

Эллиптические кривые

Лекция 3. Точки n -кручения. Многочлены деления

Семён Новосёлов

БФУ им. И. Канта

2025



Точки n -кращения

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

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

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

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

$$E[n] = \{ P \in E(\bar{K}) \mid [n]P = \mathcal{O} \}$$

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

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



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

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



$$y = 0$$



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

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

Случай $n = 2$, $\text{char } K = 2$

$$E : y^2 + xy = x^3 + a_2x^2 + a_6 \\ (a_6 \neq 0)$$



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



$$2y - x = 0 \\ x = 0 \text{ (т.к. } 2 = 0)$$



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

$$E : y^2 + a_3y = x^3 + a_4x + a_6 \\ (a_3 \neq 0)$$



$$\frac{dE}{dy} = a_3$$

$$a_3 \neq 0 \text{ (иначе } E - \text{сингулярная)}$$



$$E[2] = \{\mathcal{O}\}$$

Структура группы 2-кручения

Лемма 1

Для эллиптической кривой E над K выполняется:

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

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

Структура группы n -кручения

Можно показать, что:

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

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

В общем случае:

Теорема

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

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

◁ Док-во: [Washington § 3.2]. ▷

Типы кривых

Пусть эллиптическая кривая E задана над K и $\text{char } K = p$.
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 $n : P \mapsto [n]P$
- используются в алгоритме подсчета точек кривой
- используются в вычислениях изогений:
нахождения ядер 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:

$$\psi_0 = 0$$

$$\psi_1 = 1$$

$$\psi_2 = 2y$$

$$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$$

$$\psi_4 = 4y \left(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3 \right)$$

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \quad m \geq 2$$

$$\psi_{2m} = (2y)^{-1} \cdot \psi_m \cdot \left(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2 \right), \quad m \geq 3$$

Получение: из формул сложения и свойств $\wp$ -функции Вейерштрасса (теория кривых над $\mathbb{C}$).

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

$$\varphi_m = x \cdot \psi_m^2 - \psi_{m+1}\psi_{m-1}$$

$$\omega_m = (4y)^{-1} (\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)$$

$$\varphi_n \in \mathbb{Z}[x, y^2, A, B], \forall n$$

$$\omega_n \in y\mathbb{Z}[x, y^2, A, B], n - \text{нечетное}$$

$$\omega_n \in \mathbb{Z}[x, y^2, A, B], n - \text{четное}$$

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

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

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

Многочлены деления

Теорема

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

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

◁ **Док-во:** [Washington, §9.5] ▷

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 $\mu_n = \{x \in \bar{K} | x^n = 1\}$ – группа корней степени n из единицы.

Теорема (спаривание Вейля)

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

- ❶ $e_n(T, T) = 1$
- ❷ $e_n(T, S) = e_n(S, T)^{-1}$
- ❸ $e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T)$ (билинейность)
 $e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2)$
- ❹ $e_n(S, T) = 1, \forall T \implies S = \mathcal{O}$ (невырожденность)
 $e_n(S, T) = 1, \forall S \implies T = \mathcal{O}$

Другие билинейные отображения: спаривание Тейта, эта-спаривание.

Вычисление: алгоритм Миллера на базе быстрого алгоритма скалярного умножения.

Билинейные отображения. Приложения

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

Атака на DLOG: $|\langle P \rangle| = n$, $Q = [\ell]P$.

❶ Выбрать случайную точку R .

❷ $\alpha = e_n(P, R)$

❸ $\beta = e_n(Q, R)$

$$(\beta = e_n(\ell P, R) = e_n(P, R)^\ell = \alpha^\ell)$$

❹ $\ell = \text{DLOG}(\alpha, \beta)$ в $\mathbb{F}_{q^k}$

Конструктивное использование: ZCash, IBE, BLS,
“Pairing-based crypto”

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_2025