

Эллиптические кривые

Лекция 5. Алгоритмы подсчета точек кривой I

Семён Новосёлов

БФУ им. И. Канта

2025



Мотивация

Криптография на **DLOG** в группе G :

(почти) простое $\#G \implies$ стойкость к атаке
Полига-Хелмана¹



Нужно уметь генерировать кривые с (почти) простым
числом точек.

¹вкратце: сведение задачи к подгруппам

Задачи:

- 1 подобрать кривую с **заданным** (простым) числом точек над полем $\mathbb{F}_q \implies$ СМ-метод
- 2 подобрать кривую с простым числом точек над полем $\mathbb{F}_q$:
 - выбирать случайную кривую и считать число точек пока не получится простое число точек
 - ожидаемое число попыток: $O(\log |G|)$
(следует из теоремы о распределении простых чисел)

СМ-метод даёт лучшие кривые, но при этом существенно сложнее.

Эндоморфизм Фробениуса

Алгоритмы подсчёта точек базируются на свойствах эндоморфизма:

$$\begin{aligned}\varphi_q : \overline{\mathbb{F}}_q &\rightarrow \overline{\mathbb{F}}_q \\ x &\mapsto x^q\end{aligned}$$

❶ $(x_1 + x_2)^q = x_1^q + x_2^q$

❷ $x^q = x, \forall x \in \mathbb{F}_q$

Действие φ_q на точки из $E(\overline{\mathbb{F}}_q)$:

$$\varphi_q(x, y) = (x^q, y^q), \varphi_q(\mathcal{O}) = \mathcal{O}.$$

E – кривая над $\mathbb{F}_q$, $(x, y) \in E(\overline{\mathbb{F}}_q)$.

Свойства φ_q :

❶ $\varphi_q(x, y) \in E(\overline{\mathbb{F}}_q)$

◁ $(y^2)^q = (x^3 + ax + b)^q \Leftrightarrow$

$(y^q)^2 = (x^q)^3 + ax^q + b \Leftrightarrow (x^q, y^q) \in E(\overline{\mathbb{F}}_q)$ ▷

❷ $(x, y) \in E(\mathbb{F}_q) \Leftrightarrow \varphi_q(x, y) = (x, y)$

◁ $x \in \mathbb{F}_q \Leftrightarrow \varphi_q(x) = x$ ▷

❸ $\ker(\varphi_q^n - 1) = E(\mathbb{F}_{q^n})$

❹ $\#E(\mathbb{F}_{q^n}) = \deg(\varphi_q^n - 1)$

Граница Хассе-Вейля

Теорема

Для любой кривой $E/\mathbb{F}_q$ выполняется:

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}$$

◁ Выводится из свойств (1)–(4) для φ_q (см. [Washington, § 4.2]). ▷

След эндоморфизма Фробениуса:

$$t = q + 1 - \#E(\mathbb{F}_q) = q + 1 - \deg(\varphi_q - 1)$$

- Асимптотически: $\#E(\mathbb{F}_q) \sim O(q)$

Характеристический многочлен эндоморфизма Фробениуса

Теорема

E – эллиптическая кривая над $\mathbb{F}_q$ и $t = q + 1 - \#E(\mathbb{F}_q)$. Тогда

$$\varphi_q^2 - t\varphi_q + q = 0$$

как эндоморфизм на E и t определено uniquely. Другими словами $\forall (x, y) \in E(\overline{\mathbb{F}}_q)$:

$$(x^{q^2}, y^{q^2}) - t(x^q, y^q) + q(x, y) = \mathcal{O}.$$

Кривые в подполе

Кривая E задана над $\mathbb{F}_q \implies$ можем выразить $\#E(\mathbb{F}_{q^n})$ через $\#E(\mathbb{F}_q)$.

Теорема

Пусть $\#E(\mathbb{F}_q) = q + 1 - t$. Запишем $X^2 - tX + q = (X - \alpha)(X - \beta)$. Тогда:

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n) \quad \forall n \geq 1.$$

Лемма

Пусть $t_n = \alpha^n + \beta^n$. Тогда $t_0 = 2$, $t_1 = t$ и $t_{n+1} = tt_n - qt_{n-1}$ для всех $n \geq 1$.

- Т.о., если известно $\#E(\mathbb{F}_q)$, то $\#E(\mathbb{F}_{q^n})$ находится за время $O(n)$ операций в $\mathbb{Z}$.

Алгоритмы подсчёта точек

Экспоненциальные:

- 1 перебор на основе символа Лежандра
- 2 алгоритм Baby Step-Giant Step (BSGS)
- 3 ρ -метод Полларда

Полиномиальные:

- алгоритм Схоофа и его модификации (SEA)

Подсчёт точек на основе символа Лежандра

Лемма

Для $E : y^2 = x^3 + ax + b$ над $\mathbb{F}_q$ имеем:

$$\#E(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + ax + b}{\mathbb{F}_q} \right).$$

- Сложность: $O(q \text{ polylog } q)$.

Алгоритм Baby Step-Giant Step (BSGS)

Идея: Пусть $N = \#E(\mathbb{F}_q)$ – неизвестно. По теореме Лагранжа: $[N]P = \mathcal{O}, \forall P$.

Т.к. $q + 1 - 2\sqrt{q} \leq N \leq q + 1 + 2\sqrt{q} \implies$ можем перебирать все N проверяя условие $[N]P = \mathcal{O}$.

- Наивный метод (brute force): $O(\sqrt{q})$.
- Алгоритм поиска коллизий/циклов (BSGS): $O(\sqrt[4]{q})$.
 - Основан на парадоксе дней рождений.

Алгоритм (BSGS). Нахождение порядка точки

Вход: $P \in E(\mathbb{F}_q)$.

Выход: $\text{ord}(P)$.

- 1 $Q = (q + 1)P$.
- 2 Выбрать $m > \sqrt[4]{q}$, вычислить и сохранить в списке L все пары $(j, [j]P)$ для $j = 0, \dots, m$. *(baby steps)*
- 3 Вычислять точки $Q + k(2mP)$ для $k = -m, -(m - 1), \dots, m$ пока в L не найдётся точка $\pm[j]P$ т.ч. $Q + k(2mP) = \pm[j]P$ *(giant steps)*
- 4 Имеем $[q + 1 + 2mk \mp j]P = \mathcal{O}$.
 $M = q + 1 + 2mk \mp j$.
- 5 Найдём $p_1, \dots, p_r$ – различные простые делители M .
- 6 Если $[M/p_i]P = \mathcal{O}$ для нек. i , то $M = M/p_i$ и перейти к шагу 5.
- 7 Вернуть M .

Алгоритм (BSGS). Нахождение порядка точки

Анализ сложности

Шаг 1. (быстрое умножение) $O(\log q)$ сложений на кривой
 $\implies \tilde{O}(\log^2 q)$ бит. операций

Шаг 2. $\tilde{O}(m) = \tilde{O}(q^{1/4})$ – время, $O(q^{1/4})$ – память.

Шаг 3. $\tilde{O}(2m) = \tilde{O}(q^{1/4})$ – ожидаемое количество переборов k .

Шаг 4. Элементарные операции в $\mathbb{Z}$.

Шаг 5. $L_q(1/3, c) = \exp(c(\log q)^{1/3}(\log \log q)^{2/3})$.

Шаг 6. $O(\log M) = O(\log q)$ сложений на кривой.

Итого: самый затратный шаг 3: $\tilde{O}(q^{1/4})$.

Замечания

- 1 Для оптимизации памяти достаточно хранить только координату x .
- 2 С помощью p -метода Полларда можно реализовать алгоритм, использующий только $\text{polylog } q$ памяти.

Алгоритм (BSGS). Нахождение $\#E(\mathbb{F}_q)$

Вход: $E/\mathbb{F}_q$.

Выход: $\#E(\mathbb{F}_q)$.

- 1 $L = 1$.
- 2 Выбрать случайную точку $P \in E(\mathbb{F}_q)$.
- 3 $r = \text{ord}(P)$.
- 4 $L = \text{lcm}(L, r)$.
- 5 Если L делит только одно целое N т.ч.
 $q + 1 - 2\sqrt{q} \leq N \leq q + 1 + 2\sqrt{q}$, то вернуть N . В противном случае – перейти к шагу 2.

ρ -метод Полларда

$$E/\mathbb{F}_q : y^2 = x^3 + ax + b$$

$$P \in E(\mathbb{F}_q), \text{ord } P = ?$$

Идея: задать псевдослучайную последовательность точек $P_0 = P, P_{i+1} = f(P_i)$ и экспонент $e_0, e_1, \dots$, т. ч. $P_i = [e_i]P$.
 $E(\mathbb{F}_q)$ – конечная группа $\implies \exists i, j : P_i = P_j \implies \text{ord}(P)$ делит $|e_i - e_j|$.

Для нахождения i, j т.ч. $P_i = P_j$ используются различные алгоритмы нахождения циклов.

ρ -метод Полларда

На основе алг. поиска циклов Флойда

Вход: $P \in E(\mathbb{F}_q)$, $r \in \mathbb{N}$, $h : E(\mathbb{F}_q) \rightarrow \{1, \dots, r\}$.

Выход: M т.ч., $\text{ord}(P) \mid M$

- 1 Сгенерировать r случайных чисел α_i ;
- 2 Вычислить $Q_i = [\alpha_i]P$;
- 3 Задать $f : (P, e) \mapsto (P + Q_{h(P)}, e + \alpha_{h(P)})$;
- 4 $(P_1, e_1) = (P, 1)$;
- 5 $(P_2, e_2) = f(P_1, e_1)$;
- 6 **while** $P_1 \neq P_2$ **do**:
- 7 $(P_1, e_1) = f(P_1, e_1)$;
- 8 $(P_2, e_2) = f(f(P_2, e_2))$;
- 9 **return** $M = |e_1 - e_2|$.

Сложность: $O(q^{1/4})$ по времени и $O(1)$ по памяти.

Литература



Н. Cohen и др.

Handbook of elliptic and hyperelliptic curve cryptography. 2005.



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