

Эллиптические кривые

Лекция 4. Алгоритм вычисления $E[n]$

Семён Новосёлов

БФУ им. И. Канта

2022



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}

Многочлены 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 $E[n]$

Lemma

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]. ▷

Corollary

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 -кращения. Тогда

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

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

$\triangleleft \exists x_i$ 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: $d = \ell$. \triangleright

Обобщенный символ Лежандра

Definition

$K = \mathbb{F}_q$, $x \in K$. 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 -кращения $E[n]$, 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 $n = 1$, $E[n] = \{O\}$.

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 .

Литература

- ☰ Н. Cohen и др. *Handbook of elliptic and hyperelliptic curve cryptography*. 2005.
- ☰ S. Lang. *Elliptic Curves: Diophantine Analysis*. 1978.
- ☰ A. L. van Tuyl. *The field of n -torsion points of an elliptic curve over a finite field*. 1997.
- ☰ J. Von Zur Gathen и J. Gerhard. *Modern computer algebra*. 2013.
- ☰ 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