Эллиптические кривые

Лекция 4. Алгоритм вычисления $E[n]$

Семён Новосёлов
на основе курса Елены Киршановой

БФУ им. И. Канта

2020

IKBFU

Поле определения $E[n]$

E – эллиптическая кривая над полем $K = \mathbb{F}_q$, $\mathrm{char}\, K \neq 2, 3$.
Точки n-кручения: $E[n] = \left\{ P \in E\left(\bar{K}\right) : nP = \mathcal{O} \right\}$.
В случае $p \nmid n$:

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

$$\Downarrow$$

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

где $m = n^2 - 1$.

$$\Downarrow$$

Поле, в котором лежит $E\left[n\right]$ (расширение K), можно записать как

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

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

Многочлены деления

Как вычислить $E[n]$?

Рассмотрим метод на основе факторизации многочленов деления (из лекции № 3):

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

Сложение точки P с самой собой n раз:

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

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.*

$\triangleleft$ Доказательство: [Lang, II 2.3].$\triangleright$

Следствие

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

Нахождение $E[n]$

$\psi_n^2(x) = n^2 x^{n^2-1} + \ldots$ (Washington, §3.2)

Факторизуем ψ_n в $\mathbb{F}_q[x]$.

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

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 $\mathbb{F}_q$:

$$\psi_n = f_1 \cdot \ldots \cdot f_r$$

Теорема

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

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

Таким образом, 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 (van Tuyl)

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

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

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

Тогда

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

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

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

Вход: $E/\mathbb{F}_q : y^2 = x^3 + ax + b$, $n \geqslant 3$ – нечётное.
Выход: d т.ч. $E[n] \subseteq E(\mathbb{F}_{q^d})$.

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

Оценка сложности

- Шаг 1. $\deg \psi_n = \frac{n^2-1}{2}$. Грубо: $\mathrm{poly}(n)$.
- Шаг 2. Berlakamp-Zassenhaus:
  $O((\deg \psi_n)^3 + (\deg \psi_n)^2 \cdot \lg(n^2) \cdot \lg q)$.
- Шаг 5. Наивно (baby step / giant step): $O(\sqrt{q^{d_i}})$. Можно свести к вычислению символа Лежандра над $\mathbb{F}_q$.

Итого: $\mathrm{poly}(n)$ / $O(\mathrm{poly}(n) + \sqrt{q^{d_i}})$

Литература

- 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.
- L. C. Washington. *Elliptic curves: number theory and cryptography*. 2008.

Контакты

snovoselov@kantiana.ru