Finding discrete log by Index calculus Alg in $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$

$G = \mathbb{Z}_p^\times = \{1, 2, \dots, p-1\} = \langle g \rangle$ For $a \in G$, $\log_g a$

i.e. $x \in \{1, 2, \dots, p-2, 0\}$ s.t. $g^x = a$ $g^{p-1} = e$

Index calculus method is a probabilistic method to find discrete log in $\mathbb{Z}_p^\times$.

How it works

Consider a set $B = \{q_1, q_2, \dots, q_r\}$ where q_i is a prime preferably first r primes, sometimes one of them is -1.

B is ~~not~~ referred to as a factor base

First we find $\log_g q_i$ which done relatively

↳ Pick $z_i \in \mathbb{N}$ for $1 \le i \le r$ s.t. g^{z_i} is smooth wrt B

i.e. g^{z_i} is a product of primes belonging to B (modulo p)

Say $g^{z_i} = q_1^{a_{i1}} \cdot q_2^{a_{i2}} \cdot \dots \times q_r^{a_{ir}} \pmod p$

set $x_j = \log_g q_j$ Then $g^{z_i} = g^{\sum_{j=1}^{r} a_{ij} x_j} \pmod p$

$g^{x_j} = q_j \Leftrightarrow x_j = \log_g q_j$ so that $\sum_{j=1}^{r} a_{ij} x_j = z_i \bmod p-1$, $1 \le i \le r$

By solving this system we find x_i for $1 \le i \le r$ which are $\log_g q_i$

Next finding $\log_g a$:

Factorize a in $\mathbb{Z}_p^\times$ & check if it is smooth wrt B.

Find $y \in \mathbb{N} \cup \{0\}$, s.t. $a g^y$ is smooth wrt B.

Suppose we get such a y. Then

$$a g^y = q_1^{s_1} q_2^{s_2} \cdots q_r^{s_r}$$

$$= g^{s_1 x_1} g^{s_2 x_2} \cdots g^{s_r x_r} = g^{\sum_{i=1}^{r} s_i x_i}$$

$$a = g^{\sum_{i=1}^{r} s_i x_i - y} \quad \text{so} \quad \log_g a = \sum_{i=1}^{r} s_i x_i - y \ \underline{\bmod p-1}$$

Since we know x_i & s_i for $1 \le i \le r$, y is computed.

E.g. $p = 2027$. Then $\langle 2 \rangle = \mathbb{Z}_{2027}^{\times}$

Choose $\mathcal{B} = \{2, 3, 5, 7, 11\}$, with $2 = q_1$, $3 = q_2$, $5 = q_3$, $7 = q_4$, $11 = q_5$.

$$2^{10} = 1024$$
$$2^{11} = 2048$$
$$2048 - 2027 = 21$$

$2^1 = 2$

$x_1 = \log_2 2 = 1$

Have to find $\underline{x_2, x_3, x_4, x_5}$,

$$2^{11} = 21 = 3 \times 7 \mod 2027$$
$$2^{293} = 63 = 3^2 \times 7 \mod 2027$$
$$2^{983} = 385 = 5 \times 7 \times 11 \quad " \quad "$$
$$2^{1318} = 1408 = 2^7 \times 11 \quad " \quad "$$
$$2^{1593} = 33 = 3 \times 11 \quad " \quad "$$

[$2^{11} = 2^0 \times 3^1 \times 5^0 \times 7^1 \times 11^0$, with $3 = 2^{x_2}$, $7 = 2^{x_4}$]

$$\left.\begin{aligned} x_2 + x_4 &= 11 \\ 2x_2 + x_4 &= 293 \end{aligned}\right\} \quad \begin{aligned} x_2 &= 282 \\ x_4 &= 11 - 282 + 2026 \\ &= -271 + 2026 \\ &= 1755 \end{aligned}$$

$x_3 + x_4 + x_5 = 983$, $\quad 7x_1 + x_5 = 1318$, $\quad x_2 + x_5 = 1593$

$7x_1 = 7$

$x_1 = 1$

$x_5 = 1593 - 282$

$= \underline{1311}$

$x_3 = 983 - 1755 - 1311 + 2026 \times 2$

$= 1969$ in $\mathbb{Z}_{2027}^{\times}$

So $\log_2 2 = 1$, $\log_2 3 = 282$, $\log_2 5 = 1969$, $\log_2 7 = 1755$

$\log_2 11 = 1311$

x_2 x_3

Case 1 $a = 12 = 2^2 \times 3^1$ which is smooth wrt. B.

$s_1 = 2$, $s_2 = 1$, $s_4 = s_5 = s_3 = 0$

$$\log_2 a = \sum_{i=1}^{5} s_i x_i - y$$

$$= 2 \times 1 + 1 \times 282$$

$$= 284$$

Case 2 $a = 65 = 5 \times 13$ mod 2027 not smooth wrt. B.

$65 \times 2 = 2 \times 5 \times 13$ mod 2027 not smooth,

$65 \times 2^{28} = 125 = 5^3$ mod 2027 which is smooth wrt. B.

$y = 28$

So $\log_2 65 = \sum s_i x_i - y$ where $s_i = 0$ for $i \neq 3$ & $s_3 = 3$

$= 3 \times 1969 - 28$

$= 5907 - 28$

$= 5879$ mod 2026

$= 1827$ mod 2026.

4059