Lecture – 2

$\boxed{\text{There's plenty of partial marking. So, don't jump steps.}}$

Last Time :-
Peano Axioms
$\mathbb{N} = \{0, 1, 2, \ldots\}$ is the unique set satisfying these axioms.
Note that although $\mathbb{N}$ is infinite, all of its elements are finite.

Exercise :- Show that there are no infinite natural numbers.

Today :-

We will now define some operations on $\mathbb{N}$

Def'n :- The binary operation $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is defined as follows, Suppose $m \in \mathbb{N}$, We set $0 + m = m$

$$\boxed{+(0, m) = m}$$

Inductively, suppose we have defined $m + n$, then
$$(n{+}{+}) + m = (n + m) + 1$$
Thus
$$1 + m = (0{+}{+}) + m = (0 + m){+}{+} = m{+}{+}$$

Lemma :- For $n \in \mathbb{N}$, $n + 0 = n$
Proof of Lemma :- We use induction on n.
We have $0 + 0 = 0$ (by $m = 0$ in def'n)
Suppose $n + 0 = n$, Then $(n{+}{+}) + 0 = (n + 0){+}{+} = n{+}{+}$
(By induction Hypothesis)

$\boxed{\text{Hence Proved}}$

Lemma :- For $m, n \in \mathbb{N}$, $n + (m{+}{+}) = (n + m){+}{+}$
Proof of Lemma :- Fix m and induct on n.
For $n = 0$, $0 + (m{+}{+}) = m{+}{+}$ and $0 + m = m$
$$\Rightarrow 0 + (m{+}{+}) = (0 + m){+}{+}$$
Now assume $n + (m{+}{+}) = (n + m){+}{+}$
We want to show this for $n{+}{+}$
$$\Rightarrow \text{LHS} = (n{+}{+}) + (m{+}{+}) = (n + (m{+}{+})){+}{+} \quad [\text{By def'n}]$$
$$= ((n + m){+}{+}){+}{+}$$

$\Rightarrow$ RHS $= ((n++)+m)++ = ((n+m)++)++$

LHS = RHS

$\boxed{\text{Hence Proved}}$

Corollary :- For $n \in \mathbb{N}$, $n+1 = n++$

Proof of corollary :- Set $m=0$ in previous Lemma.

Exercise :- 1. Commutativity :- $m+n = n+m$

2. Associativity :- $m+(n+p) = (m+n)+p$ [$m+n+p$ is well-defined]

3. Cancellation :- If $m+n = m+p$, then $n = p$.

Def'n :- A natural number is positive if it is not equal to zero (0)

Property :- If a is positive and $b \in \mathbb{N}$, then $a+b$ is positive.

Proof of property :- Fix a and induct on b. For $b=0$, $a+0 = a$ (by Lemma) which is positive.

Now suppose $a+b$ is positive.

Then $a+(b++) = (a+b)++$ which cannot be zero by Axiom - 3.

$\boxed{\text{Hence Proved}}$

Exercise :- 1. If $m, n \in \mathbb{N}$ st $m+n=0$, then $m+n=0$

2. Let a be positive, then there exists a unique natural number b st $b++ = a$

Def'n (Order) :- Let $m, n \in \mathbb{N}$. We say that n is greater than or equal to m denoted $n \geq m$ or $m \leq n$ if $n = m+a$ for some $a \in \mathbb{N}$. We say that n is strictly greater than m if $n \geq m$ and $n \neq m$, written $n > m$ or $m < n$.

Note that $n++ > n$ and this implies there is no largest numbers.

Properties :- Let $a, b, c \in \mathbb{N}$

i. $a \geq a$ (Reflexivity)

ii. $a \geq b$ and $b \geq a \Rightarrow a = b$ (Antisymmetry)

iii. $a \geq b$ and $b \geq c \Rightarrow a \geq c$ (Transitivity)

Partially Ordered Set. (POSET)

iv. $a \geq b \Leftrightarrow a+c \geq b+c$

iv, $a > b \iff a \geq b{+}{+}$

vi, $a > b \iff a = b + c$ for some positive c.

Property (Trichotomy) :- Let $a, b \in \mathbb{N}$, Then exactly one of the following holds:- $a > b$, $a = b$, $a < b$.

From Now on, we will assume the usual rules of addition.

Def'n:- Define the binary operator multiplication $* : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ as follows. Let $m \in \mathbb{N}$, Set $0 * m = 0$. Now suppose $(n * m)$ is defined. Then $(n{+}{+}) * m = (n * m) + m$.

Lemma :- Let $m, n \in \mathbb{N}$. Then $m * n = n * m$

Lemma (No Zero Divisors) :- Let $m, n \in \mathbb{N}$. Then $mn = 0$ iff atleast one of m and n is 0 (zero).

Property (Distributivity) :- For $a, b, c \in \mathbb{N}$, $a * (b + c) = (a * b) + (a * c)$

and $(b + c) * a = (b * a) + (c * a)$

Proof of property :- It suffices to prove the first equality by the previous Lemma.

Fix a, b and induct on c.

If $c = 0$, then LHS $= a * (b + 0) = a * b$

RHS $= (a * b) + (a * 0) = (a * b) + 0 = (a * b)$

Now assume the result holds for c.

For $c{+}{+}$, LHS $= a * (b + (c{+}{+}))$

$= a * ((b + c){+}{+})$

$= (a * (b + c)) + a$ [By def'n & Lemma]

$= (a * b) + (a * c) + a$

RHS $= (a * b) + (a * (c{+}{+})) = (a * b) + (a * c) + a$

Hence Proved

Properties :- i. Associativity :- $a * (b * c) = (a * b) * c$

ii. Order - Preserving :- If $a, b, c \in \mathbb{N}$ st $a < b$ and c is $\boxed{\text{positive}}$

then $a * c < b * c$

then $a * c < b * c$

Corollary (cancellation) :- If $ac = bc$, and c is positive then $a = b$

Property (Euclidean Algorithm) :- Let $n \in \mathbb{N}$ and m be positive, then there exists $q, r \in \mathbb{N}$ st $0 \leq r < m$ and $n = mq + r$