ВЫЧИСЛЕНИЯ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ $EC(GF(2^n))$

1. Группа точек эллиптической кривой $EC(GF(2^n))$

На множестве состоящем из точек эллиптической кривой

$$Y^2 + a_1XY = X^3 + a_2X^2 + a_3X + a_6 \tag{1}$$

и еще одного элемента — бесконечно удаленной точки $\mathcal{O}$ (формально не являющейся точкой кривой), можно определить операцию, обладающую свойствами операции абелевой группы. Принято получающуюся при этом группу рассматривать как аддитивную группу, а операцию называть операцией сложения и обозначать, как обычно, знаком $+$. Точка $\mathcal{O}$ выполняет роль нейтрального элемента (в аддитивной записи — нуля).

Упражнение 1.1. Докажите, что любая эллиптическая кривая над полем характеристики два изоморфна кривой вида

$$Y^2 + XY = X^3 + a_2X^2 + a_6, \ a_i \in GF(2^n) \tag{2}$$

или кривой вида

$$Y^2 + a_3Y = X^3 + a_4X + a_6, \ a_i \in GF(2^n). \tag{3}$$

Указание. Если $a_1 \neq 0$, сделать замену переменных $X = a_1^2X + +a_3/a_1, \ Y = a_1^3Y$ и получить уравнение вида $Y^2 + XY = X^3 + a_2X^2 + +a_4X + a_6, \ a_i \in GF(2^n)$; потом сделать замену переменных вида $X = X, Y = Y + a_4$. Если $a_1 = 0$, сделать замену $X = X + a_2, \ Y = Y$.

Кривые над полем характеристики два вида (2) называются *несуперсингулярными*, а кривые вида (3) – *суперсингулярными*.

Полагаем, что $\mathcal{O} + \mathcal{O} = \mathcal{O}$ и для любой точки $(x, y) \in \mathcal{EF}$ выполняются равенства

$$(x, y) + \mathcal{O} = \mathcal{O} + (x, y) = (x, y).$$

Чтобы определить в общем случае операцию сложения абелевой группы, сначала покажем, что каждой точке (x, y) эллиптической кривой можно сопоставить в определенном смысле симметричную точку (далее будет пояснено, что такая точка и будет точкой $-(x, y)$, противоположной относительно точки (x, y) точкой в группе данной кривой). Заметим, что вместе с точкой (x, y) кривая имеет и точку

$$(x, \tilde{y}) = (x, -a_1x - a_3 - y). \tag{4}$$

В этом нетрудно убедиться непосредственным вычислением левой и правой частей уравнения эллиптической кривой при $X = x, Y = -a_1 x - a_3 - y$ и учитывая, что при $X = x$ и $Y = y$ имеет место равенство. Симметричность проявляется в том, что, как нетрудно проверить, по тому же правилу точке $(x, \tilde{y})$ соответствует исходная точка, так как имеет место *инволютивный закон*: $(x, y) = (x, \tilde{\tilde{y}})$.

Для суперсингулярных и несуперсингулярных кривых характеристики два симметричная точка $(x, \tilde{y})$ определяется соответственно уравнениями

$$(x, \tilde{y}) = (x, y + 1) \tag{5}$$

(частный случай уравнения (4) при $a_1 = 0,\ a_3 = 1$) и

$$(x, \tilde{y}) = (x, x + y) \tag{6}$$

(частный случай уравнения (4) при $a_1 = 1, a_3 = 0$).

Будем считать, что $(x, y) + (x, \tilde{y}) = \mathcal{O}$, и обозначать $(x, \tilde{y}) = -(x, y)$. Как видим, множество $\mathcal{E}(\mathcal{F})$ удовлетворяет двум аксиомам группы (существует нулевой элемент и каждому элементу соответствует противоположный элемент).

Операция сложения определена для случаев, когда хотя бы одно слагаемое является точкой $\mathcal{O}$ или слагаемые (x_1, y_1), (x_2, y_2) таковы, что $x_1 = x_2$ и $y_2 = \tilde{y}_1$ или, что то же самое, $y_1 = \tilde{y}_2$.

Осталось определить сумму $(x_1, y_1) + (x_2, y_2)$ для остальных случаев, когда

$$x_1 \neq x_2 \tag{7}$$

или

$$x_1 = x_2 \text{ и } y_2 \neq \tilde{y}_1 \text{ (или, что то же, } y_1 \neq \tilde{y}_2). \tag{8}$$

Упражнение 1.2.Покажите, что в условиях (8) $y_2 = y_1$.

Пусть $P = (x_1, y_1)$ и $Q = (x_2, y_2)$ две точки эллиптической кривой, удовлетворяющие условию (7), и ни одна из них не есть $\mathcal{O}$. Обозначим $\lambda(x_1, x_2, y_1, y_2) \neq 0$ элемент поля F, такой, что прямая на плоскости F^2

$$\mathcal{L} = \{(x, y)/y - y_1 = \lambda(P, Q)(x - x_1)\} \tag{9}$$

содержит эти две точки эллиптической кривой $\mathcal{EF}$.

Такой элемент легко вычислить:

$$\lambda(P,Q) = \lambda(x_1,x_2,y_1,y_2) = \frac{y_2-y_1}{x_2-x_1}. \tag{10}$$

Если же $P = Q = (x', y')$ (то есть имеет место условие (8)), то вместо прямой (9) будем использовать прямую

$$\mathcal{L}' = \{(x,y)/y - y' = \lambda'(P)(x-x')\}, \tag{11}$$

где

$$\lambda'(P) = -\left.\frac{\partial F(X,Y)/\partial X}{\partial F(X,Y)/\partial Y}\right|_{X=x',Y=y'} =$$
$$= -\left.\frac{(a_1Y - 3X^2 - 2a_2X - a_4}{2Y + a_1X + a_3}\right|_{X=x',Y=y'}. \tag{12}$$

Упражнение 1.3. Проверьте, что прямая (11) содержит точку $P = Q$, а знаменатель в выражении (12) не может быть нулевым.

Покажем, что кроме точек P и Q множество (9), как и множество (11), содержит еще одну точку R эллиптической кривой (1). В случае прямой (9) эта дополнительная точка может совпасть с точками P или Q, то есть одна из этих точек может быть кратным корнем уравнения (9). Такая точка называется *точкой инфлекции.*

Уравнения прямых (9) и (11) равносильны, соответственно, уравнениям $Y = \lambda X+\beta$, где $\lambda = \lambda(P,Q)$, $\beta = y_1 - \lambda x_1$ и $Y = \lambda' x + \beta'$, где $\lambda' = \lambda'(P)$, $\beta' = y_1 - \lambda' x_1$.

Точка $(x, \lambda x + \beta) \in \mathcal{L}$ (или точка $(x, \lambda' x + \beta') \in \mathcal{L}'$) лежит на эллиптической кривой только в том случае, когда

$$(\lambda x + \beta)^2 + a_1x(\lambda x + \beta) + a_3(\lambda x + \beta) = x^3 + a_2x^2 + a_4x + a_6$$

(или, соответственно,

$$(\lambda' x + \beta')^2 + a_1x(\lambda' x + \beta') + a_3(\lambda' x + \beta') = x^3 + a_2x^2 + a_4x + a_6)).$$

Отсюда следует, что кубическое уравнение

$$(\lambda X + \beta)^2 + a_1X(\lambda X + \beta) + a_3(\lambda X + \beta) = X^3 + a_2X^2 + a_4X + a_6$$

(или, соответственно,

$$(\lambda' X+\beta')^2+a_1X(\lambda' X+\beta')+a_3(\lambda' X+\beta')=X^3+a_2X^2+a_4X+a_6)$$

имеет (с учетом кратности) три корня, среди них x_1 и x_2 (или дважды x), так как $(x_1,\lambda x_1+\beta)$ и $(x_2,\lambda x_2+\beta)$ (или $(x,\lambda' x+\beta')$) являются точками P и Q (точкой P) кривой.

Воспользовавшись теоремой Виета, согласно которой сумма корней нормированного многочлена равна взятому со знаком минус коэффициенту γ (или γ') при степени, предшествующей старшей степени, можем определить и третий корень $x_3=\gamma-x_1-x_2$ (или $x_3=\gamma'-2x$) кубического уравнения, а затем вторую координату $y_3=y_1+\lambda(x_3-x_1)$ (или $y_3=y+\lambda'(x_3-x_1)$ третьей точки эллиптической кривой, принадлежащей прямой (9) (или (11)).

Это позволяет получить выражение для x_3 и, следовательно, для обеих координат третьей точки

$$R=(x_3,y_3)=(\gamma-x_1-x_2,\ y_1+\lambda(x_3-x_1)) \tag{13}$$

эллиптической кривой на прямой (10) через координаты x_1,x_2,y_1,y_2.

Аналогично определяются координаты точки

$$R=(x_3,y_3)=(\gamma'-2x,\ y+\lambda'(x_3-x)) \tag{14}$$

на прямой (11).

Определение 1.1. При условиях (7) или (8) суммой двух (в случае (8) – совпадающих) точек эллиптической кривой объявляется точка

$$P+Q=-R=-(x_3,y_3) \tag{15}$$

или

$$P+P=2P=-R=-(x_3,y_3), \tag{16}$$

где $R=(x_3,y_3)$ – третья точка (13) или (14), принадлежащая множеству (9) или (11) соответственно.

Заметим, что соблазнительно назвать суммой точек P,Q саму точку R. Но в этом случае определяемая операция не будет удовлетворять очевидному свойству $P+Q=R\rightarrow\ P=R-Q$ операции сложения.

Общая схема алгоритма сложения или удвоения для группы точек эллиптической кривой, а также конкретные формулы для вычисления координат третьей точки, когда ни одно из слагаемых не есть точка $\mathcal{O}$ и когда эти слагаемые не являются взаимно противоположными, рассматриваются в разд. 4.

Если кривая определена над полем $\mathcal{R}$ действительных чисел, множество $\mathcal{L}$ есть в самом деле прямая, проходящая через точки P и Q кривой и пересекающая ее в третьей точке R. Суммой является точка $-R$, противоположная точке R.

Эта точка R может оказаться точкой инфлекции и совпасть с одной из точек P или Q.

Прямая $\mathcal{L}'$ является касательной к кривой в точке $P = Q$. Тогда R – точка пересечения касательной с кривой, $2P$ – точка, противоположная к R точка $-R$.

Пример 1.1. На кривой $Y^2 = X^3 - 36X$ возьмем точки $P = (-3, 9)$, $Q = (-2, 8)$. Тогда при вычислении (используя формулы для кривых характеристики, не равной двум или трем, из подразд. 2.1) $P + Q$ находим $x_3 = 6,\ y_3 = 0$, а при вычислении $2P$ определяем $x_3 = 25/4, y_3 = -35/8$.

Упражнение 1.4. Докажите, что если $P = (x, 0)$, то $2P = 0$, $3P = = P$, $4P = 0$ и т. д.

Заметим, что описанная операция коммутативна также в случаях (8) и (9), поскольку $\lambda(x_1, x_2, y_1, y_2) = \lambda(y_1, y_2, x_1, x_2)$ и $\lambda'(x, y) = = \lambda'(y, x)$.

Справедлива следующая теорема Анри Пуанкаре.

Теорема 1.1. *Множество $\mathcal{EF}$ с операцией сложения является абелевой группой.*

Доказать ассоциативность операции в этой группе можно, используя явные формулы для вычисления координат точки (x_3, y_3), рассматриваемые в подразд. 2.1. Но эти вычисления чрезвычайно громоздки.

Без вычислений можно вывести ассоциативность из известного в теории алгебраических кривых утверждения.

Пусть три прямые $\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3$ пересекают кубическую кривую в девяти точках $P_1, P_2, \ldots, P_9$ с возможными совпадениями и пусть $\mathcal{L}_1', \mathcal{L}_2', \mathcal{L}_3'$ – три прямые, пересекающие кривую в точках $Q_1, Q_2, \ldots, Q_9$. Если $P_i = Q_i$ для $i = 1, \ldots 8$, то $P_9 = Q_9$.

Эту теорему оставим без доказательства.

Порядком точки P кривой E называется минимальное натуральное число n, такое что $nP = 0$. Если такого числа не существует, то точка имеет бесконечный порядок. Понятие порядка точки на кривой является, конечно, частным случаем понятия порядка элемента в любой группе.

Точки конечного порядка в группе кривой E называются *точками кручения* и образуют подгруппу, называемую *подгруппой кручения*.

Упражнение 1.5. Проверьте, что точек порядка два всегда не более трех. Для кривой $Y^2 + Y = X^3 - X^2$ это точки $(0, -1), (1, 0), (1, -1)$.

2 . Порядок эллиптической кривой

Эллиптические кривые над конечными полями $GF(2^n)$ имеют, естественно, конечные группы точек $\mathcal{EF}$. Порядок этой группы будем называть *порядком эллиптической кривой* и обозначим $\#\mathcal{EF}$. Напомним, что *порядком точки* P эллиптической кривой называется наименьшее число k такое, что $kP = \mathcal{O}$. По теореме Лагранжа, порядок точки делит порядок эллиптической кривой. При определении порядка кривой ее можно заменить на удобную изоморфную ей кривую, так как у изоморфных кривых порядки одинаковы. Менее очевидно, что и их группы изоморфны, но это верно, поэтому всегда можно ограничиться рассмотрением кривых с уравнениями специальных видов, указанных в подразд. 1.2.1.

Известно, что задача вычисления порядка эллиптической кривой над кольцом вычетов по модулю n полиномиально эквивалентна задаче разложения числа n на множители, но эта эквивалентность доказана в классе вероятностных алгоритмов.

Тем не менее известны способы выбора эллиптических кривых над конечными полями, допускающих простое определение порядка. Эти способы важны, потому что в криптографическом отношении полезными являются эллиптические кривые, порядок которых содержит большие простые множители. Для кривых, у которых порядок является «гладким» числом (т.е. разлагающимся только на малые простые) проблема дискретного логарифмирования может быть решена сравнительно быстро алгоритмом Полига – Хеллмана – Зильбера, найденным В.И. Нечаевым до его опубликования этими авторами, но не опубликованным в открытой печати.

При нечетном n имеется три класса неизоморфных суперсингулярных эллиптических кривых (согласно [3] при четном n имеется семь классов), стандартными представителями которых являются кривые $\mathcal{E}_1 : Y^2 + Y = X^3$,
$\mathcal{E}_2 : Y^2 + Y = X^3 + X$,
$\mathcal{E}_3 : Y^2 + Y = X^3 + X + 1$.

При нечетном n число точек для первой кривой равно $2^n + 1$ и $2^n \pm \sqrt{2^{n+1}} + 1$ — для второй и третьей (знак + или − выбирается в зависимости от кривой и от сравнения n по модулю 8) (см. табл. 1.1).

Таблица 1.1. Порядок групп кривых $\mathcal{E}_1$, $\mathcal{E}_2$ и $\mathcal{E}_3$

Кривая	Степень n	Порядок группы
$\mathcal{E}_1 = y^2 + y = x^3$	нечетное	$2^n + 1$
$\mathcal{E}_2 = y^2 + y = x^3 + x$	$n \equiv 1, 7 (\mathrm{mod}\ 8)$	$2^n + 1 + 2^{(n+1)/2}$
$\mathcal{E}_2 = y^2 + y = x^3 + x$	$n \equiv 3, 5 (\mathrm{mod}\ 8)$	$2^n + 1 - 2^{(n+1)/2}$
$\mathcal{E}_3 = y^2 + y = x^3 + x + 1$	$n \equiv 1, 7 (\mathrm{mod}\ 8)$	$2^n + 1 - 2^{(n+1)/2}$
$\mathcal{E}_3 = y^2 + y = x^3 + +x + 1$	$n \equiv 3, 5 (\mathrm{mod}\ 8)$	$2^n + 1 + 2^{(n+1)/2}$

В табл. 1.2 приведены некоторые конкретные степени n, которые можно использовать для реализации групп точек с большими множителями их порядков.

Таблица 1.2. Порядки кривых над полем $GF(2^n)$.

Степень n	Кривая	Порядок группы
173	$\mathcal{E}_2$	$5 \cdot 13625405957 \cdot P42$
173	$\mathcal{E}_3$	$7152893721041 \cdot P40$
191	$\mathcal{E}_1$	$3 \cdot P58$
191	$\mathcal{E}_2$	$5 \cdot 3821 \cdot 89618875387061 \cdot P40$
191	$\mathcal{E}_3$	$25212001 \cdot 5972216269 \cdot P41$
239	$\mathcal{E}_2$	$5 \cdot 77852679293 \cdot P61$
239	$\mathcal{E}_3$	$P72$
251	$\mathcal{E}_1$	$3 \cdot 238451 \cdot P70$
323	$\mathcal{E}_3$	$137 \cdot 953 \cdot 525313 \cdot P87$

В примерах 2.2 и 2.3 указаны некоторые несуперсингулярные кривые.

Пример 2.1. Кривая

$$X^2 + XY = X^3 + X^2 + 1$$

над полем $GF(2^{163})$ имеет порядок

$$2 \times 5846\ 00654\ 93236\ 11672\ 81474\ 17535\ 98448\ 34832\ 91185\ 74063.$$

Пример 2.2. Кривая $Y^2 + XY = X^3 + 1$ над полем $GF(2^{131})$ имеет порядок

$$4 \times 6805\ 64733\ 84187\ 69269\ 32320\ 12949\ 34099\ 85129.$$

3 . Применения теоремы Хассе

Известна асимптотически точная формула для порядка эллиптической кривой над конечным полем. Она была найдена в 1930-е годы немецким математиком Хельмутом Хассе. По теореме Хассе, порядок N эллиптической кривой над полем $GF(q)$ удовлетворяет неравенству

$$|N - q - 1| \leq 2\sqrt{q}.$$

Это эквивалентно системе неравенств

$$q + 1 - 2\sqrt{q} \leq N \leq q + 1 + 2\sqrt{q}.$$

Теорема Хассе в случае простого конечного поля кажется интуитивно очевидной, так как квадратичные вычеты и невычеты по простому модулю распределены в определенном смысле равномерно и в сумме

$$\sum_{x=0}^{p-1} \left(\frac{f(x)}{p} \right)$$

слагаемые ± 1 ведут себя подобно случайному блужданию по прямой.

Справедлива и более общая теорема Хассе – Вейля.

Теорема 3.1. *Пусть $\mathcal{E}$ – эллиптическая кривая над полем $GF(q)$ и N – порядок ее группы, тогда для порядка $N(n)$ группы точек эллиптической кривой $\mathcal{E}(GF(q^n))$ над полем $GF(q^n)$ справедлива формула*

$$N(n) = q^n + 1 - \alpha^n - \beta^n,$$

где α и β – корни квадратного уравнения $X^2 - tX + q = 0$, в котором коэффициент $t = q+1-N$, всегда выполняется неравенство $t^2 \le 4q$ и в случае строгого неравенства корни квадратного уравнения α и β являются комплексно сопряженными.

В случае полей малой характеристики порядок группы эллиптической кривой легко найти по формуле (**??**).

Упражнение 3.1. Проверьте, что для кривой $Y^2 = X^3 + 2X^2 + 1$ над полем $GF(3)$ $N = N(1) = 5,\ t = 4 - N = -1$, $N(n) = 3^n + 1 - \alpha^n - \ \ -\beta^n = 3^n + 1 - ((-1+\sqrt{11}i)/2)^n - ((-1-\sqrt{11}i)/2)^n$. Убедитесь, что эта формула верна, в частности, для $n = 2$.

Упражнение 3.2. Проверьте, что для кривой $Y^2 = X^3 + 2X + 1$ над полем $GF(3)$ $N = N(1) = 7, t = 4 - N = -3$; $N(n) = 3^n + 1 - \alpha^n - \beta^n = \ = 3^n + 1 - ((-3+\sqrt{3}i)/2)^n - ((-3-\sqrt{3}i)/2)^n$. Убедитесь, что эта формула при нечетном n имеет вид
$N(n) = 3^n + 1 + 3^{(n+1)/2}$ при $n \equiv \pm 1 (\mathrm{mod}\ 12)$,
$N(n) = 3^n + 1 - 3^{(n+1)/2}$ при $n \equiv \pm 5 (\mathrm{mod}\ 12)$,
$N(n) = 3^n + 1$ при $n \equiv \pm 3 (\mathrm{mod}\ 12)$.

Указание. Так как $(-3 \pm \sqrt{3}i)/2 = \sqrt{3}\exp(\pm 5\pi i/6)$, то согласно формуле Муавра
$\alpha^n + \beta^n = 3^{n/2}(\exp(5\pi ni/6) + \exp(-5\pi ni/6)) =$
$= 3^{n/2} 2\cos(5\pi n/6)$ и при нечетном n
$\alpha^n + \beta^n = 3^{n/2} 2\cos(\pi - \pi n/6) = -3^{n/2} 2\cos(\pi n/6) = -3^{(n+1)/2}$ при $n \equiv \pm 1 (\mathrm{mod}\ 12)$,
$\alpha^n + \beta^n = -3^{n/2} 2\cos(\pi n/6) = 3^{(n+1)/2}$ при $n \equiv \pm 5 (\mathrm{mod}\ 12)$,
$\alpha^n + \beta^n = -3^{n/2} 2\cos(\pi n/6) = 0$ при $n \equiv \pm 3 (\mathrm{mod}\ 12)$.

Упражнение 3.3. Проверьте, что для кривой $Y^2 = X^3 + 2X + 2$ над полем $GF(3)$ $N = N(1) = 1, t = 4 - N = 3$;
$N(n) = 3^n + 1 - \alpha^n - \beta^n = 3^n + 1 - ((3+\sqrt{3}i)/2)^n - ((3-\sqrt{3}i)/2)^n$.

Убедитесь, что эта формула при нечетном n имеет вид
$N(n) = 3^n + 1 - 3^{(n+1)/2}$при $n \equiv \pm 1 (\mathrm{mod}\ 12)$,
$N(n) = 3^n + 1 + 3^{(n+1)/2}$при $n \equiv \pm 5 (\mathrm{mod}\ 12)$,
$N(n) = 3^n + 1$при $n \equiv \pm 3 (\mathrm{mod}\ 12)$.
Указание. Так как $(3 + \pm\sqrt{3}i)/2 = \sqrt{3}\exp(\pm\pi i/6)$, то согласно формуле Муавра
$\alpha^n + \beta^n = 3^{n/2} 2\cos(\pi n/6) = 3^{(n+1)/2}$ при $n \equiv \pm 1 (\mathrm{mod}\ 12)$,
$\alpha^n + \beta^n = -3^{(n+1)/2}$ при $n \equiv \pm 5 (\mathrm{mod}\ 12)$,
$\alpha^n + \beta^n = -3^{n/2} 2\cos(\pi n/6) = 0$ при $n \equiv \pm 3 (\mathrm{mod}\ 12)$.

Иногда можно точно вычислить порядок группы эллиптической кривой и для полей большой характеристики. Например, при $q = p^d$, $p > 2$, и $q \equiv 3 (\mathrm{mod}\ 4)$ порядок кривой $Y^2 = X^3 - n^2 x$ равен $q + 1$.

Упражнение 3.4. Докажите сформулированное утверждение.

Указание. Точки порядка два — это $(0,0), (\pm n \bmod p, 0)$ и $\mathcal{O}$. Разобьем $x \ne 0, \pm n \bmod p$ на пары $\{x, -x\}$. Так как $f(x) = x^3 - n^2 x$ нечетная функция и (-1) не является квадратом в поле $GF(q)$ (так как иначе $(-1)^{(q-1)/2} = 1$ согласно теореме Ферма, что невозможно при $q \equiv 3 (\mathrm{mod}\ 4)$), то только один из двух элементов $f(x)$ и $f(-x) = -f(x)$ является квадратичным вычетом (так как в поле $GF(q)$ произведение квадратичных вычетов — квадратичный вычет, и произведение квадратичных невычетов — тоже квадратичный вычет, поэтому каждая пара элементов $\{x, -x\}$ дает пару точек кривой.

Пусть u — произвольный квадратичный невычет в поле $GF(q)$, q нечетно. Тогда кривая $E' : Y^2 = X^3 + u^2aX + u^3b$ называется *скручиванием* кривой $E : y^2 = x^3 + ax + b$.

Упражнение 3.5. Докажите, что сумма порядков кривой и ее скручивания равна $2q + 2$.

Указание. Пусть $f(X) = X^3 + aX + b$. Когда X пробегает элементы поля $GF(q)$, то X/u тоже пробегает все это поле и каждому корню многочлена $f(X)$ соответствует одна и та же точка на обеих кривых. Каждому значению функции $f(X)$, которое есть квадратичный вычет, соответствуют две точки на E и ни одной на E' так как элемент u^3 — квадратичный невычет. Аналогично, каждому значению функции $f(X)$, которое есть квадратичный невычет, соответствуют две точки на E' и ни одной на E. Так как имеется q значений функции $f(X)$ с учетом кратности, то общее число конечных точек на обеих кривых равно $2q$.

Благодаря описанному в упр. 3.5 факту, после того как найден порядок кривой, порядок ее скручивания находится без вычислений.

Приведем еще несколько примеров кривых, для которых легко вычислить порядок.

Упражнение 3.6. Порядок кривой $Y^2 = X^3 + b \bmod p$, $p \equiv$
$\equiv 2(\bmod 3)$, равен $p + 1$.

Указание. Так как кубический корень в поле $GF(p)$ всегда существует и однозначно определен, то для каждого элемента поля y на кривой лежит ровно одна точка $((y^2 - b)^{1/3}, y)$.

Упражнение 3.7. Порядок кривой $Y^2 = X^3 + aX \bmod p$, где $p \equiv$
$\equiv 3(\bmod 4)$, $\left(\frac{a}{p}\right) = 1$, равен $p + 1$.

Указание. Так как -1 есть квадратичный невычет в $GF(p)$, то каждая пара $\{x, -x\}$, $x \neq 0$, дает два решения: $(x, (x^3 + ax)^{1/2})$, $(x,$
$-(x^3 + ax)^{1/2})$ или $(-x, (-x^3 - ax)^{1/2})$, $(-x, -(-x^3 - ax)^{1/2})$ в зависимости от того, будет ли квадратичным вычетом $x^3 + ax$ или нет. Уравнение $X^3 + aX \equiv 0(\bmod p)$ имеет только одно решение.

Для определения порядка группы эллиптической кривой в общем случае известен алгоритм Р. Шуфа и его варианты.

4 Алгоритмы сложения и удвоения точек

В соответствии с определением операции сложения в группе точек эллиптической кривой общая схема алгоритма сложения точек $P_1 = = (x_1, y_1)$ и $P_2 = (x_2, y_2)$ представляется в виде алгоритма 4.1 на рис. 1.

Алгоритм 4.1

```
Вход: Коэффициенты эллиптической кривой,
точки P1 = (x1, y1) (или P1 = O) и P2 = (x2, y2) (или P2 = O).
Выход: P = P1 + P2.
Вычислить : если P1 = O, то P = P2,
            если P2 = O, то P = P1,
            если P2 = -P1, то P = O,
            если x1 ≠ x2, то P = -(x3, y3),
            иначе P = 2P1 = -(x3, y3).
Вернуть P.
```

Рис. 1. Общая схема алгоритма сложения и удвоения точек эллиптической кривой

Координаты точек $-(x_3, y_3)$ вычисляются по формулам в зависимости от вида эллиптической кривой.

Для несуперсингулярных эллиптических кривых (2) над полем характеристики два формулы сложения и удвоения следующие:

– при $P_1 = (x_1, y_1) \neq P_2 = (x_2, y_2)$

$$P_1 + P_2 = (x_3, x_3 + y_1 + \lambda(x_3 + x_1)), \tag{17}$$

где

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1},\ x_3 = (\lambda)^2 + \lambda + a_2 + x_1 + x_2;$$

– при $P_1 = P_2 = P = (x, y)$

$$2P = (x_3, x^2 + (\lambda' + 1)x_3), \tag{18}$$

где

$$\lambda' = x + \frac{y}{x},\ x_3 = (\lambda')^2 + (\lambda') + a_2.$$

Для суперсингулярных эллиптических кривых над полем характеристики два (3) формулы сложения и удвоения имеют вид:

– при $P_1 = (x_1, y_1) \neq P_2 = (x_2, y_2)$

$$P_1 + P_2 = (x_3, \tilde{y}_3) = (x_3,\ \lambda(x_1 + x_3) + y_1 + a_3), \tag{19}$$

где

$$\lambda = \frac{y_1 + y_2}{x_1 + x_2},\ x_3 = \lambda^2 + x_1 + x_2;$$

– при $P_1 = P_2 = P = (x, y)$

$$2P = -R = (x_3, \tilde{y}_3) = (x_3, \lambda'(x + x_3) + y + a_3), \tag{20}$$

где

$$\lambda' = \frac{x^2 + a_4}{a_3},\ x_3 = \ \lambda'^2.$$

При $a_3 = a_4 = 1$ имеем

$$2P = (x^4 + 1, x^4 + y^4).$$

.

5 . Скалярное умножение на эллиптических кривых

Алгоритмы умножения точки P эллиптической кривой на числовую константу k (алгоритмы вычисления $k \cdot P$), называются также алгоритмами скалярного умножения точки и являются основными в арифметике эллиптических кривых. С эффективными алгоритмами умножения на эллиптических кривых можно ознакомиться по соответствующим разделам учебного пособия [1] и монографии [2].

Рассмотрим умножение методом аддитивных цепочек.

Чтобы вычислить точку $k \cdot P$, разложим k в системе счисления по основанию 2^m, используя отрицательные цифры, и получим:

$$k = \sum_{i=0}^{\lfloor n/m \rfloor} a_i 2^{mi}.$$

Вычислим и запомним все кратные $a_i P$ (достаточно вычислить все нечетные кратные P, $3P$, $\ldots$, $(2^{m-1}-1)P$ с помощью поочередных удвоений и прибавлений P или даже только P, $3P$, $\ldots$, $(2^{m-2}--1)P$, если использовать разложение с отрицательными цифрами $\pm 1, \pm 3, \ldots, \pm(2^{m-2}-1)$). Затем вычислим kP по схеме Горнера:

$$kP = (\ldots(a_{s-1}2^m + a_{s-2})2^m + \ldots + a_1)2^m) + a_0)P =$$

$$= (\ldots(a'_{s-1}2^{m+l_{s-1}} + a'_{s-2})2^{m+l_{s-2}} + \ldots + a'_1)2^{m+l_1}) + a'_0 2^{l_0})P,$$

используя $s = \lfloor n/m \rfloor$ сложений-вычитаний с уже вычисленными точками и столько же умножений на 2^{m+l} при подходящем l.

6 Контрольные вопросы

1. Запишите уравнение эллиптической кривой над полем $GF(p)$ характеристики $p, p > 3$.
2. какая точка противоположна точке (x, y) эллиптической кривой $EG(GF(p))$?
3. Что является единицей группы точек эллиптической кривой?
4. Как определяется сумма взаимно противоположных точек эллиптической кривой?
5. Как определяется сумма $(x, y) + \mathcal{O}$?
6. Запишите формулу удвоения точки эллиптической кривой и дайте ее интерпретацию.
7. запишите формулу для вычисления суммы двух различных, но не взаимно противоположных точек эллиптической кривой, ни одна из которых не является единицей группы точек эллиптической кривой.
8. Дайте аддитивную интерпретацию алгоритма возведения в степень (см. раздел Вычисления в числовых кольцах и полях) применительно к операции скалярного умножения точки эллиптической кривой.

Литература.

1. Болотов А.А., Гашков С.Б. , Фролов А.Б. Криптографические протоколы на эллиптических кривых: учебное пособие/ – М. : Издательский дом МЭИ, 2007. – 84 с.

2.Болотов А.А., Гашков С.Б. , Фролов А.Б., Часовских А.А. Криптографические протоколы на эллиптических кривых. – М.: Кокнига, 2006

3. Menezes A.J., Vanstone S. Elliptic Curve Cryptosystems and their implementation. Journal of Cryptology. N 6 (1993)