Number Theory

Dr. S.K. Shukla
RDS College, Muz.

- Number System

i) $\mathbb{N}$ = Set of natural numbers = $\{1, 2, 3, \ldots\}$
$\mathbb{W}$ = Set of whole nos. = $\{0, 1, 2, 3, \ldots\}$.

ii) $\mathbb{Z}$ = Set of integers = $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.

iii) $\mathbb{Q}$ = Set of rational nos.
$= \{ p/q : p, q \in \mathbb{Z}, q \neq 0 \}$.

iv) $\mathbb{R}$ = Set of real nos.

v) $\mathbb{C}$ = Set of complex nos.
$= \{ a + i \cdot b \mid a, b \in \mathbb{R} \}$

- Number theory, basically studies the properties of $\mathbb{Z}$ or $\mathbb{N}$.

. It uses techniques from variety of other fields, viz. algebra, analysis, topology, geometry, logic and computer science.

. It has plenty of applications to cryptography and coding theory.

- Basic properties of $\mathbb{N}$

1. Every natural no. n has a successor $n+1$.
   Notation: $s(n)$
   Thus $s(n) = n+1$
   - Addition is repeated application of successors.
   - Multiplication is repeated application of addition

2. Principle of Mathematical Induction (PMI)
   A property or statement $p(n)$ is true $\forall n \in \mathbb{N}$ if
   i) $p(1)$ is true,
   ii) $p(m)$ is true $\Rightarrow p(m+1)$ is true, for any $m \in \mathbb{N}$.

3. Well Ordering Principle (WOP)
   Every nonempty subset of $\mathbb{N}$ has a smallest element.

NB i) WOP may be rephrased for the set of whole numbers also.

ii) PMI $\Leftrightarrow$ WOP

Divisibility in $\mathbb{Z}$

For $a (\neq 0), b \in \mathbb{Z}$, we say that '$a$ divides b' (Symbolically, $a|b$) if $\exists$ an $x \in \mathbb{Z}$ s.t. $b = a \cdot x$.

Observe that (i) $n|0$, $\forall\, n \in \mathbb{N}$.

ii) $a|b,\ b|c \Rightarrow a|c$

iii) $a|b,\ a|c \Rightarrow a|bx+cy$, $\forall\, x, y \in \mathbb{Z}$.

Theorem (Division algorithm):
Given $a (\neq 0), b \in \mathbb{Z}$, $\exists\, q, r \in \mathbb{Z}$ s.t. $b = aq + r$, $0 \leq r < |a|$.

Proof. Consider the set
$S = \{$

Theorem (Division Algorithm)
Given $a, b \in \mathbb{Z}$ with $a > 0$, $\exists\, q, r \in \mathbb{Z}$ s.t. $b = aq + r$, $0 \leq r < a$.

Proof. Consider the set
$S = \{ b + k \cdot a \mid k \in \mathbb{Z},\ b + k \cdot a \geq 0 \}$.

Claim $S \neq \phi$
i) If $b \geq 0$, then $b + 0 \cdot a \in S$

ii) If $b<0$, we can suitably choose a $k \in \mathbb{Z}$ s.t.

$$b + k \cdot a \geq 0$$

Since S is nonempty, by WOP S has a smallest element, say $r = b + k \cdot a$ for some k.

Setting $-k = q$, we have

$$r = b - q \cdot a.$$

Since $r \in S$, $r \geq 0$

Also $r < a$, for otherwise

$$r \geq a \Rightarrow r - a \geq 0$$
$$\Rightarrow (b + k \cdot a) - a \in S, \text{ i.e.}$$
$$\Rightarrow b + (k-1)a \in S$$
$$\Rightarrow b + (k-1)a \text{ is smallest in } S.$$

($\lightning$) contradiction.

□