УДК 681.3.06

А.В. Бессалов, Д.Б. Третьяков, О.В. Цыганкова

НОВЫЙ ПОДХОД К ОПРЕДЕЛЕНИЮ ТОЧНОГО ЧИСЛА КРИВЫХ ЭДВАРДСА НАД ПРОСТЫМ ПОЛЕМ

Определена зависимость параметра d кривой Эдвардса от параметров a и b эллиптической кривой в канонической форме. Приведено новое доказательство для точных формул расчета числа кривых Эдвардса, изоморфных каноническим кривым с ненулевыми параметрами a и b.

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

Предложенная в работе [1] форма эллиптической кривой, признанная учеными как форма Эдвардса [2], имеет ряд несомненных выгод в сравнении с давно известными кривыми в канонической форме. Среди них: быстродействие, универсальность закона сложения и наличие аффинных координат нейтрального элемента (нуля) абелевой группы точек. Некоторые новые свойства кривых Эдвардса были нами рассмотрены в работах [3-6]. В работе [6] мы ввели зависимый от традиционных параметров (a,b) канонической формы кривой параметр c как единственный в поле F_p корень кубического уравнения. Это позволило получить в явном виде необходимые и достаточные условия существования одной точки 2-го порядка и 2-х точек 4-го порядка. Далее в ней 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 с ненулевыми параметрами, 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. В итоге впервые найдены формулы расчета точного числа кривых с заданными свойствами и ненулевыми параметрами (a,b) для любых модулей $p\equiv 3 \bmod 4$ и $p\equiv 1 \bmod 4$.

В данной работе, опираясь на свойства кривых в канонической форме, мы нашли функциональную связь между параметром d кривой Эдвардса и параметрами (a,b) изоморфной канонической кривой. Далее приводится новое существенно более лаконичное доказательство утверждения, определяющего формулы расчета точного числа кривых Эдвардса, изоморфных кривым в форме Вейерштрасса с ненулевыми параметрами a и b. В отличие от предыдущей работы [6], это доказательство опирается на кривую, записанную в форме Эдвардса, а не в канонической форме.

1. Определение зависимости между параметрами кривой в форме Эдвардса и канонической форме

Эллиптическая кривая Вейерштрасса в канонической форме над полем характеристики $p\neq 2, 3$ описывается известным уравнением [7]

$$\mathbf{E}_p:\ y^2 = x^3 + ax + b,\quad 4a^3 + 27b^2 \neq 0,\ \ a,b\in F_p. \tag{1}$$

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

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

Найдем условия, накладываемые на параметры a и c, при которых имеется единственная точка 2-го порядка и 2 точки 4-го порядка. Главной задачей в этом разделе будет нахождение зависимости между параметрами a и c канонической формы эллиптической кривой и параметром d кривой $x^2 + y^2 = 1 + dx^2y^2$ в форме Эдвардса.

Примем $u = x - c$, тогда уравнение представляется в форме Монтгомери [2,3]

$$y^2 = u(u^2 + 3cu + a + 3c^2). \tag{3}$$

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

$$9c^2 - 4(a + 3c^2) = -(3c^2 + 4a) \neq A^2. \tag{4}$$

Это условие гарантирует существование единственной точки 2-го порядка кривой (3), определяемой как D = (0,0). Условие $A^2 \neq 0$, входящее в (4), исключает появление кратных корней кубического уравнения и, тем самым, сингулярные кривые [7].

Пусть $P = (u_1, y_1)$ – точка 4-го порядка кривой (3). Ее удвоение $2P = D$ дает координаты точки 2-го порядка D = (0, 0). При удвоении мы строим касательную к кривой в точке P, которая проходит через точку (0,0). Таким образом, из (3) получаем

$$\frac{dy}{du}\Big|u = u_1\Big| = \frac{3u_1^2 + 6cu_1 + 3c^2 + a}{2y_1} = \frac{y_1}{u_1}.$$

Отсюда

$$2y_1^{\,2} = 3u_1^{\,3} + 6cu_1^{\,2} + (3c^2 + a)u_1\,. \tag{5}$$

С другой стороны, в этой же точке согласно (3) имеем

$$2y_1^{\,2} = 2u_1^{\,3} + 6cu_1^{\,2} + 2(3c^2 + a)u_1. \tag{6}$$

Из системы уравнений (5), (6) получим квадраты для координат точки P 4-го порядка

$$u_1^{\,2} = 3c^2 + a, \qquad y_1^{\,2} = 2u_1^{\,3} + 3cu_1^{\,2}\ . \tag{7}$$

Из последнего выражения можно теперь получить

$$3\mathrm{c} = \frac{y_1^2}{u_1^3}\left(1 - 2\frac{u_1^3}{y_1^2}\right)u_1 = 2\frac{1+d}{1-d}u_1, \tag{8}$$

где

$$d = 1 - 4\frac{u_1^3}{y_1^2}\,. \tag{9}$$

Формулы (7) ,(9) позволяют выразить параметр d через параметры a и c канонической формы кривой

$$d = \frac{3c-2u_1}{3c+2u_1}, \qquad u_1 = (-1)^{\delta}\sqrt{3c^2 + a}\ , \ \ \delta \in 0, 1. \tag{10}$$

Здесь с помощью двоичного δ выбирается одно из решений квадратного уравнения u_1, которое лежит на кривой (3) и дает ровно 2 точки 4-го порядка. Второе решение не может лежать на кривой: это порождает 4 точки 4-го порядка, что нарушает структуру группы [7].

Из (4) и (7) следует, что необходимыми условиями существования одной точки 2-го и двух точек 4-го порядков являются следующие соотношения, выраженные через символы Лежандра как

$$a)\ \left(\frac{-(3c^2+4a)}{p}\right) = -1, \qquad b)\ \ \left(\frac{(3c^2+a)}{p}\right) = 1. \tag{11}$$

Можно доказать и достаточность этих условий, но это выходит за рамки нашей задачи.

С учетом (7) и (8) и деления на $u_1^{\,3}$ уравнение (3) теперь может быть приведено к виду

$$\frac{1}{1-d}v^2 = u^3 + 2\frac{1+d}{1-d}u^2 + u. \tag{12}$$

Эта форма кривой с помощью сравнительно несложной замены переменных $(u,v) \rightarrow (x,y)$ [2,3] приводится к кривой в форме Эдвардса

$$x^2 + y^2 = 1 + dx^2y^2,\ d \neq 0, 1, \quad \left(\frac{d}{p}\right) = -1. \tag{13}$$

Класс изоморфных кривых Эдвардса

$$X^2 + Y^2 = \mathrm{e}^2(1 + \tilde{d}X^2Y^2), \quad \tilde{d} = e^{-4}d, \tag{14}$$

определяется линейной заменой переменных $x \rightarrow e^{-1}X$, $y \rightarrow e^{-1}Y$. Такая трансформация расширяет множество всех кривых в $(p - 1)/2$ раз, но практически бесполезна (более того, добавление нового параметра e усложняет групповые операции).

Как нетрудно видеть из (12), заменой $d \to d^{-1}$ получаем кривую кручения с порядком $N_E^t = p + 1 + t$, симметричным порядку $N_E = p + 1 - t$ исходной кривой относительно середины $p + 1$. Заметим, что для кривых Эдвардса порядок кривой $N_E = 0 \ mod4$, поэтому след уравнения Фробениуса $t = 0$ лишь для значений модуля $p = 3 \ mod4$. В этом случае элемент поля (-1) является квадратичным невычетом, и при значении $d = d^{-1} = -1$ пара кривых кручения вырождается в одну суперсингулярную кривую с порядком $N_E = p + 1$. Это следует также из уравнения (12), которое при $d = -1$ принимает вид $y^2 = u^3 + u$ [7]. В форме (1) это кривая с коэффициентом $b = 0$.

В криптографических стандартах не используются уязвимые к MOV-атаке кривые с нулевыми параметрами a или b. Возникает вопрос о числе кривых Эдвардса, изоморфных каноническим кривым с ненулевыми коэффициентами a и b. Эта задача получила точное решение в работе [6] на основе свойств параметров a и c канонических кривых, при этом нам пришлось сформулировать и доказать 2 леммы в теории квадратичных вычетов и утверждение. В следующем разделе мы дадим более лаконичноедоказательство полученных в [6] результатов, опираясь на свойства кривой в форме Эдвардса.

2. Новое доказательство для расчета точного числа кривых Эдвардса, изоморфных кривым в канонической форме с ненулевыми параметрами *a* и *b*

Утверждение. Число кривых Эдвардса (14), изоморфных кривым (1) в канонической форме с параметрами $a \neq 0$ и $b \neq 0$ над полем F_p с двумя точками 4-го порядка определяется формулами:

I. При $p \equiv 3 mod4$

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

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

II. При $p \equiv 1 mod4$

(γ) $M_\gamma = (p-1)^2/4$.

Доказательство

1. Пусть $p \equiv 3 mod4$, тогда (-1) – квадратичный невычет [7], т.е. $\left(\frac{-1}{p}\right) = -1$, и для (11,а) 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 (11) являются линейными функциями параметров a и c^2, следовательно, имеем невырожденную систему двух линейных уравнений над полем F_p

$$3c^2 + 4a = A^2,$$
$$3c^2 + a = B^2,$$

с решениями:

$$a = 3^{-1}(A^2 - B^2), \quad c^2 = 9^{-1}(4B^2 - A^2). \qquad (15)$$

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^2отбрасываются, так как из $c = 0 \Rightarrow b = b = -c^3 - ac = 0$). Из (11) следует, что $A^2 \neq 0$ и $B^2 \neq 0$.

Так как параметр d в форме кривой Эдвардса (13) пробегает все квадратичные невычеты поля F_p, их число равно $(p-1)/2$. Из этого числа исключим значение $d = -1$,

которое порождает коэффициенты $c = b = 0$ (формулы (1), (10)). Остается $(p - 3)/2$ квадратичных невычетов d.

Пусть $\left(\frac{3}{p}\right) = 1$. Из (15) следует, что при $a = 0$ $A^2 = B^2$ и $c^2 = 3^{-1}A^2$, т.е. существует решение для с и, соответственно, для параметра d, равного согласно (10)

$$d = \frac{3c \mp 2c\sqrt{3}}{3c \pm 2c\sqrt{3}} = \frac{\sqrt{3} \mp 2}{\sqrt{3} \pm 2} \ . \qquad (16)$$

Нетрудно видеть, что оба решения (16) являются квадратичными невычетами. Например, умножив числитель и знаменатель на знаменатель, получим в знаменателе квадрат, а в числителе разность квадратов $3 - 4 = -1$, т.е. невычет при $p \equiv 3 \bmod 4$. Следовательно, из $(p - 3)/2$ значений невычетов d, исключающих значение $b = 0$, следует удалить еще 2 значения (16), порождающих коэффициент $a = 0$. При этом остается $(p - 7)/2$ допустимых значений невычетов d. Для каждой кривой Эдвардса в форме (13) существует $(p - 1)/2$ изоморфных кривых (14) с соответствующим числом квадратов e^2. Общее число кривых Эдвардса с оговоренными свойствами равно $M_\alpha = (p - 1)(p - 7)/4$. Утверждение ($\alpha$) доказано.

Пусть теперь $\left(\frac{3}{p}\right) = -1$. В этом случае $a \neq 0$, та как при $A^2 = B^2$ уравнение $c^2 = 3^{-1}A^2$ (см.(15)) не имеет решения. Тогда имеем $(p - 3)/2$ допустимых значений невычетов d, которые вместе с $(p - 1)/2$ значениями квадратов e^2 для изоморфных кривых дает $M_\beta = (p - 1))(p - 3)/4$ кривых. Утверждение (β) доказано.

2. Пусть $p \equiv 1 \bmod 4$, тогда (-1) – квадратичный вычет, т.е. $\left(\frac{-1}{p}\right) = 1$ [7]. Тогда для (11,а), принимая А невычетом в системе уравнений

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

$3c^2 + a = B^2$, находим ее единственное решение

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

Здесь мы видим, нулевые решения для a и c^2 невозможны. Итак, мы имеем $(p - 1)/2$ допустимых значений невычетов d, которые вместе с $(p - 1)/2$ значениями квадратов e^2 для кривых в форме (14) дает $M_\gamma = (p - 1)^2/4$ кривых. Утверждение (γ) доказано.

Заметим, что приведенное здесь доказательство формул, определяющих точное число кривых Эдвардса с оговоренными свойствами, существенно проще предыдущего доказательства [6].

Рассчитанные по формулам (α), (β), (γ) мощности семейств кривых, изоморфных кривым Эдвардса при малых значениях $p = 7, 11, 13, \ldots, 47$ приведены в табл. 1.

Таблица 1

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. Требуется построить кривую Эдвардса на базе изоморфной канонической кривой с двумя точками 4-го порядка над полем F_7. Примем $A^2 = 2$, $B^2 = 1$, тогда согласно (15) $c^2 = 1$ – квадрат в поле, $a = 5$ и $b = \pm c(c^2 + a) = \pm 1$. Получили пару кривых кручения $y^2 = x^3$

+ 5x±1 с порядками $N_E = 12$ и $N_E^t = 4$. Первая кривая с параметром $c = 1$ в форме Монтгомери (3) имеет вид$y^2 = u(u^2 + 3u + 1)$. Ее точка второго порядка D= (0,0), а координаты точек 4-го порядкапервой кривой в соответствии с (7) равны

$$u_1^2 = 3c^2 + a = 1 \Rightarrow u_1 = -1,\ y_1^2 = 2u_1^3 + 3cu_1^2 = 1 \Rightarrow y_1 = \pm 1 .$$

Здесь решение $u_1 = 1$, не лежащее на кривой (3), отбрасывается. Переход к кривой Эдвардса (13) осуществляется вычислением d согласно (10)

$$d = \frac{3+2}{3-2} = 5.$$

Кривая $x^2 + y^2 = (1 + 5x^2y^2) \bmod 7$ имеет порядок 12. Соответствующая кривая кручения с параметром $d^{-1} = 3$ имеет порядок 4. Кривая с параметром $d = -1$ отбрасывается. Других кривых в форме (13) при $p = 7$ не существует. Для каждой из этих двух кривых можно получить по 3 изоморфных кривых (14) с коэффициентами $e^2 = 1, 4, 2$. Вообще над полем F_7 существует, как следует из табл. 1, 6 кривых Эдвардса, изоморфных каноническим кривым с ненулевыми параметрами a и b и двумя точками 4-го порядка. Здесь каждая пара кривых кручения содержит по 3 изоморфных пары.

Формулы (15), (17) 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) [6].

Выводы

1. Впервые удалось получить зависимость между параметром d кривой в форме Эдвардса и параметрами изоморфной ей эллиптической кривой в канонической форме с параметрами a и b. Она обеспечивает простой переход из одной формы изоморфной кривой в другую.

2. Получено новое лаконичное доказательство для формул расчета точного числа кривых Эдвардса, изоморфных каноническим кривым с ненулевыми параметрами a и b.

Литература

1. EdwardsH.M. Anormal form for elliptic curves. Bulletin of the American Mathematical Society, Volume 44, Number 3, July 2007, 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, вып. 167, 2011. 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, том 11, №2, 2012. С. 225-227.

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

6. Бессалов А.В., Дихтенко А.А., Цыганкова О.В. Мощность семейства эллиптических кривых, изоморфных кривым Эдвардса над простым полем. // Захист інформації - Том 16, №1, січень-березень 2014, с.23-28.

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

Надійшла 22.08.2014 р. Рецензент: д.т.н., проф. Барабаш О.В.