Discrete log

$\log_g a \qquad G = \langle g \rangle \qquad |G| = n$

Algorithm for finding discrete logarithm
1. Shank's Baby-step Giant-step.

$\left\{ \begin{array}{l} \mathbb{Z}_{61}^{\times} = \{1, 2, \ldots, 60\} = \langle 2 \rangle \qquad g=2, \quad a=7 \\ \text{Find } x \geq 0 \text{ s.t. } 2^x = 7 \end{array} \right.$

$g^x = a$ so $m = \lceil \sqrt{n} \rceil \qquad x = qm + r$

$0 \leq r \leq m-1 \qquad 0 \leq q \leq m-1$

$g^{qm+r} = a$

$\boxed{g^{qm} = a g^{-r}}$

$B = \{(a, 0), (ag^{-1}, 1), (ag^{-2}, 2), \ldots, (ag^{-(m-1)}, m-1)\}$

Check if $ag^{-s} = 1$ In this case $a = g^s$

Otherwise compute $g^m, (g^m)^2 = g^{2m}, (g^m)^3 = g^{3m}$ ...

$m = \lceil \sqrt{n} \rceil = \lceil \sqrt{61} \rceil = 8$

Everytime compare g^{jm} with $ag^{-r} \in B$ for each r
if $g^{jm} = ag^{-r}$ for some j & r
then stop & get $a = g^{jm+r}$ so that $x = jm+r$ is a soln.

$2^{-1} = 31$ in $\mathbb{Z}_{61}$

$B = \{ (7, 0), (7 \times 31, 1) = ((1 + 2\times 3)\times 31, 1) = (31+3, 1) = (34, 1),$
$(7 \times 31^2, 2) = (34 \times 31, 2) = (17, 2), (39, 3), (50, 4), (25, 5),$
$(25 \times 31, 6) = ((1 + 2\times 12)\times 31, 6) = (31+12, 6) = (43, 6)$
$(43 \times 31, 7) = ((1 + 2\times 21)\times 31, 7) = (31+21, 7) = (52, 7) \}$ $(m=8)$

Proceed to the Giant step.

$g^m = 2^8 = 2^6 \times 2^2 = 3 \times 4 = 12$ in $\mathbb{Z}_{61}$ → not in B

$g^{2m} = 12^2 = [(2+2\times 5)\times 12] = 24 + 2\times(-1) = 22$ → not in B

$g^{3m} = 12 \times 22 = 12 \times (5\times 4 + 2) = (-1)\times 4 + 24 = 20$ → not in B

$g^{4m} = 12 \times 20 = \underbrace{12 \times 5}\times 4 = (-1)\times 4 = -4 = 57$ → not in B

$g^{5m} = 12 \times 57 = 12 \times (5 \times 11 + 2) = -11 + 24 = 13$ → not in B

$g^{6m} = 12 \times 13 = 12\,(2\times 5 + 3) = -2 + 36 = 34$ it is in B stop.

$$g^{6m} = a g^{-1}$$

$$2^{6\times 8} = a \times g^{-1} \Rightarrow a = 2^{48+1} = \underline{2^{49}}$$

Pollard's ρ-algorithm.

Situation: $G = \langle g \rangle \quad |G| = n$

Find x s.t. $\underline{g^x = a}$

Method: Partition G into 3 parts.

Say $G = G_1 \cup G_2 \cup G_3$ where $G_i \cap G_j = \phi$ for $i \neq j$.

Define $f : G \to G$ by

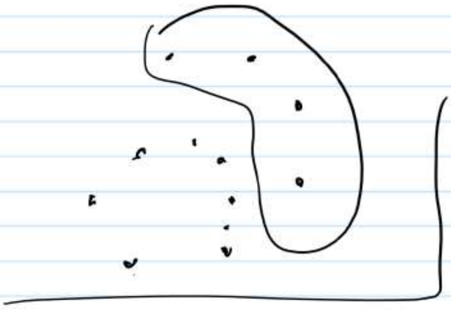
$$f(b) = \begin{cases} gb & b \in G_1 \\ b^2 & b \in G_2 \\ ab & b \in G_3 \end{cases}$$

Construct the sequence $\{b_n\}$ by

$b_0 = g^{x_0}$ for some $x_0 \in \{1, 2, \ldots n\}$ (arbitrary)

$b_1 = f(b_0)$, $\boxed{b_{i+1} = f(b_i)}$

Since G is finite $\exists\, i, k$ s.t. $\boxed{b_{i+k} = b_i}$



fix : $y_0 = 0$

$$b_1 = g(b_0) = \begin{cases} g b_0 = g\, g^{x_0} = g^{x_0+1} \cdot a^0 = g^{x_0+1} a^{y_0} & b_0 \in G_1 \\ b_0^2 = g^{2x_0}\, a^{2\cdot 0} = g^{2x_0} \cdot a^{2y_0} & b_0 \in G_2 \\ a g^{x_0} = g^{x_0} \cdot a^{1+0} = g^{x_0} \cdot a^{1+y_0} & b_0 \in G_3 \end{cases}$$

$g(b_0) = \underline{g^{x_1} a^{y_1}}$

Define $x_1 = \begin{cases} x_0 + 1 & \text{if } b_0 \in G_1 \\ 2x_0 & \text{if } b_0 \in G_2 \\ x_0 & \text{if } b_0 \in G_3 \end{cases}$ $\quad y_1 = \begin{cases} y_0 & \text{if } b_0 \in G_1 \\ 2y_0 & \text{if } b_0 \in G_2 \\ y_0 + 1 & \text{if } b_0 \in G_3 \end{cases}$

$$b_2 = f(b_1) = \begin{cases} g b_1 = g\, g^{x_1} = g^{x_1+1} \cdot a^{y_1} & \text{if } b_1 \in G_1 \\ b_1^2 = g^{2x_1} \cdot a^{2y_1} & \text{if } b_1 \in G_2 \\ a b_1 = g^{x_1}\, a^{y_1+1} & \text{if } b_1 \in G_3. \end{cases}$$

so $b_2 = g^{x_2} a^{y_2}$ where $x_2 = \begin{cases} x_1 + 1 & \text{if } b_1 \in G_1 \\ 2x_1 & \text{if } b_1 \in G_2 \\ x_1 & \text{if } b_1 \in G_3 \end{cases}$

& $y_2 = \begin{cases} y_1 & \text{if } b_1 \in G_1 \\ 2y_1 & \text{if } b_1 \in G_2 \\ y_1 + 1 & \text{if } b_1 \in G_3 \end{cases}$

Thus define (inductively) if $\underline{b_i = g^{x_i} a^{y_i}}$ & $\underset{b_{i+1}}{\underset{\|}{f(b)}} = \underline{g^{x_{i+1}} a^{y_{i+1}}}$

then $x_{i+1} = \begin{cases} x_i + 1 & \text{if } b_i \in G_1 \\ 2x_i & \text{if } b_i \in G_2 \\ x_i & \text{if } b_i \in G_3 \end{cases}$

$y_{i+1} = \begin{cases} y_i & \text{if } b_i \in G_1 \\ 2y_i & \text{if } b_i \in G_2 \\ y_i + 1 & \text{if } b_i \in G_3 \end{cases}$

Suppose $\boxed{b_{k+i} = b_i}$ $\quad (i \neq 0) \quad i, k$ smallest.

Then

$$g^{x_{i+k}} a^{y_{i+k}} = g^{x_i} a^{y_i} \quad \text{Also} \quad a = g^x \text{ (say)}$$

$$\text{So } g^{(x_{i+k} - x_i)} = a^{(y_i - y_{i+k})}$$
$$= g^{x(y_i - y_{i+k})}$$

If $x_{i+k} - x_i = x(y_i - y_{i+k})$ then the above holds (1)

So $x = (y_i - y_{i+k})^{-1}(x_{i+k} - x_i)$ if $(y_i - y_{i+k})^{-1}$ exists.

If $(y_i - y_{i+k})^{-1}$ does not exist then do (1) & find which x satisfies $a = g^x$

Examples: $G = \mathbb{Z}_{23}^{\times} = \{1, 2, \ldots, 22\} = \langle 5 \rangle$

$g = 5$

Find $\log_5 18$

Define $G_1 = \{1, 2, \ldots, 7\}$, $G_2 = \{8, 9, \ldots, 14\}$, $G_3 = \{15, 16, \ldots, 22\}$

Choose $x_0 = 2$

$b_0 = 5^{x_0} = 5^2 = 25 = 2 \in G_1$ $\quad 5^{2} \cdot 18^0$ $\quad x_1 = 2+1 = 3, y_1 = 0$

$b_1 = g^{x_1} a^{y_1} = 5^3 18^0 = 2 \times 5 = 10 \in G_2 \rightarrow x_1 = 2+1 = 3$

$b_2 = 5^{2x_1} a^{2y_1} = 5^{(2\times 3)} \cdot 18^{2\times 0} = 10^2 = 100 = 8 \in G_2 \quad x_2 = 6, y_2 = 0$

$b_3 = 5^{2\times x_2} \cdot 18^{2\times y_2} = 5^{(2\times 6)} = 8^2 = 64 = 18 \in G_3 \quad x_3 = 12, y_3 = 0$

$b_4 = 5^{x_3} \cdot 18^{1+y_3} = 5^{(12)} \times 18^{(1+0)} = 18 \times 18$
$= (-5) \times (-5)$ $\quad x_4 = 12 \quad y_4 = 1$
$= 25$
$= 2 \pmod{23}$

$b_4 = b_0$

$$g^{x_4} a^{y_4} = g^{x_0} a^{0}$$

$$\text{So } g^{x_4 - x_0} = a^{-y_4} = g^{x(-1)}$$

$$\Rightarrow g^{12-2} = g^{-x} \cancel{\Rightarrow x =} \text{ So } x = -10$$

$$= 22 - 10$$

$$= \cancel{13}\, 12$$

$$\boxed{5^{22} = 1} \bmod 23$$