# 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:

- ♣ Determine when two integers are relatively prime
- ♣ Apply divisibility properties of coprime integers and division by a prime
- ♣ Define a prime number
- ♣ State and apply Prime Factorisation Theorem
- ♣

# RELATIVELY PRIME

**Definition (2.4.1)**

*$m, n \in \mathbb{Z}$ and $\gcd(m, n) = 1$ then $m$ and $n$ are relatively prime.*

**Theorem (2.4.2)**

*Let $m, n \in \mathbb{Z}$, not both zero. $\gcd(m, n) = 1$ iff $\exists\ x, y \in \mathbb{Z}$ such that $xm + yn = 1$.*

**PROOF:**

$\Rightarrow$ If $\gcd(m, n) = 1$ then by Euclidean Algorithm $1 = xm + yn$ as required.

$\Leftarrow$ If $\exists x, y \in \mathbb{Z}$ such that $xm + yn = 1$ and $d = \gcd(m, n)$. Then $d \mid 1$. Thus $d = 1$.

## Corollary (2.4.3)

*$m, n \in \mathbb{Z}$ and $\gcd(m, n) = d$, then $\frac{m}{d}$ and $\frac{n}{d}$ are relatively prime.*

**Proof:**

$\gcd(m, n) = d, \quad \Rightarrow \quad d = xm + yn \quad \Rightarrow \quad 1 = x(\frac{m}{d}) + y(\frac{n}{d})$
and $\frac{m}{d}$ and $\frac{n}{d} \in \mathbb{Z} \quad \Rightarrow \gcd(\frac{m}{d}, \frac{n}{d}) = 1.$

## Theorem (2.4.4 - (i))

*Let* $\gcd(m,n)=1$. *Then if* $m \mid k$ *and* $n \mid k$, *then* $mn \mid k$.

show that
k=t(mn),
some t

**Proof:**

m|k n|k

$$\Rightarrow \quad k = k_1 m; \quad k = k_2 n; \quad xm + yn = 1.$$

gcd(m,n)=1

$$\Rightarrow \quad k.1 = k(xm+yn)$$

$$= \quad (k_2 n)xm + (k_1 m)yn$$

$$= \quad mn(xk_2 + yk_1)$$

$$\Rightarrow \quad mn \mid k.$$

t=xk2+yk1
integer

## Theorem (2.4.4 - (ii))

*Let* $\gcd(m, n) = 1$. *Then if* $m \mid kn$ *for some* $k$, *then* $m \mid k$.

**Proof:**

m|kn gcd(m,n)=1

$m \mid kn \quad \Rightarrow kn = k_1 m$ and $xm + yn = 1$

$\Rightarrow k = k.1 = k(xm + yn) = kxm + kyn = kxm + k_1 my = m(xk + yk_1)$.

$\Rightarrow m \mid k$. k=mt, some integer t
thus m|k

**Example**

$2 \mid 30$ and $3 \mid 30$ so $6 \mid 60$.

$2 \mid 4.5$ and $\gcd(2, 5) = 1 \Rightarrow 2 \mid 4$.

# PRIME NUMBERS

## Definition (2.5.1)

*An integer p is a prime if*

(i) $p \geq 2$

(ii) if $d \mid p$ and $d > 0$, then $d = 1$ or $d = p$.

divisors of p are 1 and p only

## Theorem (2.5.2 EUCLID'S LEMMA)

*p is prime.*

(i) If $p \mid mn \quad \Rightarrow \quad p \mid m$ or $p \mid n$.

(ii) If $p \mid m_1 m_2 m_3 \ldots\ldots m_k \quad \Rightarrow \quad p \mid m_i$ for some $i$.

**PROOF:** given that p|mn;

(i) Let $d = \gcd(p, m)$. Then $d \mid p$ so $d = 1$ or $d = p$. If $d = p$ then $p \mid m$. if $d = 1$ then $\gcd(p, m) = 1$ so $p \mid n$ by theorem2.4.4 ***[If** $m \mid kn$ **for some** $k$**, then** $m \mid k$**. ]***

$\boxed{\text{p|mn and gcd(m,n)=1, p|n}}$

(ii) Prove by Induction Use induction on $k$ to show if $p$ is prime and $p \mid m_1 m_2 m_3 .......m_k$ where $m_i \in \mathbb{Z}$ then $p \mid m_i$ for some $i$.

$k = 1$ $p \mid m_1$ we are done and $k = 2$ gives part (i).

p|mn then p|n or p|n
m_1=m, m_2=n

Assume statement true for some $k > 1$ assume true that if p|m_1m_2...m_k then p|m_i
and let $p \mid m_1 m_2 m_3 .......m_k m_{k+1}$, then part(i) shows either $p \mid m_1 m_2 m_3 .......m_k$ or $p \mid m_{k+1}$.
So either $P_{\text{p}}| \ m_i$ for some $i = 1, \cdots, k$ by induction hypothesis or $p \mid m_{k+1}$.
$\therefore P_{\text{p}}| \ m_i$ for some $i = 1, \cdots, k, k+1$.

## Theorem (2.5.3 PRIME FACTORISATION THEOREM)

(i) *Every integer $n \geq 2$ is the product of one or more primes.*

(ii) *The factorisation is unique up to the order of the factors. In fact $n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$, where the $p_i$ are distinct primes and $n_i \geq 1$ for all $i$. Then the positive divisors of $n$ are the integers of the form $d = p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r}$, where $0 \leq d_r \leq n_i$ holds for $i$.*

## Definition ( 2.5.4 Greatest common divisor/ least commom multiple)

*Let $n_1, n_2, \cdots, n_r$ be positive integers.*

**(i)** *The greatest common divisor of these integers, denoted $\gcd(n_1, n_2, \cdots, n_r)$, is the positive common divisor that is a multiple of every common divisor.*

**(ii)** *The least common multiple of these integers, denoted by $\mathrm{lcm}(n_1, n_2, \cdots, n_r)$, is the positive common multiple that is a divisor of every common multiple.*

least positive integer that is
divisible by all n_i, i=1...r

## Example

(i) *Find* $\gcd(4,6,10)$ *and lcm*$(4,6,10)$
$4 = 2^2 3^0 5^0 \qquad 6 = 2^1 3^1 5^0 \qquad 10 = 2^1 3^0 5^1$
$\gcd((4,6,10) = 2$ *and lcm*$(4,6,10) = 2^2 3^1 5^1 = 60$.

(ii) *Find* $\gcd(12,20,18)$ *and lcm*$(12,20,18)$
$12 = 2^2 3^1 5^0 \qquad 20 = 2^2 3^0 5^1 \qquad 18 = 2^1 3^2 5^0$
$\gcd(12,20,18) = 2^1 3^0 5^0 = 2$ *and*
*lcm*$(12,20,18) = 2^2 3^2 5^1 = 180$.

(iii) *Find gcd*$(63,60,245)$ *and lcm*$(63,60,245)$.
$63 = 2^0 3^2 5^0 7^1 \qquad 60 = 2^2 3^1 5^1 7^0 \qquad 245 = 2^0 3^0 5^1 7^2$
*gcd*$(63,60,245) = 2^0 3^0 5^0 7^0 = 1$ *and*
*lcm*$(63,60,245) = 2^2 3^2 5^1 7^2 = 8820$.