

Эллиптические кривые

Лекция 3. Точки n -кращения

Семён Новосёлов

БФУ им. И. Канта

2026



План

- 1 Группа точек n -кручения
- 2 Многочлены деления
- 3 Алгоритм вычисления группы n -кручения
- 4 Приложения в криптографии

I. Группа точек n -кручения

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.

II. Многочлены деления

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.

III. Алгоритм вычисления группы n -кручения

Поле определения $E[n]$

E – эллиптическая кривая над полем $K = \mathbb{F}_q$, $\text{char } K \neq 2, 3$.

Точки n -кручения: $E[n] = \{P \in E(\bar{K}) : nP = \mathcal{O}\}.$

В случае $p \nmid n$:

$$E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$



$$E[n] = \{\mathcal{O}, (x_1, y_1), \dots, (x_m, y_m)\},$$

где $m = n^2 - 1$.



Поле, в котором лежит $E[n]$ (расширение K):

$$K_{E,n} := K(x_1, y_1, \dots, x_m, y_m)$$

$$[K_{E,n} : K] = d < \infty$$

Мотивация

Зачем нужно находить $E[n]$?

- 1 нахождение точек из $E[n]$ — часть полиномиальных (от $\log q$) алгоритмов вычисления $\#E(\mathbb{F}_q)$.
- 2 $d = [K_{E,n} : K]$ — степень вложения, $K_{E,n}$ — поле определения спаривания Вейля $e_n : E[n] \times E[n] \mapsto \mu_r$.



сложность **DLOG** в $E(\mathbb{F}_q) \iff$ сложность **DLOG** в $\mathbb{F}_{q^d}$

Нахождение с помощью многочленов деления

Как вычислить $E[n]$?

Рассмотрим метод на основе факторизации многочленов деления:

- $\psi_m \in \mathbb{Z}[x, y, A, B]$
- $\varphi_m = x \cdot \psi_m^2 - \psi_{m+1}\psi_{m-1}$
- $\omega_m = \frac{1}{4y} (\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)$

Сложение точки P с самой собой n раз:

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

Нахождение $E[n]$

Лемма

Многочлены φ_n и $\psi_n^2 \in K[x]$ – взаимно просты, если $\Delta(E) \neq 0$. Т.е. для E – эллиптической кривой, φ_n, ψ_n^2 – взаимно просты.

◁ Доказательство: [Lang, II 2.3]. ▷

Следствие

Пусть $P = (x, y) \in E(\bar{K})$. Тогда $[n]P = \mathcal{O} \Leftrightarrow \psi_n^2(x) = 0$.

Нахождение $E[n]$

$$\psi_n^2(x) = n^2 x^{n^2-1} + \dots$$

(Washington, §3.2)

Факторизуем ψ_n в $\mathbb{F}_q[x]$.

$$\psi_n = f_1 \cdot \dots \cdot f_r,$$

где f_r – неприводимые над $\mathbb{F}_q$.

Замечание

- все f_i различны
- в $E[n]$ всего $n^2 - 1$ точек $\neq \mathcal{O}$
- $\forall P_i \in E[n]$ имеем $-P_i \in E[n]$
- $\deg \psi_n(x) = \frac{n^2-1}{2} \Rightarrow \psi_n(x)$ имеет $\frac{n^2-1}{2}$ корней в $\overline{\mathbb{F}}_q$ и каждый корень кратности 1 (иначе мы имели бы меньше чем $n^2 - 1$ точек $\neq \mathcal{O}$ в $E[n]$).

Определение степени вложения d

Определим $d = [K_{E,n} : K] \neq 0$ из разложения ψ_n над $\mathbb{F}_q$:

$$\psi_n = f_1 \cdot \dots \cdot f_r$$

Теорема

Пусть n – простое > 2 , $K = \mathbb{F}_q$, $n \neq \text{char}(K)$, $d_i = \deg f_i$, $\ell = \text{lcm}(d_1, \dots, d_r)$. Пусть $K'_{E,n} = K(x_1, \dots, x_{n^2-1})$, где x_i – x -координаты точек n -крючения. Тогда

$$[K'_{E,n} : K] = \ell.$$

Кроме того, $[K_{E,n} : K'_{E,n}] = 1$, либо 2. То есть $d = \ell$ либо 2ℓ .

◁ $\exists x_i$ т.ч. $y_i = \sqrt{x_i^3 + ax_i + b} \notin K'_{E,n} = \mathbb{F}_{q^\ell} \implies d = 2\ell$. В противном случае: $d = \ell$. ▷

Обобщенный символ Лежандра

Определение

$K = \mathbb{F}_q$, $x \in K$. Квадратичный характер $\left(\frac{\cdot}{K}\right)$ – это

$$\left(\frac{x}{K}\right) = \begin{cases} 1, & \exists y \in K : y^2 = x \\ -1, & \nexists y \in K : y^2 = x \\ 0, & x = 0. \end{cases}$$



чтобы определить $d = \ell$ или $d = 2\ell$, необходимо вычислить

$$\left(\frac{x_i^3 + ax_i + b}{\mathbb{F}_{q^\ell}}\right),$$

$\forall x_i$ – корней ψ_n .

Лемма

Если $K = \mathbb{F}_q$ и $d = [K_{E,n} : K]$, то $q^d \equiv 1 \pmod n$. В частности, $\text{ord}(q, n) \mid d$.

Замечание

Так как DLOG на $E(\mathbb{F}_q)$ сводится в $\mathbb{F}_{q^d}$ для проверки безопасности достаточно проверить, что $q^d \not\equiv 1 \pmod n$ для $d \leq 1000$ (требование ГОСТ и др.)

Лемма (van Tuyl)

Пусть f_i — неприводимый многочлен в разложении ψ_n , т.ч. $2d_i \nmid \ell$, $d_i = \deg f_i$. Положим

$$d^* = \text{lcm}(\text{ord}(q, n), d_i),$$

$$c = \left(\frac{x_i^3 + ax + b}{\mathbb{F}_{q^{d_i}}} \right), \text{ где } f_i(x_i) = 0.$$

Тогда

$$d = \begin{cases} \ell, & \text{если } c = 1 \text{ и } d^* | \ell \\ 2\ell & \text{иначе.} \end{cases}$$

- Лемма позволяет рассмотреть лишь один f_i (и его корень x_i) для определения d .

Алгоритм вычисления $d = [K_{E,n} : K]$

Вход: $E/\mathbb{F}_q : y^2 = x^3 + ax + b, n \geq 3$ – нечётное.

Выход: d т.ч. $E[n] \subseteq E(\mathbb{F}_{q^d})$.

- 1 Построить $\psi_n \in \mathbb{F}_q[x]$
- 2 Факторизовать $\psi_n = f_1 \cdot \dots \cdot f_r$
- 3 $\ell := \text{lcm}(\deg f_1, \dots, \deg f_r)$
- 4 Выбрать f_i т.ч. $2 \cdot \deg f_i \nmid \ell$
- 5 Вычислить $c = \left(\frac{x_i^3 + ax_i + b}{\mathbb{F}_{q^{d_i}}} \right)$, где x_i – корень f_i .
- 6 if $c = -1$:
 return $d = 2\ell$
- 7 $d^* = \text{lcm}(\text{ord}(q, n), d_i)$
 if $d^* = \ell$ or $\ell = n \cdot d^*$:
 return $d = \ell$
 return $d = 2\ell$

- Алгоритм может быть адаптирован для вычисления самой группы точек n -кручения $E[n]$, если для x_i – корня f_i , вычислять соответствующие y_i
- для $n = 2$, $E[n]$ вычисляется разложением многочлена $x^3 + ax + b$ (см. пред. лекцию)
- для $n = 1$, $E[n] = \{\mathcal{O}\}$.

Оценка сложности

- Шаг 1. $\deg \psi_n = \frac{n^2-1}{2}$. Грубо: $\text{poly}(n)$.
- Шаг 2. Факторизация многочлена

$$\tilde{O}((\deg \psi_n)^2 \log^2 q) \quad (\text{MCA, Th. 14.14})$$

Шаг 5. Обобщённый символ Лежандра:

$$\text{poly}(n) \quad (\text{CF'05, Alg. 11.69})$$

- Шаг 7. Сводится к факторизации $n - 1$. Время: $L_n(1/3)$.

Итого: $L_n(1/3) \cdot \log^2 q$ операций в $\mathbb{F}_q$.

IV. Приложения в криптографии

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”

Подпись BLS (Boneh-Lynn-Shacham)

$$e_r : G_1 \times G_2 \mapsto G_T$$

Общие параметры

- P_1, P_2 т.ч. $G_1 = \langle P_1 \rangle$ и $G_2 = \langle P_2 \rangle$
- $H : \{0, 1\}^* \rightarrow G_1$
(хэш-функция)

Генерация ключей 🐱

- 1 секретный ключ: $a \overset{\text{🐱}}{\in} [1, r]$
- 2 открытый ключ:
 $Q = [a]P_2$

Подпись сообщения ✉

- 1 $R = H(\text{✉})$
- 2 🐾 = $[a]R$

Проверка

- 1 $e_r(\text{🐾}, P_2) == e_r(H(\text{✉}), Q)?$

$$\triangleleft e_r(\text{🐾}, P_2) = e_r(R, P_2)^a = e_r(H(\text{✉}), [a]P_2) = e_r(H(\text{✉}), Q)$$

▷

BLS в Ethereum

- В Ethereum каждые 12 секунд формируется новый блок из транзакций (напр., перевод средств)
- Блок проверяется и подписывается тысячами валидаторов
- Хранение тысяч подписей валидаторов $\text{paw}_1, \dots, \text{paw}_m$ заняло бы много места в блокчейне
- Поэтому подписи объединяются в одну (96-байт):

$$\text{paw} = \text{paw}_1 + \dots + \text{paw}_m$$

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_2026