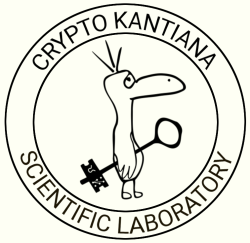
Эллиптические кривые

Лекция 3. Точки n-кручения. Многочлены деления

Семён Новосёлов

БФУ им. И. Канта

2022



IKBFU

Точки n-кручения

Пусть $n > 1$, E – эллиптической кривая над полем K.

- **Порядок точки** $P \in E$, $\operatorname{ord} P$ – минимальное $n \in \mathbb{N}$, т.ч.

$$[n]P = \mathcal{O}$$

- **Точки n-кручения** – элементы множества:

$$E[n] = \left\{ P \in E(\bar{K}) \middle| [n]P = \mathcal{O} \right\}$$

Случай $n = 2$, $\mathrm{char} K \neq 2$

$$E : y^2 = f(x),\ \deg f(x) = 3$$

$$\Downarrow$$

$$y^2 = (x - e_1)(x - e_2)(x - e_3),\ e_i \in \overline{K}.$$

$\forall P \in E$: $[2]P = \mathcal{O} \Leftrightarrow$ касательная ℓ в P – вертикальная

$$\Downarrow$$

$$y = 0$$

$$\Downarrow$$

$$E[2] = \{\mathcal{O}, (e_1, 0), (e_2, 0), (e_3, 0)\} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

Вывод: нахождение точек 2-кручения при $\mathrm{char}\, K \neq 2 \Leftrightarrow$ нахождение корней $f(x)$.

Случай $n = 2$, $\operatorname{char} K = 2$

$$E : y^2 + xy = x^3 + a_2x^2 + a_6 \qquad E : y^2 + a_3y = x^3 + a_4x + a_6$$

$$(a_6 \neq 0) \qquad (a_3 \neq 0)$$

$$\Downarrow \qquad \Downarrow$$

$$P = (x, y),\ [2]P = \mathcal{O} \Rightarrow \text{касательная к } P \text{ – вертикаль} \Rightarrow \frac{dE}{dy} = 0$$

$$\Downarrow \qquad \Downarrow$$

$$2y - x = 0 \qquad \frac{dE}{dy} = a_3$$

$$x = 0 \text{ (т.к. } 2 = 0) \qquad a_3 \neq 0 \text{ (иначе } E \text{ – сингулярная)}$$

$$\Downarrow \qquad \Downarrow$$

$$y^2 = a_6 \qquad E[2] = \{\mathcal{O}\}$$

$$P = (0, \sqrt{a_6})$$

$$E[2] = \{\mathcal{O}, (0, \sqrt{a_6})\} \simeq \mathbb{Z}_2$$

Структура группы 2-кручения

Лемма 1

Для эллиптической кривой E над K выполняется:

$$\mathrm{E}[2] \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \quad \text{при } \operatorname{char} \mathrm{K} \neq 2$$

$$\mathrm{E}[2] \simeq 0 \text{ или } \mathrm{E}[2] \simeq \mathbb{Z}_2 \quad \text{при } \operatorname{char} \mathrm{K} = 2.$$

Структура группы n-кручения

Можно показать [Washington § 3.1], что:

$$E[3] \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_3, \quad \text{при } \operatorname{char} K \neq 3$$
$$E[3] \simeq 0 \text{ или } E[3] \simeq \mathbb{Z}_3, \quad \text{при } \operatorname{char} K = 3$$

В общем случае:

Теорема

Пусть E – эллиптическая кривая над K и $n \geqslant \mathbb{N}_+$. Тогда:

- $E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$, если $\operatorname{char} K \nmid n$ или $\operatorname{char} K = 0$,
- $E[n] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'}$ или $E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_{n'}$ если $\operatorname{char} K = p > 0$, $p|n$ и $n = p^r \cdot n', p \nmid n'$.

Док-во: [Washington § 3.2].

Типы кривых

Пусть эллиптическая кривая E задана над K и $\operatorname{char} K = p$.
Тогда:

- $E[p] \simeq \mathbb{Z}_p \Rightarrow$ кривая **обычная**.
- $E[p] \simeq 0 \Rightarrow$ кривая **суперсингулярная**.
  - ⚠ Не путать с сингулярными кривыми.

Многочлены деления. Мотивация

Применение:

- описывают отображение $\mathfrak{n} : \mathrm{P} \mapsto [\mathfrak{n}]\mathrm{P}$
- используются в алгоритме подсчета точек кривой
- используются в вычислениях изогений

Многочлены деления. Определение

$$E : y^2 = x^3 + Ax + B$$

Многочлены деления $\psi_m \in \mathbb{Z}[x, y, A, B]$ определяются рекуррентными соотношениями:

$$\begin{aligned}
\psi_0 &= 0 \\
\psi_1 &= 1 \\
\psi_2 &= 2y \\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\
\psi_4 &= 4y\left(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3\right) \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \quad m \geqslant 2 \\
\psi_{2m} &= (2y)^{-1} \cdot \psi_m \cdot \left(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2\right), \quad m \geqslant 3
\end{aligned}$$

Получение: из формул сложения в координатах Якоби.

Многочлены деления. Свойства

1. $\psi_n \in \mathbb{Z}[x, y^2, A, B]$, если n – нечетное
   $\psi_n \in 2y\mathbb{Z}[x, y^2, A, B]$, если n – четное.
2. Определим

$$\varphi_m = x \cdot \psi_m^2 - \psi_{m+1}\psi_{m-1}$$
$$\omega_m = (4y)^{-1}\left(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2\right)$$
$$\varphi_n \in \mathbb{Z}\left[x, y^2, A, B\right], \forall n$$
$$\omega_n \in y\mathbb{Z}\left[x, y^2, A, B\right], n \text{ – нечетное}$$
$$\omega_n \in \mathbb{Z}\left[x, y^2, A, B\right], n \text{ – четное}$$

3. В многочленах ψ_n, ϕ_n можно сделать замену $y^2 \mapsto x^3 + Ax + B$. Тогда

$$\varphi_n(x) = x^{n^2} + \text{ мономы степени } < n^2$$
$$\psi_n^2(x) = n^2 x^{n^2-1} + \text{ мономы степени } < n^2 - 1$$

Док-во: [Washington, Lemma 3.3].

Многочлены деления

Теорема

Пусть $E : y^2 = x^3 + Ax + B$, $P = (x, y) \in E$ и $n \in \mathbb{N}_+$. Тогда

$$[n]P = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x)}{(\psi_n(x, y))^3} \right)$$

Таким образом, отображение (эндоморфизм) «умножение на n» задается рациональными функциями.

Билинейные отображения

Пусть E – эллиптическая кривая над полем K и $n \in \mathbb{N}_+$ и $\mu_n = \{x \in \overline{K} | x^n = 1\}$ – группа корней степени n из единицы.

Теорема (спаривание Вейля)

$\exists$ отображение $e_n : E[n] \times E[n] \to \mu_n$ со свойствами:

1. $e_n(T, T) = 1$
2. $e_n(T, S) = e_n(S, T)^{-1}$
3. $e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T)$ *(билинейность)*
   $e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2)$
4. $e_n(S, T) = 1, \forall T \implies S = \mathcal{O}$ *(невырожденность)*
   $e_n(S, T) = 1, \forall S \implies T = \mathcal{O}$

Другие билинейные отображения: спаривание Тейта, эта-спаривание.

Билинейные отображения. Приложения

Степень вложения: минимальное целое k т.ч. $E[n] \subseteq E(\mathbb{F}_{q^k})$.

- Атака на DLOG: $|\langle P \rangle| = n$, $Q = [l]P$.
  1. Выбрать случайную точку R.
  2. $\alpha = e_n(P, R)$
  3. $\beta = e_n(Q, R)$ $\qquad (\beta = e_n(lP, R) = e_n(P, R)^l = \alpha^l)$
  4. $l = \mathrm{DLOG}(\alpha, \beta)$ в $\mathbb{F}_{q^k}$
- Конструктивное использование: ZCash, IBE, BLS

Цифровая подпись

(дополнение к предыдущей лекции)

Общие параметры: кривая E над $\mathbb{F}_q$, $P \in E(\mathbb{F}_q)$, $r = \mathrm{ord}(P)$.

Подпись := (**Setup**, **Sign**, **Verify**).

Setup:

1. Пользователь 🕵 выбирает секретный ключ $a \in [1, r]$.
2. Открытый ключ: $Q = [a]P$.

Sign:

Для подписи сообщения m пользователь 🕵:

1. выбирает случайное $k \in [1, r]$ и вычисляет $R = [k]P = (x, y)$
2. вычисляет $s = k^{-1}(m + ax) \bmod r$
3. подпись: (m, R, s)

Verify:

Для проверки подписи пользователь 🐈:

1. вычисляет $u_1 = s^{-1}m \bmod r$ и $u_2 = s^{-1}x \bmod r$
2. $S = [u_1]P + [u_2]Q$
3. проверяет равенство $S = R$.

Корректность:

◁ $S = [u_1]P + [u_2]Q = [s^{-1}m]P + [s^{-1}x]Q =$
$[s^{-1}]([m]P + [xa]P) = [k]P = R.$ ▷

- используется повсеместно в составе протокола TLS
- для безопасности схемы требуется ряд ограничений на параметры
- ECDSA/ГОСТ 34.10-2018

Литература

- I. Blake и др. *Elliptic curves in cryptography*. 1999.
- A. J. Menezes. *Elliptic Curve Public Key Cryptosystems*. 1993.
- L. C. Washington. *Elliptic curves: number theory and cryptography*. 2008.

Контакты

snovoselov@kantiana.ru

Страница курса:

crypto-kantiana.com/semyon.novoselov/teaching/elliptic_curves_2022