$g \in G$ element of order $N$

$$\{g^0, g^1, \ldots, g^{N-1}\} \xrightarrow{\log_g} \mathbb{Z}/N.$$

## Pohlig-Hellman (I)

Chinese Remainder Theorem:

If $N = p_1^{e_1} \cdots p_r^{e_r}$,

$$\mathbb{Z}/N \cong \underbrace{\mathbb{Z}/p_1^{e_1} \times \cdots \times \mathbb{Z}/p_r^{e_r}}$$

$r$-tuples · an integer mod $p_1^{e_1}$
· an integer mod $p_2^{e_2}$
⋮
· an integer mod $p_r^{e_r}$.

CRT says we can efficiently recover an integer mod $N$ from the $r$-tuple $(n_1, \ldots, n_r)$.

So if we can calculate $\log_g(h)$ mod $p_i^{e_i}$ for each $i$, can then easily recover $\log_g(h)$.

Goal is to efficiently calculate $\log_g(h) \bmod p_i^{e_i}$.

Can compute it as a different log:

$$\{g^0, g^1, \dots, g^{N-1}\} \xrightarrow{\log_g} \mathbb{Z}/N$$

$$\downarrow \qquad\qquad \downarrow \text{ reduce mod } p_i^{e_i}$$

$$\{g_i^0, \dots, g_i^{p_i^{e_i}-1}\} \xrightarrow{\log_{g_i}} \mathbb{Z}/p_i^{e_i}$$

**Claim** If $g_i = g^{p^{-e_i}N}$ & $h_i = h^{p^{-e_i}N}$,

then $\log_{g_i}(h_i) \equiv \log_g(h) \bmod p_i^{e_i}$.

**Pf** Set $x = \log_g(h)$. Then $g^x = h$

$$\Rightarrow (g^x)^{p^{-e_i}N} = h^{p^{-e_i}N} \qquad \Rightarrow \log_{g_i}(h_i) = x := \log_g(h).$$

$$\| \qquad\qquad \|$$

$$g_i^x \qquad h_i$$

□

So under the correspondence $\mathbb{Z}/N \cong \mathbb{Z}/p_1^{e_1} \times \cdots \times \mathbb{Z}/p_r^{e_r}$

$$\log_g(h) \leftrightarrow (\log_{g_1}(h_1), \ldots, \log_{g_r}(h_r)).$$

This is Pohlig-Hellman (I).

Ex $G = \mathbb{F}_7^\times$, $g = 5$, $h = 4$. Solve

$g^x = h$ in $\mathbb{F}_7^\times$

$5^x = 4$.

Soln $\text{order}(5) = 7-1 = 6 = 2^1 \cdot 3^1$

$p_1 = 2$, $e_1 = 1$

$p_2 = 3$ $e_2 = 1$

$g_1 = 5^{2^1 \cdot 6} = 5^3 = 25 \cdot 5 \equiv 4 \cdot 5 = 20 \equiv -1 \ (7)$.

$h_1 = 4^{2^1 \cdot 6} = 4^3 = 16 \cdot 4 = 2 \cdot 4 = 8 = 1$.

$(-1)^0 = g_1^0 = h_1 = 1$

So $\log_{g_1}(h_1) = 0 \in \mathbb{Z}/p_1^{e_1} = \mathbb{Z}/2$.

$g_2 = 5^{3^{-1} \bmod 6} = 5^2 = 25 \equiv 4 \pmod{7}$

$h_2 = 4^{3^{-1} \bmod 6} = 4^2 = 16 \equiv 2 \pmod{7}$

$g_2^{\boxed{2}} = 4^2 = 16 \equiv 2 \equiv h_2 \Rightarrow \log_{g_2}(h_2) = 2 \in \mathbb{Z}/3.$

$\Leftrightarrow (\log_{g_1}(h_1), \log_{g_2}(h_2)) = (0, 2) \in \mathbb{Z}/2 \times \mathbb{Z}/3.$

$\Rightarrow \log_g(h) = 2 \in \mathbb{Z}/6.$ □

**Ex** $2^x = 3 \in \mathbb{F}_{11}^\times$. $N = 11 - 1 = 10 = 2^1 \cdot 5^1$, $p_1^{e_1} p_2^{e_2}$.

$g_1 = g^{p_1^{-e_1} N} = g^5 = 32 \equiv -1 \pmod{11}.$

$h_1 = 3^5 = 3 \cdot 9^2 \equiv 3 \cdot (-2)^2 = 3 \cdot 4 = 1. \pmod{11}$

$\Rightarrow g_1^{\boxed{0}} = h_1 \mod 11.$

$\Rightarrow \log_{g_1}(h_1) = 0$

$g_2 = g^{p_2^{-e_2} N} = g^2 = 4$.

$h_2 = h^2 = 3^2 = 9$

$4^1 = 4, \quad 4^2 = 5, \quad 4^3 = 20 = 9$

$\Rightarrow \log_4(9) = 3. = \log_{g_2}(h_2)$.

$\Rightarrow (\log_{g_1}(h_1), \log_{g_2}(h_2)) = (0, 3) \in \mathbb{Z}/2 \times \mathbb{Z}/5$

$\Rightarrow \log_g(h) = 8 \in \mathbb{Z}/10$.

---

Ex $3^x = 2 \in \mathbb{F}_{31}$. $\quad N = 31 - 1 = 2 \cdot 3 \cdot 5$

$= p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3}$.

$g_1 = 3^{p_1^{-e_1} N} = 3^{15} = 3 \cdot 3^{14} = 3 \cdot 9^7$

$= 27 \cdot 9^6 = (-4) \cdot 81^3$

$= (-4) \cdot (-12)^3$

$= 4 \cdot 3^3 \cdot 4^3$

$= 4 \cdot (-4) \cdot 2$

$= -16 \cdot 2$

$= -32$

$= -1$.

$h_1 = 2^{15} = (2^5)^3 = (32)^3 = 1^3 = 1.$

$g_1^{0} = h_1 \Rightarrow \log_{g_1}(h_1) = 0.$

$g_2 = 3^{P_2^{-e_2} N} = 3^{10} = 9^5 = 81^2 \cdot 9$

$= 19^2 \cdot 9 = 19 \cdot 171 = 19 \cdot 16$

$= 38 \cdot 8 = 7 \cdot 8 = 56 = 25$

$h_2 = 2^{10} = (2^5)^2 = 1^2 = 1$

$\Rightarrow g_2^{0} = h_2 \Rightarrow \log_{g_2}(h_2) = 0.$

$g_3 = 3^{P_3^{-e_3} N} = 3^6 = (27)^2 = (-4)^2 = 16$

$h_3 = 2^6 = 32 \cdot 2 = 1 \cdot 2 = 2.$

$g_3^{?} = h_3. \quad (2^4)^{4} = 2^{16} = (2^5)^3 \cdot 2 = 2.$

$\Rightarrow \log_{g_3}(h_3) = 4$

So $(\log_{g_1}(h_1), \log_{g_2}(h_2), \log_{g_3}(h_3)) = (0,0,4)$.

$\in \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/5$.

So $\log_g(4) = 24 \in \mathbb{Z}/30$.

Ex $3^x = 6 \pmod{31}$

$g_1 = -1$ as before.

$h_1 = 6^{15} = 6 \cdot 6^{14} = 6 \cdot 36^7 = 6 \cdot 5^7 = 30 \cdot 5^6$

$= (-1) \cdot 25^3 = (-1)(-6)^3 = 36 \cdot 6 = 5 \cdot 6 = 30 = -1$.

$\Rightarrow g_1^{1} = h_1 \Rightarrow \log_{g_1}(h_1) = 1$.

$g_2 = 25 = -6$ as before.

$h_2 = 6^{10} = (36)^5 = 5^5 = 5 \cdot 5^4 = 5 \cdot (25)^2$

$= 5(-6)^2 = 5 \cdot 36 = 5 \cdot 5 = 25 = -6.$

$\Rightarrow \log_{g_2}(h_2) = 1.$

$g_3 = 3^6 = 16$ as before.

$h_3 = 6^6 = 3^6 \cdot 2^6 = (16) \cdot (32)(2) = 1.$

$\Rightarrow \log_{g_3}(h_3) = 0.$

$\Rightarrow (\log_{g_1}(h_1), \log_{g_2}(h_2), \log_{g_3}(h_3)) \in \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/5$

$\| \quad \| \quad \|$

$(1, 1, 0)$

$\Rightarrow$ looking for $x$ s.t. $\begin{cases} x \equiv 1 \ (2) \\ x \equiv 1 \ (3) \\ x \equiv 0 \ (5) \end{cases}$

Chinese Remainder thm

$x \equiv 0 \ (5) \Rightarrow x = 5y$

$1 \equiv x \equiv 2y \ (3)$

$\Rightarrow y \equiv 2 \ (3)$.

$\Rightarrow y = 2 + 3z$

$\Rightarrow x = 5(2+3z) = 10 + 15z$

$\Rightarrow 1 \equiv x \equiv z \ (2)$

$\Rightarrow z = 1$.

$\Rightarrow x = 10 + (15)(1) = 25$.

$\Rightarrow \log_g(h) = 25$

# Pohlig-Hellman (II)

Reduce from $N = p^e$ to $N = p$.

"p-adic analysis".

Write $\log_g(h) = x = x_0 + x_1 p + \cdots + x_{e-1} p^{e-1}$

where each $x_i \in \{0, 1, \ldots, p-1\}$.

$$\log_g(h) \equiv x_0 \pmod{p}.$$

$$\log_{g^{p^{e-1}}}\left(h^{p^{e-1}}\right)$$

why?

$$h^{p^{e-1}} = \left(g^x\right)^{p^{e-1}} = \left(g^{p^{e-1}}\right)^x = \left(g^{p^{e-1}}\right)^{x_0 + p(\cdots)}$$

$$= \left(g^{p^{e-1}}\right)^{x_0} \cdot \left(g^{p^e}\right)^{x_1 + x_2 p + \cdots + x_{e-1} p^{e-2}}$$

$$= \left(g^{p^{e-1}}\right)^{x_0} \cdot (1)^{x_1 + \cdots}$$

$$= \left(g^{p^{e-1}}\right)^{x_0}$$

So $\log_{g^{p^{e-1}}}\left(h^{p^{e-1}}\right) = x_0 \in \mathbb{Z}/p.$

Now we subtract & divide.

$$\frac{x - x_0}{p} = x_1 + x_2 p + \cdots + x_{e-1} p^{e-2}.$$

$$\left(g^{p^{e-1}}\right)^{\frac{x-x_0}{p}} = \left(g^{p^{e-2}}\right)^{x-x_0} = \left(g^x \cdot g^{-x_0}\right)^{p^{e-2}}$$

$$= \left(h \cdot g^{-x_0}\right)^{p^{e-2}}$$

$$\left(g^{p^{e-1}}\right)^{x_1 + p(x_2 + \cdots)}$$

$$\left(g^{p^{e-1}}\right)^{x_1} \cdot \left(g^{p^e}\right)^{x_2 + \cdots} = \left(g^{p^{e-1}}\right)^{x_1}$$

$$\Rightarrow x_1 = \log_{g^{p^{e-1}}}\left[\left(hg^{-x_0}\right)^{p^{e-2}}\right]$$

Similarly,

$$x_2 = \log_{g^{p^{e-1}}}\left[\left(hg^{-x_0-x_1p}\right)^{p^{e-3}}\right]$$

$$x_3 = \log_{g^{p^{e-1}}}\left[\left(hg^{-x_0-x_1p-x_2p^2}\right)^{p^{e-4}}\right]$$

$$\vdots$$

$$x_{e-1} = \log_{g^{p^{e-1}}}\left[\left(hg^{-x_0-\cdots-x_{e-2}p^{e-2}}\right)^{p^0}\right]$$

Then get $x = x_0 + x_1 p + \cdots + x_{e-1} p^{e-1}$.

Ex $3^x = 4 \in \mathbb{F}_5^\times$. $N = 5 - 1 = 2^2 = p^e$

$\Rightarrow e = 2. \Rightarrow x = x_0 + x_1 p.$

$$g^{p^{e-1}} = 3^{2^{2-1}} = 9 = -1.$$

$$h^{p^{e-1}} = 4^{2^{2-1}} = 16 = 1.$$

$$\Rightarrow \log_{g^{p^{e-1}}}\left(h^{p^{e-1}}\right) = \boxed{0 = x_0}$$

$$\Rightarrow x_1 = \log_{g^{p^{e-1}}}\left(\left(h g^{-x_0}\right)^{p^{e-2}}\right)$$

$$= \log_{-1}\left(\left(4 \cdot 3^{-0}\right)^{p^0}\right)$$

$$= \log_{-1}(-1) = 1.$$

$\Rightarrow x = x_0 + x_1 p = 0 + 1(2) = 2.$

---

**Ex** $g = 3, h = 7, \mathbb{F}_{17}.$

(110)

$N = 17 - 1 = 16 = 2^4 = p^e.$

$g^{p^{e-1}} = 3^{2^3} = 3^8 = 9^4 = 81^2 = (-4)^2 = 16 = -1.$

$7^{p^{e-1}} = 7^{2^3} = 7^8 = (49)^4 = (-2)^4 = 16 = -1.$

$\Rightarrow x_0 = \log_{g^{p^{e-1}}}\left(h^{p^{e-1}}\right) = 1.$

$x_1 = \log_{g^{p^{e-1}}}\left(\left[h \cdot g^{-1}\right]^{p^{e-2}}\right)$

$g^{-1} = (3)^{-1} = 6 \quad$ b/c $6 \cdot 3 = 18 = 1.$

$$\hookrightarrow x_1 = \log_{(-1)}\left( (7 \cdot 3^{-1})^{2^{4-2}} \right)$$

$$(hg^{-1})^{p^{e-2}} = (7 \cdot (3)^{-1})^4 = (7 \cdot 6)^4 = (8)^4$$

$$= 2^{12} = (2^4)^3 = (16)^3 = (-1)^3 = -1.$$

$$x_1 = \log_{(-1)}(-1) = 1.$$

$$x_2 = \log_{g^{p^{e-1}}}\left( (h \cdot g^{-x_0 - x_1 p})^{p^{e-3}} \right)$$

$$(h \cdot g^{-x_0 - x_1 p})^{p^{e-3}} = (7 \cdot (6)^{1+1\cdot 2})^2$$

$$= (42 \cdot 36)^2$$

$$= (8 \cdot 2)^2$$

$= 16^2 = (-1)^2 = 1.$

$\Rightarrow x_2 = \log_{(-1)}(1) = 0.$

$$x_3 = \log_{g^{p-1}}\left( \left( h \cdot g^{-x_0 - x_1 p - x_2 p^2} \right)^{p-4} \right)$$

$$\left( h \cdot g^{-x_0 - x_1 p - x_2 p^2} \right)^{p-4} = \left( 7 \cdot (6)^{1 + 1\cdot 2 + 0 \cdot 2^2} \right)^{2^0}$$

$$= 7 \cdot 6^3 = 16 = -1.$$

$\Rightarrow x_3 = \log_{(-1)}(-1) = 1.$

$\Rightarrow x = x_0 + x_1 p + x_2 p^2 + x_3 p^3$

$= 1 + 1\cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3$

$= 11.$