10 - Baby-Step-Giant-Step

Thursday, 20 June 2024 17:02

Discrete-Log

Mamy a i b należące do grupy przemiennej G:

Znaleźć x: $a^x = b$.

Chcemy przedstawić x jako dwucyfrową liczbę:

$s := \lceil N^{\frac{1}{2}} \rceil$

Wygenerujmy $A = [a^0, a^1, \dots, a^{s-1}]$

Wygenerujmy $B = [b, b \cdot a^{-s}, b \cdot a^{-2s}, \dots, b \cdot a^{-(s-1)s}]$

Jeśli mają wspólny element to $a^k = b \cdot a^{-ls} \Rightarrow b = a^{ls+k}$ □