Introduction to Number Theory

Debdeep Mukhopadhyay

Assistant Professor
Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur
INDIA -721302

Objectives

- **Congruences: Modular Arithmetic**
- **Euler Totient Function**
- **Fermat's Little Theorem**

Congruences

- We say that a is congruent to b modulo m, and we write a ≡ b mod m, if m divides b-a.

- Example: -2 ≡ 19 (mod 21), 20 ≡ 0 (mod 10).

- Congruence modulo m is an equivalence relation on the integers.
  – any integer is congruent to itself modulo m (reflexivity)
  – a ≡ b mod m, implies that b ≡ a mod m (symmetry)
  – a ≡ b mod m and b ≡ c mod m implies a ≡ c mod m (transitivity)

The following are equivalent

- a ≡ b mod m
- There is k ε Z, with a = b + km
- When divided by m, both a and b leave the same remainder.
- Equivalence Class of *a modulo m* consists of all integers that are obtained by adding a with integral multiples of m
  – called residue class of *a mod m*

Example

- **Residue class of 1 mod 4:**
  {1, 1±4, 1±2*4, 1±3*4,…}
- **The set of residue classes mod m is denoted by Z/mZ.**
  - **it has m elements, 0, 1, …, m-1**
  - **this is called a complete set of incongruent residues (complete system)**
  - **Examples for complete system for mod 5 is:**
    {0, 1, …, 4}, {-12, -15, 82, -1, 31} etc.

Theorem

- **a≡b mod m, and c≡d mod m, implies that -a≡-b mod m, a + c ≡ b + d mod, and ac ≡ bd mod m.**

Example

Prove that $2^{2^5} + 1$ is divisible by 641.

Note that: $641 = 640 + 1 = 5*2^7 + 1$.

Thus, $5*2^7 \equiv -1 \mod 641$.

$\Rightarrow (5*2^7)^4 \equiv (-1)^4 \mod 641$

$\Rightarrow 5^4*2^{28} \equiv 1 \mod 641$

$\Rightarrow (625 \mod 641)*2^{28} \equiv 1 \mod 641$

$\Rightarrow (-2^4)*2^{28} \equiv 1 \mod 641$

$\Rightarrow 2^{32} \equiv -1 \mod 641$

Semigroups

- **If X is a set, a map ○: X x X → X, which transforms an element (x_1,x_2) to the element $x_1 \circ x_2$ is called an operation.**
- **The sum of the residue classes a+mZ and b+mZ is (a+b)+mZ.**
- **The product of the residue classes a+mZ and b+mZ is (a.b)+mZ**

Semigroups

- An operation ○ on X is associative if (a ○ b) ○ c=a ○ (b ○ c), for all a, b, c in X.
- It is commutative if a ○ b = b ○ a for all a, b in X.
- A pair (H, ○) consisting of a set H and an associative operation ○ on H is called a semigroup.
- The semigroup is called abelian or commutative if the operation ○ is commutative.
  - Example: (Z,+), (Z,.), (Z/mZ,+), (Z/mZ, .)

Implications

- Let (H, ○) be a semigroup.
- Set, a^1= a, a^{n+1}=a ○ a^n for a in H and natural value of n.
- Thus, $a^n \circ a^m = a^{n+m}$, $(a^n)^m=a^{nm}$, a in H, n and m are natural values.
- If a, b are in H, and a ○ b=b ○ a, then:

$$(a \circ b)^n=a^n \circ b^n$$

Monoid

- A neutral element of the semigroup (H, ○) is an element e in H, which satisfies e ○ a = a ○ e = a, for all a in H.
- If the semigroup contains a neutral element it is called monoid.
- A semigroup has at most one neutral element.
- If e ε H is a neutral element of the semigroup (H, ○), then b ε H is called an inverse of a if a ○ b=b ○ a = e.
- If a has an inverse, then a is called invertible in the semigroup H.
- In a monoid, each element has at most one inverse.

Examples

- (Z,+): Neutral element: 0, inverse: -a.
- (Z,.): Neutral element: 1, only invertible elements are +1 and -1.
- (Z/mZ,+): Neutral element: mZ, inverse: -a+mZ. Often is referred as Z_m.
- (Z/mZ,.): Neutral element: 1+mZ, inverse: those elements, t which have gcd(t,m)=1

Groups

- A group is a monoid in which every element is invertible.
- The group is commutative or abelian if the monoid is commutative.
- Example:
  - (Z,+) is an abelian group.
  - (Z,.) is not a group.
  - (Z/mZ,+) is an abelian group.

Residue class ring

- A ring is a triplet (R, +, .) such that (R,+) is an abelian group and (R,.) is a monoid.
- In addition: x.(y+z)=(x.y)+(x.z) for x, y, z ε R.
- The ring is called commutative if the semigroup (R,.) is commutative.
- A unit element of the ring is a neutral element of the semigroup (R,.)

Unit Group

- **Let R be a ring with unit element.**
- **An element a of R is called invertible or a unit, if it is invertible in the multiplicative semigroup of R.**
- **The element a is called a zero divisor if it is nonzero and there is a nonzero b in R, st. ab = 0 or ba = 0.**
- **Units of a commutative ring form a group. This is called the unit group of the ring, denoted by R*.**

Zero Divisors

- **The zero divisors of the residue class Z/mZ is a + mZ, with $1 < \gcd(a,m) < m$.**
- **Proof: If a+mZ is a zero divisor of Z/mZ, then there is an integer b with $ab \equiv 0$ mod m, but neither a nor b is 0 mod m. Thus, m|ab, but neither a nor b $\Rightarrow 1 < \gcd(a,m) < m$.**
- **Conversely, if $1 < \gcd(a,m) < m$, then define $b = m/\gcd(a,m)$, then both a and b are nonzero mod m. But $ab \equiv 0 \pmod{m}$. Thus a+mZ is a zero divisor of Z/mZ.**
- **Corollary: If p is prime, then Z/pZ has no zero divisors.**

Field

- **A field is a commutative ring (R,+,.) in which every element in the semigroup (R,.) is invertible.**
- **Example:**
  - **the set of integers is not a field.**
  - **the set of real and complex numbers form a field.**
  - **the residue class modulo a prime number except 0 is a field.**

Euler's Totient function

- **Suppose a≥1 and m≥2 are integers. If gcd(a,m)=1, then we say that a and m are relatively prime.**
- **The number of integers in Z_m (m>1), that are relatively prime to m and** does not exceed m **is denoted by Φ(m), called Euler's Totient function or phi function.**
- **Φ(1)=1**

Example

- m=26 => Φ(26)=13
- If p is prime, Φ(p)=p-1
- If n=1,2,…,24 the values of Φ(n) are:
  - 1,1,2,2,4,2,6,4,6,4,10,4,12,6,8,8,16,6,18,8, 12,10,22,8
  - Thus we see that the function is very irregular.

Properties of Φ

- If m and n are relatively prime numbers,
  - Φ(mn)= Φ(m) Φ(n)
- Φ(77)= Φ(7 x 11)=6 x 10 = 60
- Φ(1896)= Φ(3 x 8 x 79)=2 x 4 x 78 =624
- This result can be extended to more than two arguments comprising of pairwise coprime integers.

Results

- **If there are m terms of an arithmetic progression (AP) and has common difference prime to m, then the remainders form Z_m.**
- **An integer a is relatively prime to m, iff its remainder is relatively prime to m**
- **If there are m terms of an AP and has common difference prime to m, then there are Φ(m) elements in the AP which are relatively prime to m.**

An Important Result

- **If m and n are relatively prime, Φ(mn)=Φ(m)Φ(n)**

1	**2**	**…**	**k**	**…**	**n**
n+1	**n+2**	**…**	**n+k**	**…**	**n+n**
…					
(m-1)n+1	**(m-1)n+2**	**…**	**(m-1)n+k**	**…**	**(m-1)n+n**

there are Φ(m) elements which are co-prime to m

there are Φ(n) columns in which all the elements are co-prime to n.

contd.

- Thus, there are Φ(n) columns with Φ(m) elements in each which are co-prime to both m and n.
- Thus there are Φ(m) Φ(n) elements which are co-prime to mn.
  - This proves the result…

Further Result

- $\Phi(p^a)=p^a-p^{a-1}$
  - Evident for a=1
  - For a>1, out of the elements 1, 2, …, p^a the elements p, p^2, $p^{a-1}p$ are not co-prime to p^a.

  Rest are co-prime.

  Thus $\Phi(p^a)=p^a-p^{a-1}$

  $=p^a(1-1/p)$

contd.

- $n=p_1^{a1}p_2^{a2}\ldots p_k^{ak}$
- Thus, $\Phi(n)= \Phi(p_1^{a1})\ \Phi(p_2^{a2}) \ldots \Phi(p_k^{ak})$

  $=n(1-1/p_1)(1-1/p_2)\ldots(1-1/p_k)$

Thus, if m=60=4x3x5

$\Phi(60)=60(1-1/2)(1-1/3)(1-1/5)=16$

Fermat's Little Theorem

- If gcd(a,m)=1, then $a^{\Phi(m)}\equiv 1$ (mod m).
- Proof: $R=\{r_1,\ldots,r_{\Phi(m)}\}$ is a reduced system (mod m).
- If gcd(a,m)=1, we see that $\{ar_1,\ldots,ar_{\Phi(m)}\}$ is also a reduced system (mod m).
- It is a permutation of the set R.
- Thus, the product of the elements in both the sets are the same.

  Hence, $a^{\Phi(m)}\ r_1,\ldots,r_{\Phi(m)} \equiv r_1,\ldots,r_{\Phi(m)}$(mod m)

  $\Rightarrow a^{\Phi(m)}\equiv 1$ (mod m)

  Note we can cancel the residues as they are co-prime with m and hence have multiplicative inverse.

Example

- Find the remainder when 72^{1001} is divided by 31.
- Since, $72 \equiv 10$ (mod 31). Hence, $72^{1001} \equiv 10^{1001}$(mod 31).
- Now from Fermat's Theorem, $10^{30} \equiv 1$ (mod 31) [note 31 is prime]
- Raising both sides to the power 33,

$10^{990} \equiv 1$ (mod 31)

Thus,

$10^{1001}=10^{990}10^{8}10^{2}10=1(10^{2})^{4}10^{2}10=1(7)^{4}7.10=49^{2}.7.10=(-13)^{2}.7.10=(14.7).10=98.10=5.10=19$ (mod 31).

Points to Ponder

- Find the least residue of 7^{973} (mod 72) [Note 72 is not a prime number].

References

- S G Telang, “Number Theory”, TMH
- Johannes A. Buchmann, “Introduction to Cryptography”, Springer

Next Days Topic

- Probability and Information Theory