

Бессалов А.В., Ковальчук Л.В.

Точное число эллиптических кривых в канонической форме, изоморфных кривым Эдвардса над простым полем

Ключевые слова: каноническая форма эллиптической кривой, кривая Эдвардса, кривая кручения, параметры кривой, изоморфизм, квадратичный вычет, квадратичный невычет.

Keywords: canonical form of an elliptic curve, Edwards curve, twisted curve, curve parameters, isomorphism, quadratic residue, quadratic non-residue.

Ключові слова: канонічна форма еліптичної кривої, крива Едвардса, крива скручення, параметри кривої, ізоморфізм, квадратичні лишки, квадратичні нелишки.

Среди форм представления эллиптических кривых в задачах криптографии наиболее перспективными представляются кривые в форме Эдвардса [1-5], рекордные по быстродействию и удобные для программирования. Они обладают двойной симметрией в координатах поля характеристики $p > 2$, вследствие чего количество точек N_E такой кривой делится на 4: $N_E \equiv 0 \pmod{4}$. Поэтому циклические кривые Эдвардса всегда содержат одну точку 2-го порядка и 2 точки 4-го порядка. Кривых в

канонической форме $y^2 = x^3 + ax + b$ с таким свойством сравнительно немного (по предварительным оценкам – около четверти всевозможных кривых, см. работу [3]), поэтому для построения изоморфных им кривых Эдвардса возникает задача поиска кривых в форме Вейерштрасса с двумя точками 4-го порядка. Вместе с тем в известной литературе не рассматривалась задача нахождения точного числа таких кривых с ненулевыми параметрами a и b .

В данной работе впервые получены формулы для числа кривых с оговоренными свойствами (и, соответственно, изоморфных им кривых Эдвардса). Мы ввели зависимый от традиционных параметров (a, b) кривой в канонической форме параметр c как единственный в поле F_p корень кубического уравнения. Получены необходимые и достаточные условия существования 2-х точек 4-го порядка, а также система линейных уравнений для нахождения неизвестных параметров a и c^2 , в уравнения которой входят квадратичные вычеты и невычеты. Для нахождения точного числа канонических кривых, изоморфных кривым Эдвардса, потребовалось сформулировать и доказать 2 леммы о числе решений уравнений, связывающих суммы квадратичных вычетов и невычетов. Доказательства опираются на схему Гаусса распределения квадратичных вычетов [6]. В итоге авторам удалось найти формулы расчета точного числа кривых с заданными свойствами над любым простым конечным полем F_p характеристики $p > 3$. Кроме того, предложен алгоритм поиска кривых с хорошими криптографическими свойствами, изоморфных кривым Эдвардса.

1. Необходимые и достаточные условия существования ровно двух точек четвёртого порядка для эллиптической кривой, заданной в канонической форме.

Каноническая форма кривой над полем характеристики $p > 3$ описывается известным уравнением [7]:

$$E_p: y^2 = x^3 + ax + b, \quad \Delta = 4a^3 + 27b^2 \neq 0, \quad a, b \in F_p. \quad (1)$$

Согласно определению, операция удвоения точки $P = (x_1, y_1)$, которая дает координаты точки $2P = (x_3, y_3)$, задаётся следующим образом:

$$\begin{cases} x_3 = v^2 - 2x_1, \\ y_3 = -y_1 - v(x_3 - x_1), \end{cases} \quad v = \frac{3x_1^2 + a}{2y_1}. \quad (2)$$

В дальнейшем нам понадобятся следующие стандартные обозначения. Множество приведенных квадратичных вычетов по модулю простого числа p будем обозначать Q_p :

$$Q_p = \left\{ x \in F_p \mid \left(\frac{x}{p} \right) = 1 \right\},$$

где $\left(\frac{x}{p} \right)$ – символ Лежандра:

$$\left(\frac{x}{p} \right) = \begin{cases} 1, & \text{если } x \text{ – квадратичный вычет по модулю } p; \\ -1, & \text{если } x \text{ – квадратичный невычет по модулю } p; \\ 0, & \text{если } x \text{ делится на } p. \end{cases}$$

В данной работе мы будем рассматривать только такие кривые (1), порядок которых делится на 2. Легко доказать, что в этом случае кривая обязательно имеет точку второго порядка (в частности, это будет следовать из теоремы Силова). Согласно (2), точка $P = (x_1, y_1)$ будет точкой второго порядка тогда и только тогда, если $y_1 = 0$ (в этом случае при вычислении точки $2P$ в (2) возникает деление на 0), т.е. точка второго порядка будет иметь координаты $(c, 0)$, для некоторого $c \in F_p$. Подставляя в уравнение кривой (1) значение $y = 0$, получаем, что c – корень уравнения $x^3 + ax + b = 0$ в поле F_p (который обязательно существует, вследствие существования точки второго порядка). Тогда в наших обозначениях уравнение (1) можно переписать в виде

$$y^2 = (x - c)(x^2 + cx + a + c^2), \text{ где } b = -c^3 - ac, \quad c \in F_p. \quad (3)$$

Как упоминалось ранее, кривая в канонической форме изоморфна кривой Эдвардса в том и только в том случае, если она содержит ровно две точки четвёртого порядка. Следующая теорема даёт необходимые и достаточные условия (в терминах параметров кривой (1)) существования на кривой E_p ровно двух таких точек.

Теорема 1: *необходимым и достаточным условием существования ровно двух точек четвёртого порядка на кривой E_p является одновременное выполнение следующих двух равенств:*

$$a) \left(\frac{-(3c^2 + 4a)}{p} \right) = -1, \quad б) \left(\frac{\delta}{p} \right) = 1, \text{ где } \delta = 3c^2 + a. \quad (4)$$

Доказательство: докажем необходимость данных условий. Для этого предположим, что кривая имеет две точки четвёртого порядка, и покажем, что при этом выполняются условия (4). Пусть на кривой (1) существует ровно две точки четвёртого порядка. Тогда, очевидно, она не может содержать более одной точки второго порядка (т.к., согласно определению порядка точки кривой, сумма точек четвёртого и второго порядка будет точкой четвёртого порядка). Следовательно, парабола в правой части (3) не имеет корней в поле F_p , т.е. дискриминант соответствующего квадратного уравнения является квадратичным невычетом. Данный дискриминант равен

$$c^2 - 4(a + c^2) = -(3c^2 + 4a);$$

и, поскольку он квадратичный невычет, то

$$\left(\frac{-(3c^2 + 4a)}{p} \right) = -1.$$

Необходимость первого условия в (4) доказана. Заметим, что условие $(3c^2 + 4a) \neq 0$, которое следует из пункта а) формулы (4), исключает кратные корни кубического уравнения и, тем самым, сингулярные кривые с дискриминантом $\Delta = 0$ [7].

Пусть $P = (x_1, y_1)$ – точка 4-го порядка. Тогда при её удвоении, согласно (2), получаем точку второго порядка $D = (c, 0)$:

$$\begin{cases} \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 = c; \\ -y_1 - \left(\frac{3x_1^2 + a}{2y_1}\right)(c - x_1) = 0. \end{cases} \quad (5)$$

Из первого уравнения этой системы получаем выражение

$$y_1^2 = \frac{(3x_1^2 + a)^2}{4(c + 2x_1)},$$

а из второго – выражение

$$y_1^2 = -\frac{(3x_1^2 + a)(c - x_1)}{2}.$$

Приравнивая правые части этих выражений и сокращая на множитель $3x_1^2 + a$, получим квадратное уравнение для координаты x_1 этой точки:

$$x_1^2 - 2cx_1 - (2c^2 + a) = 0. \quad (6)$$

Корни этого уравнения существуют (вследствие существования точки 4-го порядка), следовательно, дискриминант δ данного уравнения либо равен нулю, либо является квадратичным вычетом. Если дискриминант равен нулю, то, при $y = 0$, уравнение (3) принимает вид:

$$(x - c)^2(x + 2c) = 0,$$

вследствие чего на кривой существуют две точки второго порядка. Но тогда непосредственными вычислениями получаем, что сумма любой такой точки с точкой четвертого порядка тоже будет точкой четвертого порядка, что противоречит предположению теоремы о существовании ровно двух точек

четвёртого порядка. Следовательно, дискриминант δ является квадратичным вычетом, т.е. выполняется условие б) формулы (4). Необходимость условий (4) доказана.

Докажем достаточность. Пусть выполняются условия (4). Покажем, что при этом существует ровно два решения системы (5). Путём преобразований уравнений данной системы получим уравнение (6) с одной переменной x_1 . Поскольку выполняется условие а) формулы (4), то существует два корня данного уравнения:

$$x_1^{(1),(2)} = c \pm \sqrt{\delta} = c \pm \sqrt{3c^2 + a}. \quad (7)$$

Подставляя эти выражения во второе уравнение системы (5), получаем:

$$\begin{aligned} y_1^2 &= -2^{-1} \left(3(c \pm \sqrt{\delta})^2 + a \right) \cdot (\mp \sqrt{\delta}) = \pm 2^{-1} \sqrt{\delta} \left(3(c^2 \pm 2c\sqrt{\delta} + \delta) + a \right) = \\ &= \pm 2^{-1} \sqrt{\delta} (3c^2 \pm 6c\sqrt{\delta} + 3\delta + a) = \pm 2^{-1} \sqrt{\delta} (\pm 6c\sqrt{\delta} + 4\delta) = \\ &= \pm \sqrt{\delta} (\pm 3c\sqrt{\delta} + 2\delta) = \pm \delta (\pm 3c + 2\sqrt{\delta}) = \delta (3c \pm 2\sqrt{\delta}). \end{aligned} \quad (8)$$

Из (8) следует, что решение системы (5) существует тогда и только тогда, если хотя бы одно из выражений

$$3c - 2\sqrt{\delta} \text{ и } 3c + 2\sqrt{\delta} \quad (9)$$

является квадратичным вычетом (т.к., по условию, $\left(\frac{\delta}{p}\right) = 1$).

Покажем, что в нашем случае в точности одно из выражений (9) будет квадратичным вычетом. Действительно, перемножив эти выражения, получим:

$$(3c - 2\sqrt{\delta}) \cdot (3c + 2\sqrt{\delta}) = 9c^2 - 4\delta = -(3c^2 + 4a),$$

что, согласно пункту а) условия (4), является квадратичным невычетом. Отсюда, вследствие свойства мультипликативности символа Лежандра, следует, что в точности одно из выражений (9) является квадратичным вычетом.

Если $3c - 2\sqrt{\delta}$ является квадратичным вычетом, то существуют

$$y_1^{(1),(2)} = \pm \sqrt{\delta(3c + 2\sqrt{\delta})};$$

в противном случае существуют

$$y_1^{(1),(2)} = \pm \sqrt{\delta(3c - 2\sqrt{\delta})},$$

и тогда либо пары $(3c - 2\sqrt{\delta}, \pm \sqrt{\delta(3c + 2\sqrt{\delta})})$, либо пары $(3c + 2\sqrt{\delta}, \pm \sqrt{\delta(3c - 2\sqrt{\delta})})$, соответственно, являются двумя решениями системы (5). Непосредственной проверкой (подстановкой в уравнение (1) или в уравнение (3)) убеждаемся, что данные пары являются решениями уравнений (1) и (3), следовательно, каждая пара задаёт координаты некоторой точки данной кривой. Вследствие выполнения (5), каждая из двух полученных точек является точкой 4-го порядка. Других решений система (5) не имеет, следовательно, на кривой (1) существуют ровно две точки четвёртого порядка, что и доказывает достаточность условий (4).

Теорема 1 полностью доказана.

Следует заметить, что кривые с нулевыми значениями параметров a или b обладают плохими криптографическими свойствами и, соответственно, не используются в криптографических приложениях [7]. Возникает вопрос: как много кривых (1) с ненулевыми параметрами a и b , для которых существует изоморфизм с кривыми Эдвардса, при различных значениях порядка поля p ? Другими словами, сколько кривых Эдвардса с указанными свойствами существует над простым конечным полем?

2. Точное число кривых в канонической форме, изоморфных кривым Эдвардса.

Для определения точного числа эллиптических кривых в форме Вейерштрасса (1), имеющих ровно 2 точки 4-го порядка, необходимо обратиться к некоторым результатам теории чисел. Г. Дэвенпорт в своей работе [6] приводит блестящее доказательство распределения квадратичных вычетов, полученное Гауссом. Рассмотрим схему Гаусса и итоги его анализа.

Произведение $n(n+1) \bmod p$, $n=1,2,\dots,p-1$, включает составляющие ВВ (оба сомножителя – квадратичные вычеты) с общим числом (ВВ), НН (оба сомножителя – квадратичные невычеты) с числом (НН), и смешанные пары ВН и НВ с числом (ВН) и (НВ). Гаусс доказал, что имеет место система уравнений:

$$(ВВ) + (НН) = \frac{(p-2-\varepsilon)}{2}, \text{ где } \varepsilon = (-1)^{(p-1)/2}; \quad (10)$$

$$(НВ) + (НН) = \frac{(p-2+\varepsilon)}{2}; \quad (11)$$

$$(ВВ) + (НВ) = \frac{(p-3)}{2}; \quad (12)$$

$$(BH) + (HH) = \frac{(p-1)}{2}; \quad (13)$$

$$(BB) + (HH) - (BH) - (HB) = -1. \quad (14)$$

Здесь первые 4 уравнения не являются линейно независимыми (суммы первой и второй пар уравнений совпадают), поэтому добавлено 5-е уравнение. Из этой системы легко найти любую из 4-х неизвестных. Комбинируя (10) – (14), можно получить:

$$(BB) = \frac{(p-4-\varepsilon)}{4}, \quad (BH) = \frac{(p-\varepsilon)}{4}; \quad (15)$$

$$(HB) + (HH) = \frac{(p-2+\varepsilon)}{4}, \text{ где } \varepsilon = (-1)^{(p-1)/2}. \quad (16)$$

Очевидно, что сумма $(BB) + (HH) + (BH) + (HB)$ при $n = 1, 2, \dots, p-2$, равна $p-2$. Заметим, что при этом $n(n+1) \bmod p \neq 0$.

Для ответа на поставленный вопрос потребуются два результата, которые мы докажем в двух приведенных ниже леммах.

Для произвольного $C \in F_p^*$ обозначим $F_C(X) = (X^2 - C^2) \bmod p$.

Лемма 2: для всех $X \in F_p^*$ число разных значений функции $F_C(X)$, принадлежащих множеству квадратичных вычетов Q_p , равно (BB) , т.е.

$$\left| \{F_C(X) : X \in F_p^*\} \cap Q_p \right| = (BB).$$

Доказательство: воспользуемся схемой Гаусса для произведения $n(n-1) \bmod p$. Функцию $F_C(X)$ при $C \neq 0$ представим как $F_C(X) = C^2((XC^{-1})^2 - 1)$. Мы видим, что если X пробегает все ненулевые значения $1, 2, \dots, p-1 \in F_p^*$, то $(XC^{-1})^2$ пробегает все значения квадратов из Q_p .

В то же время значение функции $F_C(X)$ является квадратичным вычетом в F_p^* тогда и только тогда, когда $\left((XC^{-1})^2 - 1\right) \bmod p \in Q_p$. Отсюда следует (при $z = (XC^{-1})^2$):

$$\left| \{F_C(X) : F_C(X) \in Q_p\} \right| = \left| \{z \in F_p^* : z \in Q_p \wedge z - 1 \in Q_p\} \right| = (BB).$$

Лемма 2 доказана.

На основе этой леммы и формулы (15) мы можем утверждать, что число значений функции $F_C(X)$, являющихся квадратичными вычетами, при любом фиксированном ненулевом $C \in F_p^*$ равно

$$\frac{p - 4 - (-1)^{\frac{p-1}{2}}}{4}.$$

Далее, для произвольного $C \in F_p \setminus Q_p$ обозначим

$$G_C(X) = (X^2 + C) \bmod p.$$

Лемма 3: для всех $X \in F_p^*$ число разных значений функции $G_C(X)$, принадлежащих множеству квадратичных вычетов Q_p , равно (NB) , т.е.

$$\left| \{G_C(X) : X \in F_p^*\} \cap Q_p \right| = (NB).$$

Доказательство: воспользовавшись тем, что $X \neq 0$ и разделив функцию $G_C(X)$ на X^2 , получим равенство

$$CX^{-2} + 1 = G_C(X)X^{-2}.$$

При переборе всех ненулевых значений $X \in F_p^*$ элемент CX^{-2} пробегает все значения квадратичных невычетов из $\overline{Q_p}$. При этом из нашего уравнения следует, что если $G_C(X) \in Q_p$, то и $CX^{-2} + 1 \in Q_p$. Поэтому при $z = CX^{-2}$:

$$\left| \{G_C(X) : G_C(X) \in Q_p\} \right| = \left| \{z \in F_p^* : z \in Q_p \wedge z + 1 \in Q_p\} \right| = (NB) = (NN),$$

согласно (16).

Лемма 3 доказана.

На основе формулы (16) и леммы 3 можно утверждать, что число значений функции $G_C(X)$, являющихся квадратичными вычетами, при любом фиксированном ненулевом квадратичном невычете $C \in F_p^*$ равно

$$(p - 2 + (-1)^{(p-1)/2})/4.$$

Перейдем теперь к вычислению числа кривых с ненулевыми параметрами a и b , изоморфных кривым Эдвардса. Мы исключаем кривые с параметрами $a = 0$ или $b = 0$, так как эти значения параметров порождают криптографически слабые кривые с j -инвариантом, равным 0 или 12^3 , соответственно [7]. Случай $a = b = 0$ дает сингулярную кривую и, разумеется, неприемлем.

Теорема 4: число кривых (1) в канонической форме с параметрами $a \neq 0$ и $b \neq 0$ над полем F_p с двумя точками 4-го порядка определяется следующими формулами:

1) при $p \equiv 3 \pmod{4}$:

$$(\alpha) \quad M_\alpha = \frac{(p-1)(p-7)}{4}, \text{ если } \left(\frac{3}{p}\right) = 1,$$

$$(\beta) \quad M_\beta = \frac{(p-1)(p-3)}{4} \text{ если } \left(\frac{3}{p}\right) = -1;$$

2) при $p \equiv 1 \pmod{4}$:

$$(\gamma) \quad M_\gamma = \frac{(p-1)^2}{4}.$$

Доказательство.

1. Пусть $p \equiv 3 \pmod{4}$, тогда (-1) – квадратичный невычет по модулю p [7], т.е. $\left(\frac{-1}{p}\right) = -1$, и тогда утверждение пункта $a)$ в условии (4) эквивалентно утверждению

$$\left(\frac{3c^2 + 4a}{p}\right) = 1.$$

Т.е. оба элемента $3c^2 + 4a$ и $3c^2 + a$ поля F_p являются квадратичными вычетами, следовательно, по определению квадратичного вычета, условие (4) будет эквивалентно следующему условию:

$$\exists A, B \in F_p^* : \begin{cases} 3c^2 + 4a = A^2; \\ 3c^2 + a = B^2. \end{cases}$$

Решая полученную невырожденную систему уравнений над полем F_p (линейных относительно переменных a и c^2), получаем:

$$a = 3^{-1}(A^2 - B^2), \quad c^2 = 9^{-1}(4B^2 - A^2). \quad (17)$$

Для кривых с параметрами $a \neq 0$ и $b \neq 0$ квадратичные вычеты $A^2 = B^2$ и, кроме того, $4B^2 = A^2$ (т.е. нулевые значения a и c^2) отбрасываются, так как из равенств $c = 0$ и $b = -c^3 - ac$ следует равенство $b = 0$. Из (4) следует, что $A^2 \neq 0$ и $B^2 \neq 0$. Как видим из (17), решение для c существует тогда и только тогда, если $4B^2 - A^2$ является квадратичным вычетом по модулю p .

Построим квадратную таблицу из упорядоченных $\frac{p-1}{2}$ значений всех B^2 (по столбцам) и A^2 (по строкам). В клетки таблицы запишем значения $4B^2 - A^2$ из (17), так что на главной диагонали оказываются элементы $3A^2$, которые отбрасываются вследствие условия $A^2 \neq B^2$. Кроме того, в каждой строке имеем ровно один нулевой элемент, который также отбрасывается. Требуется найти число ν ненулевых недиагональных квадратичных вычетов в строке, при которых существует значение c , согласно (17). Общее число таких элементов по всем строкам, очевидно, равно $\mu = \frac{\nu(p-1)}{2}$.

Из доказанной нами леммы 2 следует, что число ненулевых квадратичных вычетов в каждой строке таблицы при $p \equiv 3 \pmod{4}$ равно $\frac{p-3}{4}$.

В таблице 1 таких вычетов по два в каждой строке. На главной диагонали со значениями $3A^2$ имеем квадратичные вычеты, если 3 – квадратный вычет в поле, и невычеты в противном случае. Поскольку диагональные элементы отбрасываются, в каждой строке остается $\nu = \frac{p-3}{4} - 1 = \frac{p-7}{4}$ элементов при

$\left(\frac{3}{p}\right) = 1$ и $\nu = \frac{p-3}{4}$ при $\left(\frac{3}{p}\right) = -1$. Общее число пар (A, B) по всем строкам

таблицы, при которых существует значение c в (17), таким образом, равно:

$$\mu_\alpha = \frac{(p-1)(p-7)}{8} \text{ при } \left(\frac{3}{p}\right) = 1 \text{ и } \mu_\beta = \frac{(p-1)(p-3)}{8} \text{ при } \left(\frac{3}{p}\right) = -1.$$

Число эллиптических кривых M_α, M_β с заданными свойствами вдвое больше количества этих пар, так как каждому значению для c^2 отвечают два корня $\pm c$ и, соответственно, два коэффициента кривой $\pm b$. Мы доказали два первых утверждения теоремы 4.

Заметим, что условие $\left(\frac{3}{p}\right) = 1$ всегда выполняется при $p \equiv \pm 1 \pmod{12}$

[6]. В частности, 3 является квадратичным вычетом при $p = 11, 13, 23, 47$ т.д.

2. Пусть теперь $p \equiv 1 \pmod{4}$, тогда число -1 является квадратичным вычетом по модулю p , т.е. $\left(\frac{-1}{p}\right) = 1$ [7].

Тогда утверждение пункта $a)$ в условии (4) эквивалентно утверждению

$$\left(\frac{3c^2 + 4a}{p}\right) = -1,$$

а само условие (4) эквивалентно следующему условию:

$$\exists A \in \overline{\mathcal{Q}_p}, \exists B \in F_p^* : \begin{cases} 3c^2 + 4a = A; \\ 3c^2 + a = B^2. \end{cases}$$

Единственное решение данной невырожденной системы (относительно переменных a и c^2) имеет вид

$$a = 3^{-1}(A - B^2), \quad c^2 = 9^{-1}(4B^2 - A), \quad (18)$$

а решение относительно переменных a и c существует тогда и только тогда, если $4B^2 - A$ является квадратичным вычетом.

Здесь, как видим, переменные a и c^2 не могут принимать нулевые значения. Нам остается лишь найти число квадратичных вычетов в таблице ненулевых значений выражения $(4B^2 - A)$ при различных A и B^2 . Если принять $B^2 = 0$, то в формуле для c^2 мы вновь получим квадратичный невычет в правой части, поэтому и в данном случае учитываем лишь ненулевые элементы A и B^2 .

Подобно п.1, построим квадратную таблицу из $(p-1)/2$ значений всех квадратичных вычетов B^2 (по столбцам) и невычетов A (по строкам). В клетки таблицы запишем значения $(4B^2 - A)$ из (18), все не равные нулю. Необходимо найти число v квадратичных вычетов в строке, при которых существует значение c , согласно (18), и умножить это значение на число строк.

Из леммы 3 следует, что выражение $(4B^2 - A)$ с ненулевыми квадратичными вычетами B^2 и фиксированным невычетом A принимает $v_\gamma = (p - 2 + (-1)^{(p-1)/2})/4$ значений на множестве квадратичных вычетов. Это

значение равно числу квадратов в каждой строке таблицы, тогда, с учетом того, что $(-1)^{(p-1)/2} = 1$ при $p \equiv 1 \pmod{4}$ получаем общее число квадратичных вычетов в таблице:

$$\mu_\gamma = v_\gamma(p-1)/2 = (p-1)^2/8.$$

Как отмечалось выше, число кривых M_γ с заданными свойствами вдвое превосходит μ_γ . Итак, теорема 4 доказана.

Пример 5: приведём примеры построения таблиц, используемых в доказательстве теоремы 4, для значений выражений $4B^2 - A^2$ и $4B^2 - A$.

Построим таблицу значений выражения $4B^2 - A^2$ для $p=11$ (таблица 1).

Таблица 1.

Таблица 1.

Значения выражения $4B^2 - A^2$

$\begin{matrix} B \\ A \end{matrix}$	1	4	9	5	3
1	3	4	2	8	0
4	0	1	10	5	8
9	6	7	5	0	3
5	10	0	9	4	7
3	1	2	0	6	9

Построим таблицу значений выражения $4B^2 - A$ для $p = 13$ (таблица 2).

Таблица 2

Значения выражения $4B^2 - A$

$A \backslash B^2$	1	4	9	3	12	10
2	2	1	8	10	7	12
5	12	11	5	7	4	9
6	11	10	4	6	3	8
7	10	9	3	5	2	7
8	9	8	2	4	1	6
11	6	5	12	1	11	3

Следующая таблица (таблица 3) демонстрирует количество кривых, изоморфным кривым Эдвардса, рассчитанное по формулам, доказанным в теореме 4, при значениях $p = 7, 11, 13, \dots, 47$.

Таблица 3

Таблица 3

Количество кривых Эдвардса над полями характеристики p

p	7	11	13	17	19	23	29	31	37	41	43	47
M	6	10	36	64	72	88	196	210	324	400	420	529

Пример 6: требуется найти кривую с двумя точками 4-го порядка над полем F_{11} . Примем, с учетом данных таблицы 1, $A^2 = 1, B^2 = 4$. Тогда, согласно (17), $c^2 = 9$ – квадратичный вычет в заданном поле, $a = 10$ и $b = \pm c(c^2 + a) = \pm 2$. Получили пару кривых кручения $y^2 = x^3 + 10x \pm 2$ с порядками $N_E = 8$ и $N_{E'} = 16$. Их точки второго порядка $D = (-3, 0)$ и $D' = (3, 0)$, а координаты двух точек 4-го порядка первой кривой в соответствии с (6), (7) равны: $x_1 = 6, y_1 \pm 5$.

Вообще нал полем F_{11} существует, как следует из таблицы 3, 10 кривых с ненулевыми параметрами a и b и двумя точками 4-го порядка.

Так как общее число всех кривых с ненулевыми a и b , исключая кривые с нулевым дискриминантом, близко к $(p-1)^2$, количество кривых, изоморфных кривым Эдвардса, для больших полей практически равна четверти всех эллиптических кривых, т.е. доля кривых Эдвардса среди всех эллиптических кривых примерно одна четверть.

Формулы (17), (18) конструктивны, так как позволяют рассчитывать параметры a и $\pm c$ кривой (и, соответственно, $\pm b$) при заданных значениях пар квадратичных вычетов (A^2, B^2) .

На основании условий (9) и формул (17), (18) можно предложить следующий алгоритм построения канонических кривых с двумя точками 4-го порядка.

Алгоритм 7.

Случайная генерация канонической кривой, изоморфной кривой

Эдвардса.

1. В поле F_p задаем произвольное значение пары квадратичных вычетов (A^2, B^2) или пары (A, B^2) и, согласно (17) или (18), рассчитываем параметры a и c^2 . Если вычисленное значение c^2 – квадратичный невычет, меняем параметр B^2 и повторяем расчеты.

2. Если c^2 – квадратичный вычет, находим две кривые с параметрами $(a, \pm c)$ и $(a, \pm b)$. Значение параметра b рассчитываем в соответствии с (3).

3. Находим координаты точки 4-го порядка (для построения изоморфной кривой Эдвардса).

4. Вычисляем порядок одной из кривых и, в случае неприемлемого порядка, рассчитываем порядок кривой кручения. Если решение не найдено, переходим к другой паре значений (A^2, B^2) или (A, B^2) (возвращаемся в п.1).

В предложенном виде алгоритм достаточно быстро приводит к кривой с двумя точками 4-го порядка. Действительно, все операции этого алгоритма выполняются за полиномиальное время. Что касается его "вероятностной" составляющей, то, поскольку количество квадратичных вычетов в простом конечном поле равно половине количества ненулевых элементов, то среднее количество шагов до успеха (т.е. количество случайных выборов пар (A^2, B^2))

или (A, B^2) в п.1) равно двум. Далее, как описано в [3], строится изоморфная кривая в форме Эдвардса.

Литература

1. Edwards H.M. A normal form for elliptic curves // Bulletin of the American Mathematical Society. – July 2007. – 44, № 3. – P. 393-422.

2. Bernstein Daniel J., Lange Tanja. Faster addition and doubling on elliptic curves // IST Programme under Contract IST – 2002 – 507932 ECRYPT. – 2007. – P. 1-20.

3. Бессалов А.В. Число изоморфизмов и пар кручения кривых Эдвардса над простым полем // Радиотехника. – 2011. – Вып. 167. – С. 203-208.

4. Бессалов А.В., Гурьянов А.И., Дихтенко А.А. Кривые Эдвардса почти простого порядка над расширениями малых простых полей // Прикладная радиоэлектроника. – 2012. – 11, №2. – С. 225-227.

5. Бессалов А.В., Дихтенко А.А. Криптостойкие кривые Эдвардса над простыми полями // Прикладная радиоэлектроника. – 2013. – 12, №2. – С. 285-291.

6. Дэвенпорт Г. Высшая арифметика: введение в теорию чисел // Пер. с англ. под редакцией Ю.В.Линника. – М: «Наука», 1965. – 176с.

7. Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых: Учеб. пособие. – К.: ІВЦ «Політехніка», 2004. – 224с.

УДК 681.3.06

Бессалов А.В., Ковальчук Л.В.

Точное число эллиптических кривых в канонической форме, изоморфных кривым Эдвардса над простым полем

Найдены необходимые и достаточные условия для параметров кривой в канонической форме с двумя точками 4-го порядка. Доказаны две леммы о квадратичных вычетах в конечном поле с использованием схемы Гаусса для квадратичных вычетов и невычетов. На их основе получены точные формулы расчета числа эллиптических кривых с ненулевыми параметрами a и b и двумя точками четвертого порядка, изоморфных кривым Эдвардса над простым полем. Доказано, что для больших полей доля таких кривых близка к $\frac{1}{4}$.

УДК 681.3.06

Бессалов А.В., Ковальчук Л.В.

Точна кількість еліптичних кривих у канонічній формі, які ізоморфні кривим Едвардса над простим полем

Знайдені необхідні і достатні умови для параметрів кривої у канонічній формі з двома точками 4-го порядку. Доведено дві леми про квадратичні лишки у скінченному полі з використанням схеми Гауса для квадратичних лишків та нелишків. На їх основі отримано точні формули обчислення кількості еліптичних кривих з ненульовими параметрами a та b та двома точками четвертого порядку, які є ізоморфними кривим Едвардса над простим полем. Доведено, що для великих полів доля таких кривих є близькою до $\frac{1}{4}$.

УДК 681.3.06

Bessalov A. V., Kovalchuk L. V.

The exact number of elliptic curves in the canonical form, which are isomorphic to Edwards curves over the prime field/

The necessary and sufficient conditions for the parameters of the curve in the canonical form with two points of order 4 are found. It is proved two lemmas about the properties of quadratic residues, using the Gauss scheme for quadratic residues and non-residues. Based on this lemmas the exact formulas for calculating the number of elliptic curves with non-zero parameters a and b and two points of fourth-order that are isomorphic to Edwards curves over the prime field. It is proved that for a large fields proportion of such curves is close to $\frac{1}{4}$.