The Discrete Log Problem

Definition: If $b \in G = (\mathbb{Z}/m\mathbb{Z})^\times$, then

$$\langle b \rangle \;=\; \{b^n : n \in \mathbb{Z}\} \;=\; \{1, b, \ldots, b^n, \ldots\}$$

is called the *cyclic subgroup* of G *generated by* b. If $y \in \langle b \rangle$, then the smallest integer $n \geq 0$ such that

$$y \;=\; b^n \tag{1}$$

is called the *discrete log* of y *to the base* b, and is denoted by $DL_b(y)$. Thus:

$$n \;=\; DL_b(y) \quad \Leftrightarrow \quad y \;=\; b^n,\; n \geq 0 \text{ minimal.}$$

Notes: 1) Throughout, equality means equality in G. Thus, (1) is equivalent to the congruence equation $y \equiv b^n \pmod{m}$.

2) Gauss (1800) used the term "index" in place of "discrete log".

Discrete Log Problem (DLP): Given $b \in G = (\mathbb{Z}/m\mathbb{Z})^\times$ and $y \in \langle b \rangle$, determine the discrete log of y to the base b, i.e., compute $DL_b(y)$.

Remark: It turns out that this is a very hard problem and hence is suitable for use in cryptography.

Example: $m = 5$, so $G = (\mathbb{Z}/5\mathbb{Z})^\times = \{1, 2, 3, 4\}$.

Take $b = 3$. Then $b^2 \equiv 4 \pmod 5$, $b^3 \equiv 2 \pmod 5$, etc. so we we get the following table:

n	0	1	2	3	4	5	6	7	8
b^n	1	3	4	2	1	3	4	2	1

Note that the powers repeat after a cycle of 4. Thus $\langle 3\rangle = \{1, 3, 4, 2\} = G$, and the discrete logs are:

y	1	3	4	2
$DL_3(y)$	0	1	2	3

or

y	1	2	3	4
$DL_3(y)$	0	3	1	2

Remark: 1) The table of all discrete logs of the elements of $\langle b\rangle$ is called a *log-table* for the base b.

2) Clearly, if we can make a log-table, then the Discrete Log Problem can be solved.

Question: What is the size of the log-table or, equivalently, of the cyclic subgroup $\langle b\rangle$?

Definition: The *order* of $b \in G = (\mathbb{Z}/m\mathbb{Z})^\times$ is the smallest integer $n \geq 1$ such that $b^n = 1$. We denote this integer by $|b|$ or by $\mathrm{ord}(b)$.

Example: By the above table, $\mathrm{ord}(3 \bmod 5) = 4$.