Introduction to Number Theory

Contd..

Discrete Logarithms

Discrete algorithm are fundamental to number of public key cryptosystem including Diffie-Hellman key exchange and digital signature algorithm.

Discrete Logarithms

Exponentiation: $y = a^x \quad \rightarrow \quad$ **Logarithm:** $x = \log_a y$

Order of the Group

- What is the **order of group** $G = \langle Z_{21}{*}, \times \rangle$? $|G| = \varphi(21) = \varphi(3) \times \varphi(7) = 2 \times 6 = 12$. There are 12 elements in this group: 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, and 20. All are relatively prime with 21.

Order of an Element

- Find the **order of all elements** in G = <Z_{10}*, ×>.
- This group has only φ(10) = 4 elements: 1, 3, 7, 9. We can find the order of each element by trial and error.
- a. $1^1 \equiv 1 \bmod (10) \rightarrow$ ord(1) = 1.
- b. $3^4 \equiv 1 \bmod (10) \rightarrow$ ord(3) = 4.
- c. $7^4 \equiv 1 \bmod (10) \rightarrow$ ord(7) = 4.
- d. $9^2 \equiv 1 \bmod (10) \rightarrow$ ord(9) = 2.

Euler’s Theorem

- $G = <Z_8*, \times>$. $a^i = x (\text{mod } 7)$. Here $\varphi(8) = 4$. The elements are 1,3,5,7
- “If a is the member of $G = <Z_n*, \times>$ then $a^{\varphi(n)} = 1 \text{ mod } n$ holds when $i = \varphi(n)$”

Finding the orders of elements

	$i = 1$	$i = 2$	$i = 3$	$i = 4$	$i = 5$	$i = 6$	$i = 7$
$a = 1$	**x: 1**	x: 1	x: 1	x: 1	x: 1	x: 1	x: 1
$a = 3$	x: 3	**x: 1**	x: 3	x: 1	x: 3	x: 1	x: 3
$a = 5$	x: 5	**x: 1**	x: 5	x: 1	x: 5	x: 1	x: 5
$a = 7$	x: 7	**x: 1**	x: 7	x: 1	x: 7	x: 1	x: 7

Contd..

- *Primitive Roots In the group $G = <Z_n*, \times>$, when the order of an element is the same as $\varphi(n)$, that element is called the primitive root of the group.*

Discrete Logarithms

- Table 9.5 shows the result of $a^i \equiv x \pmod{7}$ for the group $G = <Z_7^*, \times>$. In this group, $\varphi(7) = 6$.

Table 9.5 *Example 9.50*

		$i = 1$	$i = 2$	$i = 3$	$i = 4$	$i = 5$	$i = 6$
	$a = 1$	x: 1	x: 1	x: 1	x: 1	x: 1	x: 1
	$a = 2$	x: 2	x: 4	x: 1	x: 2	x: 4	x: 1
Primitive root →	$a = 3$	x: 3	x: 2	x: 6	x: 4	x: 5	x: 1
	$a = 4$	x: 4	x: 2	x: 1	x: 4	x: 2	x: 1
Primitive root →	$a = 5$	x: 5	x: 4	x: 6	x: 2	x: 3	x: 1
	$a = 6$	x: 6	x: 1	x: 6	x: 1	x: 6	x: 1

Discrete Logarithms

Note:

- **The group G = <Z_n*, ×> has primitive roots only if *n* is 2, 4, p^t, or $2p^t$. (p is prime but not 2).**
- **Examples**

  a. G = <Z_{17}*, ×> has primitive roots, 17 is a prime.
- b. G = <Z_{20}*, ×> has no primitive roots.
- c. G = <Z_{38}*, ×> has primitive roots, 38 = 2 × 19 prime.
- d. G = <Z_{50}*, ×> has primitive roots, $50 = 2 \times 5^2$ and 5 is a prime.

Discrete Logarithms

Note:

- If the group $G = \langle Z_n^*, \times \rangle$ has any primitive root, the number of primitive roots is $\varphi(\varphi(n))$.
- The group $G = \langle Z_{10}^*, \times \rangle$ has two primitive roots because $\varphi(10) = 4$ and $\varphi(\varphi(10)) = 2$. It can be found that the primitive roots are 3 and 7. The following shows how we can create the whole set Z_{10}^* using each primitive root.

$g = 3 \rightarrow$	$g^1 \bmod 10 = 3$	$g^2 \bmod 10 = 9$	$g^3 \bmod 10 = 7$	$g^4 \bmod 10 = 1$
$g = 7 \rightarrow$	$g^1 \bmod 10 = 7$	$g^2 \bmod 10 = 9$	$g^3 \bmod 10 = 3$	$g^4 \bmod 10 = 1$

Discrete Logarithms

- *idea of Discrete Logarithm*
- *Properties of* $G = \langle Z_p^*, \times \rangle$ *:*
- *Its elements include all integers from 1 to* $p - 1$*.*
- *It always has primitive roots.*
- *The elements can be created using* g^x
- ***The primitive roots can be thought as the base of logarithm.***

Discrete logarithm problem

- **Def:** The problem of finding i satisfying the equation

$$b \equiv a^i \pmod{p}$$

given b, p, and $a^i \pmod{p}$ is called the ***discrete logarithm problem***. The exponent **i** is referred to as the discrete logarithm of the number b to the base a(mod p).

Discrete Logarithms

- **The discrete logarithm problem has the same complexity as the factorization problem.**