10 - Klasyczna część algorytmu Shora

Saturday, 22 June 2024 20:24

Chcemy zfaktoryzować N.

Jeśli dla dowolnego $a \in \mathbb{Z}_N^*$ potrafimy wskazać rząd to bierzemy a do momentu aż rząd r będzie parzysty.

Wtedy $N \mid (a^{r/2}-1)(a^{r/2}+1)$ i z dużą szansą $gcd(A, a^{r/2}-1)$ jest nietrywialnym dzielnikiem.

Dowód:

Niech N będzie nieparzystą, liczbą złożoną i nie p^k.

Niech $N = \prod p_i^{\alpha_i}$

Z CRT wiemy, że wystarczy wyłosować resztę $a_i \pmod{p_i^{\alpha_i}}$

Niech r_i to rząd $a_i \pmod{p_i^{\alpha_i}}$

$r = lcm(r_1, \dots, r_s)$

Żeby r było nieparzyste, to każde r_i musi być nieparzyste.

Zauważmy, że jeśli $2r_i \mid r$ to $a^{r/2} = 1 \pmod{p_i^{\alpha_i}}$

więc $a^{r/2} \neq -1 \pmod{p}$

Zatem algorytm nie znalazł dzielnika, to któreś zdarzenie musi zajść, czyli $V_2(r_1) = V_2(r_2) = \dots = V_2(r_s)$

Jaka jest na to szansa?

Rozpatrzmy grupę $G_i = \mathbb{Z}_{p_i^{\alpha_i}}^*$. Ma generator g i rząd $t = (p_i - 1)p_i^{\alpha_i - 1}$

Rozważmy zbiory $G_i' = \{g^1, g^3, \dots\}$; $G_i'' = \{1, g^2, \dots\}$

rząd każdego elementu z G_i' ma taki sam wykładnik 2-adyczny co t, więc jeśli ustalimy a, to szansa że trafimy w element o rzędzie o innym wykładniku 2-adycznym niż 2 jest $\geq \frac{1}{2}$.

Zatem szansa że nie wygrzebamy dzielnika jest $\leq 2^{1-s}$. $\square$