теоремы Хассе является следующее утверждение.

Лемма 3. *Пусть $p>3$ простое число и $f(x)$ многочлен третьей степени, не имеющий кратных кратных корней по модулю p, тогда*

$$\left|\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right)\right| < 2\sqrt{p}.$$

Перейдем к доказательству сформулированной нами теоремы 2. Для порядка группы точек эллиптической кривой E_λ, заданной уравнением (1), выполнено равенство

$$|E_\lambda| = 1+\sum_{x=0}^{p-1}\left(1+\left(\frac{x(x-1)(x-\lambda)}{p}\right)\right) \equiv 1+\sum_{x=0}^{p-1}x^{\frac{p-1}{2}}(x-1)^{\frac{p-1}{2}}(x-\lambda)^{\frac{p-1}{2}} \pmod p.$$

Положим $m=\dfrac{p-1}{2}$ и обозначим $h(x)=(x-1)^m(x-\lambda)^m=\sum_{i=0}^{2m}h_i x^i$. Тогда, используя первое утверждение леммы 1 и утверждение леммы 2, получим

$$\sum_{x=0}^{p-1}x^m(x-1)^m(x-\lambda)^m = \sum_{x=0}^{2m}\sum_{i=0}^{2m}h_i x^{m+i} \equiv -\sum_{p-1|m+i,\ i=0,\dots,2m}h_i \equiv -h_m \equiv -D_{\frac{p-1}{2}}(\lambda) \pmod p.$$

Сопоставляя последние два сравнения, получаем

$$|E_\lambda| \equiv 1 - D_{\frac{p-1}{2}}(\lambda) \pmod p. \tag{6}$$

Теперь рассмотрим систему сравнений (3). Для $|S_\lambda|$ выполнено равенство

$$|S_\lambda| = N_1 + N_\infty,$$

где N_1 число конечных точек, а N_∞ — число бесконечно удаленных точек, равное количеству решений системы

$$\begin{cases} u_1^2 + u_2^2 \equiv 0 \pmod p, \\ \lambda u_1^2 + u_3^2 \equiv 0 \pmod p. \end{cases}$$

Верно равенство

$$N_\infty = \left(1 + \left(\frac{-1}{p}\right)\right)\left(1 + \left(\frac{-\lambda}{p}\right)\right) = 1 + \left(\frac{-1}{p}\right) + \left(\frac{-\lambda}{p}\right) + \left(\frac{\lambda}{p}\right). \tag{7}$$

Для числа N_1 конечных точек выполнено равенство

$$\begin{aligned} N_1 &= \sum_{u=0}^{p-1}\left(1 + \left(\frac{1-u^2}{p}\right)\right)\left(1 + \left(\frac{1-\lambda u^2}{p}\right)\right) = \\ &= p + \sum_{u=0}^{p-1}\left(\frac{1-u^2}{p}\right) + \sum_{u=0}^{p-1}\left(\frac{1-\lambda u^2}{p}\right) + \sum_{u=0}^{p-1}\left(\frac{(1-u^2)(1-\lambda u^2)}{p}\right) = \\ &= p + Q_1 + Q_2 + Q_3. \end{aligned}$$

Применяя второе утверждение леммы 1 получаем равенства

$$\begin{aligned} Q_1 &= \sum_{u=0}^{p-1}\left(\frac{1-u^2}{p}\right) = \left(\frac{-1}{p}\right)\sum_{u=0}^{p-1}\left(\frac{u^2-1}{p}\right) = -\left(\frac{-1}{p}\right), \\ Q_2 &= \sum_{u=0}^{p-1}\left(\frac{1-\lambda u^2}{p}\right) = \left(\frac{-\lambda}{p}\right)\sum_{u=0}^{p-1}\left(\frac{u^2-\lambda^{-1}}{p}\right) = -\left(\frac{-\lambda}{p}\right), \end{aligned}$$

откуда следует равенство

$$N_1 = p - \left(\frac{-1}{p}\right) - \left(\frac{-\lambda}{p}\right) + Q_3. \tag{8}$$

Суммируя выражения для N_∞ и N_1, получаем выражение для $|S_\lambda|$

$$|S_\lambda| = p + 1 + \left(\frac{\lambda}{p}\right) + Q_3. \tag{9}$$

Вспомним, что $m = \dfrac{p-1}{2}$, и обозначим $g(u) = (1-u)^m(1-\lambda u)^m = \sum_{i=0}^{2m} g_i u^i$. Учитывая первое утверждение леммы 1 и утверждение второй леммы, запишем для суммы Q_3 сравнение

$$Q_3 = \sum_{u=0}^{p-1}\left(\frac{(1-u^2)\,(1-\lambda u^2)}{p}\right) \equiv \sum_{u=0}^{p-1}\left(1-u^2\right)^m\left(1-\lambda u^2\right)^m \pmod p =$$

$$= \sum_{u=0}^{p-1}\sum_{j=0}^{2m} g_j u^{2j} \pmod p \equiv$$

$$\equiv -\sum_{p-1|2j,\, j=0,\ldots,2m} g_j \pmod p \equiv -g_m - g_{2m} \pmod p.$$

Из определения многочлена $g(u)$ следует, что

$$g_{2m} = \lambda^m = \lambda^{\frac{p-1}{2}} \equiv \left(\frac{\lambda}{p}\right) \pmod p.$$

Тогда $Q_3 \equiv -D_{\frac{p-1}{2}}(\lambda) - \left(\dfrac{\lambda}{p}\right) \pmod p$. Подставляя полученное сравнение в равенство (9) и сравнивая его с (6), получим

$$|S_\lambda| \equiv 1 - D_{\frac{p-1}{2}}(\lambda) \equiv |E_\lambda| \pmod p.$$

Пока мы доказали утверждение более слабое, чем сформулированное в условии теоремы 2. Из теоремы Хассе тривиально следует, что $|E_\lambda|$ не превосходит величины в $2p$. Из равенства (9) и определения Q_3 также следует, что $|S_\lambda|$ не превосходит величины в $2p$. Следовательно, значения $|E_\lambda|$ и $|S_\lambda|$ либо совпадают, либо отличаются ровно на величину p.

Обозначим $|E_\lambda| = p+1+t$, тогда из теоремы Хассе и сравнения (6) следует, что

$$|t| \leqslant 2\sqrt{p}, \tag{10}$$

$$|t| \equiv \left|D_{\frac{p-1}{2}}(\lambda)\right| \pmod p \tag{11}$$

Оценим сверху величину $|Q_3|$. Сделаем замену переменных

$$u = \frac{x}{x-1} \quad \text{или} \quad u = \frac{u}{u-1},$$

которая не определена в точке $x = u = 1$. Поскольку

$$\left(1-u^2\right)\left(1-\lambda u^2\right) = \frac{(1-2x)(x^2(1-\lambda)-2x+1)}{(x-1)^4},$$

то

$$Q_3 = \sum_{u=0}^{p-1}\left(\frac{(1-u^2)\,(1-\lambda u^2)}{p}\right) = \sum_{u=0,\ u\neq 1}^{p-1}\left(\frac{(1-u^2)\,(1-\lambda u^2)}{p}\right) = \sum_{x=0,\ x\neq 1}^{p-1}\left(\frac{(1-2x)\,((1-\lambda)x^2-2x+1)}{p}\right) = \sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right) - \left(\frac{\lambda}{p}\right),$$

где $f(x) = ((1-\lambda)x^2 - 2x + 1)\,(1-2x)$ многочлен[1] третьей степени. Воспользовавшись леммой 3 получаем неравенство

$$\left|\left(\frac{\lambda}{p}\right) + Q_3\right| = \left|\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right)\right| \leqslant 2\sqrt{p}, \tag{12}$$

из которого, учитывая (9), (10), получим неравенство

$$||S_\lambda| - |E_\lambda|| = \left|\left(\frac{\lambda}{p}\right) + Q_3 + t\right| \leqslant 4\sqrt{p}.$$

Следовательно значения $|E_\lambda|$ и $|S_\lambda|$ совпадают. Теорема 2 доказана.

Для построения отображений между кривыми из (4) нам потребуется рассмотреть конечное расширение поля из p элементов. Определим элементы i, κ_1, κ_2 как решения сравнений

$$i^2 \equiv -1 \pmod p, \quad \kappa_1^2 \equiv \lambda \pmod p, \quad \kappa_2^2 \equiv 1-\lambda \pmod p.$$

В случае, если одно из значений $-1, \lambda, 1-\lambda$ не является квадратичным вычетом по модулю p, то соответствующий элемент принадлежит расширению поля из p элементов.

Используя введенные обозначения, в явном виде предъявим отображения, задающие взаимно однозначное соответствие между точками эллиптической кривой S_λ и точками кривых из (4).

$$\begin{aligned}
S_{\frac{1}{\lambda}}: &\quad v_1 = \kappa_1 u_2, \quad v_2 = \kappa_2 u_4, \quad v_3 = \kappa_2 u_1, \quad v_4 = u_3,\\
S_{1-\lambda}: &\quad v_1 = u_3, \quad v_2 = i\kappa_1 u_2, \quad v_3 = \kappa_1\kappa_2 u_1, \quad v_4 = \kappa_2 u_4,\\
S_{\frac{1}{1-\lambda}}: &\quad v_1 = u_3, \quad v_2 = \kappa_1 u_1, \quad v_3 = i\kappa_1\kappa_2 u_2, \quad v_4 = u_4,\\
S_{\frac{\lambda}{\lambda-1}}: &\quad v_1 = u_2, \quad v_2 = u_1, \quad v_3 = \frac{u_3}{\kappa_2}, \quad v_4 = u_4,\\
S_{\frac{\lambda-1}{\lambda}}: &\quad v_1 = i\kappa_1 u_2, \quad v_2 = u_3, \quad v_3 = \kappa_2 u_1, \quad v_4 = \kappa_2 u_4,
\end{aligned}$$

[1]Корни многочлена $f(x)$ равны $\frac{1}{2}$, $\frac{1}{1+\sqrt{\lambda}}$, $\frac{1}{1-\sqrt{\lambda}}$. При $\lambda \neq 0, 1$ все корни различны.

В случае, когда значения $-1, \lambda, 1-\lambda$ являются квадратичными вычетом по модулю p, приведенные отображения определены над конечным полем из p элементов и переводят рациональные точки кривой S_λ в рациональные точки кривых из (4). Следовательно, порядки групп точек этих кривых совпадают. Из последнего замечания и утверждения теоремы 2, вытекает доказательство сформулированной в начале статьи теоремы 1.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

[1] *Гельфонд А.О., Линник Ю.В.* Элементарные методы в теории чисел. — М.:Физматгиз, 1962. — 272 с.

[2] *Ленг С.* Эллиптические функции. — М.:Наука, 1984. — 312 с.

[3] *Нестеренко А.Ю.* О числе решений одной системы сравнений // Депонировано во ВИНИТИ. — № 454-в2009. — 2009. — 17 стр.

[4] *Хассе Г.* Лекции по теории чисел. — М.:ИЛ, 1953. — 527 с.

Московский педагогический государственный университет
Поступило 13.05.2010