Introduction to Number Theory

Contd..

Computation of multiplicative inverse modulo n

- Computing inverse in modulo n arithmetic is not as straight forward as in elementary arithmetic.
- Following approaches are possible to compute inverse modulo n :

1. Brute-force, or trial-and-error method
2. **Fermat's theorem, Euler's theorem, extended Euclidean algorithm may be used to compute modular inverse.**

Computing inverses

- Example 1: Given a=3 and n=7, find the multiplicative inverse of a. *By trial-and-error, we can find that the smallest* integer which solves the congruence $3x \equiv 1 \pmod{7}$ is 5.
- Find multiplicative inverse of 7, 3, 4 under modulo 6?

Fermat's Theorem

- **First Version** : If p is prime and a is an integer such that p does not divides a then

$$a^{p-1} \equiv 1 \pmod{p}$$

- **Second Version** : If p is prime and a is an integer then

$$a^{P} \equiv a \pmod{p} \Rightarrow a \equiv a^{p} \pmod{p}$$

Application-

Exponentiation and inverse - Quickly finds a solution to some exponentiations and inverses.

Contd.

- Find the result of 6^{10} mod 11
- We have 6^{10} mod 11 = 1. This is the first version of Fermat's little theorem where p = 11.
- Find the result of 3^{12} mod 11
- Here the exponent (12) and the modulus (11) are not the same

Multiplicative Inverses

- a^{-1} (mod p) = a^{p-2} (mod p)   ...if P is prime
- The answers to multiplicative inverses modulo a prime can be found without using the extended Euclidean algorithm:

a. $8^{-1} \bmod 17 = 8^{17-2} \bmod 17 = 8^{15} \bmod 17 = 15 \bmod 17$

b. $5^{-1} \bmod 23 = 5^{23-2} \bmod 23 = 5^{21} \bmod 23 = 14 \bmod 23$

c. $60^{-1} \bmod 101 = 60^{101-2} \bmod 101 = 60^{99} \bmod 101 = 32 \bmod 101$

Euler's Theorem

- First Version : If a and n are co-prime, then

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

- Second Version : if a<n, and k is any integer, then

$$a^{k \times \phi(n) + 1} \equiv a \pmod{n}$$

Contd.

- Find the result of 6^{24} mod 35.
- We have 6^{24} mod 35 = $6^{\varnothing(35)}$ mod 35 = 1.
- Find the result of 20^{62} mod 77

If we let $k = 1$ on the second version, we have

$$20^{62} \bmod 77 = (20 \bmod 77)\ (20^{\phi(77)+1} \bmod 77) \bmod 77$$
$$= (20)(20) \bmod 77 = 15.$$

Contd.

- Euler's theorem can be used to find multiplicative inverses modulo a composite.

$$a^{-1} \bmod n = a^{\phi(n)-1} \bmod n$$

Contd.

- Examples:

a. $8^{-1} \bmod 77 = 8^{\phi(77)-1} \bmod 77 = 8^{59} \bmod 77 = 29 \bmod 77$

b. $7^{-1} \bmod 15 = 7^{\phi(15)-1} \bmod 15 = 7^{7} \bmod 15 = 13 \bmod 15$

c. $60^{-1} \bmod 187 = 60^{\phi(187)-1} \bmod 187 = 60^{159} \bmod 187 = 53 \bmod 187$

CHINESE REMAINDER THEOREM

- The Chinese remainder theorem (CRT) is used to solve a set of congruent equations with one variable but different moduli, which are relatively prime, as shown

  below:

$$
\begin{gathered}
x \equiv a_1 \pmod{m_1} \\
x \equiv a_2 \pmod{m_2} \\
\cdots \\
x \equiv a_k \pmod{m_k}
\end{gathered}
$$

Solution To Chinese Remainder Theorem

1. Find $M = m_1 \times m_2 \times \ldots \times m_k$. This is the common modulus.
2. Find $M_1 = M/m_1$, $M_2 = M/m_2$, …, $M_k = M/m_k$.
3. Find the multiplicative inverse of M_1, M_2, …, M_k using the corresponding moduli (m_1, m_2, …, m_k). Call the inverses M_1^{-1}, M_2^{-1}, …, M_k^{-1}.
4. The solution to the simultaneous equations is

$$x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \cdots + a_k \times M_k \times M_k^{-1}) \bmod M$$

Contd.

solution to the simultaneous equations:

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$

- We follow the steps.
- 1. $M = 3 \times 5 \times 7 = 105$
- 2. $M1 = 105 / 3 = 35$, $M2 = 105 / 5 = 21$, $M3 = 105 / 7 = 15$ and **The inverses are $M_1^{-1} = 2, M_2^{-1} = 1, M_3^{-1} = 1$**
- 3. $x = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105 = 23 \bmod 105$

Contd.

- Solve

$x \equiv 1 \pmod{7}$, $x \equiv 6 \pmod{22}$, $x \equiv 11 \pmod{13}$ by Chinese remainder theorem.

Answer: $x \equiv 50 \pmod{2002}$,

Groups

- Definition: A non empty set G with an binary operation '*' is said to form a commutative group w.r.t '*' , if

1.) Closure holds in G:

i.e., $a*b \in G, \forall\ a, b \in G$.

2.) Associativity holds in G:

$(a*b)*c= a*(b*c), \forall\ a, b, c \in G$.

3.) Existence of identity element:

$\exists$ an unique element $e \in G$, such that

$a*e =e*a=a, \forall\ a \in G$.

4.) Existence of inverse:

$\exists\ b \in G$, such that $a*b=b*a=e, \forall\ a \in G$.

Contd..

5.) Commutativity holds in G:

$a*b = b*a, \forall a, b \in G.$

Examples:

1.) Set of integers is a group w.r.t to addition.

2.) Z_n is a group w.r.t to addition modulo n. (Ex: Z_{10}

3.) Z_n is not a group w.r.t to multiplication modulo n, when n is composite, as all elements don't have multiplicative inverse. Try for Z_{10}

if encryption define as c=a*b where **a** is plain text and **b** is key from $Z_{10.\ \text{than}}$ decryption is…..

Contd.

- For a group G with a finite number of elements, the order of the group is defined to be the number of elements, written as O(G).

Field

- <u>Definition</u> : A non empty set F equipped with two binary operations '+' and '.' is called field if :-
  F forms a group w.r.t to two binary operations '+' and '.'
- F has the properties: **Closure, Associativity, Commutativity** w.r.t binary operations '+' and '.' and having both **additive and multiplicative identities (0 and 1),** as well as both **additive and multiplicative inverses for all the non-zero elements .**
- **Ex Z**