Number Theory
(2nd book Portion)

3.2 Primes, Prime counting function, Prime number theorem

Def": ① Composite number: A natural number n is said to be composite if it has a non-trivial divisor, d s.t $1 < d < n$. If so then $n = dc$ where $c = n/d$.

② Prime Number: A natural no. p is said to be prime if $p > 1$ and p has no non-trivial divisor.

Eg: 2, 3, 5, 7.

Thm 3.1 If m is a natural number and p is a prime, then $(m, p) = \begin{cases} p & \text{if } p \mid m \\ 1 & \text{if } p \nmid m. \end{cases}$

Proof Let $(m, p) = d$

$\Rightarrow d \mid m$ & $d \mid p$.

Since $d \mid p$ and p is prime $\therefore$

$\therefore \Rightarrow d = 1$ or $d = p$.

Hence the result.

Thm 3.2 If p is a prime and $p \mid ab$ then $p \mid a$ or $p \mid b$.

Proof: Let $p \mid ab$

If $p \mid a$ we are done

If $p \nmid a \Rightarrow (p, a) = 1$.

$\Rightarrow \exists\ q$ & r s.t $pq + ar = 1$.

Multiply b on both the sides

$$pbq + abr = b$$

Now $p \mid pbq$ & $p \mid abr$

$\Rightarrow p \mid pbq + abr \Rightarrow p \mid b$. □

Thm 3.3 If p is a prime, $n \geq 2$ and $p \mid \prod_{i=1}^{n} a_i$, then $p \mid a_i$ for some i.

Proof: We will prove it by induction on n.

If $n = 2$ i.e $p \mid a_1 a_2$

$\Rightarrow p \mid a_1$ or $p \mid a_2$ which completes for this part

Let it be true for n.

We will prove it for $n+1$

If $p \mid a_1 a_2 \cdots a_{n+1} \Rightarrow p \mid (a_1 a_2 \cdots a_n)\, a_{n+1}$

$\Rightarrow p \mid a_1 a_2 \cdots a_n$ or $p \mid a_{n+1}$

$\Rightarrow p \mid a_1$ or $p \mid a_2 \cdots$ or $p \mid a_n$ or $p \mid a_{n+1}$

(By Induction hypothesis)

Hence result is true for all n.

Thm 3.5 If n is composite and if p is the least prime factor of n, then $p \leq \sqrt{n}$.

Proof: By given hypotheses

$n = pm$ as p is least prime factor of n.

with $m > 1$.

$\Rightarrow$ m has a prime factor q, so $q < m$

If $m < p \Rightarrow q < p$

and $q \mid m$ & $m \mid n \Rightarrow q \mid n$

which contradicts the fact that p is least prime factor of n

$\therefore$ $p \leq m$. so $p^2 \leq pm$.

$\Rightarrow p^2 \leq n$

$\Rightarrow p \leq \sqrt{n}$.

Thm 3.4. If $n > 1$, then n has a prime factor p.

Proof: If n is prime we are done

If n is composite, let p be the least non-trivial divisor of n.

If p is composite, then p has a non-trivial divisor d.

$d \mid p$ & $p \mid n$

$\Rightarrow d \mid n$ & $d < p$ which is a contradiction that p is least

$\therefore$ p is prime. $\square$.

Thm 3.6 There are infinitely many primes.

Done in the class.

Thm 3.7 ∃ arbitrarily large gaps b/w consecutive primes.

Proof: Let $n \geq 2$.

For each k s.t $2 \leq k \leq n$ we have

$k \mid (n! + k)$ (as $k \mid n!$ & $k \mid k$)

$\therefore n!+2, n!+3, n!+4, \ldots, n!+n$ is a sequence of $n-1$ consecutive composite numbers.

Let p be the greatest prime s.t $p \leq n!+1$

Let q be the least prime s.t $q > n! + n+1$

$\therefore p$ & q are consecutive primes and

$$q - p \geq n.$$

Def 3.3 Prime Counting function.

If x is a the real no. then prime counting function counts the no. of primes p s.t $p \leq x$ and denoted by $\pi(x)$

Eg. $\pi(10) = 4$.

Def 3.4 Let $f(x)$ & $g(x)$ be defined for $x > 0$

$f(x), g(x) \in \mathbb{R}$.

Then $f(x) \sim g(x)$ [ie $f(x)$ is asymptotic to $g(x)$ if

$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 1.$$

Thm 3.6 Prime Number Thm.

$$\Pi(x) \sim \frac{x}{\log x}$$

(Proof Not to be done)

Don't do exercise

Chapter - 5

Def 5.1 Summation function

We say $g(n)$ is summation function of $f(n)$

if $g(n) = \sum_{d|n} f(d)$. (Studied previously)

Recall $\sigma(n)$ = sum of divisors of n $= \sum_{d|n} d$.

$\tau(n) = \sum_{d|n} 1$

Multiplicative fn.

Def 5.5 Totally Multiplicative fn.

If f is number theoretic function such that

$f(mn) = f(m) \cdot f(n)$ $\forall$ m, n. then

f is totally multiplicative fn.

~~Thm 5.2 If f~~

~~and g are multiplicative and~~

~~$f(n) \neq 0$ then~~

Defⁿ 5.1 Dirichlet Product

Let f and g be arithmetic functions. We define their Dirichlet product as

$$(f*g)(n) = \sum_{d|n} f(d) g(n/d)$$

~~Eg.~~

$$\Gamma * \sigma(4) = \sum_{d|4} \Gamma(d) \sigma(4/d)$$

$$= \Gamma(1)\sigma(4) + \Gamma(2)\sigma(2) + \Gamma(4)\sigma(1)$$

$$= 1\cdot(1+2+4) + 2(1+2) + 3(1)$$

$$= 7+6+3 = 16$$

Properties

a) $f*g = g*f$.

$\rightarrow$ $f*g = \sum_{d|n} f(d) g(n/d)$

Let $n/d = c \Rightarrow c|n$.

$\therefore = \sum_{c|n} f(n/c) \cdot g(c)$

$= g*f$

b) $(f*g)*h = f*(g*h)$.

$\rightarrow (f*g)*h = \sum_{d|n} (f*g)(d)\, h(n/d)$

$= \sum_{d|n} \sum_{c|d} f(c)\, g(d/c)\, h(n/d)$.

$= \sum_{c|d|n} f(c)\, g(d/c)\, h(n/d)$

Let $n = de$ & $d = cf$. $\Rightarrow n = ecf$

$\therefore = \sum_{cde=n} f(c)\, g(f)\, h(e)$.

$ecf = n$

Illy. RHS.

c) $f * I = f$.

$\rightarrow (f*I)n = \sum_{d|n} f(d)\, I(n/d)$.

If $d < n \Rightarrow n/d > 1$ so $I(n/d) = 0$. $\Rightarrow d = n$

$\therefore (f*I)(n) = f(n) I(1) = f(n) \cdot 1 = f(n)$.

d) $f * u = \sum_{d|n} f(d)$

$\rightarrow (f*u)(n) = \sum_{d|n} f(d)\, u(n/d) = \sum_{d|n} f(d) \cdot 1$

$= \sum_{d|n} f(d)$

Thm 5.4 If f & g both are multiplicative, then so $f * g$.

Proof: Let $h = f * g$. and $(m, n) = 1$

Then $h(mn) = (f * g)(mn)$

$$= \sum_{d \mid mn} f(d)\, g\left(\frac{mn}{d}\right)$$

$$= \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1, d_2)\, g\left(\frac{mn}{d_1 d_2}\right)$$

$[\because (m, n) = 1]$

$$= \sum_{d_1 \mid m} \sum_{d_2 \mid n} f(d_1) \cdot f(d_2)\, g\left(\frac{m}{d_1}\right) g\left(\frac{n}{d_2}\right)$$

($\because f$ & g are multiplicative)

$$= \sum_{d_1 \mid m} f(d_1)\, g\left(\frac{m}{d_1}\right) \cdot \sum_{d_2 \mid n} g(d_2)\, g\left(\frac{n}{d_2}\right)$$

$$= (f * g(m)) \cdot (f * g(n))$$

□.

Thm 5.5 ~~If f is multi~~ Done already.

Thm 5.6 done already ; Thm 5.7, 5.8, 5.9 already done.

SYLLABUS COMPLETED.