Oct1

Wednesday, September 30, 2020 9:53 PM

Theorem (CRT, Sun Tzu)

Morally If $m = m_1 m_2 \cdots m_n$ w/ $\gcd(m_i, m_j) = 1$

Then

$$\left(\text{Solving a congruence mod } m\right) \Longleftrightarrow \left(\text{solving the congruence mod } m_i \text{ each } i\right)$$

$$\{\, x \equiv a \bmod m \quad \Longleftrightarrow \quad \{\, x \equiv a \bmod m_i \text{ each } i$$

Applied to studying square roots mod m.

$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$

$$\begin{tikzcd}
\text{a has a square root mod } m \arrow[r, Leftrightarrow, "CRT"] & \text{a has a square root mod } p_i^{\alpha_i} \ \forall i \arrow[dl, Leftrightarrow, "HW3"'] \\
\text{a has a square root mod } p_i \ \forall i \arrow[r, Leftrightarrow, "\boxed{HW5}"'] \arrow[ur, leftrightarrow, shift right=3] & \underline{a^{\frac{p_i-1}{2}}} \equiv 1 \bmod p_i
\end{tikzcd}$$

Lemma $a \in \mathbb{F}_p^*$ has a square root $\Longleftrightarrow a^{\frac{p-1}{2}} = 1$.

Remark/Caveat
This only works if $\gcd(p_i, a) = 1 \ \forall i$

Takeway check if a is a square mod m by raising to $\frac{p-1}{2}$ mod p each prime factor of m.

Recall

If $p \equiv 3 \bmod 4$ & a is a square mod p then $a^{p+1/4}$ is a square root.

↑ This allows us to effectively compute square roots.

Example

Solve $x^2 = 197 \bmod 437$

$437 = 19 \cdot 27$ $\quad 19, 27 \equiv 3 \bmod 4$

① Solve

$x^2 = 197 = 7 \bmod 19$

Compute

$7^{20/4} = 7^5 \equiv 11 \bmod 19$

$x^2 = 197 \equiv 13 \bmod 27$

Compute

$13^{28/4} = 13^7 = 6 \bmod 27$

If $x \equiv 11 \bmod 19$

& $x \equiv 6 \bmod 27$

$\Longrightarrow$ $x^2 \equiv 197 \bmod 19$

$x^2 \equiv 197 \bmod 27$

$\Downarrow$ CRT

some x

$\Downarrow$ CRT

$x^2 \equiv 197 \bmod 19 \cdot 27$

Let $x = 11 + 19y$

$11 + 19y \equiv 6 \bmod 27$

$y = 7 \bmod 27$

So $\boxed{x = 11 + 19 \cdot 7 = 144}$

$\boxed{144^2 \equiv 197 \bmod 437}$

!!!

Rmk $x = -11 \bmod 19$

or $x = -6 \bmod 27$

Get 4 solutions mod 437

Prop $m = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$

$\Longrightarrow$ $x^2 \equiv a \mod m$ has $\leq 2^t$ solutions mod m.

Exercise: Refine & prove this.

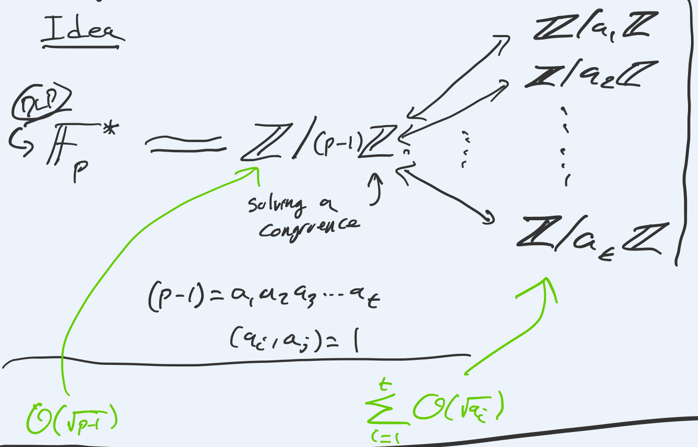
Computing square roots mod m $\longleftrightarrow$ Factor m becomes easy!

Assuming integer factorization is hard

Send me a message square & reduce mod m $\rightsquigarrow$ My secret key is factoring m & computing square root mod each prime factor.

Using the CRT to attack the DLP

Idea


DLP
$\mathbb{F}_p^*$
$=$
$\mathbb{Z}/(p-1)\mathbb{Z}$
$\mathbb{Z}/a_1\mathbb{Z}$
$\mathbb{Z}/a_2\mathbb{Z}$
$\mathbb{Z}/a_t\mathbb{Z}$
solving a congruence
$O(\sqrt{p-1})$
$\sum_{i=1}^{t} O(\sqrt{a_i})$

$$(p-1) = a_1 a_2 a_3 \cdots a_t$$

$$(a_i, a_j) = 1$$

Setup

G a group. $g \in G$ $|g| = N$.

Slogan: solutions to $g^x = h$ determined mod N.

$$\underset{\times}{\{e, g, g^2, \dots, g^{N-1}\}} \xrightarrow[\sim]{\log} \underset{+}{\{0, 1, 2, \dots, N-1\}} \underset{\mathbb{Z}/N\mathbb{Z}}{\overset{}{\|}}$$

$N = p_1^{\alpha_1} \cdots p_t^{\alpha_i}$

Finding $\log_g h$ $\longleftrightarrow$ Solving congruence mod N

$\xleftrightarrow{\text{CRT}}$ Solving congruences mod $p_i^{\alpha_i}$

Concretely DLOG order N

$$\begin{tikzcd}
g^x = h \arrow[r, leftrightarrow] & x \equiv \log_g h \mod N \arrow[d, leftrightarrow, "\text{CRT}"] \\
g_i^{x_i} = h_i \arrow[r, leftrightarrow] & x \equiv \log_g h \mod p_i^{\alpha_i} = \log_{g_i} h_i
\end{tikzcd}$$

DLOG order $p_i^{\alpha_i}$

↪ Interpret these as a simpler dlog problem

If $g^x = h$ $\xrightarrow[N/p_i^{\alpha_i}]{\text{raise both to}}$ $\left(g^{N/p_i^{\alpha_i}}\right)^x = h^{N/p_i^{\alpha_i}}$

$g_i := g^{N/p_i^{\alpha_i}}$

$h_i := h^{N/p_i^{\alpha_i}}$

If I can solve for

$x_i = \log_{g_i} \alpha_i$

Then $\underline{x \equiv x_i \mod p_i^{\alpha_i}}$ (*)

Lemma:

Let $g \in G$. $|g| = N$. $a \mid N$. $\Rightarrow$

$$|g^{N/a}| = a.$$

Pf/ $(g^{N/a})^a = g^N = 1$ ✓

$0 < b < a$

$(g^{N/a})^b \neq 1$ b/c $0 < \frac{Nb}{a} < N$ bc N is min power of g to get 1.

$\Rightarrow$ a min pos power of $g^{N/a}$ to get 1

Corollary *

$$g_i^x = g_i^{x_i}$$

$$\Rightarrow g_i^{x-x_i} = 1$$

$$\Rightarrow p_i^{\alpha_i} = |g_i| \mid x - x_i$$

Theorem (Pohlig - Hellman Algorithm)

Let G be a group. Suppose $\forall$ prime powers q^e we have a solution to the DLP for elements of order q^e & it runs in $O(S_{q^e})$ steps.

Suppose $g \in G$ of order N.

Suppose $N = q_1^{e_1} \cdots q_t^{e_t}$ prime factorization *

Then the follow algorithm solves the DLP for g in $\mathcal{O}\left(\underline{\sum_i S_{q_i^{e_i}}} + \underbrace{\log N}_{\text{usually goes away.}}\right)$

① For $0 \le i \le t$ let

$$g_i = g^{N/q_i^{e_i}} \qquad h_i = h^{N/q_i^{e_i}}$$

Use DLP for prime powers to compute

$$x_i = \log_{g_i} h_i \quad (\text{defined mod } q_i^{e_i})$$

② Use CRT to solve

$$x = x_1 \bmod q_1^{e_1}$$
$$x = x_2 \bmod q_2^{e_2}$$
$$\vdots$$
$$x = x_t \bmod q_t^{e_t}$$

Proof

Running Time

Step ① takes $\mathcal{O}(S_{q_i^{e_i}})$ each i.

So $\sum \mathcal{O}(S_{q_i^{e_i}})$

Step ② takes $\mathcal{O}(\log N)$ steps to implement CRT.

↳ HW implement & prove time complexity $\mathcal{O}(\log N)$

Correctness

Have some $x = x_i + q_{b_i}^{e_i} z_i$

$$(g^x)^{N/q_{b_i}^{e_i}} = \left(g^{x_i + \underline{q_{b_i}^{e_i}} z_i}\right)^{N/q_{b_i}^{e_i}}$$

$$= \underbrace{\left(g^{N/q_{b_i}^{e_i}}\right)}_{g_i}^{\underline{x_i}} \cdot \underbrace{\left(g^{N}\right)}_{=1}^{z_i}$$

$$= h_i$$

$$= h^{N/q_{b_i}^{e_i}}$$

$$\begin{tikzcd}
(g^x)^{N/q_{b_i}^{e_i}} \arrow[d, "\mathrm{dlog}_g"'] & h^{N/q_{b_i}^{e_i}} \arrow[d, "\log_g"] \\
\log_g (g^x)^{N/q_{b_i}^{e_i}} \arrow[r, phantom, "\shortparallel"] & \boxed{\underline{x} \cdot \underline{\frac{N}{q_{b_i}^{e_i}}} \equiv (\underline{\log_g} h) \cdot \underline{\frac{N}{q_{b_i}^{e_i}}} \mod N} \quad \underline{E_i}
\end{tikzcd}$$

$$\mathrm{GCD}\left(\frac{N}{q_1^{e_1}}, \frac{N}{q_{b_2}^{e_2}}, \ldots, \frac{N}{q_{b_t}^{e_t}}\right) = 1$$

Extended EA $c_1, c_2, \ldots, c_t \in \mathbb{Z}$

& $c_1 \frac{N}{q_{b_1}^{e_1}} + \cdots + c_t \frac{N}{q_{b_t}^{e_t}} = 1$

$$\sum c_i E_i$$

$$\sum \frac{N}{q_{b_i}^{e_i}} \cdot x = \sum \frac{N}{q_{b_i}^{e_i}} \log_g h \mod N$$

$$\Rightarrow x = \log_g h \mod N \quad \oslash$$

Remark   Baby Step Giant Step

If $|g|=N$ solve DLP in $O(\sqrt{N}\log N)$

in particular, if $|g|=p^\alpha$ $\rightsquigarrow$ $O(\sqrt{p^\alpha}\log p^\alpha)$

$\uparrow$ S_{p^α}

If $N=q_1^{e_1}\cdots q_t^{e_t}$

BSGS

$O(\sqrt{N}\log N)$

Pohlig Hellman + BSGS

$O(\sum\sqrt{q_i^{e_i}}\log q_i^{e_i}+\log N)$

Example

$N=646963230=2\cdot3\cdot5\cdot7\cdot11\cdots 29$

$\rightsquigarrow\sqrt{N}\approx 80{,}000$

$\rightsquigarrow\sum\sqrt{q_i}=\sqrt{2}+\sqrt{3}+\sqrt{5}+\cdots+\sqrt{29}\approx 40$

Notice

If N has lots of factors, Pohlig Hellman speeds up an attack of DLP considerably!

$\rightsquigarrow$ ~~D~~DLP is not hard if order of N has lots of factors.

If were doing DLP for $\mathbb{F}_p^*$

order is $p-1$ which is NEVER PRIME $(p\neq 3)$

$p-1$ always even.

So best we can do is $p-1=2q$

$\rightsquigarrow$ DLP $\longrightarrow$ PH + BSGS $\qquad q \sim p/2$

$\swarrow$

BSGS

$O(\sqrt{p-1})$

$$O(\sqrt{2}+\sqrt{q}) = O(\sqrt{q})$$
$$= O(\sqrt{p}).$$

Upshot DLP still secure for $p = 2q+1$ for q another prime.

Remark One may think $N = p^{1000}$ we're still safe because factors aren't coprime. But it turns out that's not true.

Goal Reduce DLP for elts of prime power order to the DLP for elts of prime order

---

Idea $|g| = p^\alpha \implies |g^{p^{\alpha-1}}| = p$

Theme To reduce a mod p^α question to a mod p question try raising stuff to powers of p.

Example $|g| = p^2$ Solve $g^x = h$.

x has some base p expansion

$$\underline{x = x_0 + x_1 \cdot p}$$

① $g^{px} = h^p \implies (g^p)^{x_0} = h^p \qquad |g^p| = p$

$$g^{px} \;\Big\Vert\; g^{p(x_0+x_1p)} \;\Big\Vert\; g^{px_0} \cdot \cancel{g^{p^2x_1}}$$

$\Big\{$ Mod p DLP $\Downarrow$

get x_0

② $g^x = h \longrightarrow (g^p)^{x_1} = hg^{-x_0}$

$$g^x \;\Big\Vert\; g^{x_0+x_1p} = h$$

$\Big\{$ Mod p DLP $\Downarrow$

get x_1

$x = x_0 + p \cdot x_1$ Done

Upshot Instead of a mod p^2 DLP do a mod p DLP twice

& working inductively Replace mod p^e DLP with e mod p DLPs.

Prop $g \in G \quad |g| = q^e$

Suppose can solve DLP order q in $O(S_q)$ steps.

Then solve DLP for g in $O(e \cdot S_q)$.

Remark

DLP for $N=2^{1000}$

BSGS $\rightsquigarrow O(\sqrt{N}) = O(2^{500})$

This way $\rightsquigarrow O(1000 \cdot \sqrt{2})$

“Proof” $g^x = h$

has base q expansio
$x = x_0 + x_1 q + \dots + x_{e-1} q^{e-1}$

Determine $x_0, \dots, x_{e-1}$ recursevely.

Know $x_0, \dots, x_i$ ($i=-1$ Base case worked in)

$$(g^{q^{e-i}})^x = h^{q^{e-i}}$$

NEXT TIME