Unit: 2: Integers and Matrices

This area of discrete mathematics belongs to the area of Number Theory. Number theory is a branch of mathematics that explores integers and their properties.

Integers:
→ Z integers {-----, -2, -1, 0, 1, 2 ---}
→ Z^+ positive integers {1, 2, ---}

Number theory has many application within Computer Science, including:
- Storage and Organization of data
- Encryption
- Error correcting codes
- Random number generators

Division:
Assume 2 integers 'a' and 'b' such that $a \neq 0$ (a is not equal to 0). We say that a divides b if there is an integer c such that $b = ac$. If a divides b we we say that a is a factor of b and that b is multiple of a.

- The fact that a divides b is denoted as $a|b$.

Eg: • $4|24$ True or False? True
  • 4 is a factor of 24 • and $c = 6$
  • 24 is a multiple of 4

• $3|7$ True or False? False ✗

Ex: Determine whether $5|7$ and whether $4|16$.

Sol: Here $5 \nmid 7$ since $7/5$ is not an integer.
On the other hand, $4|16$ because $16/4$ is a integer.

Theorem:
Let a, b and c be integer. Then

(i) if $a|b$ and $a|c$, then $a|(b+c)$:

Proof: Here, $a|b$ and $a|c$, so by the definition of divisibility we can say that there are integers p and q such that:

$$b = ap \quad \text{and} \quad c = aq$$

Now, we can write

$$b+c = ap+aq \text{ i.e } b+c = a(p+q)$$

So, from this we can say that a divides $b+c$.

(ii) if $a|b$, then $a|bc$ for all integers c;

Proof: Here, $a|b$, So by the definition of divisibility we can say there is an integer p such that $b = ap$.

So for any integer c we can write $bc = apc$ this means a divides bc, since pc is an integer too.

(iii) if $a|b$ and $b|c$, then $a|c$.

Proof:

Here, $a|b$ and $b|c$, So by the definition of divisibility we can say have, integers p and q such that

$b = ap$ and $c = bq$ i.e $c = apq$.

Since, pq is an integer we conclude that a divides c.

Division Algorithm

When an integer is divided by a positive integer, there is a quotient and a remainder, as the division algorithm shows:

Algorithm:- Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

Here, a is called dividend, d is called divisor, q is called quotient, and r is called remainder.

These, notation is used to express the quotient and remainder:

$q = a \operatorname{div} d$, $r = a \bmod d$.

Example, What are the quotient and remainder when 101 is divided by 11?

Soln, we have (quotient) (divisor)

(dividend) $101 = 11 \cdot 9 + 2$ (remainder)

Hence, the quotient when 101 is divided by 11 is $9 = 101 \text{ div } 11$, and the remainder is $2 = 101 \bmod 11$.

Example:

$a = 14$, $d = 3$

$\Rightarrow 14 = 3 * 4 + 2$

Hence, the quotient when 14 is divided by 3 is $4 = 14 \text{ div } 3$ and the remainder is $2 = 14 \bmod 3$.

Example

What are the quotient and remainder when -11 is divided by 3?

Soln we have,

$-11 = 3(-4) + 1$

Hence, the quotient when -11 is divided by 3 is

$-4 = -11 \text{ div } 3$, and the remainder is

$1 = -11 \bmod 3$.

Note, that the remainder cannot be $-ve$. Consequently the remainder is not -2, even though

$-11 = 3(-3) - 2$,

because, $r = -2$ doesn't satisfy $0 \leq r < 3$.

Modular Arithmetic

This is an arithmetic calculation system which works only with integer number. When an integer 'a' is divided by another positive integer 'm'. Then remainder 'r', is obtained -

such that $a = m * \text{quotient} + r$. The operation which gives remainder is known as modular operation and the process is called modular arithmatic

We have a notation to indicate that two integers have the same remainder when they are divided by the positive integer 'm'.

Definition:- If 'a' and 'b' are integers and 'm' is a positive integer, then 'a' is congruent to "b modulo m" if 'm' divides 'a-b'. We use the notation "$a \equiv b \pmod m$" to indicate that 'a' is congruent to "b modulo m". If 'a' and 'b' are not congruent modulo m, we write $a \not\equiv b \pmod m$.

(1) $a \equiv b \bmod m$ (If m divides a-b)

eg: $20 \equiv 3 \bmod 17$ {17 divides $(20-3) = 17$}

(2) $a \equiv b \bmod m$ (If both a and b have same remainder when divided by m)

eg: $36 \equiv 24$ and 12.

(3) If $a \equiv b \bmod m$ & $x \equiv y \bmod m$, then

$$(a+x) \equiv (b+y) \bmod m$$

eg: $17 \equiv 4 \bmod 13$ and $42 \equiv 3 \bmod 13$

$\Rightarrow 59 \equiv 7 \bmod 13$

(4) If $a \equiv b \bmod m$ and $x \equiv y \bmod m$. Then

$$(a-x) \equiv (b-y) \bmod m$$

eg: $42 \equiv 3 \bmod 13$
$14 \equiv 1 \bmod 13$ $\Big\} \rightarrow 28 \equiv 2 \bmod 13$

Example: Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6

Ans Here,

6 divides $17-5=12$, we see that $17 \equiv 5 \pmod 6$.

However, because $24-14=10$ is not divisible by 6, we see that $24 \not\equiv 14 \pmod 6$.

Example: Determine whether 19 is congruent to 1 modulo 3.

Sol^n Here $a=19$, $b=1$ and $m=3$

Then, $a \equiv b \bmod m$ divides $a-b$

i.e 3 divide $19-1 \Rightarrow 3$ divide 18 is true.

Application of Modular Arithmetic
Congruence

Number theory has applications to a wide range of areas. We will introduce ~~two~~ some few applications in this section: the use of congruence to assign memory location to computer files, the generation of pseudorandom numbers and cryptosystems based on modular arithmetic.

① Hashing Functions:

The central computer at an insurance company maintains records for each of its customers. How can memory location be assigned so that customer record can be retrieved quickly? The solution to this problem is to use a suitable chosen hashing function. Records are identified using a key, which uniquely identifies each customer's records.

For instance, customer records are often identified using the social security number of the customer as the key. A hashing function h assigns memory location $h(k)$ to the record that has k as its key.

The most common is the function

$$h(k) = k \bmod m$$

- Where m is the number of available memory locations (size of hash table)
- k is the key value
- $h(k)$ is the memory location for the records that has 'k' as its key.

The hashing function $h(k) = k \bmod m$ meets this requirement: to find $h(k)$, we need only compute the remainder when k is divided by m.

Example:

When $m = 111$, the record of the customer with social security number 064212848 is assigned to memory location 14, because

$$h(064212848) = 064212848 \bmod 111 = 14.$$

Similarly, because

$$h(037149212) = 037149212 \bmod 111 = 65.$$

The record of the customer with social security number 037149212 is assigned to memory location 65.

Example: which memory location are assigned by the hashing function $h(k) = k \bmod 100$, the records of bank customers with following A/C numbers?

(a) 104578690 (b) 472222187

Sol: Here, $k = 104578690$

$m = 100$

Then, $h(k) = k \bmod m$

$h(104578690) = 104578690 \bmod 100$

$= 90$ i.e memory location is 90.

(b) Pseudo Random Number

Numbers that are generated by a process or algorithm or machine whose outcome is unpredictable, are called random numbers.

- Numbers that are generated by a process or algorithm or machine whose outcome is unpredictable, are called random numbers.
- Pseudo means false (not true), so pseudo random numbers means numbers are that are generated using computer or machine.
- The most commonly used method/procedure to generate pseudo-random numbers is linear congruential method.
- The linear congruential method produces sequence of integer between zero and m - 1.

Using the following recursive formula:

$x_{i+1} = (ax_i + c) \bmod m$

Where,

x_0 = is the sled or initial value

a & c are constant

m is the modulus

For example: Generate first five random numbers using LCM method with $X_0 = 27$, a = 17, C = 43 and m = 100.

Solution

Here,

$x_0 = 27$

$x_1 = (a*x_0 + c) \bmod 100$

$= (17 * 27 + 43) \bmod 100$

$= 502 \bmod 100$

$= 2$

Similarly,

$x_2 = (a * x_1 + c) \bmod 100$

$= (17 * 2 + 43) \bmod 100$

$= 77 \bmod 100 = 77$

$x_3 = (a * x_2 + c) \bmod 100$

$= (17 * 22 + 43) \bmod 100$

$= 1352 \bmod 100$

$= 52$

$x_4 = (a * x_3 + c) \bmod 100$

$= (17 * 52 + 43) \bmod 100$

$= 927 \bmod 100 = 27$

Therefore, sequence of random number is 27, 2, 77, 52, 27, ...