MODULE I

- Number Theory: $(\mathbb{N}, \mathbb{Z})$

Well-ordering Principle: Any subset S of $\mathbb{N}$ has a minimum element.

Divisors, quotient, remainder, divisibility:

THEOREM 1.1

If $a \& b$ are integers and $b>0$, then there is a unique pair of integers $q \& r$ s.t $a = qb+r$ and $0 \le r < b$

Eg: $a=5$ $b=3$ $5 = q \cdot 3 + r$ $0 \le r < 3$ $r = 0, 1, 2$

$\hookrightarrow 1 \cdot 3 + 2$

$q \Rightarrow$ quotient

$r \Rightarrow$ remainder.

Proof: To prove: There is a pair (q, r) which satisfies the condition $a = qb+r$ and $0 \le r < b$.

It is a unique pair. $(q_1, r_1) \& (q_2, r_2)$ which satisfy $a = q_1 b + r_1 = q_2 b + r_2$ $0 \le r_1, r_2 < b$ then $q_1 = q_2$ & $r_1 = r_2$

Existence of the pair

Define $S = \{ a - ub \mid u \in \mathbb{Z} \} = \{ a, a \pm b, a \pm 2b, \dots a \pm ib, \dots \}$

S contains +ve integers. Therefore $S \cap \mathbb{N}$ is non-empty and obviously a subset of $\mathbb{N}$. By well ordering property $S \cap \mathbb{N}$ has a minimum element, r. Since $r \in \mathbb{N}$, $0 \le r$. and $r \in S$, $r = a - qb$ for some $q \in \mathbb{Z}$. $r < b$, for if $r > b$ then $0 \le r - b = a - qb - b = a - (q+1)b \in S \cap \mathbb{N}$ and $r - b < r$ contradicting the fact that r is the minimum element of $S \cap \mathbb{N}$. Now $a = qb + r$ and $0 \le r < b$.

Uniqueness

Let us say there are two pairs $(q_1, r_1) \& (q_2, r_2)$ which satisfy $a = qb + r$ & $0 \le r < b$.

ie $a = q_1 b + r_1 = q_2 b + r_2$.

$\therefore (q_1 - q_2) b = (r_2 - r_1)$ Since both $r_1 \& r_2$ satisfy $0 \le r < b$, the magnitude of the difference $|r_2 - r_1| < b$. Hence $r_2 - r_1$ cannot be a multiple of b. Therefore $r_1 = r_2$ and hence $q_1 = q_2$

∎

Eg: Any square n produces a remainder 0 or 1 with 4.

Proof: $n = a^2$, $a \in \mathbb{N}$.

Case 1: a is even: i.e. $a = 2k$ $k \in \mathbb{N}$

$n = a^2 = 4k^2 = 4q + r$ $\quad r = 0$, $q = k^2$

Case 2: a is odd i.e. $a = 2k+1$

$n = (2k+1)^2 = 4k^2 + 4k + 1 = 4(k^2+k) + 1$

$= 4q + r$

$r = 1$

$q = k^2 + k$.

Case: when $b < 0$

Since $b < 0$, we have $-b > 0$. and hence Theorem 1.1 applies to $-b$ and $a = q \times (-b) + r$ $\quad 0 \le r < -b = |b|$. Therefore a can be written as $a = (-q) \times b + r$ which is unique because (q, r) is unique by Theorem 1.1.

Divisors

→ a is a divisor of b if $b = qa$ for some integer q ($q \in \mathbb{Z}$)

a is referred to as a multiple of b (q)

Eg: 3 is a divisor of 6 ($6 = 2 \times 3$)

3 is a divisor of -6 ($-6 = -2 \times 3$)

→ Notation: $a|b$ ⇒ a divides b

(a is a divisor of b)

↳ a

(*) PROVE THE FOLLOWING (Home work)

(a) if $a|b$ and $b|c$ then $a|c$;

(b) if $a|b$ and $c|d$ then $ac|bd$;

(c) if $m \neq 0$, then $a|b$ if and only if $ma|mb$;

(d) if $d|a$ and $a \neq 0$ then $|d| \leq |a|$.

Theorem 1.3

(a) If c divides $a_1, \ldots, a_k$, then c divides $a_1u_1 + \cdots + a_ku_k$ for all integers $u_1, \ldots, u_k$.

(b) $a|b$ and $b|a$ if and only if $a = \pm b$.

Eg: $c = 3$ $a_1 = 6$ $a_2 = 18$ $a_3 = 9$ $6u_1 + 18u_2 + 9u_3$ $u_1, u_2, u_3 \in \mathbb{Z}$

PROOF:

(a) $c|a_1, c|a_2 \ldots c|a_k$ ⇒ Therefore $a_i = q_i c$ $i = 1 \ldots k$

Hence $a_1u_1 + a_2u_2 + a_3u_3 + \cdots + a_ku_k$

$= c(q_1u_1 + q_2u_2 + \cdots + q_ku_k) = c\hat{q}$ $\hat{q} = \sum_{i=1}^{k} q_iu_i \in \mathbb{Z}$.

$\therefore c|(a_1u_1 + a_2u_2 + \cdots a_ku_k)$ by the definition of divisibility

(b) If $a \neq 0, b \neq 0$

$a|b$ ⇒ $b = q_1a$ → ① Similarly $b|a$ ⇒ $a = q_2b$ → ②

Plugging ② into ① we get $b = q_1q_2b$.

$q_1 q_2 = 1$ which is possible only if q_1 and q_2 satisfy ± 1.

On the other hand if $a=b=0$ then obviously $a = \pm b$

GREATEST COMMON DIVISOR

If $d|a$ & $d|b$ then d is called a common divisor.

The greatest common divisor (GCD) of a and b denoted by (a,b) is a number d which satisfies:

(i) If c is a common divisor of a & b then $c \leq d$

(ii) d is a common divisor ($d|a$ & $d|b$)

Eg $(6,4) = 2$ $\quad (100,75) = 25$ $\quad (21,18) = 3$

$0 = 0 \cdot q + 0$ (q, r)

Theorem (Euclids Algorithm)

If $a = qb + r$ then $\gcd(a,b) = \gcd(b,r)$. $\Rightarrow$ Eg: $(27,18) = (18,9)$ (q, $r=9$)

$= (9,0) \Rightarrow 9$ ✓

PROOF:

Let c be any divisor of a & b. Now $r = a - qb$

By Theorem 1.3, $c \mid a - qb = r$. That is any common divisor of a & b is also a divisor of r. Hence c is a common divisor of b & r. GCD is also a divisor of a & b and hence of b & r. Hence $(a,b) = (b,r)$ ▨