Introduction to Number Theory

Prof. NSN Sastry

IIT Dharwad

<u>Number</u> <u>Theory</u> (also, called Arithmetic)

1. <u>Introduction:</u> Study of properties of natural numbers

$\mathbb{N}$ = {1, 2, 3, …..}

Studied in all civilizations from antiquity;

Babilonian, Chinese, Mayan, Indian, Arab, Greek, etc.

Its conceptual elegence is the main motivation, apart from its use in trade record keeping, etc.,

Since 1970's, some elementary aspects of it is extensively used in secure communication.

Different "Number systems" are devised and used for different purposes:

the number system we normally use in geometry, calculus,…, is very different from the

number system we use for digital communication.

For the construction of various number systems, the starting point is the set of natural numbers ($\mathbb{N}$).

Though the concept of natural numbers in all civilizations is essentially the same, it was put on a logical foundation by G.Peano in late 19th century [Peano axioms].

However, here we assume familiarity with basic properties of $\mathbb{N}$.

Addition : +: $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ is a well defined, commutative and associative binary operation .

Associativity allows adding any finite number of elements of $\mathbb{N}$ unambigiously.

For n ϵ $\mathbb{N}$, φ_n : $\mathbb{N} \rightarrow \mathbb{N}$ defined by φ_n (a) = n+a (a ϵ $\mathbb{N}$) is one to one, but not an on to map.

Multiplication : $\times$: $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ is a well defined, commutative, associative binary operation on $\mathbb{N}$.

Notation: a $\times$ b, a $\cdot$ b, ab

— Multiplication is repeated addition :

ab is the same as adding a to itself b times,….

— For n ϵ $\mathbb{N}$, ψ_n : $\mathbb{N} \rightarrow \mathbb{N}$ defined by ψ_n(a) = an is a 1-1 fuction ;

it is on to if n = 1 in which case it is the identity map.

Addition and multiplication are related by the associative law : for a, b, c ϵ $\mathbb{N}$,

$$a(b+c) = ab+ac$$

and so, by the commutativity of multiplication ,

$$(a+b)c = ac+bc.$$

Induction Principle :

If $A \subseteq \mathbb{N}$ contains $1 \in \mathbb{N}$ and a+1 for each $a \in A$, then $A = \mathbb{N}$.

Number systems from $\mathbb{N}$:

$$F_{p^n} \leftarrow F_P \leftarrow \mathbb{N} \rightarrow \mathbb{Z} \rightarrow \mathbb{Q} \rightarrow \mathbb{R} \rightarrow \mathbb{C}$$

$$\searrow \mathbb{Z}_P \rightarrow \mathbb{Q}_p \rightarrow \overline{\mathbb{Q}}_p$$

P – a prime here

$\overline{\mathbb{N}}$: = $\mathbb{N}$ U {0}, where 0 (called zero) is a new symbol

$$\text{Define} \begin{cases} 0+n = n+0 = n & \text{for each } n \in \mathbb{N} \\ 0 \times n = n \times 0 = 0 \end{cases}$$

$\mathbb{Z}$:= $\mathbb{N}$ ∪ { 0} ∪ (-$\mathbb{N}$), $where\ -\mathbb{N}$={-n : n ∈ $\mathbb{N}$} .

The system $\overline{\mathbb{N}}$ is extended by adding a new symbol –n for each n ϵ $\mathbb{N}$

such that – n ≠ - m for all n, m ∈ $\mathbb{N}$, n ≠ m.

We define addition and multiplication of elements of $\mathbb{Z}$ in "the usual way".

<u>Some important properties of</u> $\mathbb{Z}$

(i) ($\mathbb{Z}$, +) is an abelian group.

(ii) ($\mathbb{Z}$, +, ·) is a commutative ring with identity.

(iii) The ring $\mathbb{Z}$ is

(a) an integral domain (this means :if m, n ∈ $\mathbb{Z}$, then (m n = 0<=> m = 0 or n=0) and
(b) a principal ideal domain (P I D) :

this means: any proper subgroup and any proper idea consists of the set

n ∈ $\mathbb{Z}$ = {na : a ∈ $\mathbb{Z}$} of all multiples of a fixed n ∈ $\mathbb{Z}$.

We discuss in the coming lectures the construction of :

- **Finite fields**
- $\mathbb{Q}$, $\mathbb{R}$,
- **P-adic integers** $\mathbb{Z}_p$, $\mathbb{Q}_p$, $\overline{\mathbb{Q}}_p$ **(for all primes p)**

(iv) 'Order' is a relation $\mathbb{Z}$ **(read as "less than") between pairs {a, b}, a**$\neq$**b, of integers, written as a<b, such that for all a, b** $\in \mathbb{Z}$**, the following holds:**

(a) **a<b, or a=b or b<a holds for all a, b** $\in \mathbb{Z}$

(b) **a<b if , and only if, b-a>0**

(c) **a<b and c** $\in \mathbb{Z}$**, then a+c < b+c**

(d) **if a<b and c** $\in \mathbb{N}$ **then a c < b c**

(v) (well – order principle)

Each subset of $\mathbb{N}$ **contains a smallest element.**

This is a fundamental property of integers.

(v) Absolute Value on $\mathbb{Z}$ is fuction $|\cdot| : \mathbb{Z} \to \overline{\mathbb{N}}$ such that

(a) $|n| = 0$ if, and only if, $n=0$

(b) $|x+y| \leq |x| + |y|$

(c) $|x \cdot y| = |x| \cdot |y|$.

Ex: 1) $$|n| = \begin{cases} n & \text{if } n \in \overline{\mathbb{N}} \\ -n & \text{if } n \in \mathbb{Z} \setminus \overline{\mathbb{N}} \end{cases}$$

2) We later define another absolute value fuction $|\cdot|_p$ on $\mathbb{Z}$, one for each prime number p.

It is a fundamental fact due to Ostrowski that these are the only 'absolute value ' functions on $\mathbb{Z}$.