Bharathidasan University
Tiruchirappalli - 620 024
Tamil Nadu, India

Programme: M.Sc., Mathematics

Course Title :Theory of Numbers
COurse Code : 21M04CC

Pime Numbers

Dr. V. Piramanantham
Professor
Department of Mathematics

Prime number:

① a number $c > 1$ is called reducible if

$$c = ab \quad \text{—①}$$

for some a & b integers s.t.

$$1 < a, b < c.$$

Eqn ① $\Rightarrow$ $a \mid c$ for some a with $1 < a < c$

② An integer $c > 1$ is reducible if

$\exists$ an integer a s.t. $1 < a < c$

and $a \mid c$

③ An integer $c > 1$ is irreducible if

$\nexists$ no integer a s.t. $1 < a < c$

& $a \mid c$

Prime:

An integer $p > 1$ is said to be prime if whenever $p \mid ab$, either $p \mid a$ or $p \mid b$.

Irreducible integer is always prime and vice-versa

Theorem: Let p be an integer greater than 1. The following are equivalent:

irreducible

(prime)

(1) There is no integer a s.t. $1 < a < p$ and $a \mid p$

(2) If $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Proof: (1) $\Rightarrow$ (2)

$1 < k < p \Rightarrow k \nmid p$

Let $p \mid ab$. Then we prove that $p \mid a$ or $p \mid b$.

Assume that $p \nmid a$.

Let $k = (a, p)$.

$k \mid p \Rightarrow k = 1$ or $k = p$

$k \mid a$. If $k = p$

then $p \mid a$ $\Rightarrow\Leftarrow$ to our assumption

$\therefore k = 1$

(ie) $(p, a) = 1$

$\therefore p \mid b$ By the result stating that: if $a \mid bc$ & $(a,b) = 1$ then $a \mid c$.

(2) holds.

(2) $\Rightarrow$ (1).

To prove (1), let $p = ab$. — (1)

Then we have to prove that $a = 1$ or $a = p$

$p = ab \Rightarrow p \mid ab \overset{(2)}{\Longrightarrow} p \mid a$ or $p \mid b$

If $p \mid a$, then $a \neq 1$ & $\exists\ c \in \mathbb{Z}$ s.t. $a = pc$ — (2)

Substituting (2) into (1), we get

$$p = pcb$$
$$\Rightarrow cb = 1$$
$$\Rightarrow c = 1 \ \& \ b = 1$$

If $p \nmid b$, the similar argument leads that $a = 1$.

Hence if $p = ab$, then either $a = 1$ or $a = b$

(e) the only +ve divisors of p are 1 & p itself

(1) is proved //

2nd definition:

An integer $p > 1$ is called prime if there is no divisor d of p satisfying $1 < d < p$

If $a > 1$ is not a prime number, then it is called a composite number.

Theorem: Let p be a prime. If $p \mid ab$ then either $p \mid a$ or $p \mid b$

Corollary: Let p be a prime. If $p \mid a_1 a_2 \cdots a_n$ then $p \mid a_i$ for some $i = 1, 2, \cdots n$.

Proof Use induction on n to prove it.

$p \mid a_1 a_2 \cdots a_n$ $\Leftarrow$ $n = 2$, $p \mid a_1 a_2$

Theorem An integer $n > 1$ can be expressed as a product of primes

Ex: p is prime $1 < d < p$, $d \nmid p$

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~

11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 20

primes are blocks of number theory

$n > 1$, $n = p_1 p_2 \cdots p_n$, $p_1, p_2, \ldots, p_n$ are primes

$356 = 2 \cdot 2 \cdot 2$

$2 \mid 356$

$356 = 2 \cdot 178$

$2 \mid 178$

$178 = 2 \cdot 89$

$356 = 4 \cdot 89$

$= 2 \cdot 2 \cdot 89$

Theorem: An integer $n>1$ can be expressed as a product of primes

Proof

If n is prime, single integer n stands a product

n is not prime, $n = n_1 n_2$, $1 < n_1, n_2 < n$

If n_1 & n_2 are prime, $n = n_1 n_2$

If n_1 & n_2 are prime, $n = n_1 n_2$

If any one of n_1 & n_2 is not prime say n_1.

$n_1 = n_3 n_4$, $1 < n_3, n_4 < n_1 < n$

$\vdots$

finite stage.

$n = p_1 p_2 \cdots p_n$

Theorem

If $n = ab$, then either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$

Ex: $100 = ab$, $a \leq 10$ or $b \geq 10$

$\sqrt{100} = 10$

Corollary: Let $n > 1$ be an integer

If there is not divisor d such that $1 < d \leq \sqrt{n}$,

then n is prime

Proof of the Theorem

If $n = ab$
$\Rightarrow$ either $a \leq \sqrt{n}$
or $b \leq \sqrt{n}$

suppose that both
a & b are greater than $\sqrt{n}$

$$a > \sqrt{n} \quad \& \quad b > \sqrt{n}$$

$$ab > \sqrt{n} \cdot \sqrt{n} > n$$

$\Rightarrow \Leftarrow$ to $n = ab$

Corollary (proof)

There is no divisor d s.t. $1 < d \leq \sqrt{n}$

claim n is prime

suppose n is not prime

$\exists$ a & b s.t.

$n = ab$, $1 < a, b < n$

Here a & b are divisors of n

$\Rightarrow$ both a & $b > \sqrt{n}$

$\Rightarrow \Leftarrow$ to the theorem.