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:

- use the Euclidean Algorithm to find the greatest common divisor of two integers.
- use the Euclidean algorithm to express the greatest common divisor as a linear combination of integers m and n .

EUCLIDEAN ALGORITHIM

Theorem (2.3.1)

$m, n \in \mathbb{Z}$, not both zero. $d = \gcd(m, n)$ exists and $d = xm + yn$ for some integers x, y.

NOTE

If $n = 0$ (or $m = 0$), then $\gcd(m, n) = m$ (or n) because $m \mid 0$ (and $n \mid 0$).

for t=n and s=m we have sm+tn>=1 since m and n are not both zero

PROOF: Let $X = \{sm + tn \mid s, t \in \mathbb{Z}, sm + tn \geq 1\}$.

SHOW $X \neq \emptyset$

Now $m^2 + n^2 \geq 1$, so $m^2 + n^2 \in X$ and $X \neq \emptyset$ and bounded below by 1. So X has a smallest element by W.O.A.

Let d be the smallest element in X. Then $d \geq 1$ and $d = xm + yn$, $x, y \in \mathbb{Z}$. If k is any divisor of m and n then k is a divisor of d. We show d is a divisor of both m and n and hence d is the $\gcd(m, n)$.

given any m and n integers such that m and n are not both zero, can we find integers s and t such that sm+tn>=1?

By Division algorithm

(show $d \mid n$): $n = qd + r, \qquad 0 \leq r < d, \qquad q, r \in \mathbb{Z}.$

$$\begin{aligned} r &= n - qd \\ &= n - q(xm + yn) \\ &= (-qx)m + (1 - qy)n \text{ [so } r \in X\text{]}. \end{aligned}$$

r=sm+tn where
s=-qx, t=1-qy
are integers.
so r is in set X

If $r \in X$ and $0 < r < d$, then a contradiction to the choice of d. Therefore $r = 0$ and so $d \mid n$. Similarly $d \mid m$.
$\therefore d = gcd(m, n)$.

r is X since r=sm+tn for some integers s and t. but r<d, a contradiction since d is the smallest integer such that d=sm+tn for some integers s and t. then r cannot be less than d. thus, from the condition that 0<= r<d, the only possibility is that r=0. now from the fact that n=qd+r we have n=qd and d divides n.

Corollary (2.3.2)

If $m = qn + r$, then $\gcd(m, n) = \gcd(n, r)$.

PROOF:

Let $d = \gcd(m, n), \qquad k = \gcd(n, r)$

$k \mid n$ and $k \mid r$ so $k \mid qn + r$ and so $k \mid m$.

$\therefore \quad k \mid d$ since $d = \gcd(m, n)$

Using $r = -qn + m$ we can show similarly that $d \mid k$.

$\therefore \quad d = \pm k$ But d, k both ≥ 1 by definition.

$\therefore \quad d = k$.

EXERCISE

Find $\gcd(78, 30)$ using the Euclidean algorithm. Let $m = 78$ and $n = 30$.

$$\begin{aligned} 78 &= m = q_1 n + r_1 = 2.30 + 18 \\ 30 &= n = q_2 r_1 + r_2 = 1.18 + 12 \\ 18 &= r_1 = q_3 r_2 + r_3 = 1.12 + 6 \\ 12 &= r_2 = q_4 r_3 + r_4 = 2.6 + 0 \end{aligned}$$

So $r_4 = 0$ and $6 = 2(78) - 5(30)$.
$\gcd(m, n) = \gcd(n, r_1) = \gcd(r_1, r_2) = \gcd(r_2, r_3) = \gcd(r_3, r_4) = r_3 = 6$ since $r_4 = 0$.

See NOTE on Euclidean Algorithm.
Further, we note $0 = r_4 < r_3 < r_2 < r_1 < n$.
Since the remainders are all non negative integers less than n, the process must stop in a finite no of steps.

Example (2.3.3)

Find $\gcd(41, 12)$.

$$
\begin{aligned}
41 &= 12.3 + 5 \qquad r_1 = 5\\
12 &= 2.5 + 2 \qquad r_2 = 2\\
5 &= 2.2 + 1 \qquad r_3 = 1\\
2 &= 2.1 \qquad r_4 = 0
\end{aligned}
$$

Last nonzero remainder is $\gcd$. i.e $\gcd(41, 12) = 1$ thus 41 and 12 are coprime. 41 is a prime number.

In this exercise, substituting back we have, from last non zero remainder

$$\begin{aligned} 1 &= 5 - 2.2 \\ &= 5 - 2(12 - 2.5) \\ &= 5 - 2.12 + 4.5 \\ &= 5.5 - 2.12 \\ &= 5(41 - 3.12) - 2.12 \\ &= 5.41 - 17.12 = xm + yn. \end{aligned}$$

$x = 5$ and $y = -17$.