

## 32 Эллиптические кривые в криптографии

### 32.1 Основные понятия

Пусть  $K$  — поле и  $\text{char } K \neq 2, 3$ .

**Пример 32.1.** Примеры подходящих полей ( $p \neq 2, 3$ ):  $\mathbb{Q}$  — поле рациональных чисел,  $\mathbb{R}$  — поле вещественных чисел,  $\mathbb{C}$  — поле комплексных чисел,  $\mathbb{F}_p$  — простое конечное поле,  $\mathbb{F}_{p^n}$  — конечное поле.  $\square$

Нам потребуется понятие алгебраического замыкания  $\bar{K}$  поля  $K$ :  $\bar{K}$  — расширение  $K$ , которое содержит все корни всех многочленов  $f(x) \in K[x]$ .

**Пример 32.2.**  $\bar{\mathbb{R}} = \mathbb{C}$  (основная теорема алгебры),  $\bar{\mathbb{F}}_p = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$ .  $\square$

**Определение 32.1.** Эллиптическая кривая над полем  $K$  задается уравнением

$$E: y^2 = x^3 + ax + b, \quad a, b \in K, \quad 4a^3 + 27b^2 \neq 0.$$

Решения  $(x, y) \in \bar{K}$  этого уравнения называются *аффинными точками* кривой. Добавляется еще одна точка, которая называется *точкой на бесконечности* и обозначается через  $O$ .  $\square$

**Замечание 32.1.** Уравнение  $E$  — это, так называемая, короткая форма Вейерштрасса. Общая форма уравнения, подходящая для полей любой характеристики:

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

**Замечание 32.2.** Кривые Фрея — это кривые над  $\mathbb{Q}$  следующего вида:

$$E: y^2 = x(x - a^n)(x + b^n).$$

Если  $(a, b, c)$  — тройка Ферма для показателя  $n$ , т. е.  $a^n + b^n = c^n$ , то соответствующая кривая Фрея обладает особенностью — она не является модулярной. Этот факт позволил в конце концов доказать последнюю теорему Ферма.  $\square$

**Определение 32.2.** Если  $P = (x, y)$  — аффинная точка  $E$  и  $x, y \in L$ , где  $L$  — некоторое расширение  $K$ , то  $P$  называется  *$L$ -рациональной*,  $E(L)$  — множество всех таких точек с добавлением  $O$ . Вместо  $E(\bar{K})$  пишем просто  $E$ .  $\square$

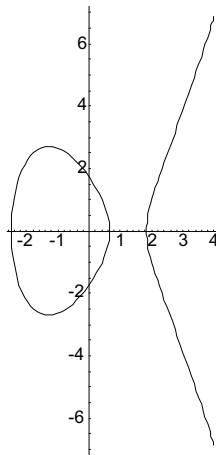


Рис. 5: Эллиптическая кривая  $y^2 = x^3 - 5x + 3$  над  $\mathbb{R}$  (нарисована в **Mathematica** командой `ImplicitPlot[y^2==x^3-5x+3, {x, -5, 4}]`)

Далее нас в основном будут интересовать кривые над простым полем  $\mathbb{F}_p$ . На кривой  $E$  найдется точка с абсциссой  $x$  тогда и только тогда, когда  $z = x^3 + ax + b$  является квадратом  $\text{mod } p$ : существует вычет  $y$  (квадратный корень) такой, что  $y^2 \equiv z \pmod{p}$ .

В теории чисел принято разделять два случая:

1)  $z = 0$  и имеется единственный корень  $y = 0$ ;

2)  $z \neq 0$  и имеется два корня.

В последнем случае  $z$  называется *квадратичным вычетом*  $\bmod p$ . Неквадраты принято называть *квадратичными невычетами*.

**Упражнение 32.1.** Доказать, что среди вычетов по нечетному простому модулю  $p$  имеется  $(p-1)/2$  квадратичных вычетов и столько же невычетов.  $\square$

**Упражнение 32.2.** Пусть  $p$  — нечетное простое число. *Символ Лежандра* определяется следующим образом:

$$\left(\frac{z}{p}\right) = \begin{cases} 1, & z \text{ — квадратичный вычет } (\bmod p), \\ 0, & z \equiv 0 (\bmod p), \\ -1, & z \text{ — квадратичный невычет } (\bmod p). \end{cases}$$

Доказать, что

$$\left(\frac{z}{p}\right) = z^{(p-1)/2} \bmod p.$$

(критерий Эйлера).  $\square$

**Пример 32.3.** Пусть  $E: y^2 = x^3 + 4x + 1$  — кривая над  $\mathbb{F}_7$ . Квадратичные вычеты  $\bmod 7$ : 1, 2, 4. Квадратичные невычеты: 3, 5, 6. Рациональные точки эллиптической кривой:  $E(\mathbb{F}_7) = \{O, (0, 1), (0, 6), (4, 2), (4, 5)\}$ .  $\square$

**Замечание 32.3.** Точка  $O$  присоединяется к эллиптической кривой точно также, как к комплексной плоскости присоединяется бесконечно удаленная точка и тем самым образуется риманова сфера. Поясним, как происходит присоединение  $O$ .

Запишем уравнение кривой:

$$F(x, y) = y^2 - x^3 - ax - b = 0.$$

С помощью замены  $x = X/Z$ ,  $y = Y/Z$  и умножения на  $Z^3$  перейдем к однородному уравнению

$$F^*(X, Y, Z) = Y^2Z - X^3 - aXZ^2 - bZ^3 = 0.$$

Пусть  $(X, Y, Z) \neq (0, 0, 0)$  — корень  $F^*$ . Тогда корнями  $F^*$  являются и все точки прямой

$$\{(\lambda X, \lambda Y, \lambda Z) : \lambda \in K\}.$$

Данная прямая считается точкой (!) специальной алгебраической структуры — так называемой *проективной плоскости*  $P_K^2$ .

Точке  $\{(\lambda X, \lambda Y, \lambda Z)\}$ , у которой  $Z \neq 0$ , соответствует аффинная точка  $(X/Z, Y/Z) \in E$ . Если же  $Z = 0$ , то  $X = 0$  и мы получаем точку  $\{(0, \lambda Y, 0)\}$  проективной плоскости, которая и соответствует бесконечно удаленной точке  $O$  кривой  $E$ .  $\square$

## 32.2 Дискриминант

Величина  $\Delta(E) = 4a^3 + 27b^2$  называется *дискриминантом* кривой  $E$ . Условие  $\Delta(E) \neq 0$  в определении эллиптической кривой требуется в доказательстве следующей теоремы.

**Теорема 32.1.** В любой аффинной точке эллиптической кривой можно провести единственную касательную.

*Доказательство.* Зададим эллиптическую кривую неявным образом:

$$F(x, y) = 0, \quad F(x, y) = y^2 - x^3 - ax - b.$$

Касательную к кривой в точке  $(x, y)$  можно провести, если хотя бы одна частная производная в этой точке ненулевая, т. е. выполнено по меньшей мере одно из условий

$$\frac{\partial F}{\partial x}(x, y) = -3x^2 - a \neq 0, \quad \frac{\partial F}{\partial y}(x, y) = 2y \neq 0.$$

Пусть, от противного,  $3x^2 + a = y = 0$ . Тогда

$$\begin{cases} x^3 + ax + b = 0, \\ 3x^3 + ax = 0. \end{cases}$$

Если  $b = 0$ , то  $x = a = 0$  (упр.) и  $\Delta(E) = 0$ , противоречие.

Пусть  $b \neq 0$ . Вычитая из второго уравнения первое и вычитая из первого уравнения второе, домноженное на 3, получаем

$$\begin{cases} 2x^3 - b = 0, \\ 2ax + 3b = 0 \end{cases} \quad \text{или} \quad \begin{cases} 2x^3 = b, \\ (2ax)^3 = -27b^3. \end{cases}$$

Отсюда  $4a^3b + 27b^3 = 0$  и, поскольку  $b \neq 0$ ,  $4a^3 + 27b^2 = 0$ . Противоречие.  $\square$

**Замечание 32.4.** Дискриминант многочлена  $x^3 + ax + b = (x - r_1)(x - r_2)(x - r_3)$  определяется как  $(r_1 - r_2)(r_1 - r_3)(r_2 - r_3)$  и совпадает с  $16\Delta(E)$ . Таким образом, для гладкости кривой  $E$  достаточно, чтобы многочлен не имел кратных корней.  $\square$

### 32.3 Сложение точек

Рассмотрим эллиптическую кривую  $E: y^2 = x^3 + ax + b$ . Изучим точки ее пересечения с прямыми.

Невертикальная прямая  $y = \lambda x + \beta$  дает кубическое уравнение  $(\lambda x + \beta)^2 = x^3 + ax + b$ , которое имеет 3 корня (с учетом кратности) в  $\bar{K}$ . Вертикальная прямая  $x = \gamma$  дает квадратное уравнение  $y^2 = \gamma^3 + a\gamma + b$ , которое имеет 2 корня (снова с учетом кратности). Будем считать, что вертикальная прямая проходит через точку  $O$ .

В итоге:

- 1) любая прямая, проходящая через две различные аффинные точки  $E$  пересекает кривую в единственной третьей точке;
- 2) в любой аффинной точке  $E$  можно провести касательную и касательная пересекает  $E$  в еще одной точке;

Дополнительно обратим внимание, что

- 3) если  $P = (x, y) \in E$ , то и  $(x, -y)$  лежит на  $E$ . При этом  $(x, -y)$  называется *обратной* к  $P$  точкой и обозначается  $-P$ . Обратной к  $O$  будем считать саму точку  $O$ .

Данные геометрические соображения позволяют ввести следующую операцию сложения точек  $E$ .

**Определение 32.3.** Суммой аффинных точек  $P = (x_1, y_1)$  и  $Q = (x_2, y_2)$  называется точка  $R = P + Q = (x_3, y_3)$ , обратная точке пересечения прямой  $PQ$  с кривой  $E$  (считаем, что прямая  $PP$  — это касательная в  $P$ ).  $\square$

Распространим операцию сложения на бесконечно удаленную точку и укажем правила определения координат суммы:

1.  $O + P = P$ .
2.  $P + (-P) = O$ .

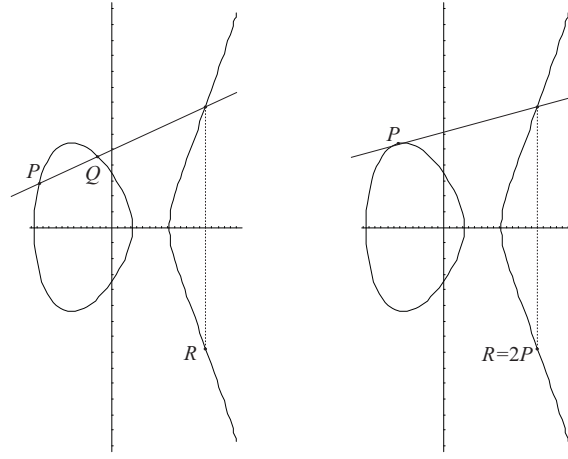


Рис. 6: Сложение точек

3. Пусть  $P \neq \pm Q$ ,  $P, Q \neq O$ .

Уравнение прямой, проходящей через  $P$  и  $Q$  имеет вид:

$$y = \lambda x + \beta, \quad \lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \beta = y_1 - \lambda x_1.$$

Точки пересечения прямой с  $E$  являются решениями уравнения

$$(\lambda x + \beta)^2 - x^3 - ax - b = 0 \text{ или } -(x - x_1)(x - x_2)(x - x_3) = 0.$$

Приравнявая в обоих уравнениях коэффициенты при  $x^2$  получаем

$$\lambda^2 = x_1 + x_2 + x_3 \Rightarrow x_3 = \lambda^2 - x_1 - x_2.$$

Параметр  $\lambda$  можно также выразить как

$$\lambda = \frac{-y_3 - y_1}{x_3 - x_1}.$$

Отсюда находим  $y_3 = \lambda(x_1 - x_3) - y_1$ .

Окончательно,

$$R = (x_3, y_3), \quad x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1, \quad \lambda = \frac{y_2 - y_1}{x_2 - x_1}.$$

4. Пусть  $Q = P \neq O$ , т. е.  $R = 2P$ .

Уравнение касательной к кривой  $F(x, y) = 0$  в точке  $(x_1, y_1)$  имеет вид:

$$(x - x_1) \frac{\partial F}{\partial x} \Big|_{(x,y)=(x_1,y_1)} + (y - y_1) \frac{\partial F}{\partial y} \Big|_{(x,y)=(x_1,y_1)} = 0.$$

Если  $\frac{\partial F}{\partial y} \Big|_{(x,y)=(x_1,y_1)} = 0$ , то касательная является вертикальной прямой и  $2P = O$ .

В противном случае касательная имеет вид  $y = \lambda x + \beta$ , где

$$\lambda = - \frac{\partial F / \partial x}{\partial F / \partial y} \Big|_{x=x_1, y=y_1} = \frac{3x_1^2 + a}{2y_1}.$$

Используя рассуждения, аналогичные предыдущим, получаем

$$R = (x_3, y_3), \quad x_3 = \lambda^2 - 2x_1, \quad y_3 = \lambda(x_1 - x_3) - y_1, \quad \lambda = \frac{3x_1^2 + a}{2y_1}.$$

**Пример 32.4.** Пусть  $E$  — кривая над  $\mathbb{F}_7$ , заданная уравнением  $y^2 = x^3 + 4x + 1$ . Тогда  $E(\mathbb{F}_7) = \{0, (0, 1), (0, 6), (4, 2), (4, 5)\}$ . Для точек кривой, описанной в предыдущем примере, выполняется:

$$(0, 1) + (4, 2) = (0, 6), \quad (4, 2) + (4, 2) = (0, 1).$$

Интересно, что этих равенств хватает для определения полной таблицы сложения точек  $E(\mathbb{F}_7)$ . Эта таблица при  $P = (0, 1)$  и  $Q = (4, 2)$  выглядит следующим образом:

$+$	$O$	$P$	$Q$	$-P$	$-Q$
$O$	$O$	$P$	$Q$	$-P$	$-Q$
$P$	$P$	$-Q$	$-P$	$O$	$Q$
$Q$	$Q$	$-Q$	$-P$	$P$	$O$
$-P$	$-P$	$O$	$-Q$	$Q$	$P$
$-Q$	$-Q$	$Q$	$O$	$P$	$-P$

При заполнении таблицы нам помогает:

- симметрия относительно главной диагонали;
- латинское свойство: в любой строке и в любом столбце таблицы нет двух одинаковых элементов;
- простое соотношение между взаимно обратными элементами.

□

Отметим, что формулы сложения точек справедливы для любых полей  $K$ , характеристики которых отличны от 2 и 3. Для полей характеристик 2, 3 имеются другие канонические формы записи кривых и действуют другие правила сложения точек.

## 32.4 Группа точек эллиптической кривой

**Теорема 32.2 (Пуанкаре).** Множество точек кривой  $E$  с введенной операцией сложения является абелевой группой.

*Доказательство.* Имеется единица  $O$ , определен обратный элемент, очевидно выполняется закон коммутативности. Проверка закона ассоциативности

$$(P + Q) + R = P + (Q + R)$$

может быть выполнена прямыми расчетами (опускаем ввиду громоздкости).<sup>1</sup>

□

**Следствие 32.1.** Пусть  $L$  — расширение  $K$ . Множество  $E(L)$  с введенной операцией сложения является абелевой группой.

*Доказательство.* Множество  $E(L)$  замкнуто относительно введенной операции сложения и, следовательно,  $E(L)$  является подгруппой  $E = E(\bar{K})$ .

□

Пусть  $K = \mathbb{F}_q$  — конечное поле. Для любого  $x \in \mathbb{F}_q$  уравнение  $y^2 = x^3 + ax + b$  имеет не более двух решений относительно  $y \in \mathbb{F}_q$ . Поэтому справедлива оценка

$$|E(\mathbb{F}_q)| \leq 1 + 2q.$$

Существует более точная оценка.

**Теорема 32.3 (Хассе).**  $|E(\mathbb{F}_q) - (q + 1)| \leq 2\sqrt{q}$ .

**Замечание 32.5.** Теорема Хассе следует из следующих построений. Пусть  $N_r = |E(\mathbb{F}_{q^r})|$ . Построим ряд

$$Z(E; T) = \exp \left( \sum_{r \geq 1} \frac{N_r T^r}{r} \right),$$

<sup>1</sup>См. Friedl S. An elementary proof of the group law for elliptic curves, <https://arxiv.org/pdf/1710.00214> (9 стр.).

который в соответствии с оценкой  $N_r \leq 1 + 2q^r$  сходится равномерно и абсолютно на отрезке  $|T| \leq T_0$  при любом  $T_0 < 1/q$  и, следовательно, определяет аналитическую функцию.

Функция  $Z(E; T)$  называется *дзета-функцией* кривой  $E$ . Оказывается, что дзета-функция имеет достаточно простой вид:

$$Z(E; T) = \frac{1 - tT + qT^2}{(1 - T)(1 - qT)},$$

где  $t$  определяется равенством  $N_1 = q + 1 - t$ , а дискриминант числителя  $\leq 0$ . □

**Упражнение 32.3.** Доказать, что

$$|E(\mathbb{F}_p)| = 1 + p + \sum_{x \in \mathbb{F}_p} \left( \frac{x^3 + ax + b}{p} \right).$$

Пусть кривая  $E$  определена над простым полем  $\mathbb{F}_p$ . Пусть  $P \in E(\mathbb{F}_p)$ ,  $P \neq O$ . Сумму  $nP = \underbrace{P + P + \dots + P}_{n \text{ раз}}$ , назовем  *$n$ -кратным* точки  $P$ .

Напомним, что минимальное натуральное  $n$  такое, что  $nP = O$  называется *порядком*  $P$  в группе  $E(\mathbb{F}_p)$  и обозначается через  $\text{ord } P$ . По теореме Лагранжа  $\text{ord } P \mid N = |E(\mathbb{F}_p)|$ .

**Упражнение 32.4.** Доказать, что  $\text{ord } P = \text{ord } (-P)$ . □

**Пример 32.5 (порядки точек кривой над  $\mathbb{F}_7$ ).** Вернемся к предыдущему примеру. Для  $P = (0, 1)$  имеем:

$$\begin{aligned} 2P &= -Q, \\ 3P &= -Q + P = Q, \\ 4P &= Q + P = -P, \\ 5P &= O. \end{aligned}$$

Отсюда  $\text{ord } P = 5$  и  $E(\mathbb{F}_7) = \langle P \rangle$ .

Нетрудно понять, что  $\text{ord } R = 5$  для любой другой точки  $R \in E(\mathbb{F}_7) \setminus \{O\}$ . Это следует из двух фактов:  $\text{ord } R \mid 5$  и  $\text{ord } R \neq 1$ . □

**Пример 32.6 (порядки точек кривой над  $\mathbb{F}_5$ ).** Рассмотрим кривую  $E: y^2 = x^3 + 1$  над полем  $\mathbb{F}_5$ . Будем выбирать  $x$  и решать уравнение  $E$  относительно  $y$ :

$x$	0	1	2	3	4
$x^3 + 1$	1	2	4	3	0
$y$	$\pm 1$	—	$\pm 2$	—	0

Таким образом, найдены все точки  $E(\mathbb{F}_5)$ :

$$O, P = (0, 1), -P, Q = (2, 2), -Q, R = (4, 0).$$

Всего имеется  $6 = p + 1$  точек, что соответствует оценке теоремы Хассе.

По формулам сложения найдем удвоенные точки:

$$\begin{aligned} 2P &= 2(0, 1) = [v = 3 \cdot 0/2 = 0] = (0 - 0, -1) = -P, \\ 2Q &= 2(2, 2) = [v = 3 \cdot 4/4 = 2 \cdot 4 = 3] = (3^2 - 4, -2 - 3(0 - 2)) = -P, \\ 2R &= 2(4, 0) = O. \end{aligned}$$

Отсюда:  $3P = O \Rightarrow \text{ord } P = 3$ ,  $6Q = -3P = O \Rightarrow \text{ord } Q \mid 6$ ,  $\text{ord } R = 2$ . Докажем, что  $\text{ord } Q = 6$ . Единственной альтернативой является  $\text{ord } Q = 3$ . Но тогда  $3Q = Q - P = O \Rightarrow Q = P$ , противоречие.

Обратим внимание, что  $E(\mathbb{F}_5)$  — циклическая группа:  $E(\mathbb{F}_5) = \{O, Q, 2Q, 3Q, 4Q, 5Q\}$ , которую можно представить в виде прямой суммы  $\{O, R\} \oplus \{O, P, 2P\}$  двух циклических подгрупп порядка 2 и 3. □

**Замечание 32.6.** Известно, что всякая группа  $E(\mathbb{F}_q)$  порядка  $n$  является либо циклической, либо представляется в виде прямой суммы двух циклических групп порядков  $n_1$  и  $n_2$  таких, что  $n_1 \mid n_2 \mid n$ . □

Для нахождения кратной точки можно воспользоваться бинарными методами и выполнить за полиномиальное время.

## 32.5 Задача дискретного логарифмирования на ЭК

Нахождение кратной точки является аддитивным аналогом возведения в степень в мультипликативных группах (напр.,  $\mathbb{F}_p^*$ ). При аддитивной записи задача дискретного логарифмирования трансформируется следующим образом.

Задача DL на эллиптической кривой (ECDLP)	
Вход	описание группы $\mathbb{G} = E(\mathbb{F}_p)$ порядка $n$ базовая точка $G \in \mathbb{G}$ порядка $q$ точка $Q \in \langle G \rangle$ (порядки $q$ и $n$ входят в условие задачи)
Выход	дискретный логарифм $d \in \{0, 1, \dots, q-1\}$ : $Q = dG$

**Обозначения:**  $d = \text{DL}[\mathbb{G}](G, Q)$ ,  $d = \text{DL}(G, Q)$ ,  $d = \log_G Q$ .

Нам потребуется следующее

**Определение 32.4.** Пусть  $\langle \mathbb{H}, \circ \rangle$  и  $\langle \mathbb{G}, \star \rangle$  — группы. Функция  $f: \mathbb{H} \rightarrow \mathbb{G}$  называется *гомоморфизмом*, если

$$f(a \circ b) = f(a) \star f(b), \quad \forall a, b \in \mathbb{H}.$$

Биективный гомоморфизм называется *изоморфизмом*. □

**Упражнение 32.5.** Пусть  $f$  — гомоморфизм  $\mathbb{H} \rightarrow \mathbb{G}$ . Доказать:

- 1)  $f(e_{\mathbb{H}}) = e_{\mathbb{G}}$ , где  $e_{\mathbb{H}}$  и  $e_{\mathbb{G}}$  — единицы  $\mathbb{H}$  и  $\mathbb{G}$  соответственно;
- 2)  $f(-a) = -f(a)$  для любого  $a \in \mathbb{H}$ ;
- 3)  $\text{ord } f(a) \mid \text{ord } a$  для любого  $a \in \mathbb{H}$ . □

Рассмотрим известные пути решения задачи  $\text{DL}[\mathbb{G}](G, Q)$ .

1. Использовать  $\rho$ - и  $\lambda$ -методы. Сложность:  $O(\sqrt{q})$ .
2. Использовать метод Полига – Хеллмана. Сложность:  $O(\sum \alpha_i \sqrt{q_i})$ ,  $q = \prod q_i^{\alpha_i}$ ,  $q_i$  — простые.
3. Если  $n = p$  (кривая называется *аномальной*), то можно использовать метод Семаева.

Суть метода: можно построить эффективно вычислимый изоморфизм  $\varphi: \langle E(\mathbb{F}_p), + \rangle \rightarrow \langle \mathbb{F}_p, + \rangle$ . Задача сводится к решению уравнения  $d\varphi(G) \equiv \varphi(Q) \pmod{p}$  (расширенный алгоритм Евклида!).

4. Если  $n \mid p^m - 1$ ,  $m$  — невелико, то можно использовать метод Менезеса — Окамoto — Ванстоуна (MOV-атака).

Суть метода: строится эффективно вычислимый изоморфизм  $\psi: \langle E(\mathbb{F}_p), + \rangle \rightarrow \langle \mathbb{F}_{p^m}^*, * \rangle$ . Задача сводится к решению уравнения  $\psi(G)^d = \psi(Q)$  в поле  $\mathbb{F}_{p^m}$  (субэкспоненциальные алгоритмы д.л.).

5. Для кривых общего вида субэкспоненциальные (от  $\log p$ ) алгоритмы д.л. неизвестны!

Таким образом, переход к ЭК дает выигрыш в производительности за счет использования параметра  $p$  меньшей длины (чем в случае использования группы  $\mathbb{F}_p^*$ ).

Критерии выбора параметров ЭК:

1.  $4a^3 + 27b^2 \neq 0$  — гладкая кривая.
2.  $q$  — простое (против метода Полига — Хеллмана).
3.  $q \neq p$  (против метода Семаева).
4.  $q \nmid p^m - 1$ ,  $m = 1, \dots, 20 - 50$  (против MOV-атаки).

**Упражнение 32.6.** В СТБ 34.101.45 к ЭК предъявляются дополнительные свойства:  $2^{2\ell-1} < p, q < 2^{2\ell}$ ;  $p \equiv 3 \pmod{4}$ ;  $b$  — квадратичный вычет по модулю  $p$ . При  $\ell = 2$  найти подходящую кривую с  $a = -3$  и минимальным  $b$ .  $\square$

**Замечание 32.7.** Пусть  $|E(\mathbb{F}_p)| = p + 1 - t$ , где  $|t| \leq 2\sqrt{p}$  по теореме Хассе (параметр  $t$  называют следом Фробениуса). Пусть  $s^2$  — максимальный квадрат, который делит  $t^2 - 4p$ .  $CM$ -дискриминантом  $E$  называется число

$$D = \begin{cases} (t^2 - 4p)/s^2, & (t^2 - 4p)/s^2 \equiv 1 \pmod{4}, \\ 4(t^2 - 4p)/s^2, & \text{в противном случае.} \end{cases}$$

Если  $D$  мал, то  $\rho$ -метод можно ускорить. Поэтому дополнительно требуют, что дискриминант  $D$  был большим ( $D > 2^{100}$  в системе критериев `safecurves.cr.yp.to`).  $\square$