Scribe: Cryptography and Network Security (Class.1.D)

Venu Gopal Bandhakavi

4-Sep-2020

1 Introduction

Number theory is a field of mathematics which studies integers and their properties. Number theory is widely used in cryptography for encryption and decryption purposes.

2 Congruences

We say that a is congruent to b modulo m i.e $a \equiv b$ (mod m), if m divides $a - b$. The number m is said to be the modulus.

Examples:

$$5 \equiv 15 \ (mod\ 10)$$

$$-1 \equiv 99 \ (mod\ 100)$$

It can be also said that a is the remainder obtained when b is divided by m.

$$a = q * m + b$$

a congruent to b modulo m is also equivalent to:

- $a \equiv b \ (mod\ m)$
- $a = q * m + b$, where q is quotient and a is the remainder.
- $m \mid (a - b)$ means m divides $(a - b)$.
- 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 .

2.1 Equivalence Relation

A relation R is said to be equivalence relation if it is a:

1. Reflexive Relation: a binary relation R over a set X is reflexive if it relates every element of X to itself. $\forall x \in X : xRx$

2. Symmetric Relation: Let A be a set in which the relation R defined. Then R is said to be a symmetric relation, if $(a, b) \in R \Rightarrow (b, a) \in R$, that is, $aRb \Rightarrow bRa$ for all $(a, b) \in R$.

3. Transitive Relation : A relation R over set A is said to be trasitive relation if for all elements $x, y, z \in A$ if x relates y and y relates z then x also relates z. $\forall x, y, z \in A : (xRy) \wedge (yRz) \Rightarrow (xRz)$.

Congruence modulo m is an equivalence relation on the set $\mathbb{Z}$. We can prove it by showing that it satisfies all the three requirements which are:

1. Reflexive nature : $a \equiv a \ (mod\ m)$ as $m \mid (a - a)$.It is true for all values of $a \in \mathbb{Z}$.

2. Symmetric nature: $\forall (a, b) \in \mathbb{Z}$ if $a \equiv b(mod\ m)$. This means that

$$\begin{align} a &= q * m + b \tag{1} \\ a - b &= q * m, \quad q \in \mathbb{Z} \tag{2} \\ b &= (-q) * m + a, \quad -q \in \mathbb{Z} \tag{3} \end{align}$$

   from (1) and (3) we can see that if $a \equiv b \ (mod\ m)$ then $b \equiv a \ (mod\ m)$.

3. Transitive nature: $x, y, z \in \mathbb{Z}$ where $x \equiv y \ (mod\ m)$ and $y \equiv z \ (mod\ m)$ then

$$\begin{align} x &= q * m + y \tag{4} \\ y &= k * m + z \tag{5} \\ x &= k * m + q * m + z \tag{6} \\ x &= (k + q) * m + z \tag{7} \end{align}$$

   from the above equation we can see that it is a transitive relation.

2.2 Residue Classes

Let R be an equivalence relation then equivalence class of a where $a \in A$ denoted as $[a]$ is defined as:

$$[a] = \{x \in A \mid xRa\}$$

The union of all the equivalence classes is the set over which the relation is defined.The equivalence classes are also called as partitions. Partitions of an equivalence relation are pairwise disjoint. Let relation R have m partitions over set A then:

$$[a_1] \cup [a_1] \cup [a_1] \cup [a_1] \cup .... \cup [a_k] = A$$

$\{[a_1], [a_2], [a_3], ..., [a_m]\}$ are pairwise disjoint.

As Congruence modulus m is also an equivalence relation, $a\ (mod\ m)$ is also an equivalance class.

$$[a] = \{a,\ a \pm 1 * m,\ a \pm 2 * m,\ a \pm 3 * m,\ ....\}$$

$[a]$ is also called as residue class of $a\ (mod\ m)$.For congruence modulus m there will be m residue classes. The residue classes of mod m is denoted by $\mathbb{Z}/n\mathbb{Z}$. The m congruence classes constitute the $\mathbb{Z}/m\mathbb{Z}$.

$\mathbb{Z}/m\mathbb{Z} = \{a_i : [a_i] \text{ is a partition of modulo } m\}$

$\mathbb{Z}/m\mathbb{Z}$ is called a complete set of incongruent resdues(complete system).

For congruence modulo 5 the residue classes are:

$[0] = \{..., -10, -5, 0, 5, 10, ...\}$

$[1] = \{..., -9, -4, 1, 6, 11, ...\}$

$[2] = \{..., -8, -3, 2, 7, 12, ...\}$

$[3] = \{..., -7, -2, 3, 8, 13, ...\}$

$[4] = \{..., -6, -1, 4, 9, 14, ...\}$

The complete system for mod 5 are: $\{0, 1, 2, 3, 4\}, \{-12, -15, 82, -1, 31\}$ and so on.Each element in these complete systems are from different residue class due to which they are incongruent to each other.

2.3 Properties

Some Properties of modulo arithmetic are:

1. $a \equiv b$ (mod m) $\iff$ $b {\equiv} a$ (mod m)
2. $a \equiv b$ (mod m) $\iff$ $-a {\equiv} - b$ (mod m)
3. $a \equiv b$ (mod m) and $c {\equiv} d$ (mod m) implies that $a + c \equiv b\ +\ d$ (mod m)
4. $a \equiv b$ (mod m) and $c \equiv d$ (mod m) implies that $a * c {\equiv} b * d$ (mod m)
5. if $a \equiv b$ (mod m) then $a^n \equiv b^n$ (mod m) where n is a non-negative integer.

Example: Find $7^9 \pmod{11}$

$(7 * (7^4)(7^4)) (\text{mod } 11) = ((-4) * (16)^2 * (16)^2)(\text{mod } 11)$
$((-4) * (25) * (25)) \pmod{11} = ((-4) * 3 * 3) \pmod{11}$
$(-36) \pmod{11} = 8$
$7^9 \pmod{11} = 8$

3 Semigroups

If X is a set, a map $\circ : X$ x $X \rightarrow X$, which transforms an element $(x1, x2)$ to the element $x1 \circ x2$ is called an operation.
Example: The sum of the residue classes $a + mZ \;\; and \;\; b + mZ \; is \; (a + b) + mZ$.

Associative Property: let G be a non empty set with $*$ as Binary Operator on G then

$$\forall a, b, c \;\; if \;\; (a * b) * c \; = \; a * (b * c)$$

then G is satisfying Associative Property.

A pair $(G, *)$ consisting of a set G and an associative operation $*$ on G is called a **semigroup**.

Examples: $(Z, .)$ $(Z, +)$

The sum of residue classes $a + Z * m$ and $b + Z * m$ is $(a + b) + Z * m$. This means that $(Z/Zm, +)$ is closed under closure and in similar way it is associative.In similar way (Z/mZ) is closed under closure and associtivity making $(Z/mZ, +)$ and $(Z/mZ, .)$ are Semigroups.

Commutative Property: let G be a non empty set with $*$ as Binary Operator on G then

$$\forall a, b \;\; if \;\; a * b \; = \; b * a$$

then G is satisfying Commutative Property.

The semigroup is called abelian or commutative if the operation $*$ is commutative.
The sum of resdue classes is also a subgroup

4 Monoids

A neutral element of a semigroup $(G, *)$ is an element e which satisfies $e * a \; = \; a * e \; = \; a \; \forall \; a \in \; G$. Neutral element is also called as identity element.A semigroup atmost contains one neutral element.A semigroup which contains neutral element is known as **monoid**.

if $(G, *)$ is a semigroup and $e \in G$ is neutral element , then $b \in G$ is called an inverse of $a \in G$ if $a * b = b * a = e$. If a has a inverse then a is called invertible in $(G, *)$.An element of a given subgroup can have more than one inverses also.
In a monoid , each element has atmost one inverse.

Examples:
$(Z, +)$: Neutral element: 0, $a^{-1} = -a$.
$(Z, .)$: Neutral element: 1, $a^{-1} = -1$ and $1^{-1} = 1$. Only 1 and -1 are invertible.
$(Z/mZ, +)$: Neutral element: $0 + mZ$ or [0], inverse: $-a + mZ$. Often is referred as Zm.
$(Z/mZ, .)$: Neutral element: $1 + mZ$ or [1], inverse: those elements, t which have $gcd(t, m) = 1$.

5 Groups

If all the elements of a monoid $(G, *)$ are invertible then the monoid $(G, *)$ is called as a **group**.

Examples:

- $(Z, +)$ is a group.
- $(Z, .)$ is not a group as all the elements do not have a inverse.

6 Conclusion

Congruence Modulo m is an equivalence relation.Modular arithmetic makes it easier to solve complex arithmetic problems such as modular exponentiation.

Semigroups, monoids, groups and abelian groups properties are summarised in below table

(G,*)	Closure	Associative	Identity	Inverse	Commutative
Semigroup	✓	✓			
Monoid	✓	✓	✓		
Group	✓	✓	✓	✓	
Abelian Group	✓	✓	✓	✓	✓