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 ✗

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

Ans: Here ~~5|7~~

$5\nmid 7$ 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

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

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:

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

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

Soln, we have

$$\underset{\text{(dividend)}}{101} = \underset{\text{(divisor)}}{11} \cdot \underset{\text{(quotient)}}{9} + \underset{\text{(remainder)}}{2}$$

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

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 $2 = 14 \text{ mod } 3$.

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

$1 = -11 \text{ mod } 3$.

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 $0 \leq r < 3$.