Discrete logarithm

The group $G = \langle Z_p^*, \times \rangle$ has several properties

1. Its elements include all integers from 1 to $p-1$
2. It always has primitive roots
3. It is cyclic
4. The primitive roots can be thought as the base of logarithm. If group has k primitive roots, calculation can be done in k different bases

$y = g^x \bmod n$

$\therefore x = \log_g y$

→ for any element y in the set there is another element x that is the log of y in base g.

→ This type of logarithm is called discrete logarithm

→ We use notation L_g to show that base is g

Page No.
Date

Solution to modular logarithm using Discrete logs

How to solve problems of type $y = a^x \bmod n$ when y is given and we need to find x

Tabulation of Discrete logarithms

→ This type of table can be precalculated and saved

y	1	2	3	4	5	6
$x = L_3 y$	6	2	1	4	5	3
$x = L_5 y$	6	4	5	2	1	3

Discrete logarithm for $G = \langle Z_7^*, \times \rangle$

$3^1 = 3^1 \bmod 7 = 3$
$3^2 = 2$
$3^3 = 6$
$3^4 = 4$
$3^5 = 5$
$3^6 = 3^6 \bmod 7 = 1$
$3^7 = 3^7 \bmod 7 = 3$

$5^1 = 5 \bmod 7 = 5$
$5^2 = 25 \bmod 7 = 4$
$5^3 = 6$
$5^4 = 2$
$5^5 = 3$
$5^6 = 1$

Find x in each of following cases

① $4 \equiv 3^x \bmod 7$

$\therefore x = L_3 4 \bmod 7$

$x = 4 \bmod 7$

$3^x = 4$

$\log 3^x = \log 4$

$x \log 3 = \log 4$

$x = \frac{\log 4}{\log 3}$

$x = \log_3 4$

$x = L_3 4$

② $6 \equiv 5^x \bmod 7$

$x = L_5 6 \bmod 7$

$x = 3 \bmod 7$

→ Tabulation and properties of discrete logarithms cannot be used to solve $y = a^x \pmod{n}$ when n is very large. Several algorithms have been devised that use the basic idea of Discrete logarithm to solve the problem