Quadrant II – Transcript and Related Materials

Programme: Bachelor of Science

Subject: Mathematics

Paper Code: MTE103

Paper Title: Number Theory

Unit: 1

Module Name: Divisibility in $\mathbb{Z}$ and its properties

Name of the Presenter: Ms. Namrata Naik (Assistant Professor)

Notes

Definition:

An integer b is said to be *divisible* by an integer $a \neq 0$, if there exists some integer c such that $b = ac$.

- Here a is said to be a divisor or a factor of b, or b is said to be a multiple of a.

Notation:

- $a \mid b$ indicates that a divides b.
- $a \nmid b$ indicates that b is not divisible by a.

Examples:

$2|4, 3|9, 7|0, 6 \nmid 4.$

Proper and Improper Divisors

- An integer $a \neq 0$ is said to be a *proper divisor* of $b \in \mathbb{Z}$, if $a \mid b$ and $a \neq b$.
- A divisor a of b which is not a proper divisor is called an *improper divisor* of b.

Example:

2 is a proper divisor of 4, 4 is an improper divisor of 4.

Properties :

1. $a|0, \ 1|a, \ a|a$.

✓ $0 = a \cdot 0, a = 1 \cdot a, a = a \cdot 1.$

2. $a|1$ if and only if $a = \pm 1$.

✓ $1 = ac \ \Leftrightarrow a = 1 = c$ or $a = -1 = c$.

3. If $a|b$ and $c|d$ then $ac|bd$.

✓ $a|b \ \Longrightarrow b = ae$ and $c|d \ \Longrightarrow d = ck$ for some integers e and k.
Then $bd = (ae)(ck) = (ac)(ek)$
$\Longrightarrow \ ac|bd$.

4. If $a|b$ and $b|c$ then $a|c$.

✓ $a|b \ \Longrightarrow b = ak$ and $b|c \Longrightarrow c = bm$ for some integers k and m.
Then $c = bm = (ak)m = a(km)$
$\Longrightarrow \ a|c$.

5. $a|b$ and $b|a$ if and only if $a = \pm b$.

✓ $a|b \ \Longrightarrow b = ac$ and $b|a \ \Longrightarrow a = db$ for some integers c and d.
Then $a = db = d(ac) = a(dc) \Longrightarrow 1 = dc \Longrightarrow \ d = 1 = c$ or $d = -1 = c$

6. If $a|b$ and $b \neq 0$ then $|a| \leq |b|$.

✓ $a|b \ \Longrightarrow b = ac$ for some integer c.
$c \neq 0 \ \Longrightarrow |c| \geq 1 \ \Longrightarrow |b| = |ac| = |a||c| \geq |a|$.

7. If $a|b$ and $a|c$ then $a|(bx + cy)$ for arbitrary $x, \ y \in \mathbb{Z}$.

✓ $a|b \ \Longrightarrow b = ad$ and $a|c \Longrightarrow c = ae$ for some integers d and e.
Then $bx + cy = adx + aey = a(dx + ey) \Longrightarrow a|(bx + cy)$.

8. If $a|b$ then $a|bc$.

✓ $a|b \ \Longrightarrow b = ak$ for some integer k.
Then $bc = akc \ \Longrightarrow \ a|bc$

9. If $a|b$ and $a|c$ then $a^2|bc$.

✓ $a|b \ \Longrightarrow b = ak$ and $a|c \ \Longrightarrow c = am$ for some integers k and m.
Then, $bc = (ak)(am) = a^2(km) \ \Longrightarrow a^2|bc$.

10. $a|b$ if and only if $ac|bc$, where $c \neq 0$.

✓ $a|b \ \Leftrightarrow b = ak$ for some integer k.
$\Leftrightarrow bc = akc$
$\Leftrightarrow ac|bc$

Note:

Converse of 7 does not hold true.

i.e. $a|(bx + cy)$ not necessarily imply $a|b$ or $a|c$

e.g. $7|(4 \cdot 1 + 3 \cdot 1)$ but $7 \nmid 3$ and $7 \nmid 4$.

Problem:

1. $21|4^{n+1} + 5^{2n-1}$ for all $n \in \mathbb{N}$.

Soln.: We solve this using Induction

For $n = 1$, $4^{n+1} + 5^{2n-1} = 4^2 + 5^1 = 21$ is divisible by 21.

Assume that $4^{n+1} + 5^{2n-1}$ is divisible by 21, $n > 1$.

Now, $4^{(n+1)+1} + 5^{2(n+1)-1} = 4^{n+2} + 5^{2n+1} = 4 \cdot 4^{n+1} + 5^2 \cdot 5^{2n-1}$

$$= 4 \cdot 4^{n+1} + (21 + 4) \cdot 5^{2n-1}$$

$$= 4 \cdot (4^{n+1} + 5^{2n-1}) + 21 \cdot 5^{2n-1}$$

$$= 4 \cdot 21k + 21 \cdot 5^{2n-1}$$

$$= 21m$$

Hence, by induction $21|4^{n+1} + 5^{2n-1}$ for all $n \in \mathbb{N}$.