Announcements

- Tutorial Jamboards looked good
- Problem Set #1 due Thursday
- Notice my webpages now use https!

The Discrete Log Problem

Let g be a primitive root of $\mathbb{F}_p$ and $h \in \mathbb{F}_p^*$

The **discrete logarithm problem (DLP)** is the problem of finding an x such that

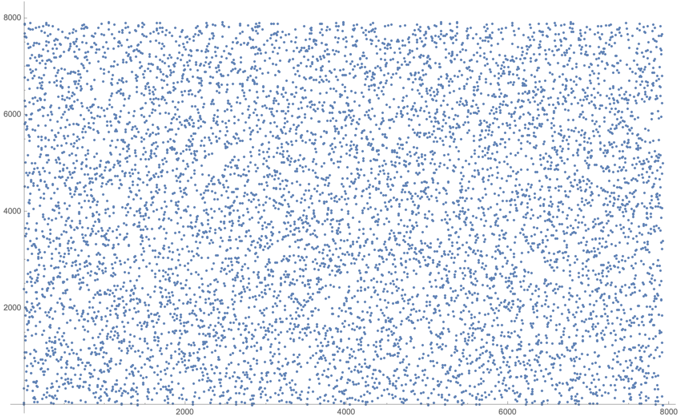
$$g^x \equiv h \mod p$$

Then x is called *the discrete log of h base g*

Why is the DLP $g^x \equiv h \mod p$ hard?

If g has large order, then exponentiation mod p mixes really well

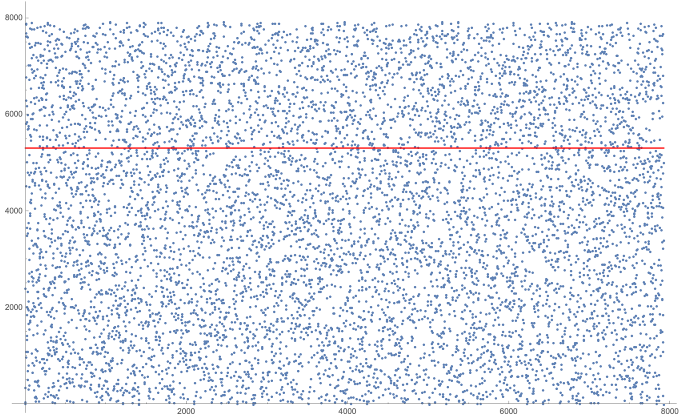
$$y = 7^x \mod 7919$$



Why is the DLP $g^x \equiv h \mod p$ hard?

If g has large order, then exponentiation mod p mixes really well

Solve $7^x \equiv 5314 \mod 7919$



Recall Diffie-Hellman Key Exchange

Trusted publishes p and $g \in \mathbb{F}_p^*$ of large prime order

- **Alice** picks secret $a \in \mathbb{Z}$, sends $A \equiv g^a \mod p$ to Bob
  Bob picks secret $b \in \mathbb{Z}$, sends $B \equiv g^b \mod p$ to Alice
- **Alice** computes $A' \equiv B^a \mod p$
  Bob computes $B' \equiv A^b \mod p$
- Shared key is $A' = B'$

The Diffie-Hellman Problem

Let p be prime and g an integer. The **Diffie-Hellman Problem (DHP)** is the problem of finding

$$A' = B' = g^{ab} \mod p$$

from the known values $A = g^a \mod p$ and $B = g^b \mod p$

Defintion of a group

A **group** consists of a set G and a rule $\star$, for combining two elements $a, b \in G$ to obtain $a \star b \in G$. In addition, $\star$ must have the following three properties:

- **Identity Law:** There exists $e \in G$ such that $e \star a = a \star e = a$ for all $a \in G$
- **Inverse Law:** For every $a \in G$, there exists $a^{-1} \in G$ such that $a \star a^{-1} = a^{-1} \star a = e$
- **Associative Law:** $a \star (b \star c) = (a \star b) \star c$ for all $a, b, c \in G$

Examples

- The **order** of a group G, denoted $|G|$, is the number of elements in G
- If $a \in G$, then the **order of** a is the smallest $d \in \mathbb{N}$ such that $a^d = e$.
  If there is no such d, then a has infinite order.

Proposition 2.13 (Corollary to Lagrange's Theorem)

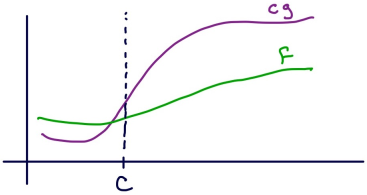
Let G be a finite group of order n and $a \in G$ of order d. Then $d \mid n$.

$\mathcal{O}$-Notation

Definition: Let $f(x)$ and $g(x)$ be functions of x such that $f(x), g(x) \geq 0$.

We say *f is big-$\mathcal{O}$of g*, denoted $f(x) = \mathcal{O}(g)$ if there exist positive constants c and C such that

$$f(x) \leq cg(x) \text{ for all } x \geq C$$



Proposition 2.14

If the limit $\lim_{x \to \infty} \frac{f(x)}{g(x)}$ exists and is finite, then $f = \mathcal{O}(g)$.