8/4/22 The Baby-Step Giant-Step Algorithm for Solving the Discrete Log Problem (Shanks 1971)

Thank Prof Vincent, Paige, & Jessie

Given cyclic group $G = \langle g \rangle$ with order $\#G$ and $h \in G$, find x where $g^x = h$ (take proof as blackbox)

IMPORTANT the number of ... grows exponentially as $\#G$ grows.

Idea: $\forall N \in \mathbb{Z}$ st $\#G \leq N^2$, can write $x = x_0 + N x_1$. $\exists x_0, x_1 \in \mathbb{Z}$ with $0 \leq x_0, x_1 \leq N$ ($x \leq \#G$)

Let $N = \lceil \sqrt{\#G} \rceil$

Construct these lists: $[1, g, g^2, \ldots, g^{N-1}]$ (contains g^{x_0})
& $[h, hg^{-N}, hg^{-2N}, \ldots, hg^{-(N-1)N}]$ (contains $hg^{-x_1 N}$)
The answer is $x = x_0 + N x_1$

Which is faster? Construct the first list first or constructing them simultaneously?

Methods 1&2:
Worst case: same amount of steps. (Ignoring ± small constants)

Method 1:
Best case: $2N$
Average case: $2N + \log N + \left(\frac{N}{2} - 1\right)(N) + \frac{1}{2}$ ($\frac{1}{2}$ steps to ...)
$\sim \frac{N^2}{2} = \frac{(\#G)^2}{2}$

$2N$: first list; $\log N$: g^{-N}; $\left(\frac{N}{2} - 1\right)(N)$: checking the first $\frac{N}{2} - 1$; $\frac{1}{2}$: checking the halfway

Method 2:
Best case: 1
Average case: $\log N + 2\sum_{i=1}^{N/2} i = \log N + 2\frac{\left(\frac{N}{2}\right)\left(\frac{N-2}{2}\right)}{2} \sim \frac{N^2}{4} = \frac{(\#G)^2}{4}$

Method 2 is faster, but both are exponential.