Осень 2019

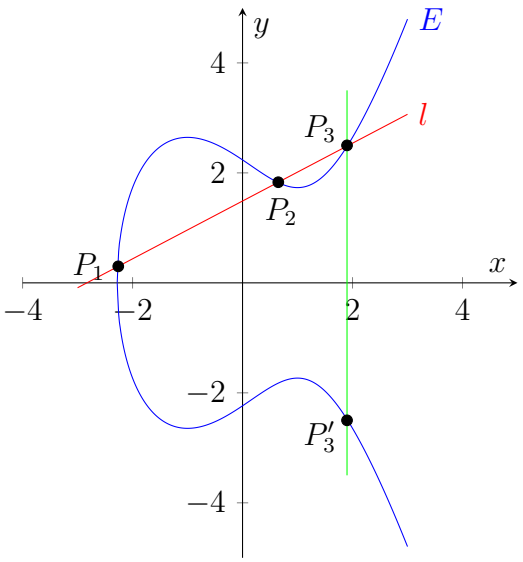
Лекция 2 — 20.09.2019

Лектор: Елена Киршанова *Оформил Филипп Максимов*

1 Групповой закон на эллиптической кривой

$$E : y^2 = x^3 + Ax + B \quad (charK \neq 2, 3)$$
$$P_1 = (x_1, y_1) \in E$$
$$P_2 = (x_2, y_2) \in E$$

1. Проведём прямую через P_1, P_2. Она пересечёт кривую в 3-ей точке P_3 (кривая задана уравнением степени 3).
2. Отразим P_3 относительно Ox
3. Положим $P_3' = P_1 + P_2$ (! $P_1 + P_2 \neq (x_1 + x_2, y_1 + y_2)$).



Получим координаты P_3':

$$m = \frac{y_2 - y_1}{x_2 - x_1} - \text{наклон } l.$$

- Положим $x_2 \neq x_1 \Rightarrow$ уравнение $l : y = m(x - x_1) + y_1$.

Найдём пересечение l с E : $(m(x-x_1)+y_1)^2 = x^3+Ax+B$ — уравнение 3-ей степени с 3-мя корнями, два корня известны (x_1, x_2). Кроме того, для любого кубического уравнения с корнями r, s, t :

$$x^3 + ax^2 + bx + c = (x-r)(x-s)(x-t) = x^3 - (r+s+t)x^2 + ...$$
$$\Rightarrow r + s + t = -a$$
$$\Rightarrow t = -a - r - s$$

В нашем случае $x^3 - m^2x^2 + ... = 0 \Rightarrow$ 3-ий корень:

$$x_3 = m^2 - x_1 - x^2 \text{ и } y = m(x - x_1) + y_1$$
$$P_3 = (m^2 - x_1 - x_2,\ m(x - x_1) + y_1)$$

Отражение относительно Ox :

$$P_3' = (m^3 - x_1 - x_2,\ m(x_1 - x) - y_1)$$

- Положим $x_2 = x_1,\ y_1 \neq y_2 \Rightarrow l$ — вертикальная прямая $\Rightarrow$ пересекает E в $\mathcal{O}$. $\mathcal{O}$ относительно Ox $= \mathcal{O} \Rightarrow P_3' = \mathcal{O}$

- Положим $x_2 = x_1,\ y_1 = y_2\ \ (P_1 = P_2) \Rightarrow l$ — касательная к $E \Rightarrow m = \frac{dy}{dx}$, где $y = f(x)$.

$$2y\frac{dy}{dx} = 3x^2 + A \Rightarrow$$
$$m = \frac{3x_1^2 + A}{2y_1} \text{ в } m : P_1 = P_2$$

Если $y_1 = 0 \Rightarrow$ вертикальная прямая $\Rightarrow P_1 + P_2 = \infty$
Важно: $3x_1^2 + A \neq \mathcal{O}$ при $y_1 = 0$.

Если $y_1 \neq 0 \Rightarrow l : y = m\,(x - x_1) + y_1$. Аналогично получаем кубическое уравнение

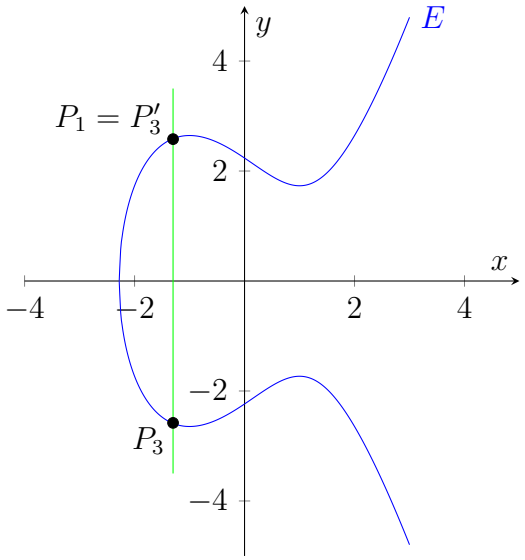
$$0 = x^3 - m^2x^2 + \ldots,$$

однако теперь нам известен 1 корень, x_1 степени 2. Аналогичными рассуждениями, приходим:

$$x_3 = m^2 - 2x_1, \quad y_3 = m\,(x_1 - x_3) - y_1$$
$$P_3' = (x_3,\ y_3)$$

- Положим $P_2 = \mathcal{O}$, проходящая через P_1 и $\mathcal{O}$ — вертикальная прямая $\cap E = P_1$. Отражение относительно OX даст

$$P_1 \Rightarrow P_1 + \mathcal{O} = P_1 \quad \forall P_1 \in E.$$



Следствие 1 (Закон сложения «+» на E)**.**

$$E : y^2 = x^3 + Ax + B, \quad P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E, P_1, P_2 \neq \mathcal{O}$$

определим $P_3 = P_1 + P_2 = (x_3, y_3)$:

1. *Если* $x_1 \neq x_2$*;*

$$x_3 = m^2 - x_1 - x_2$$
$$y_3 = m(x_1 - x_3) - y_1,$$
$$\text{где } m = \frac{y_2 - y_1}{x_2 - x_1}$$

$$\boxed{1Inv + 3Mul \text{ в } K}$$

2. *Если* $x_1 = x_2$*, но* $y_1 \neq y_2$*:*

$$P_1 + P_2 = \mathcal{O}$$

3. *Если* $P_1 = P_2$*, но* $y_1 \neq 0$*:*

$$x_3 = m^2 - 2x_1$$
$$y_3 = m(x_1 - x_3) - y_1, \text{ где } m = \frac{3x_1^2 + A}{2y_1}$$

4. *Если* $P_1 = P_2$, $y_1 = 0$, *то*

$$P_1 + P_2 = \mathcal{O}$$
$$\forall P \in E$$

$$\boxed{1I + 4M}$$

5. *Определим* $P + \mathcal{O} = P$.
   Если $P = (x_1, y_1) \in \underbrace{K \times K}_{поле}$, $P_2 = (x_2, y_2) \in K^2$ *и* $A, B \in K \Rightarrow P_3 \in K^2$.

Теорема 2. *Операция сложения на* E, *заданная в Следствии 1, обладает следующими свойствами:*

1. *Коммутативность:* $P_1 + P_2 = P_2 + P_1 \ \forall P_1, P_2 \in E$
2. $\exists$ *нейтральный элемент:* $P + \mathcal{O} = P \ \forall P \in E$
3. $\exists$ *обратный элемент:* $\forall P \in E \ \exists P' \in E : \ P + P' = \mathcal{O}$ *(обычно* P' *обозначается* $-P$*)*
4. *Ассоциативность:* $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3) \ \forall P_1, P_2, P_3 \in E$.

Вывод: закон сложения «+» точек на E задает аддитивную абелеву группу.

Доказательство. 1 – 5 тривиально; 4 – см. Washington, Sec. 2.4. □

Замечания

1. Для сокращённого уравнения Вейерштрасса ($charK \neq 2, 3$) для $P = (x, y)$

$$-P = (x, -y)\,.$$

   Однако, для обобщенного уравнения ($y^2 + a_1xy + a_3y = X^3 + a_2X^2 + a_4X + a_6$)

$$-P = (X,\ -a_1X - a_3 - y)$$

2. Если E задана над $\mathbb{F}_q \Rightarrow$ получаем конечную абелеву группу ($\Rightarrow$ приложения в криптографии).

   Если E задана над $\mathbb{Q}$, $E(\mathbb{Q})$ — конечно-порожденная абелева группа.

3. Если $char(K) = 2, \quad E: \ y^2 + xy = x^3 + a_2x^2 + a_6$.
   Если $P_1 \neq P_2$:

$$m = \frac{y_1 + y_2}{x_1 + x_2}$$
$$x_3 = m^2 + m + x_1 + x_2 + a_2$$
$$y_3 = (x_1 + x_3)m + x_3 + y_1$$

   Если $P_1 = P_2$:

$$m = \frac{y_1}{x_1} + x_1$$
$$x_3 = m^2 + m + a_2$$
$$y_3 = (x_1 + x_3)m + x_3 + y_1$$

2 Умножение точки на число

$P \to [k] \cdot P = \underbrace{P + P + \ldots + P}_{k \text{ раз}}$ (наивно: $k - 1$ Операций сложения k раз).

2.1 Алгоритм à la быстрое возведение в степень (бинарный метод)

$$k = \sum_{j=0}^{l-1} k_j 2^j, \quad k_j \in \{0, 1\}$$

1. $Q \leftarrow \mathcal{O}$
2. For j = $l - 1$ to 0 by - 1:
   $Q \leftarrow [2]\, Q = Q + Q$
   If $K_j = 1$:
   $Q \leftarrow Q + P$
3. Return Q

Пример

$k = 5, k_0 = 1, k_2 = 1$

$Q \leftarrow \mathcal{O}$

$j = 2: \quad Q \leftarrow P$

$j = 1: \quad Q = 2P$

$j = 0: \quad Q = 4P + P = 5P.$

Сложность:

количество операций дублирования точки: $\mathcal{O}(\lg K)$

количество операций сложения двух точек: $\omega t(K) \sim O(\lg K)$ (ω – вес Хэмминга K) $\Rightarrow \mathcal{O}(\lg k)$ операций сложения (дублирования).

3 Ускорение операции «+» с проективным координатами

$$x = \frac{X}{Z}, y = \frac{Y}{Z}$$

$$\Rightarrow m = \frac{\frac{Y_2}{Z_2} - \frac{Y_1}{Z_1}}{\frac{X_2}{Z_2} - \frac{X_1}{Z_1}} = \frac{Y_2 Z_1 - Y_1 Z_2}{X_2 Z_1 - X_1 Z_2} := \begin{matrix} u \\ v \end{matrix}$$

$$\Rightarrow \frac{X_3}{Z_3} = \frac{u^2}{v^2} - \frac{X_1}{Z_1} - \frac{X_2}{Z_2},$$

$$\frac{Y_3}{Z_3} = \frac{u}{v}\left(\frac{X_1}{Z_1} - \frac{X_3}{z_3}\right) - \frac{Y_1}{Z_1}.$$

$$\text{Пусть } Z_3 = v^3 Z_1 Z_2.$$

$$\Rightarrow X_3 = v(\underbrace{u^2 Z_1 Z_2 - v^3 - 2v^2 X_1 Z_2}_{w}),$$

$$Y_3 = u(X_1 v^2 Z_2 - w) - v^3 Z_2 Y_1$$

В результате получаем алгоритм вычисления суммы точек за 12 умножений в K (вместо 3х умножений + 1 деление в K).