

Эллиптические кривые

Лекция 6. Алгоритмы подсчета \mathbb{F}_q -рациональных точек кривой. Часть II

Семён Новосёлов

БФУ им. И. Канта

2021



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 $f : (P, e) \mapsto (P + Q_{h(P)}, K + \alpha_{h(P)})$;
- 4 $(P_1, K_1) = (P, 1)$;
- 5 $(P_2, K_2) = f(P_1, K_1)$;
- 6 **while** $P_1 \neq P_2$ **do**:
- 7 $(P_1, K_1) = f(P_1, K_1)$;
- 8 $(P_2, K_2) = f(f(P_2, K_2))$;
- 9 **return** $M = |K_1 - K_2|$.

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

Алгоритм Схоофа¹

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

Имеем:

- $|E(\mathbb{F}_q)| = q + 1 - t$, где t – след эндоморфизма Фробениуса, $|t| \leq 2\sqrt{q}$.

Идея: найти $t \pmod{\ell_i}$ для малых простых чисел ℓ_1, \dots, ℓ_n и восстановить t по КТО и неравенству для следа t .

- $|t| \leq 2\sqrt{q} \implies \prod_{i=1}^n \ell_i > 4\sqrt{q} \implies \ell_n = O(\log q)$

¹(гол.) Schoof = Схооф, в рус. лит. больше известен как Шуф.

Число точек по модулю $\ell = 2$

- $\#E(\mathbb{F}_q) - \text{чётно} \iff E(\mathbb{F}_q)$ содержит точку ($\neq \mathcal{O}$) порядка 2
- точка P порядка 2 имеет $y_P = 0 \iff x_P^3 + ax_P + b = 0$ в \mathbb{F}_q
- Проверка наличия точек порядка 2:
 $\gcd(x^q - x, x^3 + ax + b) \neq 1$ в $\mathbb{F}_q[x]$
 $\implies O(\log^3 q)$, быстрое возведение в степень в $\mathbb{F}_q[x]/(x^3 + ax + b)$

Число точек по модулю $\ell > 2$

$$E[\ell] = \{P \in E(\overline{\mathbb{F}}_q) \mid [\ell]P = \mathcal{O}\} \simeq \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$$

- $\varphi_q : (x, y) \mapsto (x^q, y^q)$ – эндоморфизм Фробениуса,

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

или

$$(x^{q^2}, y^{q^2}) - [t](x^q, y^q) + [q](x, y) = P_\infty.$$

- для ограничения φ_q на $E[\ell]$ имеем:

$$(x^{q^2}, y^{q^2}) - [t'](x^q, y^q) + [q'](x, y) = P_\infty,$$

где $t', q' \in \{0, \dots, \ell - 1\}$ и $t = t' \pmod{\ell}$, $q = q' \pmod{\ell}$.

$$(x^{q^2}, y^{q^2}) - [t'](x^q, y^q) + [q'](x, y) = P_\infty \quad (1)$$

- $\psi_\ell(x) \in \mathbb{F}_q[x]$, ℓ -многочлен деления (может быть эффективно вычислен по рек. формуле)
- $P = (x_P, y_P) \in E[\ell] \iff \psi_\ell(x_P) = 0$
- из (1) получаем

$$(x^{q^2}, y^{q^2}) + [q'](x, y) = [t'](x^q, y^q)$$

по модулю $\psi_\ell(x)$ и $E(x, y) = y^2 - x^3 - ax - b$

$$(x^{q^2}, y^{q^2}) + [q'](x, y) = [t'](x^q, y^q) \pmod{(\psi_\ell(x), E(x, y))} \quad (2)$$

- $x^q, y^q, x^{q^2}, y^{q^2} \pmod{\psi_\ell} \implies$ быстрое возведение в степень
- $[q'](x, y)$ и $[t'](x^q, y^q) \pmod{\psi_\ell(x)} \implies$ многочлены q' и t' -деления

Значение $t' = t \pmod{\ell}$ и соответственно $\#E(\mathbb{F}_q) \pmod{\ell}$ находим перебором возможных вариантов для (t', q') пока не выполнится (2).

Алгоритм Схоофа

Вход: E/\mathbb{F}_q

Выход: $\#E(\mathbb{F}_q)$

- 1 $M = 2, \ell = 3, S = \{(t \bmod 2, 2)\}$
- 2 **while** $M < 4\sqrt{q}$ **do:**
- 3 **for** $t' = 0, \dots, \ell - 1$ **do:**
- 4 **if** $\varphi_q^2(P) + [q']P = [t']\varphi_q(P) \pmod{(\psi_\ell, E)}$ **do:**
 break
- 5 $S = S \cup \{(t', \ell)\}$
- 6 $M = M \cdot \ell$
- 7 $\ell = \text{next_prime}(\ell)$
- 8 найти t по КТО, используя S
- 9 **return** $q + 1 - t$

Анализ сложности

Оценка размера ℓ .

$$\ell = O(\log q)$$



1. для однозначного восстановления t по $M = \prod_{i=1}^n \ell_i$,
необх. $M > 4\sqrt{q}$.
2. $M = p_n\#$ – праймориал $\implies M = n^{(1+o(1))n}$.

Объединяя пункты 1 и 2 получаем: $n \log n = O(\log q) \implies$
 $n = O\left(\frac{\log q}{\log \log q}\right)$.

$\ell = \ell_n = O(n \log n)$ (теорема о распределении простых чисел) $\implies \ell = O(\log q)$.



Оценка сложности операций.

Базовые операции:²

- Редукция многочлена степени d по модулю ψ_ℓ и E :
 $\tilde{O}(d^2 + \deg \psi_\ell^2)$ операций в \mathbb{F}_q .
 $\deg \psi = \frac{\ell^2-1}{2} \implies \tilde{O}(d^2 + \ell^4)$.
- Умножение в кольце $\mathbb{F}_q[x, y]/(\psi_\ell, E)$:
 $\tilde{O}(\ell^4)$ операций в \mathbb{F}_q .

²Hoeven J.v.d., Larrieu R. - Fast reduction of bivariate polynomials with respect to sufficiently regular Gröbner bases. 2018.

Проверка условия $\varphi_q^2(P) + [q']P = [t']\varphi_q(P) \pmod{(\psi_\ell, E)}$:

- $(x^q, y^q), (x^{q^2}, y^{q^2}) \pmod{\psi_\ell, E} \implies$ быстрое возведение в степени q и $q^2 \implies O(\log q)$ умножений в $\mathbb{F}_q[x, y]/(\psi_\ell, E) \implies \tilde{O}(\ell^4 \log q)$ операций в \mathbb{F}_q .
- $[q']P \implies$ рекур. формулы для многочленов деления
- $[t'](x^q, y^q) \pmod{\psi_\ell, E}$:
 x^q и $y^q \pmod{\psi_\ell, E}$ – многочлены степени $< \ell^2$, уже известны, $t' < \ell \implies$ используя рек. формулы для мн. деления имеем макс. ℓ операций умножения + редукции многочленов степени $< 2\ell^2$ в $\mathbb{F}_q[x, y]/(\psi_\ell, E) \implies \tilde{O}(\ell^5)$ операций в \mathbb{F}_q .

Перебирая t' нужно проверять условие макс. ℓ раз \implies

$\tilde{O}(\ell^5 \log q + \ell^6) = \tilde{O}(\ell^5 \log q)$ операций в \mathbb{F}_q .

Всего в алгоритме делается $n = O\left(\frac{\log q}{\log \log q}\right)$ итераций.

Итого: $O\left(\frac{\log q}{\log \log q}\right) \cdot \tilde{O}(\ell^5 \log q) = \tilde{O}(\log^7 q)$ операций в \mathbb{F}_q
или $\tilde{O}(\log^8 q)$ битовых операций.

Алгоритм Схоофа: дальнейшие улучшения

Schoof-Elkies-Atkin (SEA):

- замена многочленов деления на многочлены g_ℓ , задающие изогении (степени: $O(\ell^2) \implies O(\ell)$)
- факторизация модулярных многочленов для нахождения ядер изогений (нулей g_ℓ)
- эвристическая сложность: $O(\log^4 q)$

Литература

- ☰ I. Blake и др. *Elliptic curves in cryptography*. 1999.
- ☰ H. Cohen и др. *Handbook of elliptic and hyperelliptic curve cryptography*. 2005.
- ☰ R. Schoof. *Elliptic curves over finite fields and the computation of square roots mod p* . 1985.
- ☰ L. C. Washington. *Elliptic curves: number theory and cryptography*. 2008.

Контакты

snovoselov@kantiana.ru