Осень 2019

Лекция №7 — 1.11.19

Лектор: Елена Киршанова *Оформил Филипп Максимов*

1 Алгоритм факторизации на эллиптических кривых

1.1 (p-1)-метод Полларда

Не умалаяя общности, $N = pq$ (легко обобщается на случай нескольких простых множителей)
$p - 1$ факторизуется на «малые» простые
$q - 1$ <u>не</u> факторизуется на «малые» простые

Точнее, $p - 1 = \prod p_i^{e_i},\ p_i \leq B_1, p_i^{e_i} \leq B_2$ (такие p называются "B_1-гладкими")

<u>Идея метода:</u>

- $\forall a \in \mathbb{Z}_n^*$ и $\forall K$ - кратное $p - 1$:
$$a^k = (a^l)^{p-1} \equiv 1 \ mod\ p$$
- (Теорема Ферма) Если $a^k \not\equiv 1\ mod\ q$, то $GCD(N, a^K - 1) = p$

1.1.1 Алгоритм

Вход: $N = p \cdot q$

Выход: $p, q = \frac{N}{p}$, или «делители не найдены».

1. Выбрать B_1, B_2 — границы.
$$a \xleftarrow{\$} \mathbb{Z}_N^*$$
2. Для всех простых $p_i \leqslant B_1$:
   $a \leftarrow a^{p_i^{e_i}}$ mod N, где e_i — макс., удовлетворяющее $p_i^{e_i} \leqslant B_2$.
3. Если $\gcd(a-1, N) \notin \{1, N\}$
   вернуть $\gcd(a-1, N), \quad \dfrac{N}{\gcd(a-1,\ N)}$.

   иначе

   вернуть "делители не найдены".

Корректность

Лемма 1. *Пусть $N = p \cdot q$, $B_1, B_2 \in \mathbb{N}$, т.ч. $(p-1)$ — B_i-гладкое и*

$p - 1 = \Pi p_i^{e_i}$, $\varphi_i^{e_i} \leqslant B_2$. А $(q-1)$ — не B_i-гладкое.

Тогда алгоритм $(p-1)$ Полларда находит p за время $\mathcal{O}(B_1 \lg^3 N)$ с вероятностью $1 - \frac{1}{B_1}$.

Доказательство. Положим $K = \prod\limits_{\substack{p_i \leqslant B_1 \\ p_i - \text{простые}}} p_i^{e_i}$

Так как $(q-1)$ — не B_1-гладкое $\exists$ r — простое, $r > B_1 : r | q-1$.

Если $r | \operatorname{ord}_{\mathbb{Z}_q^*}(a)$, то $\operatorname{ord}_{\mathbb{Z}_q^*}(a) \not| K \Rightarrow a^K \neq 1 \bmod q$.

С другой стороны, k — кратно $p - 1 \Rightarrow a^K = 1 \bmod p$ и $\gcd(a^k - 1, N) = p$.

Т.е. необходимо показать, что $r | \operatorname{ord}_{\mathbb{Z}_q^*}(a)$ с большой вероятностью для $a \xleftarrow{\$} \mathbb{Z}_N^*$.

$\mathbb{Z}_q^* = \{\alpha^1 \ldots \alpha^{q-1}\}$ — циклическая группа, т.е. $a \bmod q = \alpha^i$ для $i \in (1, q-1)$.

Кроме того, $\operatorname{ord}_{\mathbb{Z}_q^N}(\alpha^i) = \dfrac{q-1}{\gcd(i,\ q-1)}$ $\square$

Лемма 2. *Покажем, что* $\operatorname{ord}_{\mathbb{Z}_q^*}(\alpha') = \dfrac{q-1}{\gcd(i,\ q-1)}$*; Пусть* $t = \operatorname{ord}(\alpha')$

$$\left.\begin{array}{l} (\alpha^i)^t = 1 \\ \operatorname{ord}(\alpha)^0 = q-1 \end{array}\right\} \Leftrightarrow (q-1) | i \cdot t;$$

Доказательство. Положим $(q-1)m = i \cdot t$ $(m \in \mathbb{Z})$.

$$\begin{array}{l} \gcd(q-1,\ i) |\ q-1,\ \text{положим } (q-1) = q' \cdot \gcd(q-1, i) \\ \gcd(q-1,\ i) |\ i,\ \text{положим } i = i' \cdot \gcd(q-1, i) \end{array} \Rightarrow \gcd(q', i') = 1.$$

Заметим, что $q' = \dfrac{q-1}{\gcd(q-1, i)}$; покажем, что $t = q'$.

$(q-1)m = i \cdot t$

$q' \cdot \gcd(q-1, i) \cdot m = i' \cdot \gcd(q-1, i) \cdot t$

$q' \cdot m = i' \cdot t \ \Rightarrow\ q' | i' \cdot t$, т.к. $\gcd(q', i') = 1$, $q' | t \ \Rightarrow\ q' \leqslant t$.

Покажем обратное неравенство:

$$(\alpha^i)^{q_i} = \alpha^i \cdot \frac{q-1}{\gcd(i, q-1)} = \alpha^{(q-1) \cdot i'} = (1)^{i'} = 1 \bmod q$$

$$\Rightarrow \text{Вывод: } \frac{t \leqslant q'}{t = q'}$$

$$r \not| \operatorname{ord}(\alpha^i) \Leftrightarrow r|i$$

т.к. i — случайное число $[1 \dots q-1]$, i — кратно r с вероятностью $\dfrac{q}{r} \cdot \dfrac{1}{q} = \dfrac{1}{r} \Rightarrow r|\operatorname{ord}(\alpha^i)$ с вероятностью $1 - \frac{1}{r} > 1 - \frac{1}{B_1}$ $(r > B_1)$.

$\square$

<u>Сложность</u> Существует не более B_1 простых p_i, таких что $p_i < B_1$ (точнее $\exists \sim \dfrac{B_1}{\lg(B_1)}$)

Шаг 2: $\mathcal{O}(\lg^3 N)$

Шаг 3: $\mathcal{O}(\lg^2 N)$

$\Rightarrow \mathcal{O}(B_1 \cdot \lg^3 N)$.

<u>Замечание</u>. Вероятность успеха и сложность алгоритма зависят от $|\mathbb{Z}_p^*| = p - 1$: Если $\frac{p-1}{2}$ — простое (т.е. $p-1 = 2 \cdot p'$) $\Rightarrow B_1 \approx p \Rightarrow$ сложность $\mathcal{O}(p \cdot \lg^3 N)$ — не лучше наивного брутфорса.

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 существует много гладких чисел.

1.2 Эллиптические кривые $\bmod N$

$$\begin{aligned} &E(\mathbb{Z}_N) = \big\{(x, y) \in \mathbb{Z}_N \times \mathbb{Z}_N :\ y^2 = x^3 + ax + b \bmod N \\ &\text{для } \gcd(\mathbb{N},\ 4a^3 + 27b^2) = 1\big\} \cup \{0\} \end{aligned}$$

<u>Важно!</u> Точки на $E(\mathbb{Z}_N)$ не образуют аддитивную группу!

(Пример: $E:\ y^2 = x^3 + 1 \bmod 55,\ P = (10, 11) \in E$,
для вычисления $2P$, необходимо найти $(2y)^{-1} = 2 \cdot 11)^{-1} \bmod 55$, но $\gcd(22, 25) = 1$
$\Rightarrow$ обратного $\nexists$).

1.2.1 Закон "+" на $E(\mathbb{Z}_N)$:

<u>Вход</u> $P, Q \in E(\mathbb{Z}_N)$ $(P, Q \neq \mathcal{O})$;

<u>Выход</u> либо $P + Q = (x_3, y_3)$,

либо $d|N$.

1. Если $x_1 \equiv x_2 \bmod N$ и $y_1 = -y_2 \bmod N$

   Вернуть $\mathcal{O}$

2. $d = \gcd(x_1 - x_2, N)$

   Если $d \notin \{1, N\}$

   Вернуть d

3. Если $x_1 \equiv x_2 \bmod N$

   $d = \gcd(y_1 + y_2,\ N)$

   Если $d > 1$

   Вернуть d

4. $$\alpha = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & x_1 \neq x_2 \\ \dfrac{3x_1^2 + a}{y_1 + y_2}, & x_1 = x_2 \end{cases}$$
$$\beta = y_1 - \alpha x_1$$

5. $x_3 = \alpha^2 - x_1 - x_2 \bmod N$

   $x_3 = -(\alpha x_3 + \beta) \bmod N$

   Вернуть (x_3, y_3)

Теорема 3. *Пусть* $P, Q \in E(\mathbb{Z}_N)$.

Тогда $P + Q$ *на* $E(\mathbb{Z}_N)$ *либо идентично сложению на* $E(\mathbb{F}_p), E(\mathbb{F}_q)$, *либо дает делитель* N.

Доказательство. $P = (x_1, y_1), Q(x_2, y_2)$.

Случай 1. $P + Q = \mathcal{O}$ на $E(\mathbb{F}_p)$ и на $E(\mathbb{F}_q)$

$$\Rightarrow \left\{ \begin{array}{l} \left| \begin{array}{l} x \equiv x_1 \\ y_1 \equiv y_2 \end{array} \right. \bmod p \\ \left| \begin{array}{l} x \equiv x_1 \\ y_1 \equiv y_2 \end{array} \right. \bmod q \end{array} \right\} \Rightarrow \begin{array}{l} x = x_1 \\ x = y_1 \end{array} \bmod N \Rightarrow$$
$$\Rightarrow P + Q = \mathcal{O} \text{ на } E(\mathbb{F}_N)$$

Случай 2. $P + Q \neq \mathcal{O}$ на $E(\mathbb{F}_p)$, $E(\mathbb{F}_q)$.

2.1. $x_1 \not\equiv x_2 \bmod p$ и $x_1 \not\equiv x_2 \bmod q$
$\Rightarrow$ формулы сложения $E(\mathbb{F}_p), E(\mathbb{F}_q)$, $E(N)$ идентичны.

2.2. $x_1 \not\equiv x_2 \bmod p$, $x_1 \equiv x_2 \bmod q \Rightarrow$

Шаг 2: $\gcd(x_1 - x_2, N) = q$

(Аналогично $x_1 = x_2 \bmod p$, $x_1 \neq x_2 \bmod q$)

2.3. $\begin{cases} x_1 = x_2 \bmod N \\ y_1 \neq -y_2 \bmod p \end{cases} \Rightarrow$ уравнение $y^2 = x_1^3 + ax_1 + b$ (для y) имеет в точности 2 решения.

$y_{1,2} = \pm y \bmod p$, т.ч. $y_1 \neq -y_2 \bmod p \Leftrightarrow y_1 = y_2 \bmod p$.

В таком случае $y_1 + y_2 = 2y_1 \bmod p$, формулы сложения идентичны (то же самое при $q \leftrightarrow p$). □

Следствие 4. *Пусть $P + Q = \mathcal{O}$ на $E(\mathbb{F}_p)$ и $P + Q \neq \mathcal{O}$ на $E(\mathbb{F}_q)$. Тогда $P + Q$ на $E(\mathbb{F}_N)$ даст делитель N.*

Доказательство. $P + Q = \mathcal{O}$ на $E(\mathbb{F}_p) \Leftrightarrow \begin{cases} x_1 \equiv x_2 \bmod p \\ y_1 \equiv y_2 \bmod p \end{cases}$

$P + Q \neq \mathcal{O}$ на $E(\mathbb{F}_q) \Leftrightarrow \left[\begin{array}{l} x_1 \not\equiv x_2 \bmod q \Rightarrow \gcd(x_1 - x_2, N) = p \,(\text{Шаг } 2) \\ y_1 \not\equiv -y_2 \bmod q \Rightarrow \gcd(y_1 + y_2, N) = q. \end{array} \right.$ □

Алгоритм факторизации ECM

Вход: $N = p \cdot q \quad (p \sim q)$

Выход: p, q или "делители не найдены"

1. Выберем границы B_1, B_2
2. Выберем $(a, x, y) \leftarrow \mathbb{Z}_N \times \mathbb{Z}_N \times \mathbb{Z}_N$

   $b = y^2 - x^3 - ax \bmod N$ // Таким образом, мы выбираем точку с координатами (x, y) на кривой $y^2 = x^3 + ax + b$.
3. Если $\gcd(4a^3 + 27b^2,\ N) = \begin{cases} 1, & \text{положим} \quad P = (x, y) \\ N, & \text{идем на шаг } 2 \\ \text{иное, вернуть } p, q \in \{p, q\} \end{cases}$
4. Для всех простых $p_1 < B_1$:

   $$P = p_i^{e_i} \cdot P \text{ на } E(\mathbb{Z}_N) \text{ т.е. } p_i^{e_i} < B_i$$

   Если какое-либо вычисление "+" на $E(\mathbb{Z}_N)$ позволяет делитель N, вернуть его.
5. Либо повторить с Шаг 2, либо вернуть "делитель не найден".

Корректность

Лемма 5. *Пусть $N = p \cdot q$, $E(\mathbb{Z}_N)$ — эллиптическая кривая, т. е. $|E(\mathbb{F}_p)|$ — B_1 — гладкое и $|E(\mathbb{F}_q)|$ — не B_i-гладкое. Тогда алгоритм ECM возвращает p, q за время $\mathcal{O}(B_1 \lg^3 N)$ с вероятностью $\geqslant 1 - \frac{1}{B_1}$.*

Доказательство. Пусть $K = \prod\limits_{\substack{p_i - \text{простое} \\ p_i \leqslant B_1}} p_i^{e_i}$

Так как $E(\mathbb{F}_q)$ — не B_i-гладкое, то $\exists r > B_1$, т. ч.

Если $r | \operatorname{ord}_{E(\mathbb{F}_q)}(P)$, то $kP \neq \mathcal{O}$ на $E(\mathbb{F}_q)$.

С другой стороны, K — кратно $\#E(\mathbb{F}_p) \Rightarrow k \cdot P = \mathcal{O}$ на $E(\mathbb{F}_q)$.

Т. е. когда мы вычисляем kP на $E(\mathbb{Z}_N)$ мы получаем

$$\begin{matrix} P' + Q' = \mathcal{O} \text{ на } E(\mathbb{F}_p) \\ P' + Q' = \mathcal{O} \text{ на } E(\mathbb{F}_q) \end{matrix} \Rightarrow \text{по следствию 5 алгоритм вернет } (p, q).$$

сложность и вероятность — аналогично $(p-1)$-методу. □

Замечание Баланс выбора B_1:

малое $B_1 \Rightarrow$ быстрый алгоритм, малая вероятность успеха

большое $B \Rightarrow$ 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: $L_p[\frac{1}{2},\ \frac{1}{\sqrt{2}}]$ при 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.