Mathematical & Statistical Foundations (MSF)

Unit-1 : Notes-1

Basics

1

[illegible]

Unit-1 :- Greatest Common Divisors & Prime Factorization :-

Part -A :-

$\boxed{\text{Greatest Common divisors}-(GCD)}$ → Main thing is this Unit.

The Euclidean algorithm -

The Fundamental theorem of arithmetic -

Factorization of integers -

& the Fermat numbers. , Fermat's Factorization

Part - B :- Congruences :-

Introduction to Congruences - $a \equiv b \pmod{m}$ → Congruence very bad.

Linear Congruences -

The chinese remainder theorem -

Systems of Linear Congruences. → System of Linear Congrues (or [illegible] [illegible] Congruences [illegible].)

29 NSF

MSF(

Introduction:- Airthmetic:-

Airthmetic, branch of mathematics in which numbers, relations among numbers, observations on numbers are studied.

&

Used to solve problems.

Elementary Number Theory:-

Elementary Number theory is the study numbers especially (in particular), the study of the set of positive integers.

Number theory:-

Definition:- (Modern definition)

"The theory associated with numbers has been applied to the problems associated with the transmission, coding, manipulation of numerical data, Cryptography & study of secret messages.

General Definition:-

Number theory is a branch of pure mathematics & especially to the ~~study~~ of the integers & arithmetic functions.

Great mathematician Gauss said

"Mathematics" is the Queen of the Sciences-
&
"Number theory" is the Queen of Mathematics."

Algorithms 3

Course objectives:—

→ To identify the greatest Common divisor using Prime Factorization.

ie GCD $\xrightarrow{\text{using}}$ Prime Factorization

→ To apply " Euclidean Algorithm & Compute gcd of 2 (or) large integers.

→ To understand the Concept of Congruence & Use Various results related to Congruence including " The chinese Remainder theorem "

GCD → P. Factorization

Euclidean Algorithm → 2 (or) more integers

Congruence → chinese remainder theorem

Algorithms

Euclidean

MSF

Unit-1

Course Outcomes:-

After learning the Contents of this Course, the student must be able to

→ Apply the $\boxed{\text{Number theory}}$ Concepts to Cryptography or Cryptography domain

→ Apply the Concepts of $\boxed{\text{probability \& distributions}}$ to some $\boxed{\text{Case Studies}}$.

→ Correlate the material of One Unit to material in other Units.

i.e Unit-2 (R.V, DRV) ↓ Unit-3 (CRV) ↓ Unit-4 (Estimation, Testing of hypothesis)	& Finally Unit-5 ↓ Stochastic Process

→ Reduce the potential

Misconceptions & Hazards in early

topic of Study

→ Realise the potential

$\boxed{\text{Misconceptions}}$ & $\boxed{\text{Hazards}}$ in each

topic of study.

Scanned with CamScanner

→ Resolve the potential

$\boxed{\text{MisConceptions}}$ & $\boxed{\text{Hazards}}$ in each

topic of study.

Introduction:-

→ This unit Continuously to deal with $\boxed{\text{Divisibility}}$ in Number theory.

→ We start to begin, Exploring the Common Set of factors of 2 or more positive integers.

→ Here, we use +ve integers

→ We use notation $a | b \Rightarrow$ read as a divides b.

divide

$a \nmid b \Rightarrow \boxed{a}$ does not divide $\boxed{b}$

We will establish "the Fundamental theorem of Arithmetic." (one of the best results in Number theory)

move to

Algorithms

Then, We can move to

Common Multiplies of 2 or more positive integers.

Positive Integers

Here, Some +ve integers have exactly

1

2 +ve Factors

2

Some have more than 2

1 7 2 9

7 + 10

7 + 12

12 = 2×6

ie 6 ≠ 2×6

we can move to

Prime Factorization [i.e P.F is a process of factoring a number in terms of Prime numbers.]

move to

It would be pretty difficult without

to perform Prime Factorization

Integers:— (or) Set of Integers:—

It is represented with $\boxed{Z}$

we use here this only

include 0

+ve integers

$\downarrow$

1, 2, 3, 4 . . .

-ve integers

$\downarrow$

-1, -2, -3, -4 .

$$\therefore\ Z = \{0, \pm 1, \pm 2 \cdots\}$$

Prime Factorization :—

Define Prime Factorization :—

or

Explain Prime Factorization :—

"Prime Factorization" is finding in which Prime numbers $\boxed{\text{multiply}}$ together to make the Original number.

→ [The Method of prime factorization is used to break down or Express a given number as a product of prime numbers.]

Euclides Lemma Method.

Developing theory of Real numbers :—

Developing theory of Real numbers we used Peano

Explain Peano's Axioms?

@ ⓐ Dedekind-Peano axioms

(or) Write the 3 - peano's axioms in detail?

→ The basic Mathematical System is the Set $\boxed{N}$ of +ve integers.

→ The +ve integers always can be defined by a set of axioms, are called as peano's axioms. In this, we have THREE Axioms

Axiom-1 :- Gives that N is non-empty

here we use 1 instead of 0

i.e $\exists$ Natural number = 1

Axiom-2 :- gives that $\boxed{f(m)=f(n) \Rightarrow m=n}$

It tells equality relation.

Axiom-3 :- States that " Natural number $\boxed{1}$ is non - Successor.

(or)

0 is not the Successor of any numbers.

Axiom - II

A → 1 ⇒ N· ● = this is Zero

A → 2 ⇒ N=0 1 2 3 ————

● —— O — O — O

here N = n ⇒ Natural number,

successor successor successor

O —— 1 ——— 2 ——— 3

i.e for Every Natural number n,

there is another natural number called

Successor [n]

$f(n) = n+1$ → always it

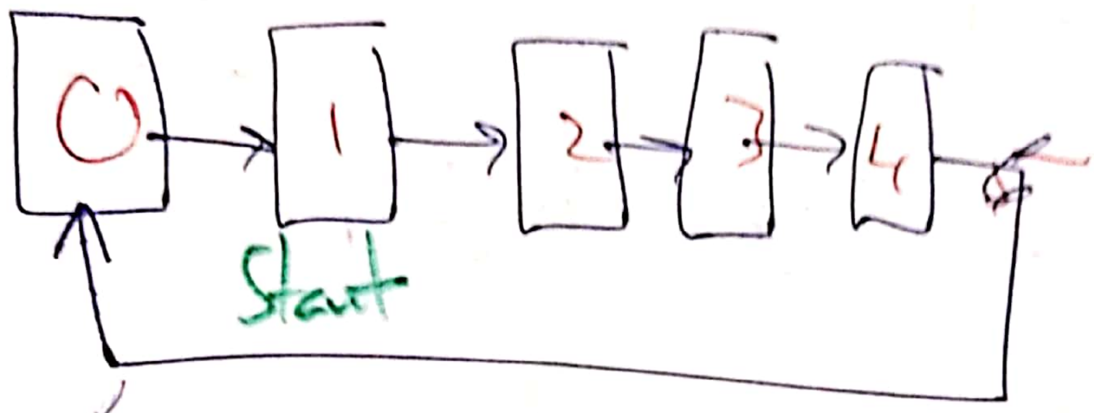
is increasing only. called Successor

Axiom 3 ⇒

1 2 3

○ —— ● —— O —— O —— O ...

ie No natural number has $\boxed{0}$ as its successor.



It can't go like that

ie 0 = first Natural Numbers.

0 1 2 3

Axiom - 2

we will write $2 = 1+1$

$3 = 2+1$

Write Basic Properties of Integers

We represent
the set of positive integers by $\boxed{N}$
&
the set of integers by $\boxed{Z}$

$N = \{1, 2, 3 \dots\}$

$Z = \{\dots -2, -1, 0, 1, 2 \dots\}$

There are six (6) properties are there

with $\boxed{\text{Addition \& Multiplication.}}$

1) Commutative laws :—

$$\boxed{\begin{aligned} a+b &= b+a \\ a \cdot b &= b \cdot a \end{aligned}} \quad \forall\, a, b \in Z$$

2) Associative Laws :—

$$\boxed{\begin{aligned} a+(b+c) &= (a+b)+c \\ a \cdot (b \cdot c) &= (a \cdot b) \cdot c \end{aligned}} \quad \forall\, a, b, c \in Z$$

(3) Additive Inverse:—

$(\bar{a}^{1})$ or $-a$

$$\boxed{a+(-a)=0=(-a)+a} \quad \forall\, a \in Z$$

The integer $\boxed{-a}$ is called the additive inverse of $\boxed{a}$.

(4) Identity elements:—

(0 — additive identity
1 — multiplicative identity)

$$\boxed{\begin{aligned} a+0 &= a = 0+a \\ a\cdot 1 &= a = 1\cdot a \end{aligned}} \quad \forall\, a \in Z$$

where 0 = Additive Identity
1 = Multiplicative identity.

(5). Distribution Laws:—

+, · in one equation

$$\boxed{\begin{aligned} a\cdot(b+c) &= a\cdot b + a\cdot c \\ (b+c)\cdot a &= b\cdot a + c\cdot a \end{aligned}} \quad \forall\, a \in Z$$

6) Well-ordering principle: positive integers

at least one element in +ve integers

Any non-empty subset of non-negative integer has a least element.

i.e

If S = Non-empty subset of non-negative integers. Then $\exists\ n \in S$ such that $\boxed{n \leq m}$ $\forall\ m \in S$.

---

i.e
non-negative integer = +ve integers

i.e
Set of integers $= \{\ldots -2, -1, 0, 1, 2, \ldots\}$
but all set of all integers are not well ordered.

This principle we use in many theory division algorithm also ... etc

Since we will use in Prime factorization (product of primes). So, Ex:- N = Set of Natural Number

$N = \{1, 2, 3, \ldots\}$

1 at least number

$S = \{2, 4, 6, \ldots\}$

$a < b$

$1 < 2$	$2 < 4$
$2 < 3$	$4 < 6$

It is following

Note:-

1. Natural Numbers are also called as +ve integers.

$N = \{1, 2, 3 \ldots \infty\}$

Integers = $\{\ldots -2, -1, 0, 1, 2 \ldots\}$

whole Numbers = $\{0, 1, 2 \ldots\}$

$N = \{1, 2, 3 \ldots\}$

i.e N = we should not include fractions, decimals, irrationals or -ve numbers.

Set of Integers :-

22 MSF

Unit-I

$Z = \{0, \pm 1, \pm 2 \cdots \cdots\}$

Set of +ve integers $= N =$ Set of Natural Numbers

$= \{1, 2, 3, \cdots \cdots\}$

Scanned with CamScanner

Algorithm

Divisibility :- Define Divisibility ?

Let $a, b \in Z$ a, b = Two integers.

where $b \neq 0$. Then $\boxed{b \text{ divides } a \text{ (or) } b|a}$ if $\exists$

an integer q : $\boxed{a = bq}$ (or) $b = ac$ quotient

Representation :- (Notation)

b divides a $\Rightarrow b|a \Rightarrow 2|4$; $3|9$; $4|16$

factor of b
multiple of b

b doesnot divides a $\Rightarrow b \nmid a \Rightarrow 2 \nmid 5$; $2 \nmid 7$;

b =

$b|a$ = b divisor of a (or) Factor of a

(or) a is called multiple of b

$2|4$ =

Here b = factor of a
& also
multiple of b $(2 \times 2 = 4)$

Algorithm

te:-

$\boxed{\text{/a is the quotient when b is divided by a}}$

$b|a$ is b divides a

Ex:- $a|b \Rightarrow b = a(2)$

✓ $2|12 \Rightarrow 12 = 2(6)$ or 2×6

$2|6 \Rightarrow 6 = 2 \times 3$

$2|20 \Rightarrow 20 = 2 \times 10$

over Problem

$3 \mid 15 \Rightarrow b \mid a$ i.e

b divides a.

This we can write multipleng 3

3×5 or

factors of 3.

Divident

Divisor $b = 3 \overset{a}{)\,15 = (}\, 5$ = quotient = q

or

15

0 → remainder = r

i.e a = divident

b = divisor

q = quotient

r = remainder

$\Rightarrow a = bq + r$ → division algorithm theorem.

NSF

Proper divisors:-

$a, b \in \mathbb{Z}, a \neq 0$

Then, we can say that

$\boxed{a}$ divided $\boxed{b}$ is a

proper divisors.

$$\boxed{\begin{array}{l} a \neq \pm 1 \\ a \neq \pm b \end{array}}$$

Ex:- Divisiors of 8 :-

i.e $b = 8$

$a = \boxed{\pm 1}, \pm 2, \pm 4, \boxed{\pm 8}$

$\times \qquad \times$

$\therefore$ Here 2 & 4 are properdivisiors

Improper divisors:-

Here, its mandatory,

it has to satisfy the

Conditions.

$$\boxed{a = \pm 1 \ \& \ a = \pm b}$$

$\therefore$ 1 & 8 are Improper divisors.

prime. The

prime

integer

integers

Divisors of $\boxed{8}$ are:- ① Indepth

$\pm 1, \pm 2, \pm 4, \pm 8$

$8 = \pm 1, \pm 2, \pm 4, \pm 8$

Proper divisors $= \pm 2, \pm 4$ (2, 4)

Improper divisors $= \pm 1, \pm 8$. (1, 8)

② Divisors of $\boxed{25}$ are:- $\pm 1, \pm 5, \pm 25$

Proper divisors $= \pm 5$ (5)

Improper divisors $= \pm 1, \pm 25$ (1, 25)

③ Divisors of $\boxed{-25}$ are:- $\pm 1, \pm 5, \pm 25$

proper divisors $= \pm 5$ (5)

Improper divisors $= \pm 1, \pm 25$. (1, 25)

~~Note:-~~ bitir

Divisors of $\boxed{a \& -a}$ are same.

Properties of division:— Write 3 properties of division

exive Property:- (Reflexive)

$a|a$ for every $a \neq 0 \in Z$

2) Transitive Property:-

$a|b$ & $b|c \Rightarrow a|c$

3)

$a|b$ & $a|c \Rightarrow a|mb+nc$, where $m,n \in Z$

4) $a|b \Rightarrow am|bm$, where $m \neq 0 \in Z$

5) $\pm 1|a \quad \forall a \in Z$

(± 1 are Universal divisors)

6) $a|c \quad \forall a \neq \in Z$

(7) If $a|b$ & $b \neq 0$

(8) If $a|b$ & $b|a$. Then $|a| = |b|$.

Ex: $5|-5 \Rightarrow |5| \leq |-5|$

$2|8 \Rightarrow |2| < |8|$

$3|-12 \Rightarrow |3| < |-12|$

$b \neq 0$: $3|0 \Rightarrow |3| \nleq |0|$

(9) $\boxed{a \text{ \& } -a}$ have same divisors.