Эллиптические кривые

Лекция 7. Алгоритм факторизации на эллиптических кривых

Семён Новосёлов

БФУ им. И. Канта

2021

Мотивация

- Метод используется на практике для нахождения малых множителей числа N, перед запуском более эффективных на больших числах методов (но и более громоздких)

$(p-1)$-метод Полларда

Алгоритм ECM – обобщение метода $(p-1)$-метода факторизации Полларда.

Малая теорема Ферма

p – простое, $a \in \mathbb{Z}$ и $p \nmid a \implies a^{p-1} \equiv 1 \pmod{p}$.

Число наз-ся **B-гладким**, если все его простые множители $\leq B$.

Пусть $N = pq$, где p, q – простые и

- $p - 1$ факторизуется на **малые** простые
- $q - 1$ **не** факторизуется на **малые** простые

Точнее:

$p - 1 = \prod p_i^{e_i},\ p_i \leq B_1, p_i^{e_i} \leq B_2$, т. е. $p - 1$ явл-ся B_1**-гладким**.

Идея метода:

- (из теор. Ферма): $\forall a \in \mathbb{Z}_N^\times$ и $\forall k$ – кратного $p - 1$:

$$a^k = (a^l)^{p-1} \equiv 1 \bmod p$$

- $a^k \not\equiv 1 \bmod q \implies \gcd(N, a^k - 1) = p$

Алгоритм

Вход: $N = p \cdot q$ и границы B_1, B_2.
Выход: $p, q = \frac{N}{p}$, или «делители не найдены».

1. $a \leftarrow \mathbb{Z}_N^\times$
2. **for** всех простых $p_i \leqslant B_1$:
   $a \leftarrow a^{p_i^{e_i}} \bmod N$, где e_i – макс.: $p_i^{e_i} \leqslant B_2$.
3. **if** $\gcd(a-1, N) \notin \{1, N\}$
   return $\gcd(a-1, N), \frac{N}{\gcd(a-1,N)}$.
   else:
   return «делители не найдены».

Корректность

Лемма
Пусть $N = p \cdot q$, $B_1, B_2 \in \mathbb{N}$, т.ч. $(p-1)$ – B_i-гладкое и $p - 1 = \prod p_i^{e_i}$, $p_i^{e_i} \leqslant B_2$. А $(q-1)$ — не B_i-гладкое.
Тогда алгоритм $(p-1)$ Полларда находит p за время $O(B_1 \lg^3 N)$ с вероятностью $1 - \frac{1}{B_1}$.

$\triangleleft$ Положим $K = \prod\limits_{p_i \leq B_1} p_i^{e_i}$.

Т. к. $(q-1)$ – не B_1-гладкое, $\exists r$ – простое, $r > B_1 : r \mid q - 1$.
Если $r \mid \operatorname{ord}_{\mathbb{Z}_q^\times}(a)$, то $\operatorname{ord}_{\mathbb{Z}_q^\times}(a) \nmid K \implies a^K \not\equiv 1 \mod q$.
С другой стороны K – кратно $p - 1 \implies a^K \equiv 1 \mod p$ и $\gcd(a^K - 1, N) = p$.
Так как $\operatorname{ord}_{\mathbb{Z}_q^\times}(a)$ – целое число, то вероятность того, что $\operatorname{ord}_{\mathbb{Z}_q^\times}(a) \nmid K$ равна $1 - \frac{1}{K} = 1 - \frac{1}{B_1}$. $\triangleright$

Сложность

Существует не более B_1 простых p_i, таких что $p_i < B_1$ (точнее: $\exists \sim \dfrac{B_1}{\lg(B_1)}$ по теореме о распределении простых чисел.)

- Шаг 2: $O(\lg^3 N)$
- Шаг 3: $O(\lg^2 N)$

Итого: $O(B_1 \cdot \lg^3 N)$.

Замечание. Вероятность успеха и сложность алгоритма зависят от $|\mathbb{Z}_p^\times| = p - 1$:

- $\frac{p-1}{2}$ – простое $\Rightarrow B_1 \approx p \Rightarrow$ сложность $O(p \cdot \lg^3 N)$ – не лучше простого перебора.

Решение: использовать эллиптические кривые, т.к. $\#E(\mathbb{Z}_p) \in [p + 1 - 2\sqrt{p},\ p + 1 + 2\sqrt{p}]$, и в этом интервале $\exists$ много гладких чисел.

Метод факторизации на эллиптических кривых (ECM)

$$E : y^2 = x^3 + ax + b \bmod N$$

- $E(\mathbb{Z}_N) \simeq E(\mathbb{Z}_p) \times E(\mathbb{Z}_q)$.
- Т.к. кольцо $\mathbb{Z}_N$ содержит делители 0 групповой закон корректно определять в проективных координатах.
- **Идея алгоритма:** использовать ошибки «деление на 0» для нахождения множителей N при работе в аффинных координатах.

Нахождение множителя из группового закона

Вход: $P, Q \in E(\mathbb{Z}_N) - \{\mathcal{O}\}$

Выход: либо $P + Q = (x_3, y_3)$, либо $d | N$.

1. **if** $x_1 \equiv x_2 \mod N$ и $y_1 = -y_2 \mod N$
   return $\mathcal{O}$
2. $d = \gcd(x_1 - x_2, N)$
   if $d \notin \{1, N\}$: **return** d
3. **if** $x_1 \equiv x_2 \mod N$
   $d = \gcd(y_1 + y_2,\ N)$
   if $d > 1$: **return** d
4. $$\alpha = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & x_1 \neq x_2 \\ \frac{3x_1^2 + a}{y_1 + y_2}, & x_1 = x_2. \end{cases}$$
   $\beta = y_1 - \alpha x_1$
5. $x_3 = \alpha^2 - x_1 - x_2 \mod N$
   $x_3 = -(\alpha x_3 + \beta) \mod N$
   return (x_3, y_3)

Алгоритм факторизации ECM

Вход: $N = p \cdot q$, границы B_1, B_2
Выход: p, q или «делители не найдены»

1. Выбрать $(a, x, y) \leftarrow \mathbb{Z}_N \times \mathbb{Z}_N \times \mathbb{Z}_N$,
   $b = y^2 - x^3 - ax \bmod N$
2. **if** $\gcd(4a^3 + 27b^2,\ N) = \begin{cases} 1, & \text{положим} \quad P = (x, y) \\ N, & \text{идем на шаг 1} \\ \text{иное, вернуть } p, q \end{cases}$
3. **for** всех простых $p_i < B_1$ и $e_i : p_i^{e_i} < B_2$:
   $P = [p_i^{e_i}]P$ на $E : y^2 = x^3 + ax + b$
   при ошибке «деление на 0» вернуть делитель N.
4. перейти к Шагу 1 или вернуть «делитель не найден».

Корректность

Лемма

Пусть $N = p \cdot q$, $E(\mathbb{Z}_N)$ – эллиптическая кривая, т. ч. $|E(\mathbb{F}_p)|$ – B_1-гладкое и $|E(\mathbb{F}_q)|$ – не B_1-гладкое. Тогда алгоритм ECM возвращает p, q за время $O(B_1 \lg^3 N)$ с вероятностью $\geqslant 1 - \frac{1}{B_1}$.

$\triangleleft$ Пусть $K = \prod\limits_{p_i \le B_1} p_i^{e_i}$.

Т. к. $\#E(\mathbb{F}_q)$ – не B_1-гладкое, то $\exists r > B_1$ т. ч. $r \mid \#E(\mathbb{F}_q)$.
Имеем: $r \mid \mathrm{ord}_{E(\mathbb{F}_q)}(P) \implies K \cdot P \ne \mathcal{O}$ на $E(\mathbb{F}_q)$.

С другой стороны: $\#E(\mathbb{F}_p) \mid K \implies K \cdot P = \mathcal{O}$ на $E(\mathbb{F}_q)$.
Вычисляем $K \cdot P$ на $E(\mathbb{Z}_N) \implies$ получаем $P' + Q' = \mathcal{O}$ на $E(\mathbb{F}_p)$ и $P' + Q' \ne \mathcal{O}$ на $E(\mathbb{F}_q) \implies$ Алгоритм вернёт (p, q).

Сложность и вероятность: аналогично $(p - 1)$ методу Полларда. $\triangleright$

Замечание. Баланс выбора B_1:

- малое $B_1 \Rightarrow$ быстрый алгоритм, малая вероятность успеха
- большое $B_1 \Rightarrow$ медленный алгоритм, большая вероятность успеха.

Оптимально: $B_1 \approx L_p[\frac{1}{2}, \ \frac{1}{\sqrt{2}}] = e^{\frac{1}{\sqrt{2}}(\log p)^{\frac{1}{2}}(\log\log p)^{\frac{1}{2}}} \Rightarrow$ время работы алгоритма: $L_p[\frac{1}{2}, \ \frac{1}{\sqrt{2}}]$ в предположении о гладкости чисел в интервале $[p + 1 - 2\sqrt{p}, \ p + 1 + 2\sqrt{p}]$.

- ECM – лучший на сегодня алгоритм для нахождения делителей < 100 бит.

Литература

- I. Blake и др. *Elliptic curves in cryptography*. 1999.
- H. Cohen и др. *Handbook of elliptic and hyperelliptic curve cryptography*. 2005.
- H. W. Lenstra Jr. *Factoring integers with elliptic curves*. 1987.
- L. C. Washington. *Elliptic curves: number theory and cryptography*. 2008.

Контакты

snovoselov@kantiana.ru