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:

- define a divisor of an integer n
- state the Division Algorithm Theorem
- prove the Division Algorithm Theorem
- find the quotient and theremainder when n is divided by d, where n and d are integers
-

We will use several less familiar properties of divisibility and primes in $\mathbb{Z}$.

WELL-ORDERING AXIOM
Every non-empty set of positive integers has a smallest member.
We know from Basic Analysis that every non empty set of reals that is bounded below, has an infimum. Hence every nonempty set of positive integers(bounded below by 0) has an infimum in $\mathbb{R}$ and hence a smallest member.

DIVISION ALGORITHM

Definition (2.2.1)

Let $n, d \in \mathbb{Z}$. If $n = qd$, $q \in \mathbb{Z}$ then d is a divisor of n.

NOTE $q \in \mathbb{Z}$ (not $\mathbb{R}$) then we write $d \mid n$, we say
d divides n
If d is not a divisor of n, we write $d \nmid n$.

if r=0 then n=qd and d divides n

Theorem (2.2.2 Division Algorithm theorem)

Let n and d be integers with $d \geq 1$. $\exists q, r \in \mathbb{Z}$ such that $n = qd + r$ where $0 \leq r < d$ and q and r are unique.

q and r are called quotient and remainder respectively.

PROOF:

Let $X = \{n - td | t \in \mathbb{Z}, n - td \geq 0\}$

for any n,d integers, r=n-td exists and is greater than or equal to 0

- SHOW X is non empty.

If $n \geq 0$ then $n - 0d = n \in X$. and
If $n < 0$ then $n - nd = n(1 - d) \geq 0$ Recall [(-)(-) =+]
$\therefore n - nd \in X$. So $X \neq \emptyset$ and is bounded below by 0. By Well Ordering Axiom, X has a smallest element. Let r be the smallest element of X. So $r \geq 0$ and $r = n - qd$ for some $q \in \mathbb{Z}$. That is $n = qd + r$, $q \in \mathbb{Z}$, $r \geq 0$.

proof by contradiction

- SHOW $r < d$.

Assume $r \geq d$ then
$0 \leq r - d = n - qd - d = n - (q+1)d \in X$ but $r - d < r$ and r is smallest element in X. (CONTRADICTION!) So $0 \leq r < d$.

we assume the contrary and reach a contradiction. thus our assumption is wrong and the given statement is correct.

SHOW uniqueness

Say $\exists$ q_1 and r_1 $\in \mathbb{Z}$ such that $n = q_1 d + r_1$, $0 \leq r_1 < d$. W.L.O.G assume $r \leq r_1$. Thus if we let $n = q_1 d + r_1$, then $qd + r = q_1 d + r_1 \Rightarrow (q - q_1)d = r_1 - r$ but $r_1 - r \leq r_1 < d$ and $r_1 - r$ is a multiple of d which is less than d. So the only multiple of d strictly less than d is 0. Thus $r_1 - r = 0$ and $q - q_1 = 0$ so $r_1 = r$ and $q - q_1$

we show that if n=qd+r and n=q_1 d+r_1 then r=r_1 and q=q_1
since for any n and d, q and r are unique

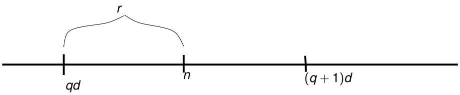
EXAMPLE:

Find the quotient and the remainder of n.

(i) $n = -17$; $\quad d = 5$ then $q = -4 \quad$ and $\quad r = 3$. That is

$$\frac{n}{d} = \frac{-17}{5} = -4 + \frac{3}{5} \text{ or } -17 = 5(-4) + 3.$$

Geometrically



Mark real line off in multiples of d. n must lie between multiples, qd and $(q+1)d$ for $q \in \mathbb{Z}$. Thus $qd \leq n < (q+1)d$ or $0 \leq n - qd < d$ with $r = n - qd$.

(ii) $n = 17$ and $d = 5$.

$$\frac{n}{d} = \frac{17}{5} = 3 + \frac{2}{5} \text{ or } 17 = 5(3) + 2.$$

Note that $q = [\frac{n}{d}]$ is the integer part of $x = \frac{n}{d}$.

$$[7.5] = 7 \qquad [-5.1] = -6 \qquad [\pi] = 3.$$

(iii) $n = 4187$ and $d = 129$.

$$\frac{n}{d} = \frac{4187}{129} = 32 + \frac{59}{129} \text{ or } 4187 = 129(32) + 59.$$

Example $129 \nmid 4187$ but $129 | 4128$.