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. $a = 2k+1$

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

$= 4q + r$

$r = 1$

$q = k^2 + k$.