Осень 2019

Лекция №5 — 11.10.19

Лектор: Елена Киршанова *Оформил Филипп Максимов*

1 Вычисление символа Лежандра $\left(\frac{\cdot}{\mathbb{F}_{q^{d_i}}}\right)$

В алгоритме вычисление $d = [K_{E,n} : K = \mathbb{F}_q]$ (Лекция №4) вызывается алгоритм вычисления символа $\left(\frac{x_i^3 + ax_i + b}{\mathbb{F}_{q^{d_i}}}\right)$.

$$\left(\frac{x}{\mathbb{F}_{q^{d_i}}}\right) = \begin{cases} 1, & \exists t \in (\mathbb{F}_{q^{d_i}})^\times : t^2 = x \bmod q^{d_i} \\ -1, & \nexists t \in (\mathbb{F}_{q^{d_i}})^\times : t^2 = x \bmod q^{d_i} \\ 0, & x = 0. \end{cases}$$

Покажем, что вычисление $\left(\frac{\cdot}{\mathbb{F}_{q^{d_i}}}\right)$ сводится к вычислению $\left(\frac{\cdot}{\mathbb{F}_q}\right)$.

В наших примерах q — простое $\Rightarrow \left(\frac{\cdot}{\mathbb{F}_q}\right) = \left(\frac{\cdot}{q}\right)$ — символ Лежандра $\Rightarrow \exists$ эффективный алгоритм, т. ч. $\left(\frac{x}{q}\right) = x^{\frac{q-1}{2}} \bmod q$.

Напоминание: L/K — конечное расширение, $G = \mathrm{Gal}(L/K)$.

Норма $d : N_{L/K}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha) \in K$

для $L = \mathbb{F}_{q^d}, K = \mathbb{F}_q : N_{\mathbb{F}_{q^d}/\mathbb{F}_q}(\alpha) = \prod_{i=0}^{d} \alpha^{q^i} = \alpha^{\prod_{i=0}^{d} q^i} = \alpha^{\frac{q^d-1}{q-1}}$

Лемма 1. *Пусть L/K — конечное расширение степени d, $[L : K] = d$, $|K| = q$ ($charK,\ charL \neq 2$). Для $x \in L$ справедливо*

$$\left(\frac{x}{L}\right) \cdot \left(\frac{N_{L/K}(x)}{k}\right), \ \textit{где}\ N_{L/K}(x) = x^{\frac{q^d-1}{q-1}}.$$

Доказательство. Положим $(\frac{x}{L}) = 1 \Rightarrow \exists y \in L : y^2 = x$. Тогда

$$N_{L/K}(x) = N_{L/K}(y^2) = (N'_{L/K}(y))^2,$$

т.к.

$$N_{L/K}(y) \in K \Rightarrow \left(\frac{N_{L/K}(y)}{k}\right) = 1.$$

Положим обратное $\left(\frac{N_{L/K}(x)}{K}\right) = 1$.

Запишем $x = gt$ для g — образующий L. Покажем, что t — чётно ($\Rightarrow x$ — квадратичный вычет в L).

Т.к. $\left(\frac{N_{L/K}(x)}{K}\right) = 1 \Rightarrow \exists y \in K : y^2 = N_{L/K}(x) = x^{\frac{q^d-1}{q-1}} \Leftrightarrow$

$\Leftrightarrow 1 = g^{t \cdot \frac{q^d \pm 1}{2}} \Rightarrow$ т. к. g — образующий (ord $g = q^d - 1$), то $2 \mid t$. $\square$

В случае алгоритма вычисления d:

$$\left(\frac{N_{\mathbb{F}_{q^{d_i}}/\mathbb{F}_q}(x_i^3 + ax_i + b)}{\mathbb{F}_q}\right) = \left(\frac{(x_i^3 + ax_i + b)^{\frac{q^{d_i}-1}{q^d-1}}[q]}{\mathbb{F}_q}\right)$$

Для вычисления q^{d_i} пользоваться быстрым возведением в степень.
Последняя скобка в равенстве — символ Лежандра, т.к. $\mathbb{F}_q$ — простое.

2 Вычисление порядка группы точек эллиптической кривой

2.1 Эндоморфизм Фробениуса

$\varphi_q : \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q \; x \mapsto x^q$ — эндоморфизм (отображение) Фробениуса.

Действие φ_q на кривую E над $\mathbb{F}_q$: $\varphi_q(x, y) = (x^q, y^q)$. $\varphi_q(0) = \mathcal{O}$.

Свойства φ_q :

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

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

Используя $(a + b)^q = a^q + b^q$ (q — степень характеристики роля) и $a^q = a \; \forall a \in \mathbb{F}_q$:

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

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

.

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

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

3. $\ker(\varphi_q^n - 1) = E(\mathbb{F}_{q^n})$
Отображение $(x, y) \mapsto (x^q, y^q) - (x, y)$, где «$-$» это вычитание на E.

4. $\#E(\mathbb{F}_q) = \deg(\varphi_q^n - 1)$

Из свойств (1)–(4) для φ_q можно доказать (см. Washington § 4.2) следующую теорему.

Теорема 2 (Теорема Хассе)**.** *(Описывает границы $\#E(\mathbb{F}_q)$)*

Пусть E — кривая над $\mathbb{F}_q$. Тогда справедливо

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

(Неформально: асимптотически $\#E(\mathbb{F}_q) \sim q$).

Положим $a = q + 1 - \#E(\mathbb{F}_q) = q + 1 - \deg(\varphi_q - 1)$. Число a — след эндоморфизма Фробениуса.

Теорема 3. *E — эллиптическая кривая над $\mathbb{F}_q$, число $a = q + 1 + \#E(\mathbb{F}_q)$. Тогда*

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

— эндоморфизм на E и a определено уникально. То есть $\forall (x, y) \in F(\bar{\mathbb{F}}_q)$:

$$(x^{q^2},\ y^{q^2}) - a(x^q, y^q) + q(x, y) = \mathcal{O}, \tag{1}$$

и $a \in \mathbb{Z}$ — уникально определено, что выражение (1) справедливо $\forall (x, y) \in E(\mathbb{F}_q)$.

Число a можно определить как

$$\boxed{\begin{array}{l} a = Tr\,(\varphi_q)_m \bmod m \\ q = \det\,(\varphi_q)_m \bmod m \end{array}} \quad \forall m :\ (m, q) = 1,$$

Обозначение «$(\varphi_q)_m$»:

φ_q действует на $E \Rightarrow$ на $E[m]$.

$E[m] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n \Rightarrow \forall$ элементы из $E[m]$ можно представить в виде $m_1\beta_1 + m_2\beta_2$, где $m_i \in \mathbb{Z}$,

$\{\beta_1, \beta_2\}$ — базис $\mathbb{Z}_n \oplus \mathbb{Z}_n$. тогда $\forall$ эндоморфизмов $d : E[n] \to E[n]$ действует на $E[m]$ через действие на $\{\beta_1, \beta_2\}$:

$$\begin{array}{l} d(\beta_1) = a\beta_1 + b\beta_2 \\ d(\beta_2) = c\beta_1 + d\beta_2 \end{array} \Rightarrow$$

$\Rightarrow$ для $\forall$ элементов из $E[m]$ действие d описывается матрицей

$$d_m = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

2.2 Неэффективные асимптотически алгоритмы подсчета точек

A. Кривые в подполе: кривая E задана над $\mathbb{F}_q$, мы можем выразить $\#E(\mathbb{F}_{q^n})$ через $\#E(\mathbb{F}_q)$.

Теорема 4. *Пусть* $\#E(\mathbb{F}_q) = q+1-a$. *Запишем* $X^2 - aX + q = (X-\alpha)(X-\beta)$. *Тогда*

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

Доказательство.
1. Покажем, что $\alpha^n + \beta^n \in \mathbb{Z}$ через рекуррентные соотношения.

Пусть $s_n = \alpha^n + \beta^n$, $s_0 = 2$, $s_1 = 0$. Тогда $s_{n+1} = as_n - qs_{n-1}$.

Доказательство. α — корень $x^2 - ax + q \Rightarrow$

$\alpha^2 - a\alpha + q = 0 \mid \cdot \alpha^{n-1}$.

$\alpha^{n+1} - a\alpha^n + q\alpha^{n-1} = 0$

Аналогично для β:

$\beta^{n+1} - a\beta^n + q\beta^{n-1} = 0$.

Сложим: $\underbrace{\alpha^{n+1} + \beta^{n+1}}_{s_{n+1}} = a(\underbrace{\alpha^n + \beta^n}_{s_n}) - q(\alpha^{n-1} + \beta^{n-1})$.

2. $f(x) = (x^n - \alpha^n)(x^n - \beta^n)$

$= x^{2n} - (\alpha^n + \beta^n)x^n + q^n \quad (\alpha\beta = q)$

Тогда $x^2 - ax + q = (x-\alpha)(x-\beta)$ делит $f(x)$ (т.к. α, β — корни $f(x)$).

$Q(x)$ — частное от деление. Подставим вместо x φ_q

$$(\varphi_q^n)^2 - (\alpha^n + \beta^n)\varphi_q^n + q^n = f(\varphi_q) = Q(\varphi_q)(\varphi_q^2 - a\varphi_q + q) = 0$$

По теореме 1 число: $(\alpha^n + \beta^n)$. А т.к. $\varphi_{q^n}^2 - a\varphi_{q^n} + q^n = 0$ определно единственным образом $\Rightarrow a = \alpha^n + \beta^n$ и $\alpha^n + \beta^n = q^n + 1 - \#E(\mathbb{F}_{q^n})$. □

B. Метод вычисления $\#E(\mathbb{F}_q)$ через обобщенный символ Лехандра $\left(\frac{\cdot}{\mathbb{F}_q}\right)$

Лемма 5. $E : y^2 = x^3 + ax + b$ *над* $\mathbb{F}_q$. *Тогда*

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

Доказательство. Для $x_0 \in \mathbb{F}_q$ существуют либо
2 точки на E (x, y) с $x = x_0$ т.ч. $x_0^3 + ax_0 + b \neq 0$ и является кв. вычетов в $\mathbb{F}_q$, либо

1 точка на E с $x = x_0$ т.ч. $x_0^3 + ax_0 + b = 0$, либо

0 точек на E с $x = x_0$ т.ч. $x_0^3 + ax_0 + b$ — не квадратичный вычет в $\mathbb{F}_q$

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

□

Сложность вычисления $\#E(\mathbb{F}_q)$ через квадратичные характеры: $\mathcal{O}(q \cdot \operatorname{poly}\log q)$, где $\operatorname{poly}\log q$ — вычисление $\left(\frac{\cdot}{\mathbb{F}_q}\right)$.