УДК 681.3.06

МОЩНОСТЬ СЕМЕЙСТВА ЭЛЛИПТИЧЕСКИХ КРИВЫХ, ИЗОМОРФНЫХ КРИВЫМ ЭДВАРДСА НАД ПРОСТЫМ ПОЛЕМ

Анатолий Бессалов, Алиса Дихтенко, Оксана Цыганкова

Форма Эдвардса эллиптической кривой обладает рядом преимуществ, как перед каноническими кривыми, так и перед другими известными формами представления эллиптических кривых. Главное из них – рекордное быстродействие. Двойная координатная симметрия, характерная для любой кривой Эдвардса над простым полем, обуславливает наличие минимального кофактора 4 в ее порядке. Так, проблема поиска кривой Эдвардса сводится к задаче построения изоморфной канонической кривой с единственной точкой 2-го порядка и двумя точками 4-го порядка. В работе поставлена задача определения точного числа таких кривых над простым полем. Для решения данной задачи в работе предложен подход, основанный на замене параметров (a, b) канонической кривой парой параметров (a, c), где c – единственный в поле корень кубического уравнения. Как условия существования двух точек 4-го порядка, получена система двух линейных уравнений, связывающих неизвестные параметры c^2 и a искомой кривой и произвольные значения квадратичных вычетов (невычетов) поля. Далее в работе доказаны две леммы в теории квадратичных вычетов, построенной на схеме Гаусса. На основе предложенного подхода и доказанных лемм получены точные формулы расчета числа эллиптических кривых с ненулевыми параметрами a и b и двумя точками 4-го порядка, изоморфных кривым Эдвардса над простым полем. Они определяют точное число кривых Эдвардса. В работе описан простой алгоритм поиска канонических кривых, изоморфных кривым Эдвардса. Доказано, что для больших полей относительная доля таких кривых близка к $\frac{1}{4}$.

Ключевые слова: *каноническая эллиптическая кривая, кривая Эдвардса, кривая кручения, параметры кривой, изоморфизм, квадратичный вычет, квадратичный невычет.*

Введение. Среди форм представления эллиптических кривых в задачах криптографии наиболее перспективными представляются кривые Эдвардса [2-4, 6-7], рекордные по быстродействию и удобные для программирования. Они обладают двойной симметрией в координатах поля характеристики $p>2$ и, как следствие, четырехкратной избыточностью по числу точек N_E. Так как $N_E \equiv 0 \bmod 4$, циклические кривые Эдвардса всегда содержат одну точку 2-го порядка и 2 точки 4-го порядка. Канонических кривых с таким свойством сравнительно немного, поэтому для построения изоморфных им кривых Эдвардса возникает задача поиска кривых в форме Вейерштрасса с двумя точками 4-го порядка. В данной работе мы ввели зависимый от традиционных параметров (a,b) канонической кривой параметр c как единственный в поле F_p корень кубического уравнения. Получены системы линейных уравнений для неизвестных параметров a и c^2 с решениями, выраженными через квадратичные вычеты и невычеты. Для нахождения точного числа канонических кривых, изоморфных форме Эдвардса, потребовалось сформулировать и доказать 2 леммы о числе решений уравнений, связывающих суммы вычетов и невычетов. Доказательства опираются на схему Гаусса распределения квадратичных вычетов [5]. В итоге удалось найти формулы расчета точного числа кривых с заданными свойствами для любых $p \equiv 3 \bmod 4$ и $p \equiv 1 \bmod 4$. Кроме того, предложен алгоритм поиска изоморфных форме Эдвардса кривых, полезных для криптографии.

1. Условия, порождающие 2 точки 4-го порядка канонической кривой.

Каноническая кривая над полем характеристики $p \neq 2,3$ описывается известным уравнением [1]

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

Далее нам потребуется операция удвоения точки $P=(x_1, y_1)$, которая дает координаты точки $2P=(x_3, y_3)$, равные:

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

Пусть c – единственный в поле F_p корень кубического уравнения $x^3 + ax + b = 0$, тогда вместо (1) можно записать

$$y^2 = (x-c)\left(x^2 + cx + a + c^2\right),$$
$$b = -c^3 - ac,\ c \in F_p. \qquad (3)$$

Парабола в правой части (3) не имеет корней в поле F_p, если дискриминант квадратного уравнения является квадратичным невычетом, т.е.

$$c^2 - 4\left(a + c^2\right) = -\left(3c^2 + 4a\right) \neq A^2, \qquad (4)$$

это условие гарантирует существование единственной точки 2-го порядка кривой (3), определяемой как $D = (c, 0)$. Условие $A^2 \neq 0$, входящее в (4), исключает появление кратных корней кубического уравнения и, тем самым сингулярные кривые [1].

Пусть $P = (x_1, y_1)$ – точка 4-го порядка. Ее удвоение в соответствии с (2) дает координаты точки $D = (c, 0)$:

$$\begin{cases} x_3 = \left(\dfrac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 = c, \\ y_3 = -y_1 - \left(\dfrac{3x_1^2 + a}{2y_1}\right)(c - x_1) = 0. \end{cases} \qquad (5)$$

Из этой системы после сокращения сомножителя $\left(3x_1^2 + a\right)$ получим квадратное уравнение для координаты x_1 точки 4-го порядка:

$$x_1^2 - 2cx_1 - \left(2c^2 + a\right) = 0.$$

Корни этого уравнения находятся из

$$x_1 = c \pm \sqrt{\delta} = c \pm \sqrt{3c^2 + a}\,,\ \delta = 3c^2 + a. \qquad (6)$$

Из двух возможных решений в (6) выбирается значение x_1, лежащее на кривой E_p. Из (5) можно также получить формулу для вычисления координаты y_1 точки 4-го порядка:

$$y_1^2 = \delta\left(\pm 2\sqrt{\delta} + 3c\right). \qquad (7)$$

Из (6) следует, что точка 4-го порядка существует, если дискриминант квадратного уравнения 4δ является квадратом в поле, т.е.

$$\delta = 3c^2 + a = B^2 \neq 0. \qquad (8)$$

Здесь $B^2 \neq 0$, так как иначе, согласно (7), $y_1 = 0$ и получаем еще одну точку 2-го порядка. Теперь условия существования точек 2-го и 4-го порядков (4) и (8) можно выразить через символы Лежандра как

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

$$\text{b)}\ \left(\frac{\delta}{p}\right) = \left(\frac{3c^2 + a}{p}\right) = 1. \qquad (9)$$

Возникает закономерный вопрос: для какого числа канонических кривых существует изоморфизм с кривыми Эдвардса при любых значениях порядка поля *p*? Иными словами: какое точное число кривых Эдвардса над простым полем?

2. Определение точного числа канонических кривых, 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 [5] приводит блестящее доказательство распределения квадратичных вычетов, полученное Гауссом. Рассмотрим схему Гаусса и итоги его анализа.

Произведение $n(n+1) \bmod p$, $n = 1, 2, 3, ..., p-1$, включает составляющие ВВ (оба сомножителя – квадратичные вычеты) с общим числом (BB), НН (оба сомножителя – квадратичные невычеты) с числом (HH), и смешанные пары ВН и НВ с числом (BH) и (HB). Гаусс доказал, что имеет место система уравнений:

$$(BB) + (BH) = \frac{p - 2 - \varepsilon}{2},\ \varepsilon = (-1)^{\frac{p-1}{2}}, \qquad (10)$$

$$(HB) + (HH) = \frac{p - 2 + \varepsilon}{2}, \qquad (11)$$

$$(BB) + (HB) = \frac{p - 3}{2}, \qquad (12)$$

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

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

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:

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

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

Сумма всех сочетаний вычетов и невычетов равна $(BB) + (HH) + (BH) + (HB) = p - 2$, так как для сомножителя $(n+1)$ в произведении $n(n+1)$ последний элемент равен 0 (он исключается из решений). В нашей задаче потребуются два результата, которые мы докажем как две приведенные ниже леммы.

Лемма 1. *Уравнение* $X^2 - C^2 = Y^2 \bmod p$ *при всех ненулевых квадратах* X^2, C^2, *и* Y^2, *и фиксированном* C^2 *имеет ровно* $\dfrac{p - 4 - (-1)^{\frac{p-1}{2}}}{4}$ *решений.*

Доказательство. Воспользуемся схемой Гаусса для сомножителей $n(n+1) \bmod p$. Очевидно, что все результаты обобщаются на произведение

$n(n+C)$ при любом C. Уравнение $X^2-C^2=Y^2$ после замены $Z=(X-C)$ имеет вид $Z(Z+2C)=Y^2$. Можно принять, например, $2C=-1$ и рассмотреть уравнение $Z(Z-1)=Y^2$. Оно отвечает схеме Гаусса. В этой схеме в первой строке вместо расположения чисел Z в порядке нарастания запишем слева все ненулевые квадраты $Z=n^2=1^2,2^2,3^2,...,\left(\frac{p-1}{2}\right)^2$, а справа – все квадратичные невычеты. Вторая строка $(Z-1)$ содержит вычеты и невычеты. Число ненулевых вычетов во второй строке в левой половине таблицы равно числу (BB), которое определяется формулой (15). Это же число определяет число ненулевых решений уравнения $X^2-C^2=Y^2$. Лемма 1 доказана.

Лемма 2. *Уравнение* $X^2+C=Y^2 \bmod p$ *при всех ненулевых квадратах* X^2 *и* Y^2, *и фиксированном квадратичном невычете* C *имеет ровно* $\frac{p-2+(-1)^{\frac{p-1}{2}}}{4}$ *решений.*

Доказательство. После замены $Z=X^{-1}$, $V=YX^{-1}$, $X\neq 0$, наше уравнение примет вид $CZ^2+1=V^2$. В схеме Гаусса в первой строке расположим слева все квадраты Z^2 (сегмент длины $\frac{p-1}{2}$), справа – все квадратичные невычеты CZ^2 с таким же числом элементов. Во второй строке имеем, соответственно, (Z^2+1) слева и (CZ^2+1) – справа. Такая структура отвечает схеме Гаусса с перестановкой столбцов таблицы. Число решений уравнения $X^2+C=Y^2$ равно числу вычетов V^2 во второй строке правой половины таблицы (CZ^2+1), что, в свою очередь, равно числу $(HB)=\frac{p-2+\varepsilon}{4}$, определяемому формулой (16). Лемма 2 доказана.

Перейдем теперь к вычислению числа кривых с ненулевыми параметрами *a* и *b*, изоморфных кривым Эдвардса.

Утверждение. Число канонических кривых (1) с параметрами $a\neq 0$ и $b\neq 0$ над полем F_p с двумя точками 4-го порядка определяется формулами:

I. При $p\equiv 3 \bmod 4$

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

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

II. При $p\equiv 1 \bmod 4$

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

Доказательство.

I. Пусть $p\equiv 3 \bmod 4$, тогда (-1) – квадратичный невычет [1], т.е. $\left(\frac{-1}{p}\right)=-1$ и для (9a) невычет заменяем квадратичным вычетом:

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

Аргументы символов Лежандра (9) являются линейными функциями параметров a и c^2, следовательно, имеем невырожденную систему двух линейных уравнений над полем F_p с решениями:

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

Для кривых с параметрами $a\neq 0$ и $b\neq 0$ квадратичные вычеты $A^2\neq B^2$ и, кроме того, $4B^2\neq A^2$ (нулевые вычеты c^2 отбрасываются, так как из $c=0 \Rightarrow b=-c^3-ac=0$). Из (9) следует, что $A^2\neq 0$ и $B^2\neq 0$.

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 по условию $A^2\neq B^2$ отбрасываются из искомых решений. Кроме того, в каждой строке имеем ровно один 0, который также отбрасывается. Требуется найти число ν ненулевых недиагональных квадратов в строке, что дает решения для значений c^2 в (17). Общее число решений по всем строкам, очевидно, равно $\mu=\nu\frac{p-1}{2}$. Для примера приведем такое построение для $p=11$, таблица 1.

Из доказанной нами леммы 1 следует, что число ненулевых квадратов в каждой строке таблицы при $p\equiv 3 \bmod 4$ равно $\frac{p-3}{4}$. В таблице 1 таких квадратов по 2 в каждой строке. На главной диагонали со значениями $3A^2$ имеем квадратич-

ные вычеты, если 3 – квадрат в поле, и невычеты в противном случае.

Таблица 1

Возможные значения величины $\left(4B^2 - A^2\right)$

при $p = 11 \equiv 3 \bmod 4$

A^2 \ B^2	**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

Поскольку диагональные элементы таблицы отбрасываются из решений, в каждой строке остается $\nu = \frac{p-3}{4} - 1 = \frac{p-7}{4}$ при $\left(\frac{3}{p}\right) = 1$ либо $\nu = \frac{p-3}{4}$ при $\left(\frac{3}{p}\right) = -1$. Общее число решений для ненулевых квадратов по всем строкам, таким образом, составляет:

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

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

Число эллиптических кривых M_α, M_β с заданными свойствами вдвое выше этих значений, так как каждому решению для c^2 отвечают два корня кубики $\pm c$ и, соответственно, два коэффициента кривой $\pm b$. Мы доказали две первые формулы утверждения. Заметим, что $\left(\frac{3}{p}\right) = 1$ для всех $p \equiv \pm 1 \bmod 12$ [5]. В частности, 3 является квадратичным вычетом при $p = 11, 13, 23, 47$ и др.

II. Пусть теперь $p \equiv 1 \bmod 4$, тогда (-1) – квадратичный вычет, т.е. $\left(\frac{-1}{p}\right) = 1$ [1]. Тогда для (9а), принимая A невычетом в соответствующей системе уравнений, можно найти ее единственное решение:

$$\begin{cases} 3c^2 + 4a = A, \\ 3c^2 + a = B^2 \end{cases} \quad \left(\frac{A}{p}\right) = -1 \Rightarrow \begin{cases} a = 3^{-1}\left(A - B^2\right), \\ c^2 = 9^{-1}\left(4B^2 - A^2\right). \end{cases} \qquad (18)$$

Здесь, как видим, нулевые решения для a и c^2 невозможны. Нам остается лишь найти число квадратов в таблице ненулевых значений $\left(4B^2 - A\right)$. Если принять $B^2 = 0$, в формуле для c^2 мы получим невычет в правой части, поэтому и в данном случае учитываем лишь ненулевые элементы A и B^2.

Подобно п.1 построим квадратную таблицу из $\frac{p-1}{2}$ значений всех B^2 (по столбцам) и невычетов A (по строкам). В клетки таблицы запишем значения $\left(4B^2 - A\right)$ из (18), все не равные 0. Необходимо найти число ν квадратов в строке, что дает решения для значений c^2 в (18), и умножить это значение на число строк. Пример такого построения для $p = 13$ дан в таблице 2.

Таблица 2

Возможные значения величины $\left(4B^2 - A\right)$

при $p = 13 \equiv 1 \bmod 4$

A \ 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

Из леммы 2 следует, что уравнение $4B^2 - A = Y^2$ с ненулевыми вычетами и фиксированным невычетом A имеет $\nu_\gamma = \frac{p - 2 + (-1)^{\frac{p-1}{2}}}{4}$ решений. Это значение равно числу квадратов в каждой строке таблицы, тогда с учетом $(-1)^{\frac{p-1}{2}} = 1$ при $p \equiv 1 \bmod 4$ получаем общее число решений уравнения $\mu_\gamma = \nu_\gamma \frac{(p-1)}{2} = \frac{(p-1)^2}{8}$.

Как отмечалось выше, число кривых M_γ с заданными свойствами вдвое превосходит μ_γ. Итак, сформулированное утверждение доказано. Важно отметить, что формулы утверждения определяют точное число кривых Эдвардса над простым полем.

Замечание. За формулировку и доказательство лемм 1 и 2 и утверждения берет на себя ответственность первый автор статьи.

Рассчитанные по формулам (α), (β), (γ) мощности семейств кривых, изоморфных кривым Эдвардса, при значениях $p = 7, 11, 13, ..., 47$ приведены в таблице 3.

Пример. 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) $c^2=9$ – квадрат в поле, $a=10$ и $b=\pm c\left(c^2+a\right)=\pm 2$. Получили пару кривых кручения $y^2=x^3+10x\pm 2$ с порядками $N_E=8$ и $N_{E^t}=16$. Их точки второго порядка $D=(-3,0)$ и $D^t=(3,0)$, а координаты точки 4-го порядка первой кривой в соответствии с (6), (7) равны $x_1=c\pm\sqrt{\delta}=-3\pm 2$, $\Rightarrow$ $x_1=6$ и $y_1=\pm 5$. Здесь решения, не лежащие на кривой, отбрасываются. Вообще нал полем F_{11} существует, как следует из таблицы 3, всего 10 кривых с ненулевыми параметрами a и b и двумя точками 4-го порядка.

Таблица 3

Мощности семейств кривых, изоморфных кривым Эдвардса при $p=7, 11, 13, ..., 47$

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

Так как общее число всех кривых с ненулевыми a и b за вычетом кривых с нулевым дискриминантом близко к $(p-1)^2$, относительная доля кривых, изоморфных кривым Эдвардса, для больших полей практически равна четверти всех эллиптических кривых. Формулы (17), (18) конструктивны, так как позволяют рассчитывать параметры a и $\pm c$ кривой (и, соответственно, $\pm b$) при заданных значениях пар квадратичных вычетов $\left(A^2,B^2\right)$ или пар $\left(A,B^2\right)$. На основе условий (9) и формул (17), (18) можно предложить следующий алгоритм построения канонических кривых с двумя точками 4-го порядка:

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

2. Если c^2 – квадратичный вычет, находим 2 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 $\left(A^2,B^2\right)$ или $\left(A,B^2\right)$ (возвращаемся в п.1).

В предложенном виде алгоритм достаточно быстро приводит к кривой с двумя точками 4-го порядка. Далее, как описано в [2], строится изоморфная кривая в форме Эдвардса.

ЛИТЕРАТУРА

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

[2]. Бессалов А.В. Число изоморфизмов и пар кручения кривых Эдвардса над простым полем. Радиотехника, вып. 167, 2011. С. 203-208.

[3]. Бессалов А.В., Гурьянов А.И., Дихтенко А.А. Кривые Эдвардса почти простого порядка над расширениями малых простых полей. Прикладная радиоэлектроника №2, 2012. С.225-227.

[4]. Бессалов А.В., Дихтенко А.А., Криптостойкие кривые Эдвардса над простыми полями. Прикладная радиоэлектроника том 12 №2, 2013. С.107-113.

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

[6]. Bernstein Daniel J., Lange Tanja. Faster addition and doubling on elliptic curves. IST Programme under Contract IST–2002–507932 ECRYPT, 2007, PP. 1-20.

[7]. Edwards H.M. A normal form for elliptic curves. Bulletin of the American Mathematical Society, Volume 44, Number 3, July 2007, Pages 393-422.

REFERENCES

[1]. Bessalov A.V., Telizhenko A.B. Elliptic Curves Cryptosystems. K.: «Polytechnik», 2004, 224 p.

[2]. Bessalov A.V. (2011), "The Number of Edwards curves Isomorphisms and Twisted Pairs over the Prime Field", *Radiotechnics*, edition 167, pp. 203-208.

[3]. Bessalov A.V., Hurianov A.I., Dikhtenko A.A. (2012), "The Edwards Curves with Almost Prime Order over Prime Fields of Small Characteristics Extensions", *Applied Rhadioelectronics* No.2, pp. 225-227.

[4]. Bessalov A.V., Dikhtenko A.A. "The Cryptographically Secure Edwards Curves over Finite Fields" (2013), Applied Rhadioelectronics, Vol. 12, No 2, pp. 107-113.

[5]. Davenport H. The Higher Arithmetic: An Introduction To The Theory Of Numbers/Translated from English, edited by Linnik U.V. M: «Science», 1965, 176 p.

[6]. Bernstein Daniel J., Lange Tanja. "Faster addition and doubling on elliptic curves" (2007), *IST Programme under Contract IST–2002–507932 ECRYPT*, pp. 1-20.

[7]. Edwards H.M. "A normal form for elliptic curves" (2007), *Bulletin of the American Mathematical Society*, Vol. 44, No. 3, pp.393-422.

ПОТУЖНІСТЬ СІМЕЙСВА ЕЛІПТИЧНИХ КРИВИХ, ЩО ІЗОМОРФНІ КРИВИМ ЕДВАРДСА НАД ПРОСТИМ ПОЛЕМ

Форма Едвардса еліптичної кривої має низку переваг, як перед канонічними кривими, так і перед іншими відомими формами представлення еліптичних кривих. Головна з них – рекордна швидкодія. Подвійна координатна симетрія, що характерна для будь-якої кривої Едвардса над простим полем, обумовлює наявність мінімального кофактору 4 в її порядку. Таким чином, проблема пошуку кривої Едвардса зводиться до задачі побудови ізоморфної канонічної кривої з єдиною точкою 2-го порядку та двома точками 4-го порядку. В роботі поставлена задача визначення точного числа таких кривих над простим полем. Для розв'язання даної задачі в роботі запропонований підхід, що оснований на заміні параметрів *(a, b)* канонічної кривої парою параметрів *(a, c)*, де *c* – єдиний в полі корінь кубічного рівняння. Як умови існування двох точок 4-го порядку, отримана система двох лінійних рівнянь, що зв'язують невідомі параметри c^2 та a потрібної кривої та довільні значення квадратичних лишків (нелишків) поля. Далі в роботі доведені дві леми в теорії квадратичних лишків, яка побудована на схемі Гауса. Базуючись на запропонованому підході та доведених лемах отримані точні формули розрахунку числа еліптичних кривих з ненульовими параметрами *a* та *b* та двома точками 4-го порядку, ізоморфних кривим Едвардса над простим полем. Вони визначають точне число кривих Едвардса. В роботі описаний простий алгоритм пошуку канонічних кривих, ізоморфних кривим Едвардса. Доведено, що для великих полів відносна доля таких кривих близька до $\frac{1}{4}$.

Ключові слова: канонічна еліптична крива, крива Едвардса, крива кручіння, параметри кривої, ізоморфізм, квадратичний лишок, квадратичний нелишок.

THE CARDINAL NUMBER OF ELLIPTIC CURVES WHICH ARE ISOMORPHIC TO EDWARDS CURVES OVER A PRIME FIELD

The Edwards form of elliptic curve has advantages over canonical curves as well as over the other known forms of elliptic curves representations. Speed record is the main of them. Double symmetry of coordinates, which is typical for each Edwards curve over a prime field, leads to existence of the smallest cofactor 4 in the order of the curve. Thus, the problem of finding an Edwards curve is reduced to constructing an isomorphic canonical curve with the only point of order 2 and a couple of points of order 4. The problem of defining precise number of such curves is posed in this work. The approach, which is based on a parameters' substitution is proposed. A canonical curve parameters pair *(a, b)* is replaced by *(a, c)*, where *c* is the only root of a cube equation in the field. A system of two linear equations is obtained as the conditions for existence of two points of order 4. The equations bind the unknown parameters c^2 and *a* of the curve and the field quadratic residues (non-residues) arbitrary values. Two lemmas are proved in the quadratic residues theory, which is constructed on the Gauss scheme. Basing on the approach and the lemmas, precise formulas are obtained for counting the number of elliptic curves, which are isomorphic to Edwards curves over the prime field and have non-zero *a* and *b* parameters and a pair of points of order 4 as well. The formulas define precise number of Edwards curves. An easy algorithm is described to find canonical curves isomorphic to Edwards curves. It is proved that the rate of such curves for large fields is close to $\frac{1}{4}$.

Key words: canonical elliptic curve, Edwards curve, curve twist, curve parameters, isomorphism, quadratic residue, quadratic non-residue.

Бессалов Анатолій Володимирович, доктор технічних наук, професор, професор кафедри ММЗІ ФТІ НТУУ «КПІ».
E-mail: bessalov@ukr.net
Бессалов Анатолий Владимирович, доктор технических наук, профессор, профессор кафедры ММЗИ ФТИ НТУУ «КПИ».
Bessalov Anatoliy, D.Sc., Professor, professor of the MMIS department in FTI NTUU «KPI».

Діхтенко Аліса Анатоліївна, аспірант кафедри ТП та ОМ ДонНУ.
E-mail: alice.dikhtenko@gmail.com
Дихтенко Алиса Анатольевна, аспирант кафедры ТУ и ВМ ДонНУ.
Dikhtenko Alisa, post-graduate student of the ET and CM in DonNU.

Циганкова Оксана Валентіновна, аспірант кафедри ММЗІ ФТІ НТУУ «КПІ».
E-mail: cig@pti.kpi.ua, oksana.valent@gmail.com
Цыганкова Оксана Валентиновна, аспирант кафедры ММЗИ ФТИ НТУУ «КПИ».
Tsygankova Oksana, post-graduate student of the MMIS department in FTI NTUU «KPI».