Chapter 2: THE INTEGERS

Mphako-Banda

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

SCHOOL OF MATHEMATICS

LEARNING OUTCOMES FOR THE LECTURE

By the end of this lecture, students will be able to:

- give proof to divisibility theorems/properties
- apply divisibility properties to given examples
-
-
-

Theorem (2.2.3 -(1))

Let $m, n, d \in \mathbb{Z}$. Then $n \mid n \quad \forall n$.

Proof: $n = 1.n$ so by defn $n \mid n$.

Theorem (2.2.3 -(2))

Let $m, n, d \in \mathbb{Z}$. If $d \mid m$ and $m \mid n$ then $d \mid n$.

Proof: $d \mid m \Rightarrow m = k_1 d$ and $m \mid n \Rightarrow n = k_2 m$
$\Rightarrow n = k_2 k_1 d \Rightarrow d \mid n$ since $k_2 k_1 \in \mathbb{Z}$.

Theorem (2.2.3 -(3))

Let $m, n, d \in \mathbb{Z}$. If $d \mid n$ and $n \mid d$ then $d = \pm n$.

Proof:

Thus if $d \mid n$ and $n \mid d \Rightarrow n = k_1 d$ and $d = k_2 n$ where $k_1, k_2 \in \mathbb{Z}. \Rightarrow n = k_1 k_2 n \Rightarrow k_1 k_2 = 1 \Rightarrow k_1 = k_2 = 1, -1$ since $k_1, k_2 \in \mathbb{Z} \Rightarrow n = d$ or $n = -d$.

Theorem (2.2.3 -(4))

Let $m, n, d \in \mathbb{Z}$. If $d \mid n$ and $d \mid m$ then $d \mid (xn + ym)$.

Proof

Thus if $d \mid n$ and

$d \mid m \quad \Rightarrow \quad m = k_1 d, \quad n = k_2 d, \quad k_1, k_2 \in \mathbb{Z}$

$\Rightarrow xn + ym \quad = \quad xk_2 d + yk_1 d \quad = \quad (xk_2 + yk_1)d$

$\Rightarrow d \mid (xn + ym)$ if $x, y \in \mathbb{Z}$ as then $xk_2 + yk_1 \in \mathbb{Z}$.

NOTE: $xn + ym$ is called a linear combination of n and m.

if d divides integers n and m then d divides the sum of the integers and also d divides the sum of the multiples of the integers

EXAMPLE:

If $d \geq 1$ and $d \mid (3k+5)$ and $d \mid (7k+2)$. Show that $d=1$ or $d=29$.

(i) $3k+5=k_1 d$; (ii) $7k+2=k_2 d$.

$7(3k+5)=7(k_1 d)$; $3(7k+2)=3(k_2 d)$ ***(to eliminate k)***

$\therefore 21k=-35+7k_1 d$ and $21k=-6+3k_2 d$

$\therefore -35+7k_1 d=-6+3k_2 d$

$\therefore d(7k_1-3k_2)=35-6=29$

But 29 is prime so $d=29$ or $d=1$.

Definition (2.2.4 GREATEST COMMON DIVISOR)

$m, n \in \mathbb{Z}$, *not both zero*, d *is* $\gcd(m, n)$ *if*

(i) $d \geq 1$

(ii) $d \mid m$ *and* $d \mid n$

(iii) *if* $k \mid m$ *and* $k \mid n$, *then* $k \mid d$.

d is the greatest common divisor, any other common divisor of m and n must divide d

Note:
$\gcd(0, 0)$ is undefined.

EXAMPLE:

$\gcd(18, 30) = 6$ $\gcd(6, 7) = 1$ $\gcd(-9, 15) = 3.$

$\gcd(78, 30) =?$ $78 = 2.3.13$ and $30 = 2.3.5$

$\therefore \gcd(78, 30) = 2.3 = 6$

Is there an easier way to find $\gcd$?