Index Calculus

p = prime

$g^a g^b = g^{a+b}$

$(\mathbb{Z}/p\mathbb{Z})^*$

Idea: turn multiplicative relations into linear relations

$$h = g^x \qquad L_g(h) = x$$

$$h^a g^b = h^c g^d \pmod p \quad \longleftrightarrow \quad a L_g(h) + b = c \cdot L_g(h) + d \pmod{p-1}$$

So plan:

1. collect lots of relations (linear in exponents)
2. solve a linear system

"Factor Base" $2, 3, 5, 7, 11, 13, \ldots$

$p_1, p_2, p_3, \ldots, p_m < B$ ← parameter (bound on primes I take)

Find relations: For random k, compute g^k

to try to write $g^k = p_1^{e_1} \cdots p_m^{e_m}$

If so, get an equation $k = e_1 L_g(p_1) + e_2 L_g(p_2) + \cdots + e_m L_g(p_m)$

variables

Example. $p = 127$, $g = 3$, $h = 34$

Solve $g^x = h \pmod p$.

Factor Base: $2, 3, 5, 7$

$g^{108} = 2^5$

$g^{36} = 2^4$

$g^7 = 2^2 \cdot 7$

$108 = 5\,Lg(2)$

$36 = 4\,Lg(2)$

? Can't solve for $Lg(2)$ since 2^{-1} doesn't exist mod 126.

$7 = 2\,Lg(2) + Lg(7)$

$120 = Lg(2) + 2\,Lg(5)$

$48 = 2\,Lg(5)$

$21 = 2\,Lg(2) + 3\,Lg(3)$

$90 = 3 \cdot Lg(2)$

$33 = Lg(2) + Lg(5)$

$72 = Lg(2)$

mod $p-1$
= mod 126

$Lg(2) \equiv 72$

$Lg(3) \equiv 1$ (freebie!)

$Lg(5) \equiv 33 - Lg(2)$
$\equiv 33 - 72$
$\equiv 87$

$$\text{Lg}(7) \equiv 7 - 2 \cdot \text{Lg}(2)$$
$$\equiv 7 - 2 \cdot 72 \equiv 115$$

Phase 2: ~~Use~~ h.

$$h \cdot g^{95} = 2^3 \cdot 7$$

$$\text{Lg}(h) + 95 \equiv 3 \cdot \text{Lg}(2) + \text{Lg}(7)$$

x

$$x \equiv \text{Lg}(h) \equiv 3 \cdot 72 + 115 - 95$$
$$\equiv 110$$

Check: $g^x \equiv 3^{110} \equiv 34 \equiv h$ ✓

Alternate Phase 2

$$hg^{78} \equiv 2 \cdot 3 \cdot 7$$

$$x + 78 \equiv 72 + 1 + 115$$
$$x \equiv 72 + 1 + 115 - 78 \equiv 110$$

Runtime of Index Calculus

Ring $\mathbb{Z}/p\mathbb{Z}$.

Depends on size of factor base $p_1, \ldots, p_m < B$

Larger B: ☺ more likely to succeed in factoring g^k ("g^k is "smooth"" (depends on B) "B-smooth")

☹ more work to factor each g^k

Fact: If $u = \frac{\log p}{\log B}$ the the probability a random integer in range $0, \ldots, p-1$ is B-smooth is $\sim u^{-u}$.

Let $\pi(B)$ size of factor base $\sim \frac{B}{\log B}$.

Approx. Runtime $\approx$ (# of relations we need) · (# of tries to get each relation) · (# of trial divisions each g^k) · (cost of a trial division)

to collect relations: $\pi(B) \cdot u^u \cdot \pi(B) \cdot \text{poly}(\log p)$

$\approx B^2 u^u \times$ poly factors

This is a f^n in B, p. Minimize it. (choose B as fn of p).

Minimizes @ runtime $e^{\sqrt{\log p (\log \log p)}}$.

SUBexponential