# Эллиптические кривые

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

Семён Новосёлов
на основе курса Елены Киршановой

БФУ им. И. Канта

2020

IKBFU

# Алгоритм Схоофа[1]

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

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

**Идея:** найти $t \pmod{\ell_i}$ для малых простых чисел $\ell_1, ..., \ell_n$ и восстановить $t$ по КТО.

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

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

# Число точек по модулю $\ell = 2$

- $\#E(\mathbb{F}_q)$ – 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 $\mathbb{F}_q[x]$

  $\Longrightarrow$ $O(\log^3 q)$, 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 $\varphi_q$ на $E[\ell]$ имеем:

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

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

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

- $\psi_\ell(x) \in \mathbb{F}_q[x]$, $\ell$-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 $E(x, y) = y^2 - x^3 - ax - b$

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

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

Значение $t' = t \bmod \ell$ и соответственно $\#E(\mathbb{F}_q) \bmod \ell$ 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** $t' = 0, ..., \ell - 1$ **do:**
4. **if** $\varphi_q^2(P) + [q']P = [t']\varphi_q(P)$ **do: break**
5. $S = S \cup \{(t', \ell)\}$
6. $M = M \cdot \ell$
7. $\ell = \mathrm{next\_prime}(\ell)$
8. найти $t$ по КТО используя $S$
9. **return** $q + 1 - t$

# Анализ сложности

- $\ell = O(\log q)$
- $(x^q, y^q), (x^{q^2}, y^{q^2}) \pmod{\psi_\ell} \Longrightarrow$ быстрое возведение в степень, $\deg \psi_\ell = \frac{\ell^2-1}{2} = O(\ell^2) \Longrightarrow O((\log q)(\ell^2 \log q)^2)$
- $[t'](x^q, y^q) \pmod{\psi_\ell(x)} \Longrightarrow$ макс. $\ell$ раз, $O(\ell(\ell^2 \log q)^2)$

**Итого:** $O(\log q \cdot (\log q(\ell^2 \log q)^2 + \ell(\ell^2 \log q)^2)) = O(\log^8 q)$

# Алгоритм Схоофа: дальнейшие улучшения

**Schoof-Elkies-Atkin (SEA)**:

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

# 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