Лекция #7

Алгоритм факторизации на эпп. кривых

0. Коррекция предыдущей лекции:

В алгоритме вычисления $\#E(\mathbb{F}_q)$ (помощью алгоритма нахождения $\operatorname{ord} P$ методом BS-GS) мы написали

$$L = \operatorname{lcm}(\{\operatorname{ord} P_i\}_i).$$

На самом деле: ← макс. число случайных точек $P \in E$

For $i = 1 \dots N$

$L = \operatorname{lcm}(L, \operatorname{ord}(P_i))$

if $L \geq q+1-2\sqrt{q}$ (т.е. $L \in [q+1-2\sqrt{q}, q+1+2\sqrt{q}]$)

return L

elif $L \geq 4\sqrt{q}$ ($\Rightarrow \exists$ единственный мн-ль M для L т.ч. $L \cdot M \in [q+1-2\sqrt{q}, q+1+2\sqrt{q}]$ и именно $M = \lceil q+1+2\sqrt{q} \rfloor // L$)

$M = q+1+\lceil 2\sqrt{q} \rfloor // L$

return $M \cdot L$

else

return 'fail'.

I. Идея использовать кривые для факторизации принадлежит H. Lenstra, ("Factoring integers with elliptic curves" 1987).

I. $(p-1)$-метод Полларда

W.l.o.g. $N = pq$, (легко обобщается на случай нескольких простых множителей)

$p-1$ факторизуется (раскладается) на "малые" простые,

$q-1$ не факторизуется на "малые" простые.

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

↑ граница (известна)

Идея метода: • $\forall a \in \mathbb{Z}_N^*$ и $\forall K$ - кратное $p-1$:

$$a^K = (a^{p-1})^{\cdot} \equiv 1 \bmod p$$

(т-ма Ферма).

• Если $a^K \not\equiv 1 \bmod q$, то $\boxed{\operatorname{GCD}(N, a^K - 1) = p}$

Алгоритм Полларда $(p-1)$-метод

Вход: $N = p \cdot q$

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

1. Выбрать B_1, B_2 – границы.
   $a \xleftarrow{R} \mathbb{Z}_N^*$ ← что означает
2. Для всех простых $p_i \le B_1$:
   $a \leftarrow a^{p_i^{e_i}} \bmod N$, где e_i - макс, удовлетворяющее $p_i^{e_i} \le B_2$
3. Если $\gcd(a-1, N) \notin \{1, N\}$.
   Вернуть $\gcd(a-1, N)$, $\frac{N}{\gcd(a-1,N)}$

   Иначе
   Вернуть "делители не найдены".

Корректность

Лемма 1] $N = p \cdot q$, $B_1, B_2 \in \mathbb{N}$ т.ч. $(p-1)$ – B_1-гладкое и $p-1 = \prod p_i^{e_i}$, $p_i^{e_i} \le B_2$. А $(q-1)$ - не B_1-гладкое.
Тогда Алгоритм $(p-1)$ Полларда находит p за время $O(B_1 \log^3 N)$ с в-тью $1 - \frac{1}{B_1}$.

◁ Положим $K = \prod\limits_{\substack{p_i \le B_1 \\ p_i - \text{простые}}} p_i^{e_i}$

Так как $(q-1)$ – не B_1-гладкое, $\exists\ r$ - простое, $r > B_1 : r \mid q-1$

Если $r \mid \operatorname{ord}_{\mathbb{Z}_q^*}(a)$, то $\operatorname{ord}_{\mathbb{Z}_q^*}(a) \nmid K \Rightarrow a^K \neq 1 \bmod q$

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

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

$\mathbb{Z}_q^* = \{\alpha^1 \dots \alpha^{q-1}\}$ – цикл. группа, т.е. $a \bmod q = \alpha^i$ для $i \in \{1, q-1\}$

Лемма 2. Кроме того $\operatorname{ord}_{\mathbb{Z}_q^*}(\alpha^i) = \frac{q-1}{\gcd(i, q-1)}$

(Покажем, что $\operatorname{ord}_{\mathbb{Z}_q^*}(\alpha^i) = \frac{q-1}{\gcd(i,q-1)}$; $\exists\ t = \operatorname{ord}(\alpha^i)$

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

положим $(q-1) \cdot m = i \cdot t \quad (m \in \mathbb{Z})$

$gcd(q-1, i) \mid q-1$, положим $(q-1) = q' \cdot gcd(q-1, i)$ $\Rightarrow gcd(q', i') = 1$.
$gcd(q-1, i) \mid i$, положим $i = i' \cdot gcd(q-1, i)$

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

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

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

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

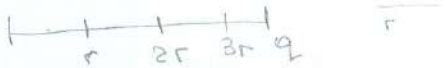
покажем обратное н-во:

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

$\Rightarrow t \le q'$

Вывод: $t = q'$)

$r \nmid ord(\alpha^i) \Leftrightarrow r \mid i$



т.к. i - случ. число $[1 .. q-1]$, $\frac{1}{r}$ - кратно r с вероятностью $\frac{q}{r} \cdot \frac{1}{q} = \frac{1}{r}$

$\Rightarrow r \mid ord(\alpha^i)$ с вероятностью $1 - \frac{1}{r} > 1 - \frac{1}{B_1}$ $(r > B_1)$ ▷.

Сложность ∃ не более B_1 простых p_i, т.ч. $p_i < B_1$ (точнее $\exists \nu \frac{B_1}{\ln(B_1)}$)

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

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

Замечание: Вероятность успеха и сложность алгоритма зависят от $|\mathbb{Z}_p^*| = p-1$: Если $\frac{p-1}{2}$ - простое (т.е. $p-1 = 2 \cdot p'_{\text{проста}}$) $\Rightarrow B_1 \approx p \Rightarrow$ сложность $O(p \cdot \lg^3 N)$ - не лучше наивного брут-форса.

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

II Теорема 3 (Дойринг). Пусть $p \neq 2,3$ - простое. Для $\forall t \in \mathbb{Z}$, $|t| \leq 2\sqrt{p}$, число эл. кривых $E(\mathbb{F}_p)$ ф.ч. $|E| = p+1+t$ равно $\Omega\left(\frac{p^{3/2}}{\lg p}\right)$

Замечание
- Число эл. кривых $E^{=} \bmod p$: $p^2 - p$
(т.к. имеем p^2 пар (a,b) - коэфф. кривой и для p пар справедливо $4a^3 + 27b^2 \equiv 0 \bmod p$
$a^3 \equiv -\frac{27}{4} b^2 \bmod p$
$x \mapsto x^3$ - биекция)
- $\exists$ $4\sqrt{p}+1$ целых $t \in \mathbb{Z}$ т.ч. $|t| \leq 2\sqrt{p}$
- $\Rightarrow$ для каждого t $\exists$-ет "в среднем" $\frac{p^2-p}{4\sqrt{p}+1} = \Omega(p^{3/2})$ кривых порядка $|E| = p+1+t$.
- Теорема Дойринга гласит, что аргументы "в среднем" верны до мн-ля $(\log p)$.

ни к чему

III Эллиптические кривые mod N

$$E(\mathbb{Z}_N) = \{ (x,y) \in \mathbb{Z}_N \times \mathbb{Z}_N : y^2 \equiv x^3 + ax + b \bmod N \text{ для } \gcd(N, 4a^3+27b^2) = 1 \} \cup \{O\}.$$

ВАЖНО! Точки на $E(\mathbb{Z}_N)$ не образуют аддитивную группу!
(Пример: $E: y^2 \equiv x^3 + 1 \bmod 55$, $P = (10,11) \in E$,
для вычисления $2P$, необходимо найти $(2y)^{-1} = (2 \cdot 11)^{-1} \bmod 55$,
но $\gcd(22, 55) = 1 \Rightarrow$ обратного ✗).

Закон "+" на $E(\mathbb{Z}_N)$:

Вход: $P, Q \in E(\mathbb{Z}_N)$ $(P, Q \neq O)$; Выход: либо $P+Q = (x_3, y_3)$, либо $d \mid N$
$P = (x_1, y_1)$, $Q = (x_2, y_2)$

1. Если $x_1 \equiv x_2 \bmod N$ и $y_1 \equiv -y_2 \bmod N$
вернуть O
2. $d = \gcd(x_1 - x_2, N)$.
Если $d \neq \{1, N\}$
вернуть d
3. Если $x_1 \equiv x_2 \bmod N$
$d = \gcd(y_1 + y_2, N)$
Если $d > 1$
вернуть d

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

$$\beta = y_1 - \lambda x_1$$

5. $x_3 = \lambda^2 - x_1 - x_2 \mod N$
$y_3 = -(\lambda x_3 + \beta) \mod N$
Вернуть (x_3, y_3).

Теорема 4 $\exists P, Q \in E(\mathbb{Z}_N)$.
Тогда $P+Q$ на $E(\mathbb{Z}_N)$ либо идентично сложению на $E(\mathbb{F}_p)$, $E(\mathbb{F}_q)$, либо даёт делитель N.

◁ $P = (x_1, y_1)$
$Q = (x_2, y_2)$

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

$$\Rightarrow \begin{cases} \begin{cases} x \equiv x_1 \\ y_1 \equiv -y_2 \end{cases} \mod p, \\ \begin{cases} x \equiv x_1 \\ y_1 \equiv -y_2 \end{cases} \mod q \end{cases} \Rightarrow \begin{matrix} x = x_1 \\ x = y_1 \end{matrix} \mod N \Rightarrow P+Q = O \text{ на } E(\mathbb{Z}_N)$$

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

2.1. $x_1 \neq x_2 \mod p$ и $x_1 \neq x_2 \mod q$
$\Rightarrow$ ф-лы сложения $E(\mathbb{F}_p)$, $E(\mathbb{F}_q)$, $E(N)$ идентичны.

2.2. $x_1 \neq x_2 \mod p$, $x_1 = x_2 \mod q \Rightarrow$
шаг 2: $\gcd(x_1 - x_2, N) = q$
(аналог. $x_1 = x_2 \mod p$, $x_1 \neq x_2 \mod q$)

2.3. $\begin{cases} x_1 = x_2 \mod N \\ y_1 \neq -y_2 \mod p \end{cases} \Rightarrow$ ур-ие $y^2 = x_1^3 + ax_1 + b$ (для y) имеет в точности 2 решения $y_{1,2} = \pm y \mod p$ т.ч. $y_1 \neq -y_2 \mod p$
$\Leftrightarrow y_1 = y_2 \mod p$.

В таком случае $y_1 + y_2 = 2y_1 \mod p$, ф-лы сложения идентичны.

(тоже самое при $q \leftrightarrow p$). ▷.

Следствие 5 $\exists\ P+Q=\mathcal{O}$ на $E(\mathbb{F}_p)$ и $P+Q\neq\mathcal{O}$ на $E(\mathbb{F}_q)$.
Тогда $P+Q$ на $E(\mathbb{Z}_N)$ даст делитель N.

▷ $P+Q=\mathcal{O}$ 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 $E(\mathbb{F}_q) \Leftrightarrow \begin{cases} x_1 \not\equiv x_2 \bmod q \Rightarrow \gcd(x_1-x_2, N) = p \text{ (шаг 2)} \\ y_1 \not\equiv -y_2 \bmod q \Rightarrow \gcd(x_1+y_2, N) = q. \end{cases}$

~~Если $x_1 \neq x_2$ ...~~

Алгоритм факторизации ECM

Вход: $N = p \cdot q$ $(p \sim q)$
Выход: p, q или "делители не найдены"

1. Выберем границы B_1, B_2
2. Выберем $(a, x, y) \in \mathbb{Z}_N \times \mathbb{Z}_N \times \mathbb{Z}_N$,
   $b = y^2 - x^3 - ax \bmod N$ // таким образом, мы выбрали точку с координатами (x,y) на кривой $y^2 = x^3 + ax + b$
3. Если $\gcd(4a^3+27b^2, N) = \begin{cases} 1, & \text{положим } P = (x, y) \\ N, & \text{идем на шаг 2} \\ \text{иное } \in (1, N), & \text{вернуть } p, q \end{cases}$
4. Для всех простых $p_i < B_1$:
   $P := p_i^{e_i} \cdot P$ на $E(\mathbb{Z}_N)$ т.ч. $p_i^{e_i} < B_i$
   Если какое-либо вычисление "+" на $E(\mathbb{Z}_N)$ возвращает делитель N, вернуть его.
5. Либо повторить с шага 2, либо вернуть "дел-ли не найдены".

Корректность

Лемма 6 $\exists\ N = p \cdot q$, E ~~ком~~ $(\mathbb{Z}_N)$ – эл. кривая, т.ч.
$|E(\mathbb{F}_p)|$ – B_1-гладкое и $|E(\mathbb{F}_q)|$ – не B_1-гладкое.
$\#E(\mathbb{F}_p)$ ← Тогда Алгоритм ECM возвращает p, q за время $O(B_1 \lg^3 N)$ с вероятностью $\geq 1 - \frac{1}{B_1}$.

◁. $\exists\, k = \prod_{\substack{p_i - \text{простые} \\ p_i \le B_1}} p_i^{e_i}$

Т. к. $\#E(\mathbb{F}_q)$ – не B_1-гладкое, то $\exists\, r^{B_1}$ т. ч. ~~$r \mid \#E(\mathbb{F}_q)$~~

Если $r \mid \mathrm{ord}_{E(\mathbb{F}_q)}(P)$, то $kP \neq 0$ на $E(\mathbb{F}_q)$ $r \mid \#E(\mathbb{F}_q)$.

С другой стороны, k – кратно $\#E(\mathbb{F}_p) \Rightarrow k \cdot P = 0$ на $E(\mathbb{F}_q)$

$\Rightarrow$ т. е. когда мы вычисляем kP на $E(\mathbb{Z}_N)$, мы получим

$P' + Q' = 0$ на $E(\mathbb{F}_p)$

$P' + Q' \neq 0$ на $E(\mathbb{F}_q)$ $\Rightarrow$ по следствию 5 алгоритм вернёт (p, q).

сложность и вероятность – аналогично $(p-1)$-методу. ▷

Замечание Баланс выбора B_1: малое $B_1 \Rightarrow$ быстрый алгоритм, малая в-ть успеха

большое $B \Rightarrow$ медленный алг-м, большая в-ть успеха

оптимально: $B_1 \approx L_p\left[\frac{1}{2}, \frac{1}{\sqrt{2}}\right] = e^{\frac{1}{\sqrt{2}}(\ln p)^{1/2}(\ln\ln p)^{1/2}}$

$\Rightarrow$ время работы алг-ма: $L_p\left[\frac{1}{2}, \frac{1}{\sqrt{2}}\right]$ 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.