Осень 2019

Лекция №4 Алгоритм вычисления $E[n]$

Лектор: Елена Киршанова *Оформил Филипп Максимов*

E–эллиптическая кривая над полем $K = \mathbb{F}_q$, $\mathrm{char}(K) \neq 2, 3$

В Лекции # 3 мы определили

- точки n-крученая $E[n] = \left\{P \in E\left(\overline{K}\right) : nP = \mathcal{O}\right\}$
- $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \Rightarrow E[n]$ можно записать

$$E[n] = \{\mathcal{O},\ (x_1,\ y_1), ... (x_m,\ y_m)\} \text{ где } m = n^2 - 1$$

$$\Rightarrow \text{поле, где лежит } E[n], (\text{ расширение } K) \text{ можно записать}$$

$$K_{E,n} = K(x_1, y_1 \quad x_m y_m),$$

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

В этой лекции мы построим алгоритм вычисления $E[n]$, основанный на факторизации многочленов деления

- $\psi_m \in \mathbb{Z}[x, y, A, B]$ — многочлены деления, заданные рекуррентными соотношениями (см. лекцию 3)
- $\varphi_m = x \cdot \psi_m^2 - \psi_{m+1}\psi_{m-1}$
  $\omega_m = \dfrac{1}{4y}\left(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2\right)$
- Сложениие точки P с самой собой n раз:

$$nP = \left(\frac{\varphi_n(x)}{\psi_n^2(x)},\ \frac{\omega_n(x)}{\psi_n^3(x,y)}\right) \tag{1}$$

Лемма 1 (Доказательство см. в Serge Lang "Elliptic Curves Diophantine analysis"II 2.3)**.** *Многочлены φ_n и $\psi_n^2 \in K[x]$ — взаимно просты, если $\Delta(E) \neq \mathcal{O}$.*
Т.е. для E — эллиптической кривой, ϕ_n, ψ_n^2 — взаимно просты.

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

Доказательство. Из (1) x — координата P задается $\dfrac{\varphi_n(x)}{\psi_n^2(x)} \in K(x)$
(из Лекции 3: $\varphi_n(x),\ \psi_n^2(x) \in K[x]$ для фиксированной кривой E).

$\Rightarrow nP = \mathcal{O} \Leftrightarrow \dfrac{\varphi_n(x)}{\psi_n^2(x)}$ имеет полюс в x, Z — координата в проективных координатах.

Так как $\gcd(\varphi_n(x),\ \psi_n^2(x)) = 1 \Rightarrow \dfrac{\varphi_n(x)}{\psi_n^2(x)}$ имеет полюс в $\psi_n^2(x) = 0$ □

$$\psi_n^2(x) \in K[X] = n^2 x^{n^2-1} + \dots \text{ мономы меньших степеней (см. Wash. §3.2)}$$

Если n — нечетно, то и $\psi_n(x) \in K[X]$ (см. степень x в $\psi_n^2(x)$.

Факторизуем ψ_n над $\mathbb{F}_q[x]$.

$$\psi_n = f_1 ... f_r, f_i \text{ – неприводимые над } \mathbb{F}_q \tag{2}$$

Замечание 3. Все f_i — различные (т. е. все f_i встречаются в разложении с степенью 1)

- Всего $n^2 - 1$ точек $E[n] \neq \mathcal{O}$
- Для фиксированного $x_i \in \underbrace{\{x_1 \dots x_{n^2-s}\}}_{x-\text{координаты точек } n-\text{кручения}}$, существует две точки P, $P' \in E[n]$ с координатой x_i (т.к. $E: y^2 = x^3 + Ax + B$).
- Так как $\deg \psi_n(x) = \dfrac{n^2-1}{2} \Rightarrow \psi_n(x)$ имеет $\dfrac{n^2-1}{2}$ корней в $\overline{\mathbb{F}_q}$ и каждый корень кратности 1 (иначе мы имели бы меньше чем $n^2 - 1$ точек $\neq 0$ в $E[n]$).

Покажем, что мы можем определить $d = [K_{E,n} : K] \neq 0$ фактора 2 из разложения 2.

Теорема 4. *Пусть n — простое > 2, $K = \mathbb{F}_q$, $n \neq char(K)$.*

$d_i = \deg f_i$ *в разложении* (2).

$\ell = \operatorname{lcm}(\{d_i\}_{i=1}^m)$

$K'_{E,n} = K(x_1 \dots x_{n^2-1})$, 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.

Доказательство. Из следствия 2: x_i — корни $\psi_n \Rightarrow K'_{E,n}$ — поле разложения ψ_n над K

$\Rightarrow [K'_{E,n} : K] = \operatorname{lcm}(d_i)$.

(Поле разложения f_i над $\mathbb{F}_q$: $\mathbb{F}_{q^{d_i}}$.
Поле разложения f над $\mathbb{F}_q$ — наименьшие расширение $\mathbb{F}_q$, содержащие все $\mathbb{F}_{q^{d_i}}$.
$\mathbb{F}_{q^a} \subset \mathbb{F}_{q^b} \Leftrightarrow a|b$)

Для второй части теоремы, положим $K_{E,n} \neq K'_{E,n}$

$\Rightarrow \exists\, x_i : y_i = \sqrt{x_i^3 + Ax_i + B} \notin K'_{E,n} = \mathbb{F}_{q^\ell}$

$\Rightarrow K'_{E,n}(y_i) = \mathbb{F}_{q^{2\ell}}$ и $\forall x \in \mathbb{F}_{q^\ell}$ имеет квадратный корень в $\mathbb{F}_{q^\ell}$

$\Rightarrow \forall y_i \in \mathbb{F}_{q^{2\ell}}$.

$d = [K_{E,n} : \bar{K}'_{E,n}] \cdot [K'_{E,n} : K]$. $\square$

Значит, чтобы определить $d = \ell$, нужно показать что

$\forall x_i \in \bar{K}$ — корень ψ_n^2, $y_i = \sqrt{x_i^3 + Ax_i + b} \in \mathbb{F}_{q^\ell}$.

Если существует хотя бы один x_j т. ч. $y_j \notin \mathbb{F}_{q^\ell}$, делаем вывод, что $d = 2\ell$.

Следующее определение обобщает символ Лежандра.

Определение 5. $K = \mathbb{F}_q$, $x \in K$. Квадратичный характер $(\frac{\cdot}{K})$ — это

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

Таким образом, чтобы определить $d = \ell$ или $d = 2\ell$, необходимо вычислить

$$\left(\frac{x_i^3 + Ax_i + B}{\mathbb{F}_{q^\ell}}\right)$$

$\forall x_i$ — корни ψ_n^2.

Так как x_i — корень какого-то f_i из (2), $d_1 = \deg f_i$, то
$y_i^2 = x_i^3 + Ax_i + b \in \mathbb{F}_{q^{d_i}}$,
т.к. $f_i -$ min многочлен x_i над K, $d_i | \ell \Rightarrow x_i \in \mathbb{F}_{q^{d_i}}$ – кв. в $\mathbb{F}_{q^\ell} \Rightarrow y_i \in \mathbb{F}_{q^\ell}$,
т.е. x_i — корень f_i, т.ч. $2d_i | \ell$, то $y_i \in \mathbb{F}_{q^\ell}$. Т.е. нам достаточно считать квадратные характеры тех x_i, которые являются корнями f_i с $\deg f_i$, т.ч. $2d_i \nmid \ell$.

Лемма 6. *Если $K = \mathbb{F}_q$ и $d = [K_{E,n} : K]$, то $q^d \equiv 1 \bmod n$. В частности,* $\mathrm{ord}(q, n) | c$

Лемма 7 (A.L. van Tuyl "The shield of N-Torsion Points of an Elliptic Curve over a Finite Field")**.** *Пусть f_i — неприводимый многочлен в разложении ψ_n (2), т.ч. $2d_i | \ell$, $d_i = \deg f$. Положим*

$$d^* = \mathrm{lcm}(\mathrm{ord}(q, n),\ d_i),$$
$$= \left(\frac{x_i^3 + Ax + B}{\mathbb{F}_{q^{d_i}}}\right), \text{ где } f(x_i) = \mathcal{O}.$$

Тогда

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

Эта лемма позволяет рассмотреть лишь один f_i (и его корень x_i) для определения d.

Алгоритм вычисления d – степени расширения $[K_{E,n} : K]$

Вход: $n \geqslant 3$ – нечётное, q, A, B ($E: \ y^2 = x^3 + Ax + B, \ \ A, B \in \mathbb{F}_q$)

Выход: d.

1. Построить $\psi_n \in \mathbb{F}_q[x]$
2. Факторизовать $\psi_n = f_1 \dots f_r$ над $\mathbb{F}_q[x]$
3. $\ell := \mathrm{lcm}(\{\deg f\}_{i=1,5})$
4. Выбрать f_i т.ч. $2 \cdot \deg f_i \not| \, l$
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 $c_i = -1$:
   return $d = 2\ell$
7. $d^* = (\mathrm{ord}(q, n), d_i)$
   if $d^* = \ell$ or $\ell = n \cdot d^*$:
   return $d = \ell$
   return $d = 2\ell$

Оценка сложности

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

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

Замечание 8. Алгоритм может быть адаптирован для вычисления самой группы точек n-кручения $E[n]$, если $\forall x_i$ – корень f_i, вычислить соответствующие y_i:
для $n = 2, E[n]$ вычисляется разложением многочлена $x^3 + Ax + B$ (см. лекцию # 3)
для $n = 1, E[n] = \{\mathcal{O}\}$.