Лекция #6

Алгоритмы подсчёта точек эллиптической кривой над $\mathbb{F}_q$

0. Из предыдущей лекции:

$E(\mathbb{F}_q): y^2 = x^3 + Ax + B$ - эллиптическая

$\#E(\mathbb{F}_q) = |E(\mathbb{F}_q)|$ - число q-рациональных точек кривой (или порядок кривой)

Т-ма Хассе даёт верхнюю и нижнюю оценки для $|E(\mathbb{F}_q)|$:

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

Асимптотика: $\#E(\mathbb{F}_q) = O(q)$

Если $a = q + 1 - \#E(\mathbb{F}_q)$, то $|a| \le 2\sqrt{q}$, a - след Фробениуса

Мы доказали, что $\#E(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + Ax + B}{\mathbb{F}_q} \right)$, где $\left(\frac{\cdot}{\mathbb{F}_q}\right)$ - кв. вычет в $\mathbb{F}_q$

Время работы алгоритма $\nearrow$ $O(q \lg q) = \tilde{O}(q)$ - (если q - простое $\Rightarrow$ символ Лежандра)

- экспоненциальное от числа бит q.

I. Алгоритм подсчёта точек Baby Step - Giant Step $V^{BS\text{-}GS}$ =

= алгоритм нахождения порядка точки $P \in E(\mathbb{F}_q)$ (т.е. $\min k : kP = O$).

Идея: $\exists N = \#E(\mathbb{F}_q)$ - неизвестно

По т-ме Лагранжа: $NP = O \quad \forall P$

т.к. $q + 1 - 2\sqrt{q} \le N \le q + 1 + 2\sqrt{q}$ (т.е. N лежит в интервале р-ра $4\sqrt{q}$),

мы можем проверить все N из этого интервала; проверка: $NP \stackrel{?}{=} O$.

Наивный метод (brute force): $O(\sqrt{q})$.

Алгоритм BS-GS (стандартный алгоритм нахождения коллизий / цикла ф-ии)

ускоряет до $O(q^{1/4})$.

Для начала опишем алгоритм нахождения порядка точки $P \in E$

Algorithm BS-GS для нахождения порядка точки P

Вход: $P \in E(\mathbb{F}_q)$; Выход: $k = ord(P)$

1. $Q = (q+1)P$

2. Выберем $m \in \mathbb{Z}$: $m > q^{1/4}$

"Baby Step" Вычислим и сохраним (в список L) все $\pm j \cdot P$, $j = 0, \dots, m$. сортируем L.

L:

$(j, j \cdot P)$
⋮

3. Вычисляем точки $Q + k \cdot (2mP)$ для всех $k = -m, -(m-1), \dots, m$

"Giant Step" пока не найдём в списке L точку $\pm jP$ т.ч.

$$Q + k(2mP) = \pm jP$$

4. $Q + k(2mP) = \pm jP \iff (q+1+2mk \mp j)P = O$

4. $M = q+1+2mk \overset{\text{нужный знак}}{(\mp)} j$. (порядок P - делитель M)

5. Факторизуем $M = p_1^{e_1} \cdots p_r^{e_r}$

6. Вычислим для $i = 1 \dots r$

Вычислим (M/p_i).

Если $\left(\frac{M}{p_i}\right)P = O$

$M \leftarrow \frac{M}{p_i}$,

Вернуться к Шагу 5 (неоптимально, но корректно)

Если $\left(\frac{M}{p_i}\right)P_i \neq O \ \forall i \Rightarrow$

Вернуть M.

Оптимальнее: хранить $I = \{[p_i, e_i], i = 1, r\}$, уменьшать эн-ия e_i в шаге 6.

Корректность

1. Найдём ли мы коллизию на шаге 3?

Лемма 1 $\exists x \in \mathbb{Z}$: $|x| \leq 2m^2$. Тогда $\exists x_0, x_1 \in \mathbb{Z}$ т.ч. $-m < x_0 \leq m$ и $-m \leq x_1 \leq m$

(разбиение эл-та x на $2m$ старших бит и $(\lg x - 2m)$ младших)

$$x = x_0 + 2m x_1$$

$\triangle$ $\exists\, x_0 = x \bmod 2m$ (где $\bmod B \in (-\frac{B}{2}, \frac{B}{2}]$)

$x_1 = \frac{x - x_0}{2m}$.

Тогда $|x_1| \le \frac{(2m^2 + m)}{2m} < m + 1$. $\triangleright$

2. Почему шаг 6 возвращает порядок P?

Лемма 2 $\exists$ G – абелева группа, $g \in G$. Положим $M \overset{\text{т.ч.}}{=} 0$, $Mg = 0$ и $M = p_1^{e_1} \dots p_r^{e_r}$, p_i – различные простые. Тогда если $\left(\frac{M}{p_i}\right) g \neq 0 \ \forall i \in \overline{1,r}$, то M – порядок g.

$\triangle$ $\exists\, k$ – порядок g. Тогда $k \mid M$. Положим $k \neq M$. (от противного).

$\exists p_i$ – простое делящее $\frac{M}{k}$.

Тогда $(p_i \cdot k) \mid M$, или $k \mid \left(\frac{M}{p_i}\right)$ (кратно порядку) $\Rightarrow \left(\frac{M}{p_i}\right) g = 0$ (т.е. мы нашли $p_i : \left(\frac{M}{p_i}\right) g = 0$) $\rightarrow$ против. утверждению Т-ии $\Rightarrow$

$\rightarrow k = M$. $\triangleright$

Анализ сложности алгоритма

Шаг 1 ("быстрое" сложение): $O(\lg q)$ операций "+" на кривой, каждый "+" $\text{poly} \lg q \Rightarrow$

$\Rightarrow O(\text{poly} \lg q)$.

Шаг 2: $\gamma(m) = \tilde{O}(q^{1/4})$ – времени

$O(q^{1/4})$ – память

Шаг 3: $\gamma(2m) = \tilde{O}(q^{1/4})$ – ожидаемое кол-во переборов k.

Шаг 4: элементарные операции в $\mathbb{F}_q$

Шаг 5: оh-оh. $L\left[\frac{1}{3}, \sqrt[3]{\frac{64}{9}}\right] = \exp\left(\left[\sqrt[3]{\frac{64}{9}} + o(1)\right] (\ln q)^{\frac{1}{3}} (\lg \ln q)^{\frac{2}{3}}\right)$

Шаг 6 $\tilde{\delta}\left(\sqrt{\lg M} \cdot \text{poly} \lg(q)\right) = \gamma\left(\sqrt{\lg M}\right) = \tilde{O}(\text{poly} \lg q)$

макс. $r \approx \sqrt{\lg M}$ $\quad \sqrt{\lg q}$

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

Замечания к алгоритму

1. Для оптимизации памяти (вычислений) на шаге 3 достаточно хранить x-координату

2. Классическим алгоритмом cycle finding (Поллард-ρ), можно реализовать алгоритм, используя только $\text{poly}\lg q$ - памяти;

Алгоритм вычисления $\#E(\mathbb{F}_q)$:

1. Выбрать $P \in E(\mathbb{F}_q)$ (случайно x-coo, вычислить y: $y^2 = x^3 + Ax + B$)
2. Найти $k_P = \text{ord} P$
3. Повторить шаги (1)-(2), получив мн-во порядков $\{k_{P_i} = \text{ord} P_i\}_{i \le t}$.
4. $L = \text{lcm}(k_{P_i})$, пока $L \notin [q+1-2\sqrt{q}, q+1+2\sqrt{q}]$.

Всевозможные порядки, которые могут быть получены на шаге 3:

$$\text{ord} P_i \in \{ \prod_{0 \le l_i \le e_i} p_i^{l_i} \}, \text{ где } \#E(\mathbb{F}_q) = \prod p_i^{e_i}$$

↑ Всевозможные делители $\#E(\mathbb{F}_q)$.

Всего $\prod_{i=1}^{r} e_i$ всевозможных порядков

$\times O(\lg M)$ = $\#E(\mathbb{F}_q)$ повторов на шаге 3.

Лекция #6 (7)

Алгоритм Схофа (Schoof's Algorithm)

$E: y^2 = x^3 + Ax + B$

R. Schoof "Counting points on elliptic curves over finite fields".

Оригинальная статья: R. Schoof "Elliptic curves over finite fields and the computation of square roots" mod p".

Полиномиальный алгоритм от $\lg q$! q - простое

Основная идея: вычислить $\#E(\mathbb{F}_q) \bmod \{2, 3, .., p\}$ - простые числа, и, затем, восстановить $\#E(\mathbb{F}_q)$ по CRT.

1. Вычисление $\#E(\mathbb{F}_q) \bmod 2$: $\#E(\mathbb{F}_q)$ - чётно $\Leftrightarrow$ $E(\mathbb{F}_p)$ содержит точку $\neq O$ порядка 2.

Точки порядка 2 имеют y-координату $= 0 \Leftrightarrow x^3 + Ax + B = 0$ в $\mathbb{F}_q$

Как определить, есть ли у x^3+Ax+B корни в $\mathbb{F}_q$?

- все эл-ты $\mathbb{F}_q$ - корни $x^q - x$. Т.е. $x^3+Ax+B = 0$ в $\mathbb{F}_p \Leftrightarrow$

$$\gcd(x^q - x,\ x^3+Ax+B) \neq 1 \quad \text{в } \mathbb{F}_p[x].$$

$\exists$ эффективный алгоритм. (вычисление x^q проводятся в $\mathbb{F}_p[x]/(x^3+Ax+B)$ ускоренным алг-мом возведения в степень).

сложность: $O(\lg^3 q)$

2. Обобщим на другие $\ell \in \{2, 3, .., p\}$, $\ell \neq 2$.

Т.к. $|\#E(\mathbb{F}_q) - q - 1| < 2\sqrt{q}$, для получения $\#E(\mathbb{F}_q)$ достаточно рассмотреть простые ℓ т.ч.

$$\prod_{\ell} \ell > 4\sqrt{q}.$$

Т-ма о распределении простых чисел ($p_n \sim n \lg n$); нам будет достаточно взять $O(\lg q)$ простых ℓ, каждый р-ром $O(\lg q)$

2.1 Как и в случае $\ell = 2$, рассмотрим группу точек ℓ-кручения

$$E[\ell] = \{P \in E(\bar{\mathbb{F}}_q) : \ell \cdot P = O\} \simeq \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}.$$

$\psi_\ell(x) \in \mathbb{F}_q[x]$ - ℓ-ми-на деления ($\in \mathbb{F}_q[x]$ т.к. мы берём простые (=> нечётные) ℓ).

↑ могут быть эффективно получены в явном виде с помощью рекуррентных соотношений

2.2. Эндоморфизм Фробениуса $\varphi_q : E \to E$, $(x,y) \mapsto (x^q, y^q)$ удовлетворяет соотношению (см. лекцию #5)

$$(*) \quad \varphi_q^2 - a\varphi + q = 0, \text{ где } a - \text{след Фробениуса } (a = q+1-\#E(\mathbb{F}_q))$$

$$(\text{т.е. } (x^{q^2}, y^{q^2}) - [a](x^q, y^q) + [q] = O).$$

~~Алгоритм Скуфа~~

Соотношение $(*)$ справедливо и $\bmod\ \ell$, т.е.

$$\varphi_q^2 - a'\varphi + q' = 0 \quad \text{для некоторых } a' \in \{0, .., \ell-1\} \text{ т.ч. } a \equiv a' \bmod \ell, \; q' \in \{0, .. \ell-1\}, \; q = q' \bmod \ell.$$

ВАЖНО: соотношение $(*)$ может быть задано с помощью многочленов $\Rightarrow$ для кандидатов a' $\exists$ эффективная проверка:

$$q' P = \left(\frac{\varphi_{q'}(x)}{\psi_{q'}^2(x)}, \frac{\omega_{q'}(x,y)}{\psi_n^3(x,y)} \right).$$

$$\underbrace{(x^{q^2}, y^{q^2})}_{} + \overbrace{q'(X,Y)} = \underbrace{a'(x^q, y^q)}_{\text{аналог.}} \bmod \psi_\ell(x) \text{ и } \bmod Y^2 - X^3 - AX - B$$

мн-ны от X, Y $\bmod \psi_\ell(x)$, $Y^2 - X^3 - AX - B$
(быстрое возв. в степень по модулю)

$\in \mathbb{F}_q[x,y]/(\psi_\ell(x), Y^2 - X^3 - AX - B)$

Сложность алгоритма

Повторяем для каждого ℓ. Всего $O(\lg q)$ различных ℓ.

- для фиксированного $\ell \in \{2 \dots p\}$: $\deg \psi_\ell(x) = \frac{\ell^2 - 1}{2} = O(\ell^2)$
  - подсчёт x^{q^2}, x^q mod $\psi_\ell(x)$: $O(\lg q \cdot (\ell^2 \lg q)^2)$ (возв. в степень q, q^2; кол-во бит в многочлене; сложность операции $\times$, в $\mathbb{F}_q$)
  - умножение точки (x^q, y^q) $\leq \ell$ раз для каждого кандидата a: $O(\ell \cdot (\ell^2 \cdot \lg q)^2)$ (макс. ℓ кандидатов)

Всего: $O(\lg q \cdot (O(\lg q (\ell^2 \lg q)^2 + O(\ell(\ell^2 \lg q)^2)) \underset{\ell = \lg q}{=}$

$= O(\lg^8 q)$.