УДК 681.3.06

А.В. БЕССАЛОВ, д-р техн. наук, О.В. ЦЫГАНКОВА

СУЕПЕРСИНГУЛЯРНЫЕ ПОЛНЫЕ КРИВЫЕ ЭДВАРДСА НАД ПРОСТЫМ ПОЛЕМ

Введение

Эллиптические кривые в форме Эдвардса над простым полем наиболее перспективны для современных криптосистем. Производительность операции экспоненцирования точки такой кривой в среднем более чем в 1,5 раза выше, чем для кривой в форме Вейерштрасса [1]. Арифметика этих кривых и их программирование существенно упрощаются в связи с наличием нейтрального элемента группы как аффинной точки кривой O = (1,0).

Суперсингулярные эллиптические кривые, интерес к которым был потерян в 90-е годы в связи с уязвимостью к MOV-атаке изоморфизма [2], в начале нынешнего столетия стали основой криптографии на спаривании точек эллиптической кривой [3]. Несомненные технологические преимущества кривых в форме Эдвардса делают актуальной задачу исследования свойств суперсингулярных кривых этого типа.

В настоящей работе дан анализ свойств суперсингулярных кривых одного из классов кривых в обобщенной форме Эдвардса [1] над простым полем – полных кривых Эдвардса. В разд. 1 вводятся основные понятия и определения в соответствии с новой классификацией кривых Эдвардса [1]. В разд. 2 сформулированы и доказаны три теоремы об условиях существования суперсингулярных кривых с j-инвариантами, равными $0,\ 12^3$ и 66^3.

1. Кривые в обобщенной форме Эдвардса и суперсингулярные кривые

В работе [4] *скрученные кривые Эдвардса* (*twisted Edwards curves*) определены как обобщение кривых Эдвардса $x^2 + y^2 = 1 + dx^2y^2$ [5] путем ввода нового параметра a в уравнение

$$\mathrm{E}_{a,d}: ax^2 + y^2 = 1 + dx^2y^2,\ a,d \in \mathrm{F_p}^*,\ d \neq 1,\ a \neq d,\ p \neq 2.$$

Наряду с вводом параметра a авторы [4] сняли ограничения на пару параметров a и d, допуская любые значения $\left(\frac{ad}{p}\right) = \pm 1$. Здесь и далее $\left(\frac{z}{p}\right)$ – символ Лежандра элемента z [3]. При $a = 1$ такая кривая получила в [4] название *кривой Эдвардса*, а если у нее d – квадратичный невычет (т.е. $\left(\frac{d}{p}\right) = -1$), то – *полной кривой Эдвардса*. Этот термин связан с полнотой закона сложения точек кривой [5]. В работе [6] мы предложили поменять местами координаты x и y в форме кривой Эдвардса с целью сохранения горизонтальной симметрии обратных точек, принятой в теории эллиптических кривых. Опираясь на это свойство, определим *кривую в обобщенной форме Эдвардса* уравнением

$$E_{a,d}: x^2 + ay^2 = 1 + dx^2y^2,\ a,d \in \mathrm{F_p}^*,\ d(d-a) \neq 0,\ d \neq 1,\ p \neq 2. \quad (1)$$

Тогда модифицированный универсальный закон сложения точек имеет вид

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1x_2 - ay_1y_2}{(1-dx_1x_2y_1y_2)}, \frac{x_1y_2 + x_2y_1}{(1+dx_1x_2y_1y_2)}\right). \quad (2)$$

При совпадении двух точек получим из (2) закон удвоения точек

$$2(x_1, y_1) = \left(\frac{x_1^2 - ay_1^2}{(1-dx_1^2y_1^2)}, \frac{2x_1y_1}{(1+dx_1^2y_1^2)}\right). \quad (3)$$

Определяя теперь обратную точку как $-P = (x_1, -y_1)$, согласно закону (2) получаем координаты нейтрального элемента группы $(x_1, y_1) + (x_1, -y_1) = \mathrm{O} = (1, 0)$. На оси x также всегда лежит точка $D_0 = (-1, 0)$ второго порядка, для которой в соответствии с (3) $2D_0 = (1, 0) = \mathrm{O}$. В зависимости от свойств параметров a и d можно получить еще две особые

точки второго порядка и две особые точки 4-го порядка. Как следует из (1), на оси y могут также лежать не особые точки 4-го порядка $\pm F_0 = (0, \pm 1/\sqrt{a})$, для которых $\pm 2F_0 = D_0 = (-1, 0)$. Эти точки существуют над полем F_p, если параметр a является квадратом (квадратичным вычетом).

Согласно нашей классификации кривых в форме (1), обоснованной в [1, 7, 8], скрученная кривая имеет параметры a и d со свойствами квадратичных невычетов $\left(\frac{a}{p}\right) = \left(\frac{d}{p}\right) = -1$, тогда как при $a = 1$ определены полные кривые Эдвардса с параметром d, являющимся квадратичным невычетом $\left(\frac{d}{p}\right) = -1$, и квадратичные кривые Эдвардса, для которых $\left(\frac{d}{p}\right) = 1$. Полные кривые Эдвардса являются циклическими в отношении точек четных порядков и не содержат особых точек. Важно, что нециклические скрученные и квадратичные кривые Эдвардса образуют пары квадратичного кручения, параметры которых связаны линейным преобразованием $a' = ca, d' = cd$, где $\left(\frac{c}{p}\right) = -1$ [1,8]. Этим свойством удобно пользоваться при анализе суперсингулярных кривых этих классов, для которых можно принять $a = 1$ и ограничиться одним параметром со свойством $\left(\frac{d}{p}\right) = 1, d \neq 1$. Другими словами, анализ суперсингулярных кривых двух классов – скрученных и квадратичных кривых Эдвардса – сводится к анализу последних с одним параметром d.

Порядок N_E эллиптической кривой над конечным полем $F_q, q = p^m$ определяется на основе следа уравнения Фробениуса t как $N_E = q + 1 - t$. Для кривой квадратичного кручения E^t соответствующий порядок будет $N_E^t = q + 1 + t$. Эллиптическая кривая является суперсингулярной тогда и только тогда, когда над любым расширением простого поля F_p след $t \equiv 0 mod p$. [3]. Иными словами, в алгебраическом замыкании $\overleftarrow{F_p}$ суперсингулярная кривая не содержит точек порядка p. Над простым полем F_p такая кривая всегда имеет порядок $N_E = p + 1$, а над любым расширением этого поля $N_E \equiv 1 mod p$.

Для кривой

$$E: \quad Y^2 = X^3 + AX + B \tag{4}$$

в канонической форме Вейерштрасса с j-инвариантом [3, 9]

$$j(E) = \frac{12^3\, 4A^3}{4A^3 + 27B^2} \tag{5}$$

характерными являются значения $j(E) = 0$ при $A = 0$ и $j(E) = 12^3$ при $B = 0$. Эти значения j-инварианта часто (но не всегда) порождают суперсингулярную кривую.

Изоморфизм кривых в формах (1) и (4) достигается лишь приблизительно для четверти всех кривых в форме Вейерштрасса, содержащих одну или три точки 2-го порядка. Порядок таких кривых $N_E \equiv 0 mod 4$. Наиболее удобной формой их представления является кривая в форме Монтгомери [4]

$$E_{C,D}: \quad Dv^2 = u^3 + Cu^2 + u, C = 2\frac{a+d}{a-d}, D = \frac{4}{a-d}, a = \frac{C+2}{D}, d = \frac{C-2}{D}, \tag{6}$$

$$C^2 \neq 4.$$

Как частный случай канонической кривой (4) в форме Вейерштрасса, уравнение (6) часто используется при анализе свойств кривой в обобщенной форме Эдвардса (1). Так как кривые (1) и (6)) изоморфны ($E_{a,d} \sim E_{C,D}$) [1, 4], доказательства условий существования таких суперсингулярных кривых равнозначны.

Для кривой (1) j-инвариант [10]

$$j(a, d) = \frac{16(a^2 + d^2 + 14ad)^3}{ad(a-d)^4}, ad(a - d) \neq 0. \tag{7}$$

Так как j-инвариант сохраняет свое значение для всех изоморфных кривых и пар квадратичного кручения [3], он является полезным инструментом при поиске суперсингулярных кривых. Как отмечалось, для этих целей параметр a в (7) является избыточным, т.е. можно принять $a = 1$ и рассматривать свойства лишь полных и квадратичных кривых Эдвардса. Если квадратичная кривая – суперсингулярная, то и соответствующая ей скрученная кривая (как пара квадратичного кручения) – также суперсингулярная. В этой связи в дальнейшем принимаем $a = 1$ и будем пользоваться j-инвариантом $j(1, d)$.

Одним из свойств j-инварианта является

$$j(1, d) = j(1, d^{-1}). \tag{8}$$

Это свойство легко доказать, обращая элемент d в (7) и умножая числитель и знаменатель на d^6, после чего можно получить равенство (8). Как известно, обращение параметра $d \to d^{-1}$ дает кривую квадратичного кручения для полной кривой Эдвардса [5], и изоморфную – для квадратичной кривой Эдвардса [1].

2. Необходимые условия существования суперсингулярных полных кривых Эдвардса

Порядок кривых Эдвардса $N_E \equiv 0 mod 4$, тогда суперсингулярные кривые в форме Эдвардса с порядком $N_E = p + 1$ существуют лишь при $p \equiv 3 mod 4$. Поэтому в данной работе рассматриваем лишь этот случай как первое необходимое условие существования суперсингулярных кривых этого класса.

Полная кривая Эдвардса определена в работах [4, 5] как частный случай кривой (1):

$$\mathrm{E}_{1,d}: \quad x^2 + y^2 = 1 + dx^2y^2 \,,\ d \in \mathrm{F_p}^*,\ d(d-1) \neq 0,\ \left(\frac{d}{p}\right) = -1 \tag{9}$$

Характерными свойствами этого класса кривых являются цикличность группы точек четного порядка и отсутствие особых точек (или полнота закона сложения точек) [5].

2.1. Суперсингулярные полные кривые Эдвардса с нулевым j-инвариантом

Такие кривые изоморфны подклассу кривых (4) в форме Вейерштрасса вида $Y^2 = X^3 + B$ с j-инвариантом (5), равным 0. Хотя любая кривая этого вида имеет нулевой j-инвариант, не все они являются суперсингулярными. Кроме того, не любая из этих кривых сводится к форме Монтгомери (6).

Теорема 1. *При* $p \equiv -1 mod 12$ *полная кривая Эдвардса над простым полем с нулевым j-инвариантом* и *с параметрами* $d_{1,2} = -7 \pm 4\sqrt{3}$, *является суперсингулярной.*

Доказательство. При нулевом значении j-инварианта (7) решения для параметра d кривой определяются корнями квадратного уравнения $d^2 + 14d + 1 = 0$

$$d_{1,2} = -7 \pm 4\sqrt{3}, d_1 d_2 = 1. \tag{10}$$

Отсюда следует, что кривые с нулевым j-инвариантом существуют лишь при существовании элемента простого поля $\sqrt{3}$. Элемент 3 является квадратичным вычетом при $p \equiv \pm 1 mod 12$ [11]. При $p \equiv 1 mod 12$ имеет место сравнение $p \equiv 1 mod 4$, при этом кривые Эдвардса несуперсингулярны. Итак, в условиях теоремы кривая с параметрами (10) имеет нулевой инвариант $j(1, d) = 0$.

Докажем, что порядок кривой в условиях теоремы $N_E = p + 1$. Сначала покажем, что при выполнении сравнения $p \equiv -1 mod 12$ выполняется и условие $p \equiv 3 mod 4$. Действительно, из $p = 12k - 1$ следует $p \equiv -1 mod 4 = 3 mod 4$. Далее, любая кривая с нулевым j-инвариантом (5) изоморфна кривой (4) вида $Y^2 = X^3 + B$. При выполнении условия $p \equiv -1 mod 12$ теоремы также справедливо сравнение $p \equiv -1 mod 3 \equiv 2 mod 3$, тогда порядок $(p - 1)$ мультипликативной группы поля не делится на 3. При этом группа не

содержит подгруппы (и, соответственно, элементов) 3-го порядка и НОД$(p-1,3)=1$ [12]. Если $g-$ примитивный элемент мультипликативной группы поля F_p, то и g^3 – также примитивный элемент. В уравнении $Y^2=X^3+B$ для всех $X=0\ldots(p-1)$ правая часть уравнения при любом B пробегает все те же значения. Из них $\frac{p-1}{2}$ квадратичных вычетов, которые дают ровно $(p-1)$ точек кривой, элемент 0 из множества значений X^3+B дает одну точку 2-го порядка, тогда с добавлением точки на бесконечности получаем порядок кривой $N_E=p+1$. Подчеркнем, что данная кривая циклическая с одной точкой 2-го порядка и двумя точками 4-го порядка (т.к. при $p\equiv 3mod4$ имеет место $4|(p+1)$), и, следовательно, она изоморфна полной кривой Эдвардса, при этом все корни в (10) – квадратичные невычеты. Таким образом, в условиях теоремы кривая (1), изоморфная кривой в форме Вейерштрасса $Y^2=X^3+B$, имеет порядок $N_E=p+1$ и, следовательно, является суперсингулярной.

Если в уравнении $Y^2=X^3+B$ принять $B=-e^3$ и $u=X-e$, можно получить изоморфную кривой (4) кривую (6) в форме Монтгомери вида

$$y^2=u^3+3eu^2+3e^2u.$$

Делением на $(\sqrt{3}e)^3$ она приводится к виду (6)

$$v^2=u^3+\sqrt{3}u^2+u.$$

Тогда с учетом уравнения (6) из равенства $2\frac{1+d}{1-d}=\sqrt{3}$ получаем

$$d=\frac{\sqrt{3}-2}{\sqrt{3}+2}$$

и два решения для этого параметра

$$d_{1,2}=\left(\frac{\sqrt{3}-2}{\sqrt{3}+2}\right)^{\pm 1}.$$

Эти значения совпадают с решениями (10), в чем можно убедиться умножением числителя и знаменателя d_1 на $\left(\sqrt{3}-2\right)$, тогда $.-\left(\sqrt{3}-2\right)^2=-7+4\sqrt{3}$. Аналогично получаем и второе решение для инверсии ${d_1}^{-1}$. В произведении $\left(\sqrt{3}+2\right)\left(\sqrt{3}-2\right)=-1$ один из сомножителей – квадратичный вычет, другой – квадратичный невычет, так как $p\equiv 3mod4$ и $\left(\frac{-1}{p}\right)=-1$ [9]. Это доказывает, что параметры (10) – квадратичные невычеты и кривая входит в класс полных кривых Эдвардса. Теорема доказана. ▲

В табл. 1 в качестве примера приведены значения p в первой сотне чисел, для которых справедливы условия теоремы, вместе со взаимно обратными значениями $d_{1,2}$, вычисленными согласно (10). Они определяют все суперсингулярные полные кривые Эдвардса с нулевым j-инвариантом и порядком $N_E=p+1$.

Таблица 1

p	11	23	47	59	71	83
$d_{1,2}$	(2, 6)	(11,21)	(39,41)	(8,37)	(23,34)	(24,45)

Все полные кривые Эдвардса с нулевым j-инвариантом при $p\equiv 1mod12$ (при этом $p\equiv 1mod4$) являются несуперсингулярными. Это очевидно, так как в этом случае $(p+1)$ не делится на 4.

2.2. Суперсингулярные полные кривые Эдвардса с j-инвариантом $j(1,d)=12^3$

Приведем условия существования суперсингулярных кривых этого класса.

Теорема 2. *При* $p\equiv 3mod4$ *полная кривая Эдвардса над простым полем с j-инвариантом* $j(1,d)=12^3$ и *с параметром* $d=-1$ *является суперсингулярной.*

Доказательство. Для кривой в форме Вейерштрасса (4) вида $Y^2=X^3+AX$ $(B=0)$ согласно (5) получаем $j(E)=12^3$. Изоморфизм с полной кривой Эдвардса здесь существует лишь в случае, если $A=G^2$, тогда кривая (4) сводится к форме Монтгомери (6). Разделим правую часть уравнения (4) при $B=0$ на G^3, тогда после замены $\frac{X}{G}\to u, \frac{Y}{G}\to v$ приходим к кривой (6) вида $Dv^2=u^3+Cu^2+u$, при этом $C=2\frac{1+d}{1-d}=0$. Отсюда следует, что $1+d==0, \Rightarrow d=-1$. Это значение есть квадратичный невычет при $p\equiv 3mod4$ [9], и изоморфная кривой (6) кривая (1) – полная кривая Эдвардса.

С другой стороны, суперсингулярные кривые над простым полем со следом Фробениуса $t=0$ изоморфны своему квадратичному кручению: $E\sim E^t$. Переход к кривой кручения в классе полных кривых Эдвардса $x^2+y^2=1+dx^2y^2, \left(\frac{d}{p}\right)=-1,$ достигается, как отмечалось, обращением параметра $d\to d^{-1}$ [5]. Тривиальным примером суперсингулярной кривой в этом классе является значение $d=d^{-1}=-1$, найденное выше для кривой в форме Монтгомери. В этом случае пара квадратичного кручения вырождается в одну кривую, след Фробениуса $t=0$ и порядок кривой $N_E=p+1$. Теорема доказана. ▲

Для пары $(1,d)=(1,-1)$ согласно (7) получим

$$j(1,d)=\frac{16(-12)^3}{-4^2}=12^3.$$

Заметим, что кривая (4) при $B=0$ может оказаться нециклической (с тремя точками 2-го порядка), но всегда является суперсингулярной при $p\equiv 3mod4$ [9].

В общем случае для нахождения кривой Эдвардса с j-инвариантом $j(1,d)=12^3$ в соответствии с (7) следует решить уравнение 6-й степени:

$$\frac{16(1+d^2+14d)^3}{d(1-d)^4}=12^3\Rightarrow(1+d^2+14d)^3-2^23^3\,d(1-d)^4=0. \qquad (11)$$

Уравнение (11) может дать до шести корней или три пары взаимно-обратных значений $d_i^{\pm1}, i=1,2,3$. Пары корней, являющихся квадратичными невычетами, отвечают полной кривой Эдвардса, в противном случае – квадратичной кривой. Как следует из приведенного анализа, существует единственная полная кривая Эдвардса с j-инвариантом $j(1,d)=12^3$ при $d=-1$ (этот корень уравнения (11) имеет кратность 2).

Значениями $j(1,d)=0,12^3$ не исчерпываются все суперсингулярные кривые. В работах [1, 6] мы обнаружили и привели доказательство теоремы об условии существования полной суперсингулярной кривой с параметрами $d=2^{\pm1}$. Здесь дадим новое строгое доказательство этой теоремы.

2.3. Суперсингулярные полные кривые Эдвардса с j-инвариантом $j(1,d)=66^3$

Принимая $x,y\neq 0,1$, разделим уравнение (9) на x^2y^2, тогда получим

$$E_{1,d}\colon (y^{-2}-1)(x^{-2}-1)=1-d\Rightarrow y^{-2}-1=\frac{1-d}{x^{-2}-1}, x,y\neq 0,1 \qquad (12)$$

Иногда это уравнение удобней записать в форме

$$y^{-2}=\frac{x^{-2}-d}{x^{-2}-1}, x,y\neq 0,1.$$

Для квадратичной кривой Эдвардса отсюда сразу определяются координаты особых точек $x^{-2}=d, y^{-2}=d$.

После исключения четырех базовых точек $O, D, \pm F$ $(x, y \neq 0,1)$ суперсингулярные кривые следует искать на основе нахождения числа решений уравнения (12) со значениями параметра $d^{\pm 1}$, дающими одинаковое число решений (это справедливо для полных кривых, у которых замена $d \to d^{-1}$ дает пару квадратичного кручения [5]).

Уравнение (12) можно использовать для поиска параметров d суперсингулярных кривых, для которых подмножества левой и правой части уравнения, включающие квадратичные вычеты и невычеты, пересекаются, т.е. содержат одинаковые элементы. Такой подход требует изучения свойств множества $\{x^{-2} - 1\}$ с учетом структуры полных кривых Эдвардса (без особых точек) и квадратичных кривых Эдвардса (с особыми точками 2-го и 4-го порядков). В данной работе мы рассматриваем лишь первый класс этих кривых. Подобный же анализ для квадратичных и скрученных кривых Эдвардса мы дадим в следующей работе.

Обозначим множество всех элементов в знаменателе (12) как

$$U = \{u^{-2} = x^{-2} - 1, x = 2,3, \dots, \tfrac{(p-1)}{2}\}. \quad (13)$$

Мощность этого множества $|U| = \frac{(p-3)}{2}$.

Пусть

$$Q_p = \{1^2, 2^2, 3^2, \dots \left(\tfrac{(p-1)}{2}\right)^2\} -$$

множество всех ненулевых квадратов, и, соответственно, $\overline{Q_p}$ – множество всех квадратичных невычетов. При $p \equiv 3 mod 4$, очевидно, $\overline{Q_p} = -Q_p$.

Множество U (13) является суммой непересекающихся подмножеств квадратичных вычетов из множества Q_p

$$S = \{u^{-2} = (x^{-2} - 1) \in Q_p, x = 2,3, \dots, \tfrac{(p-1)}{2}\} \quad (14)$$

и невычетов

$$\bar{S} = \{u^{-2} = (x^{-2} - 1) \in \overline{Q_p}, x = 2,3, \dots, \tfrac{(p-1)}{2}\} \quad (15)$$

с элементами из множества $\overline{Q_p}$ квадратичных невычетов. Мы рассматриваем множества как наборы элементов поля F_p, вычисленных при различных значениях $x, y \neq 0,1$.

Для доказательства теоремы нам потребуются доказать следующие леммы.

Лемма 1. *При p* ≡ 3mod4 *мощности множеств ненулевых квадратов*

$$S = \{u^{-2} = (x^{-2} - 1) \in Q_p, x = 2,3, \dots, \tfrac{(p-1)}{2}\}$$

и квадратичных невычетов

$$\bar{S} = \{u^{-2} = (x^{-2} - 1) \in \overline{Q_p}, x = 2,3, \dots, \tfrac{(p-1)}{2}\}$$

одинаковы и равны $|S| = |\bar{S}| = \frac{(p-3)}{4}$.

Доказательство. Число решений уравнения $u^{-2} = x^{-2} - 1$ определяется числом квадратов в правой части. Подобная задача была рассмотрена в работе [13]. Согласно лемме 2 этой работы при p ≡ 3mod4 число ненулевых квадратичных вычетов в множестве элементов $\{(x^{-2} - 1), x = 1,2,3, \dots, \frac{(p-1)}{2}\}$, равно $(p - 3)/4$. При $x = 1$ получаем $(x^{-2} - 1) = 0 -$ элемент, не входящий в число вычетов, поэтому число ненулевых квадратичных вычетов u^{-2} равно $(p - 3)/4$. Так как по условию $x \neq 1$, то множество всех элементов $\{x^{-2} - 1\}$ мощности $(p - 3)/2$ содержит равное число $(p - 3)/4$ квадратичных вычетов и невычетов, т.е. $|S| = |\bar{S}| = \frac{(p-3)}{4}$. Лемма доказана.

Очевидно, что утверждение леммы инвариантно к замене $x^{-2} \to x^2$.

Лемма 2. *При* $p \equiv 3\mathrm{mod}8$ *множество ненулевых квадратов* $S = \{u^{-2} = (x^{-2} - 1) \in Q_p, x = 2,3,\dots,\frac{(p-1)}{2}\}$ и множество квадратичных невычетов $-S = \{-u^{-2} = (1 - x-2) \in Qp\ x=2,3,\dots, p-12\}$ содержат *ровно по* $(p-3)8$ *пар взаимно-обратных элементов.*

Доказательство. Пусть для некоторого $z^2 \neq x^2$ существует элемент из множества $\{u^{-2} = x^{-2} - 1\}$, такой, что $(z^{-2} - 1)(x^{-2} - 1) = 1$. Тогда элементы $((z^{-2} - 1), (x^{-2} - 1)) \in S$ взаимно-обратны. Уравнение для z^{-2} можно записать как

$$z^{-2} - 1 = \frac{1}{x^{-2}-1},$$

или

$$z^{-2} = \frac{x^{-2}}{x^{-2}-1} \Rightarrow z^2 = 1 - x^2, x, z \neq 0,1. \quad (16)$$

Согласно лемме 1 число решений этого уравнения для всех $x = 2,3,\dots,\frac{(p-1)}{2}$ равно $(p - 3)/4$. При $p \equiv 3\mathrm{mod}8$ для каждого квадрата из множества квадратов S найдется элемент $(z^{-2} - 1)$ этого множества, обратный первому. Так как при $p \equiv 3\mathrm{mod}8$ элемент $2 \in \overline{Q_p}$ [9], то $x^{-2} \neq 2$ и $x^{-2} - 1 \neq 1$. Другими словами, множество S не содержит 1. Таким образом, множество S в условиях леммы включает ровно $(p - 3)/8$ пар взаимно-обратных элементов. В множестве $-S$ все квадратичные вычеты множества S становятся невычетами с сохранением свойства обратимости (но уже только для квадратичных невычетов) и числа элементов. Лемма доказана.

Лемма 3. *При* $p \equiv 3\mathrm{mod}8$ *подмножество* $\bar{S}$ *множества* U *не содержит пар взаимно-обратных элементов.*

Доказательство. Допустим обратное, и справедливо уравнение (16) для квадратичных невычетов подмножества $\bar{S}$. Тогда

$$z^{-2} = \frac{x^{-2}}{x^{-2}-1} \Rightarrow \left(\frac{z}{x}\right)^{-2} = \frac{1}{x^{-2}-1}. \quad (17)$$

Правая часть равенства согласно допущению есть квадратичный невычет, а левая – квадрат. Для половины квадратов множества $S = \{x^{-2} - 1\}$ дает согласно лемме 2 $\frac{(p-3)}{8}$ решений, тогда как для половины невычетов $\bar{S}$ таких решений нет. Следовательно, все элементы в подмножестве $\bar{S}$ необратимы (т.е. $\bar{S}$ не содержит пар мультипликативно обратных элементов). Лемма доказана.

С другой стороны, если допустить обратимость элементов $\bar{S}$, то вместе с обратимостью элементов S это даст $(p - 3)/2$ решений уравнения (12) и $2(p - 3)$ точек кривой, что невозможно.

Лемма 4. *При* $p \equiv 3\mathrm{mod}8$ *множества* $U = \{u^{-2} = x^{-2} - 1, x = 2,3,\dots,\frac{(p-1)}{2}\}$ *и* $-U$ *содержат по* $(p - 3)/8$ *одинаковых квадратичных вычетов и невычетов, и мощность их пересечения равна* $(p - 3)/4$.

Доказательство. Обозначим пересечение множеств U и $-U$ как $V = U * (-U)$. Тогда оно имеет подмножества S_v квадратичных вычетов и $\overline{S_v}$ квадратичных невычетов, причем $V = S_v + \overline{S_v}$. Одинаковые элементы этих множеств определяются из равенства

$$x^{-2} - 1 = 1 - z^{-2} \Rightarrow z^{-2} = 2 - x^{-2}, x = 2,3,\dots,\frac{(p-1)}{2}.$$

Как и в лемме 1, это уравнение имеет $(p - 3)/4$ решений [13], а множество $\{1 - z^{-2}\} = -U$ является суммой подмножеств квадратов $-\bar{S}$ и квадратичных невычетов $-S$ равной мощности $(p - 3)/8$. Это следует из того, что множество U также содержит два непересекающихся подмножества S и $\bar{S}$ с числом элементов по $(p - 3)/8$. Таким образом, ровно половина всех квадратов S множества U и невычетов $\bar{S}$ этого множества совпадают с

соответствующими подмножествами множества $-U$, при этом $|S_v| = |\overline{S_v}| = (p - 3)/8$. Тогда общее число совпадающих элементов этих множеств $|V| = |U * (-U)| = (p - 3)/4$. Это доказывает утверждение леммы.

Лемма 5. *При $p \equiv 3 mod 8$ для каждой пары взаимно-обратных квадратов $u^{\pm 2}$ множества S существует единственный элемент множества невычетов $\bar{S}$, равный $-u^2$ или $-u^{-2}$.*

Доказательство. Как следует из леммы 2, множества вычетов S и невычетов $-S$ состоят из $\frac{(p-3)}{8}$ пар взаимно-обратных элементов. Вместе с тем, согласно лемме 4 множества невычетов $\bar{S}$ и $-S$ пересекаются лишь наполовину и содержат $\frac{(p-3)}{8}$ одинаковых элементов. Требуется доказать, что из каждой пары взаимно-обратных элементов множества $-S$ лишь один элемент попадает в множество $\bar{S}$.

Пусть $u_1^{\pm 2} = (x_1^{-2} - 1)^{\pm 1}$ – пара квадратов множества S. Предположим, что существует квадратичный невычет $u_2^{-2} = (x_2^{-2} - 1) \in \bar{S}$, такой, что справедливо

a) $(x_2^{-2} - 1) = -u_1^{-2} = (1 - x_1^{-2}) \Rightarrow x_2^{-2} = (2 - x_1^{-2})$

b) $(x_2^{-2} - 1) = -u_1^{2} = (1 - x_1^{-2})^{-1} \Rightarrow x_2^{-2} = \frac{(2 - x_1^{-2})}{(1 - x_1^{-2})}$

Поскольку при $p \equiv 3 mod 8$, элемент $2 \in \overline{Q_p}$ [12], правая часть равенств a) и b) не равна 0 (это тождественно отсутствию особых точек деления на 0 у полной кривой Эдвардса (12) при $d = 2^{\pm 1}$). По условию элемент $(1 - x_1^{-2})$ является квадратичным невычетом. Отсюда ясно, что существует единственное решение для невычета $-u_1^{-2}$ или $-u_1^2$ множеств $\bar{S}$ и $-S$, так как при выполнении равенства a) не выполняется равенство b), и наоборот. Лемма доказана.

Теорема 3. *При $p \equiv 3 mod 8$ полная кривая Эдвардса над $\mathbf{F}_p$ с параметрами $d = 2^{\pm 1}$ является суперсингулярной.*

Доказательство. Из сравнения $p \equiv 3 mod 8$ сразу следует $p \equiv 3 mod 4$, так как редукция первого сравнения $8k + 3, k = 1,2, \ldots$, по модулю 4 дает второе. Следовательно, $4|(p + 1)$ и порядок кривой делится на 4. При выполнении сравнения $p \equiv 3 mod 8$ элемент 2 поля F_p является квадратичным невычетом, т.е. $\left(\frac{2}{p}\right) = -1$ [12], тогда при $d = 2^{\pm 1}$ имеем полную кривую Эдвардса. Требуется доказать, что при $d = 2$ порядок кривой (9) равен $p + 1$ и кривая суперсингулярная.

При $d = 2$ уравнение (12) имеет вид

$$y^{-2} - 1 = \frac{1}{1 - x^{-2}}, x = 2,3, \ldots, \frac{(p-1)}{2}. \quad (18)$$

Как следует из леммы 1, одинаковые множества $U = \{y^{-2} - 1\}$ и $\{x^{-2} - 1\}$ содержат по $\frac{(p-3)}{4}$ квадратичных вычетов и невычетов, что составляет ровно половину всех вычетов (без элемента 1) и невычетов (без элемента -1). В соответствии с (18) надо найти число совпадающих элементов множества U и множества обратных элементов $-U^{-1} = \{u^2 = (1 - x^{-2}), x = 2,3, \ldots, \frac{(p-1)}{2}\}\}$.

Свойства множеств квадратов S и квадратичных невычетов $\bar{S}$ (леммы 2 и 3) сводятся к тому, что множество S состоит из $\frac{(p-3)}{8}$ пар $u^{\pm 2}$ взаимно-обратных квадратов, тогда как множество $\bar{S}$ не содержит таких пар.

Лемма 4 утверждает, что пересечение множеств U и $-U$ содержит подмножества S_v квадратичных вычетов и $\overline{S_v}$ квадратичных невычетов с мощностями $|S_v| = |\overline{S_v}| = (p - 3)/8$. Тогда согласно лемме 5 для каждой пары квадратов $u_1^{\pm 2} \in S$ существует единственный квадратичный невычет из пары $-u_1^{\pm 2}$, который принадлежит множеству квадратичных невычетов $\bar{S}$.

С учетом этих свойств существует одно из двух альтернативных подмножеств $G_1 \in U$ или $G_1^* \in U$ из четырех элементов

$$G_1 = \{u_1^{-2}, u_1^2, -u_1^{-2}, -u_2^{-2}\} \in U, \quad (19)$$

$$G_1^* = \{u_1^{-2}, u_1^2, -u_1^2, -u_2^{-2}\} \in U, \quad (20)$$

из которых первые два являются парой взаимно-обратных квадратов, а последние – парой необратимых квадратичных невычетов $(u_1^{\pm 2} * u_2^{-2} \neq 1)$. Необратимость последних невычетов следует из леммы 3. Последний элемент в (19) или (20) может быть любым отличным от первого невычетом множества $\bar{S}$. Умножая все его элементы на -1 и обращая каждый из них, получим одно из подмножеств

$$-G_1{}^{-1} = \{-u_1^2, -u_1^{-2}, u_1^2, u_2^2\} \in -U^{-1},$$

$$(-G_1^*)^{-1} = \{-u_1^2, -u_1^{-2}, u_1^{-2}, u_2^2\} \in -U^{-1}.$$

Отсюда следует, что их пересечение с подмножествами соответственно (19) и (20) имеет две альтернативы:

$$G_1 * (-G_1{}^{-1}) = \{u_1^2, -u_1^{-2}\}, \text{ или } G_1^* * (-G_1^*)^{-1}) = \{u_1^{-2}, -u_1^2\}.$$

Каждая из них содержит ровно два элемента, один из которых – квадратичный вычет, а другой – невычет. Так как все множество U согласно лемме 2 содержит $\frac{(p-3)}{8}$ пар взаимно-обратных квадратов, то можно построить то же число его подмножеств G_1 (или G_1^*), элементы которых определены подмножествами (19) или (20). Тогда мощность пересечения двух множеств U и $(-U)^{-1}$

$$|U * (-U)^{-1}| = \frac{(p-3)}{4}.$$

Итак, имеется ровно $\frac{(p-3)}{4}$ решений уравнения (18), из которых половину решений дают квадратичные вычеты, половину – невычеты. Так как каждое решение уравнения (18) дает по четыре точки $(\pm x, \pm y)$ кривой (9), получаем $(p-3)$ точек, удовлетворяющих уравнению (18). Добавляя четыре отброшенные при анализе точки O = (1, 0), D = (– 1, 0) и $\pm F = (0, \pm 1)$, получаем при $d = 2$ порядок кривой (9) $N_E = p + 1$. Такая кривая является суперсингулярной со следом Фробениуса $t = 0$, поэтому пара квадратичного кручения с параметром $d = 2^{-1}$ имеет тот же порядок. Теорема доказана. ▲

Пример. При $p = 19 \equiv 3 \bmod 8$ в табл. 2 представлены элементы всех множеств, используемых в теореме 3.

Таблица 2

x^{-1}	2	3	4	5	6	7	8	9
x^{-2}	4	9	16	6	17	11	7	5
$U = \{u^{-2} = x^{-2} - 1\}$	3	8	15	5	16	10	6	4
S				5	16		6	4
$\bar{S}$	3	8	15			10		
$-U$	16	11	4	14	3	9	13	15
$-U^{-1}$	6	7	5	15	13	17	3	14
$-S$	16	11	4			9		
$-\bar{S}$				14	3		13	15
$V = U * (-U)$	16		4		3			15
S_v	16		4					
$\bar{S_v}$					3			15
$U * (-U)^{-1}$	3		15	5			6	

Здесь два подмножества (19) или (20) можно построить как

$$G_1 = \{4, 5, -u_1^{-2} = 15, -u_2^{-2} = 10\},$$
$$G_1^{'} = \{16, 6, -u_1^{-2} = 3, -u_2^{-2} = 8\}.$$

Тогда

$$-G_1 = \{15, 14, u_1^{-2} = 4, u_2^{-2} = 9\} \Rightarrow (-G_1)^{-1} = \{14, 15, 5, 17\},$$
$$-G_1^{'} = \{3, 13, u_1^{-2} = 16, u_2^{-2} = 11\} \Rightarrow (-G_1^{'})^{-1} = \{13, 3, 6, 7\},$$

а пересечения соответствующих подмножеств включают элементы:

$$G_1 * (-G_1)^{-1} = \{5, 15\},$$
$$G_1^{'} * (-G_1^{'})^{-1} = \{6, 3\}.$$

Итак, получены $\frac{(p-3)}{4} = 4$ решения уравнения (18), причем два из них – для квадратичных вычетов, и два – для невычетов, что отвечает теореме 3. Приведенный пример дает наиболее простую иллюстрацию схемы доказательства.

При $d = 2^{\pm 1}$ j-инвариант (7) полной суперсингулярной кривой Эдвардса равен $j(1,2) = 2^3 \cdot 3^3 \cdot 11^3 = 66^3$.

При $x, y \neq 0,1$ уравнения кривой (12) при $d = 2^{\pm 1}$ для пары квадратичного кручения имеют вид:

$$E_{1,d}: (y^{-2} - 1) = \frac{-1}{(x^{-2} - 1)}, x = 2,3, \dots, \frac{(p-1)}{2},$$
$$E_{1,d}^{t}: (y^{-2} - 1) = \frac{2^{-1}}{(x^{-2} - 1)}, x = 2,3, \dots, \frac{(p-1)}{2}. \quad (21)$$

Так как элементы (–1) и 2 – квадратичные невычеты, то в соответствии с леммой 1 в правой части уравнений имеется равное число $\frac{(p-3)}{4}$ квадратичных вычетов и невычетов. Такое же соотношение их для левых частей уравнений. Из доказанной теоремы 3 следует, что при $p \equiv 3 \bmod 8$ ровно половина всех квадратичных вычетов множеств в левой и правой части этих уравнений совпадают. Такое же утверждение справедливо для квадратичных невычетов.

Интересно заметить, что для суперсингулярной кривой с параметром $d = -1$ и j-инвариантом $j(1, -1) = 12^3$ два уравнения (12) для пары квадратичного кручения вырождаются в одно уравнение

$$E_{1,d}: (y^{-2} - 1) = \frac{2}{(x^{-2} - 1)}, x = 2,3, \dots, \frac{(p-1)}{2},$$

совпадающее с (21) после замены $2 \rightarrow 2^{-1}$.

Существуют ли другие суперсингулярные полные кривые Эдвардса, кроме рассмотренных выше? Вопрос открытый. Пока нам удалось установить с помощью вычислений на компьютере, что в первой сотне значений модуля p других кривых этого класса не существует.

Список литературы: 1. *Бессалов А.В.* Эллиптические кривые в форме Эдвардса и криптография: монография / А.В. Бессалов – Киев : Политехника, 2017. – 272с. 2. *Menezes A.J, Okamoto T., Vanstone S. A.* Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field. University of Waterloo, sep. 1990. And // IEEE Transactions on Information Theory, V39, 1993. – PP 1639-1646. 3. *Washington L. C.* Elliptic Curvres. Number Theory and Cryptography. Second Edition. CRC Press, 2008. 4. *Bernstein Daniel J., Birkner Peter , Joye Marc , Lange Tanja, Peters Christiane.* Twisted Edwards Curves. IST Programme under Contract IST–2002–507932 ECRYPT,and in part by the National Science Foundation under grant ITR–0716498, 2008, PP. 1-17. 5. *Bernstein Daniel J., Lange Tanja.* Faster Addition and Doubling on Elliptic Curves // Advancesin Cryptology—ASIACRYPT'2007 (Proc. 13th Int. Conf. On the Theory and Applicationof Cryptology and Information Security. Kuching, Malaysia. December 2–6, 2007).

Lect. Notes Comp. Sci. V. 4833. Berlin: Springer, 2007. PP. 29–50. 6. *Бессалов А.В., Цыганкова О.В.* Взаимосвязь семейств точек больших порядков кривой Эдвардса над простым полем // Проблемы передачи информации. – 2015. – Т. 51, вып 4. – С.92-98. 7. *Бессалов А.В., Цыганкова О.В.* Классификация кривых в форме Эдвардса над простым полем. Прикладная радиоэлектроника. – 2015. – Т. 14. №4. – С.197 – 203. 8. *Бессалов А.В., Цыганкова О.В.* Число кривых в обобщенной форме Эдвардса с минимальным четным кофактором порядка кривой // Проблемы передачи информации. – 2017. – Т.53, вып 1. – С.101-111. 9. *Бессалов А.В., Телиженко А.Б.* Криптосистемы на эллиптических кривых : учеб. пособие. – К. : Політехніка, 2004. – 224с. 10. *Morain F.* Edwards curves and CM curves. ArXiv 0904/2243v1 [Math.NT] Apr.15, 2009. 11. *Дэвенпорт Г.* Высшая арифметика: введение в теорию чисел ; пер. с англ. под ред. Ю.В. Линника. – М. : Наука, 1965. – 176с. 12. *Ковальчук Л.В., Беспалов О.Ю, Огнєв П.І.* Рекурентні алгоритми обчислення кореня довільного степеню у кільці лишків // Правове нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2013. – Вип.1(25). – С.58 – 67. 13. *Бессалов А.В., Ковальчук Л.В.* Точное число эллиптических кривых в канонической форме, изоморфных кривым Эдвардса над простым полем // Кибернетика и системный анализ. – 2015. – Т.51, №2. – С.3-12.

Национальный технический университет «КПИ» *Поступила в редколлегию 04.11.2017*