5 - Pohlig-Hellman

Friday, 21 June 2024 15:28

Mamy grupę G: $N = |G|$, g - generator g, $b \in G$.

Chcemy znaleźć x: $g^x = b$. HEURYSTYKA

Przypadek pierwszy:

N jest pierwsze → Baby-Step-Giant-Step $O(N^{\frac{1}{2}})$

Przypadek 2:

$N = p^k$

przedstawmy x w podstawie p: $x = x_0 + x_1 p + \dots + x_{k-1} p^{k-1}$

Podnieśmy $g^x = b$ do p^{k-1}. $g^{x \cdot p^{k-1}} = b^{p^{k-1}}$

Wszystko poza $x_0 p^{k-1}$ „znika" bo $g^{p^k} = 1$.

Niech $\gamma = g^{p^{k-1}}$. Chcemy znaleźć x_0: $\gamma^{x_0} = b^{p^{k-1}}$

Jednak γ ma rząd p, więc potrafimy to zrobić w $O(p^{\frac{1}{2}})$.

Mając x_0 przekształcamy nasze równanie:

$g^{x_1 p + \dots + x_{k-1} p^{k-1}} = b \cdot g^{-x_0}$

Podnosimy do potęgi p^{k-2} i powtarzamy.

Złożoność: $O(k \cdot p^{\frac{1}{2}})$

Przypadek 3:

$N = Q_1 \cdot Q_2$ $\gcd(Q_1, Q_2) = 1$.

$g^x = b$. Niech $x = k \cdot Q_1 + r$.

Podnieśmy nasze równanie do Q_2:

$g^{k \cdot Q_1 \cdot Q_2 + r \cdot Q_2} = g^{r \cdot Q_2} = b^{Q_2}$

Niech $h = g^{Q_2}$. Rozwiązujemy rekurencyjnie $h^r = b^{Q_2}$.

h ma rząd Q_1 więc istotnie go zmniejszyliśmy.

Analogicznie rozwiązujemy dzieląc przez Q_2 i CRT.

Złożoność: $N = \prod p_i^{\alpha_i} \to O(\sum \alpha_i p_i^{\frac{1}{2}}) = O(\log n \cdot \max_i p_i^{\frac{1}{2}})$ □