# 9 - Pierwiastek dyskretny -> faktoryzacja

Tuesday, 18 June 2024 19:47

Potrafimy liczyć pierwiastek dyskretny w $\mathbb{Z}_n \to$ faktoryzacja $n$.

Wylosujmy $u < n$ i obliczmy $v = u^2 \pmod n$

Pokażemy, że $x^2 = v \pmod{p \cdot q}$ ma conajmniej 4 rozwiązania.

$x^2 = v \pmod p$

$x^2 = v \pmod q$ każde ma $\geq 2$ rozwiązania $\pm x_p$ i $\pm x_q$

Zatem:

$x = \pm k_p \pmod p$

$x = \pm k_q \pmod q$

i dla każdego wyboru $\pm$ dostajemy (inne?) rozwiązanie.

Algorytm zwrócił jakiś pierwiastek, ale nasz był wylosowany.

Zatem z $p = \frac{1}{2}$ wylosował inny niż $\pm u$.

Mamy zatem $u^2 = v^2 \pmod N \Rightarrow N \mid (u-v)(u+v)$

$u \neq \pm v \Rightarrow u-v$ lub $u+v$ ma nietrywialny dzielnik z $N$. $\square$