4 - Miller-Rabin

Wednesday, 19 June 2024 16:18

Algorytm Millera-Rabina PRIMES $\in$ BPP

Wylosuj $a \in [1, N-1]$

$m := N-1$
$x := a^m$
while $(x == 1$ and $2 | m)$
  $m = \frac{1}{2} m$
  $x = a^m$
if $(x == \pm 1)$
  return PIERWSZA
return ZŁOŻONA

Dowód poprawności

Jeśli zwróci ZŁOŻONA to faktycznie złożona:

$a^{p-1} = 1$ dla pierwszego p

$x^2 = 1 \pmod p \Rightarrow x = \pm 1 \pmod p$

Jeśli PIERWSZA to pierwsza z $p \geq \frac{1}{2}$

Przypadek 1:

$N = P \cdot Q$, $\gcd(P, Q) = 1$

Rozważmy grupę $\mathbb{Z}_n^* = \{1 \leq a \leq n : \gcd(a, n) = 1\}$

Niech $N-1 = 2^r \cdot t$ $2 \nmid t$

Rozważmy „tabelkę" $|\mathbb{Z}_n^*| \times r$ - reszty z dzielenia elementów z $\mathbb{Z}_n^*$ dla odpowiednich $\frac{N-1}{2^j}$.

Na pewnym poziomie nie ma samych 1: $(-1)^t$

Weźmy pierwszy poziom na którym $\exists_b : b^m \neq 1$

Pokażemy, że istnieje taki b': $b'^m \notin \{-1, 1\}$

Jeśli $b^m \neq -1$ to $b' := b$, zatem $b^m = -1$.

Rozważmy układ równań:

$$\begin{cases} x \equiv 1 \pmod p \\ x \equiv b \pmod Q \end{cases}$$

Z CRT istnieje rozwiązanie. $b' := x$.

$b' \neq 1 \pmod{PQ}$ bo $b'^m \equiv -1 \pmod Q$

$b'^m \neq -1 \pmod{PQ}$ bo $b'^m = 1 \pmod p$.

Rozważmy zatem grupę $M = \{a \in \mathbb{Z}_n^* : a^m = \pm 1\}$

Jest to podgrupa $\mathbb{Z}_n^*$, zatem $|M| \leq \frac{1}{2} |\mathbb{Z}_n^*|$ (bo b' istnieje)

Zatem losując element a z szansą $\geq \frac{1}{2}$ trafimy na świadka złożoności.

Przypadek 2:

$N = p^k$, p jest pierwsze, $k \geq 2$

Pokażemy, że istnieje b: $b^{N-1} \neq 1 \pmod N$

Wtedy szansa na wylosowanie elementu z grupy $\{a : a^{N-1} = 1\} \leq \frac{1}{2}$.

Niech $b := p+1$. Policzmy $b^p \pmod{p^2}$

$b^p = \sum \binom{p^k}{j} p^j \equiv 1 \pmod{p^2}$

Zatem $b^n \equiv 1 \pmod{p^2}$

Gdyby $b^{n-1} \equiv 1 \pmod N$ to $b^{n-1} = 1 \pmod{p^2}$ bo $p^2 | N$

Wtedy $b^n \equiv b \equiv p+1 \pmod{p^2} \Rightarrow$ sprzeczność. Zatem $b^{n-1} \neq 1$. $\square$