Discrete Logarithms (D.L.)

- p prime
  $\alpha, \beta (\neq 0)$ integers mod p and suppose
  $$\beta \equiv \alpha^{x} \pmod p$$
- The problem of finding x is called <u>discrete log problem</u>

- If n is the smallest +ve integer s.t.
  $\alpha^{n} \equiv 1 \pmod p$, we may assume $0 \leq x < n$

we denote $x = L_\alpha(\beta) :=$ discrete log of β w.r.t. to α

Example $p = 11$, $\alpha = 2$

$$2^6 \equiv 9 \pmod{11} \Rightarrow L_2(9) = 6$$

Of course $2^{6} \equiv 2^{16} \equiv 2^{26} \equiv 9 \pmod{11}$
so we take smallest 6 out of 6, 16, 26.
(could be true as does 6 mod 10)

- Often α primitive root mod p ($\Rightarrow$ every β is a power of $\alpha \pmod p$). If α is not prime. root then disc. log will not be defined for certain values.

- If α is a primitive root mod p,
  $$L_\alpha(\beta_1\beta_2) = L_\alpha(\beta_1) + L_\alpha(\beta_2) \pmod{p-1}$$

- For small p using Exhaustive search one can compute D.L.

$\boxed{\text{Computing D.L.}}$

$\boxed{\text{Idea}}$ $\because$ α is p.e. mod p

$$\Rightarrow o(\alpha) = p-1$$

$$\Rightarrow \alpha^{m_1} \equiv \alpha^{m_2} \pmod{p} \Leftrightarrow m_1 \equiv m_2 \pmod{p-1}$$

Assume that $\beta \equiv \alpha^{x}, 0 \le x < p-1$

find x?

it is easy to determine $x \pmod 2$

Note $\left(\alpha^{(p-1)/2}\right)^2 \equiv \alpha^{p-1} \equiv 1 \pmod{p}$

$$\therefore \alpha^{(p-1)/2} \equiv \pm 1 \pmod{p}$$

However $p-1$ is the smallest exponent to yield $+1$

$$\therefore \alpha^{(p-1)/2} \equiv -1 \pmod{p}$$

Now $\beta \equiv \alpha^{x} \pmod{p}$

$$\Rightarrow \beta^{(p-1)/2} \equiv \alpha^{x(p-1)/2} \equiv (-1)^{x} \pmod{p}$$

$\therefore$ if $\beta^{(p-1)/2} \equiv +1$ then x is even
$\equiv -1$ then x is odd.

$\boxed{\text{Example}}$ $2^{x} \equiv 9 \pmod{11}$

$$\because \beta^{(p-1)/2} \equiv 9^5 \equiv 1 \pmod{11}$$

$\therefore x$ must be ~~an~~ even

(Infact $x = 6$)

THE POHLIG-HELLMAN ALGO

let $p-1 = \prod_i q_i^{r_i}$

prime factor $q^r \mid (p-1)$ $\qquad L_\alpha(\beta) \pmod{q^r}$

Write $x = x_0 + x_1 q + x_2 q^2 + \cdots \qquad 0 \le x_i \le q-1$

We will compute $x \pmod{q^r}$

$$x\left(\frac{p-1}{q}\right) = x_0\left(\frac{p-1}{q}\right) + (p-1)(x_1 + x_2 q + x_3 q^2 + \cdots)$$

$$= x_0\left(\frac{p-1}{q}\right) + (p-1)\cdot n \quad (n \text{ integer})$$

Now $\qquad \beta \equiv \alpha^x$

$$\Rightarrow \beta^{(p-1)/q} \equiv \alpha^{x(p-1)/q} = \alpha^{x_0(p-1)/q}\left(\alpha^{p-1}\right)^n$$

$$\equiv \alpha^{x_0(p-1)/q} \pmod p$$

$(\because \alpha^{p-1} \equiv 1 \pmod p)$ F.L.T.

To find x_0, look at the powers $\alpha^{k(p-1)/q} \pmod p$

$k = 0, 1, 2, \ldots, q-1$

until one of them yields $\beta^{(p-1)/q}$

then $x_0 = k$

[Note that $\because \alpha^{m_1} \equiv \alpha^{m_2} \Leftrightarrow m_1 \equiv m_2 \pmod{p-1}$ & $\because$ exponents $k(p-1)/q$ are distinct mod $p-1$, $\exists !\, k$]

Assume $q^2 \mid (p-1)$ let

$$\beta_1 \equiv \beta\alpha^{-x_0} \equiv \alpha^{q(x_1 + x_2 q + \cdots)} \pmod p$$

$$\Rightarrow \beta_1^{(p-1)/q^2} \equiv \alpha^{(p-1)(x_1+x_2q+\cdots)/q}$$

$$\equiv \alpha^{x_1(p-1)/q} \cdot (\alpha^{p-1})^{x_2+x_3q+\cdots}$$

$$\equiv \alpha^{x_1(p-1)/q} \pmod p$$

To find x_1 ~~see~~ look at the powers

$$\alpha^{k(p-1)/q} \pmod p, \quad k = 0, 1, 2, \ldots, q-1$$

until one of them yields $\beta_1^{(p-1)/q^2}$

Then $x_1 = k$

If $q^3 \mid (p-1)$ let $\beta_2 \equiv \beta_1 \alpha^{-x_1 q}$

$\Rightarrow$ raise to power $(p-1)/q^3$ find x_2 & so on.
continue until we find q^{r+1} does not divide $p-1$
we have find $x_0, x_1, \ldots, x_{r-1}$ so we know $x \pmod{q^r}$

Repeat for all prime factors of $p-1$

$\Rightarrow$ we get $x_i \bmod q_i^{r_i}$ $\forall i$ using CRT

$x \bmod p-1$ we find x.

$\boxed{\text{Example}}$ $p = 41$, $\alpha = 7$ & $\beta = 12$

Solve $7^x \equiv 12 \pmod{41}$

Note $41 - 1 = 2^3 \cdot 5$

let $q = 2$ lets find $x \bmod 2^3$

$$x = x_0 + 2x_1 + 4x_2 \pmod 8$$

To start $\beta^{(p-1)/2} \equiv 12^{20} \equiv 40 \equiv -1 \pmod{41}$

and $\alpha^{(p-1)/2} \equiv 7^{20} \equiv -1 \pmod{41}$

$\because \beta^{(p-1)/2} \equiv \left(\alpha^{(p-1)/2}\right)^{x_0} \pmod{41}$

$\Rightarrow x_0 = 1$

Next $\beta_1 \equiv \beta \alpha^{-x_0} \equiv 12 \cdot 7^{-1} \equiv 31 \pmod{41}$

Also, $\beta_1^{(p-1)/2^2} \equiv 31^{10} \equiv 1 \pmod{41}$

$\because \beta_1^{(p-1)/2^2} \equiv \left(\alpha^{(p-1)/2}\right)^{x_1} \pmod{41}$

we get ~~x_0~~ $x_1 = 0$

Continuing we have

$\beta_2 = \beta_1 \alpha^{-2x_1} \equiv 31 \cdot 7^0 \equiv 31 \pmod{41}$

and $(\beta_2)^{(p-1)/2^3} \equiv 31^5 \equiv -1 \equiv \left(\alpha^{(p-1)/2}\right)^{x_2} \pmod{41}$

$\Rightarrow x_2 = 1$

$\therefore x \equiv x_0 + 2x_1 + 4x_2 \equiv 1 + 4 \equiv 5 \pmod{8}$ ✓

let $q = 5$ let's find x mod 5

$\beta^{(p-1)/5} \equiv 12^8 \equiv 18 \pmod{41}$

and $\alpha^{(p-1)/q} \equiv 7^8 \equiv 37 \pmod{41}$

Trying possible values of k yields

$37^0 \equiv 1,\ 37^1 \equiv 37,\ 37^2 \equiv 16,\ 37^3 \equiv 18$

$37^4 \equiv 10 \pmod{41}$

$\therefore 37^3$ gives the answer so $x \equiv 3 \pmod{5}$

$\because \therefore x \equiv 5 \pmod{8}$ and $x \equiv 3 \pmod{5}$

b/y CRT $x \equiv 13 \pmod{40}$ $\therefore x = 13$

As $7^{13} \equiv 12 \pmod{41}$ ☒

Index Calculus Method

Trying to solve $\beta \equiv \alpha^{x} \pmod{p}$

$p \to$ large prime

$\alpha \to$ p. root

Precomputation step $B \to$ bound

let $p_1, p_2, \ldots, p_m$ primes $< B$

factor base

- Compute $\alpha^{K} \pmod{p}$ for several values of K
- For each such no. try to write it as a $\times$ of primes $< B$

if this is not the case discard α^{K}.

$\therefore$ if $\alpha^{K} \equiv \prod p_i^{a_i} \pmod{p}$ then

$$K \equiv \sum a_i L_\alpha(p_i) \pmod{p-1}$$

When we have enough relations we can solve for

$$L_\alpha(p_i) \ \forall i$$

Now for random integers r

- compute $\beta\alpha^{r} \pmod{p}$

try to write as a $\times$ of primes $< B$

if we succeed $\beta\alpha^{r} \equiv \prod p_i^{b_i} \pmod{p}$

$$\Rightarrow L_\alpha(\beta) \equiv -r + \sum b_i L_\alpha(p_i) \pmod{p-1}$$

p shd be moderate size.

$\boxed{\text{Example}}$ $p = 131$ $\alpha = 2$ let $B = 10$

$\therefore$ factor base $2, 3, 5, 7$

$\Rightarrow$ $2^1 \equiv 2 \pmod{131}$

$2^8 \equiv 5^3 \pmod{131}$

$2^{12} \equiv 5 \cdot 7 \pmod{131}$

$2^{14} \equiv 3^2 \pmod{131}$

$2^{34} \equiv 3 \cdot 5^2 \pmod{131}$

$\therefore$ $1 \equiv L_2(2) \pmod{130}$

$8 \equiv 3L_2(5) \pmod{130}$

$12 \equiv L_2(5) + L_7(7) \pmod{130}$

$14 \equiv 2L_2(3) \pmod{130}$

$34 \equiv L_2(3) + 2L_2(5) \pmod{130}$

Using (2), $L_2(5) \equiv 46 \pmod{130}$ subst. into (3)

$L_2(7) \equiv -34 \equiv 96 \pmod{130}$

4th yields $L_2(3) \pmod{65}$ $\because \gcd(2, 130) \neq 1$

$\Rightarrow$ two choices of $L_2(3) \pmod{130}$

to see which one works

Using 5th. $L_2(3) \equiv 72 \pmod{130}$

Now to find $L_2(37)$ trying random choices

$37 \cdot 2^{43} \equiv 3 \cdot 5 \cdot 7 \pmod{131}$

$\therefore L_2(37) \equiv -43 + L_2(3) + L_2(5) + L_2(7)$

$\equiv 41 \pmod{130}$

$\therefore L_2(37) = 41.$

▨