УДК 681.3.06

**Бессалов А.В.**

**Построение кривой Эдвардса на базе изоморфной эллиптической кривой в канонической форме**

Получены условия существования канонических кривых, изоморфных кривым в форме Эдвардса над простым полем. Найдена зависимость параметра *d* кривой Эдвардса от параметров канонической кривой. Приведено новое доказательство для точных формул расчета числа кривых Эдвардса, изоморфных каноническим кривым с ненулевыми параметрами *а* и *b.*

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

Отримано умови існування канонічних кривих, які ізоморфні кривим у формі Едвардса над простим полем. Знайдено зв’язок параметру *d* кривої Едвардса з параметрами канонічної кривої. Приведено новий доказ для точних формул розрахунку кількості кривих Едвардса, які є ізоморфними канонічним кривим с ненульовими параметрами *а* і *b.*

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

Перспективным классом эллиптических кривых сегодня являются кривые в форме Эдвардса [1-6], рекордные по быстродействию и удобные для программирования. Двойная симметрия их в координатах поля характеристики *р* > 2 порождает четырехкратную избыточностью по числу точек *NE* . Так как *NE* ≡ 0(mod4), циклические кривые Эдвардса всегда содержат одну точку 2-го порядка и 2 точки 4-го порядка. Кривых в канонической форме с таким свойством сравнительно немного, поэтому для построения изоморфных им кривых Эдвардса следует решить задачу поиска кривых в форме Вейерштрасса с двумя точками 4-го порядка. В работе [6] мы ввели зависимый от традиционных параметров (*a*, *b*) канонической кривой параметр *с* как единственный в поле F*p* корень кубического уравнения. В ней получены системы линейных уравнений для неизвестных параметров *а* и *с*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 удалось найти формулы расчета точного числа кривых с заданными свойствами для любых *р* ≡ 3mod4 и *р* ≡ 1mod4.

В настоящей работе, опираясь на свойства кривых в канонической форме, автор нашел функциональную связь между параметром *d* кривой Эдвардса и параметрами изоморфной канонической кривой. Далее приводится новое более лаконичное доказательство утверждения, определяющего формулы расчета точного числа кривых Эдвардса, изоморфных кривым в форме Вейерштрасса с ненулевыми параметрами *а* и *b*. Кроме того, приведен алгоритм поиска изоморфных форме Эдвардса кривых, полезных для криптографии.

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

Каноническая кривая над полем характеристики *р* ≠ 2, 3 описывается известным уравнением [7]

 **Е*р*** : *y*2 = *x*3 + *ax* + *b*, 4*a*3 + 27*b*2 ≠ 0, *a*,*b* ∈ F*p*. (1)

Пусть *с* – 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* = – c3 – *ac*, *c* ∈ F*p* . (2)

Определим условия, накладываемые на параметры а и с, при которых имеется единственная точка 2-го порядка и 2 точки 4-го порядка. Второй задачей в этом разделе будет нахождение зависимости между параметрами *а* и *с* канонической формы эллиптической кривой и параметром *d* кривой $x^{2}+ y^{2}= 1+ d x^{2}y^{2}$ в форме Эдвардса.

Примем *u* = *x* – c, тогда уравнение (3) представляется в форме Монтгомери [2,3]

 *y*2 = *u*(*u*2 + 3*cu* + *a* + 3*c*2). (3)

Парабола в правой части (4) не имеет корней в поле F*p*, если дискриминант квадратного уравнения является квадратичным невычетом, т.е.

 9*с*2 – 4(*а* +3*с*2) = – (3*с*2 + 4*а*) ≠ *А*2. (4)

Это условие гарантирует существование единственной точки 2-го порядка кривой (3), определяемой для (3) как *D* = (0,0). Условие *А*2≠ 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 2*P* = *D* дает координаты точки *D* = (0, 0). При удвоении мы строим касательную к кривой в точке *Р*, которая проходит через точку (0,0). Таким образом из (3)

 

Отсюда

2*y*12 = 3*u*13 + 6*cu*12 + (3*c*2 + *a*)*u*1 . (5)

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

2*y*12 = 2*u*13 + 6*cu*12 + 2(3*c*2 + *a*)*u*1. (6)

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

 *u*12 = 3*c*2 + *a*, *y*12 = 2*u*13 + 3*cu*12 (7)

Из последнего выражения можно теперь получить

  (8)

где

 . (9)

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

  (10)

Здесь с помощью двоичного **α** выбирается одно из решений квадратного уравнения *u*1, которое принадлежит 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

  (11)

С учетом (7) и (8) и деления на *u*13 уравнение (3) теперь может быть приведено к виду

  (12)

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

 *x*2 + *y*2 = 1 + *d x*2 *y*2, *d* ≠ 0, 1,  (13)

Класс изоморфных кривых Эдвардса

 *X*2 + *Y*2 = *e*2(1 + *d*\**X*2*Y*2), *d*\*= *e*-4*d*, (14)

определяется линейной заменой переменных *х* → *е*–1*X*, *у* $\rightarrow $ *е*–1*Y.* Такая трансформация расширяет множество всех кривых в (*р* – 1)/2 раз, но практически бесполезна (более того, добавление нового параметра *е* усложняет групповые операции).

Как нетрудно видеть из (12), заменой *d* → *d* -1 получаем кривую кручения с порядком *NE*t = *p* + 1 + *t*, симметричным порядку *NE*= *p* + 1 – *t*  исходной кривой относительно середины *p* + 1. Заметим, что для кривых Эдвардса порядок кривой *NE* = 0mod4, поэтому след уравнения Фробениуса *t* может быть равен 0 лишь для значений модуля *р* = 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 *NE*= *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 приложениях не используются уязвимые к MOV-атаке кривые с нулевыми параметрами *а* или *b*. Возникает вопрос о числе кривых Эдвардса, изоморфных каноническим кривым с ненулевыми коэффициентами *а* и *b.* Эта задача получила точное решение в работе [6] на основе свойств параметров *а* и *с* канонических кривых, при этом нам пришлось сформулировать и доказать 2 леммы в теории квадратичных вычетов и теорему. В следующем разделе мы более лаконично докажем полученные в [6] результаты, опираясь в основном на свойства кривой в форме Эдвардса.

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

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

І. При *р* ≡ 3mod4

(α) *М*α = (*р* – 1)(*р* – 7)/4, если $\left(\frac{3}{p}\right)=1$;

(β) *М*β = (*р* – 1) )(*р* – 3)/4 если $\left(\frac{3}{p}\right)=-1$;

ІI. При *р* ≡ 1mod4

(γ) *М*γ = (*р* – 1)2/4.

**Доказательство.**

1. Пусть *р* ≡ 3mod4, тогда (­– 1) – квадратичный невычет [7], т.е. $\left(\frac{-1}{p}\right)=-1,$ и для (11*а*) невычет заменяем квадратичным вычетом

 

 Аргументы символов Лежандра (11) являются линейными функциями параметров *а* и *с*2, следовательно, имеем невырожденную систему двух линейных уравнений над полем F*p*

 3*с*2 +4*а* = А2,

 3*с*2 + *а* = В2 ,

с решениями:

 *а* = 3– 1(A2– B2), *c*2 = 9– 1(4B2 – A2). (15)

Для кривых с параметрами *a* ≠ 0 и *b* ≠ 0 квадратичные вычеты A2 ≠ B2 и, кроме того, 4B2 ≠ A2 (нулевые вычеты *c*2 отбрасываются, так как из *с* = 0 ⇒ *b* = – c3 – *ac* = 0). Из (11) следует, что A2 ≠ 0 и В2 ≠ 0.

Так как параметр *d* в форме кривой Эдвардса (13) пробегает все квадратичные невычеты поля F*p*, их число равно (*р* – 1)/2. Из этого числа исключим значение *d* = – 1, которое порождает коэффициенты *с* = *b* = 0 (см. формулы (1) и (10)). Остается (*р* – 3)/2 квадратичных невычетов *d*.

 Пусть  Из (15) следует, что при *а* = 0 А2 = В2  и с2 = 3– 1А2, т.е. существует решение для с и, соответственно, для параметра *d*, равного согласно (10)

  (16)

Нетрудно видеть, что оба решения (16) являются невычетами. Например, умножив числитель и знаменатель на знаменатель, получим в знаменателе квадрат, а в числителе разность квадратов 3 – 4 = – 1 , т.е невычет при *р* ≡ 3mod4. Следовательно, из (*р* – 3)/2 значений невычетов *d*, исключающих значение *b* = 0, следует удалить еще 2 значения (16), порождающих коэффициент *а* = 0. При этом остается (*р* – 7)/2 допустимых значений невычетов *d.* Для каждой кривой Эдвардса в форме (13) существует (*р* – 1)/2 изоморфных кривых (14) с соответствующим числом квадратов *е*2. Общее число кривых Эдвардса с оговоренными свойствами равно*М*α = (*р* – 1)(*р* – 7)/4. Утверждение (α) доказано.

Пусть теперь  В этом случае *а* $\ne $ 0, та как при А2 = В2  уравнение с2 = 3–1А2 (см.(15)) не имеет решения. Тогда имеем (*р* – 3)/2 допустимых значений невычетов *d*, которые вместе с (*р* – 1)/2 значениями квадратов *е*2 для изоморфных кривых дает *М*β = (*р* – 1) )(*р* – 3)/4 кривых. Утверждение (β) доказано.

1. Пусть теперь *р* ≡ 1mod4, тогда (­– 1) – квадратичный вычет, т.е.  [7]. Тогда для (11*а*), принимая А невычетом в системе уравнений

 3*с*2 + 4*а* = А, 

 3*с*2 + *а* = В2 ,

можно найти ее единственное решение

 ⇒ *а* =3– 1(A– B2), *c*2 = 9– 1(4B2 – A). (17)

Здесь, как видим, нулевые решения для *а* и *с*2 невозможны. Итак, мы имеем (*р* – 1)/2 допустимых значений невычетов *d*, которые вместе с (*р* – 1)/2 значениями квадратов *е*2 для кривых в форме (14) дает *М*γ = (*р* – 1) 2/4 кривых. Утверждение (γ) доказано.

Можно заметить, 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 значениях *р* = 7, 11, 13,…, 47 приведены в таблице 1.

 Таблица 1

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *р* | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 | 41 | 43 | 47 |
| М | 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 F7. Примем А2 = 2, В2 = 1, тогда согласно (15) *с*2 = 1 – квадрат в поле, *а* = 5 и *b* = ±*c*(*c*2 + *a*) = ± 1. Получили пару кривых кручения *y*2 = *x*3 + 5*x* ± 1 с порядками *N*E = 12 и *N*Et = 4. Первая кривая с параметром *с* = 1 в форме Монтгомери (3) имеет вид *y*2 = *u*(*u*2 + 3*u* +1). Ее точка второго порядка *D* = (0,0), а координаты точек 4-го порядка первой кривой в соответствии с (7) равны

 *u*12 = 3*c*2 + *a* = 1 ⇒ *u*1 = – 1, *y*12 = 2*u*13 + 3*cu*12 = 1 ⇒ *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)

 

Кривая *x*2 + *y*2 = (1 + 5*x*2*y*2)mod7 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 *р* = 7 не существует. Для каждой из этих двух кривых можно получить по 3 изоморфных кривых (14) с коэффициентами е2 = 1, 4, 2. Вообще нал полем F7 существует, как следует из таблицы 1, 6 кривых Эдвардса, изоморфных каноническим кривым с ненулевыми параметрами *а* и *b* и двумя точками 4-го порядка. Здесь каждая пара кривых кручения содержит по 3 изоморфных пар.

Формулы (15), (17) конструктивны, так как позволяют рассчитывать параметры *а* и ±*с* кривой (и, соответственно, ±*b*) при заданных значениях пар квадратичных вычетов (A2, B2).

На основе условий (11) и формул (15), (17) можно предложить следующий алгоритм построения канонических кривых с двумя точками 4-го порядка:

1. В поле F*p* задаем произвольное значение пары квадратичных вычетов (A2, B2) или пары (A, B2) и согласно (15) или (17) рассчитываем параметры *а* и *с*2. Если вычисленное значение *с*2 – невычет, меняем параметр B2 и повторяем расчеты.
2. Если с2 – квадратичный вычет, находим 2 кривые с параметрами (*а*, ±*с*) и (*а*, ±*b*). Значение параметра *b* рассчитываем в соответствии с (2).
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 (A2, B2) или (A, B2) (возвращаемся в п.1).

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

**Литература**

1. Edwards H.M. A normal form for elliptic curves. Bulletin of the American Mathematical Society, Volume 44, Number 3, July 2007, Pages 393-422.
2. Bernstein Daniel J., Lange Tanja. Faster addition and doubling on elliptic curves. IST Programme under Contract IST–2002–507932 ECRYPT, 2007, PP. 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. Плотность канонических эллиптических кривых со свойством изоморфизма к форме Эдвардса. Известия ЮФУ. Технические науки.", вып. №4, 2014. – С.146-153.
7. .Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых: Учеб. пособие. – К.: ІВЦ «Політехніка», 2004. – 224с.