Date :
No:

Number theory lec3

Primes & Composite

Defination

An integer $P > 1$ is Prime if the only Positive factors of P are $1, P$ o.w P is Composite

Ex which of the following are Primes

(a) 4 $\longrightarrow$ Composite $2 | 4$
(b) 17 $\longrightarrow$ Prime
(c) 23 $\longrightarrow$ ~
(d) 27 $\longrightarrow$ Composite $3 | 27$

Theorem:

If $n \in \mathbb{Z}^+$ then there is a unique increasing sequence of primes: $P_1, P_2 \ldots P_m$ such that

$$n = P_1 P_2 \ldots P_m$$

$P_1, P_2 \ldots, P_m$ are Prime factorization of n

Date :
No:

Ex find the prime factorization of $n = 100$?

$\frac{100}{2} = 50 \qquad \frac{50}{2} = 25 \qquad \frac{25}{5} = 5 \qquad \frac{5}{5} = 1$

$$2 \times 2 \times 5 \times 5 = 100$$

Theorem:-

If let $n \in \mathbb{Z}^+$

① If $n = ab$ then the prime factorization of n is the result of merging the prime factorization of a, b

② If p is a prime, $p \mid n$ & $p_1, p_2, \ldots p_m$ is the prime factorization of n then $p = p_i$ for some $1 \leq i \leq p_m$

Theorem:-

If n is a composite then n has a prime factor $\leq \sqrt{n}$

مش محتاج علشان تشوف ان الرقم prime انك
تقسم على كل الارقام لحد n كفاية تبقى لحد $\sqrt{n}$

Proof:-
let $n = ab$
assume by contradiction. len $a > \sqrt{n}$, $b > \sqrt{n}$

$ab > n \quad \therefore \neg(a > \sqrt{n} \wedge b > \sqrt{n})$

$\therefore a \leq \sqrt{n} \vee b \leq \sqrt{n}$ assume without losing Generality That $a \leq \sqrt{n}$

Date :
No:

$a \leq \sqrt{n}$

a is Prime

$a|n$, a is Prime

a is Composite

There exist some Prime p such that $p|a$

$\therefore a|n$

$\therefore p|n$

Ex:-

Determine whether $n = 307$ is Prime or not?

Sol:-

$\sqrt{n} = \sqrt{307} = 17.\sim$

Prime $\leq \sqrt{n}$

2, 3, 5, 7, 11, 13, 17

$\frac{307}{2} \neq int$ $\quad \frac{307}{5} \neq int$ $\quad \frac{307}{11} \neq int$ $\quad \frac{307}{17} \neq int$

$\frac{307}{3} \neq int$ $\quad \frac{307}{7} \neq int$ $\quad \frac{307}{13} \neq int$

$\therefore$ 307 is Prime

Date :
No:

Theorem:-

there are infinitely many Primes

Proof:-

By Contradiction assume there are finite number of primes

assume Primes: $P_1, P_2, \dots, P_m$

let $n = P_1 P_2 \dots P_m + 1$

n should Be Composite Bec. P_m is the largest Prime & $n+1$ is also Prime

there exist P_i for some i such that $P_i \mid n$

$P_i \mid P_1 P_2 \dots P_m$ كل ال Primes *

$P_i \mid n - P_1 P_2 \dots P_m$

$P_i \mid 1$

Contradiction

لو n اكبر من Prime لازم يبقى " next Prime "

$\therefore$ There exist infinite number of Primes

Date :
No:

Uniqueness of Prime factorization

If $n \in \mathbb{Z}^+$ then there exist a unique prime factorization for it.

Proof:-

assume there exist two distinct Prime factorization for n

A2 Prime factorizations: $P_1, P_2, \ldots, P_k$ & $q_1, q_2, \ldots, q_m$

$$n = P_1 P_2 \cdots P_k = q_1 q_2 \cdots q_m$$

Dividing by common primes

$$P_1' P_2' \cdots P_k' = q_1' q_2' \cdots q_m'$$

مش موجودة ال P في وموجودة ال q

$\therefore P_1' \mid LHS$

$\therefore P_1' \mid RHS$

$P_1' = q_j'$ for some $j \in \{1, 2, \ldots m'\}$

Contradiction

$\therefore$ wrong assumption

$\therefore$ Prime factorization is unique for any $n \in \mathbb{Z}^+$

Date :
No:

Greatest Common divisors:- (GCD)

Definations:-

$\gcd(a,b)$ is the largest positive integer d that divides both a,b (not both of $a,b=0$)

$\gcd(a,b) \mid a$, $\gcd(a,b) \mid b$ & if $c \mid a \wedge c \mid b \rightarrow c \leq d$

if $c \mid a \wedge c \mid b \rightarrow c \leq d$

If $\gcd(a,b)=1$ then a,b are relativly prime ex: $25, 9$

gcd between any the integer & 0 is this the integer

Ex

$\gcd(24,16)=8$

$\gcd(9,17)=1 \rightarrow 9,17$ are relativly prime

$\gcd(239,0)=239$

Date :
No:

Euclid's lemma:-

$$d|a \wedge d|b \longleftrightarrow d|a-b \wedge d|b$$

$$d \in Z^{+} \, , \, a, b \in Z$$

So $\gcd(a,b) = \gcd(a-b, b)$

Proof:-

① let $d|a \wedge d|b$

$\therefore d|a-b$

$\therefore d|b$

$\therefore d|a-b \wedge d|b$

② let $d|a-b \wedge d|b$

$\therefore d| a-b+b$

$\therefore d|a$

$\therefore d|b$

$\therefore d|a \wedge d|b$

Theorem:-

let $a = qb + r$ where $a, b, q, r \in Z$

Then $\gcd(a,b) = \gcd(b,r)$

In other words:

$\gcd(a,b) = \gcd(b, a \bmod b)$

Date :
No:

Proof:-

① let $d|a \wedge d|b$

$\therefore d|b$

$\therefore d|a-qb$

$\therefore d|r$

$\therefore d|b \wedge d|r$

$\therefore d|a \wedge d|b \rightarrow d|b \wedge d|r$

$\therefore$ and common divisor of a, b is als
" " " b, r

② let $d|b \wedge d|r$ a

$\therefore d|b \;,\; d|(qb+r)$

$\therefore q|b \wedge d|a$

$d|b \wedge d|r \rightarrow d|a \wedge d|b$

$\therefore d|a \wedge d|b \leftrightarrow d|b \wedge d|r$

$\therefore gcd(a,b) = gcd(b,r)$

$\therefore gcd(a,b) = gcd(b, a \bmod b)$

Date :

No:

lemma:

let $a \geq b > 0$ then $a \bmod b < \frac{a}{2}$

Proof:

$b < \frac{a}{2}$	$b = a$	$b \geq \frac{a}{2}$
$a \bmod b < b$	$b \mid a$	$q = \lfloor \frac{a}{b} \rfloor = 1$
$a \bmod b < \frac{a}{2}$	$\therefore a \bmod b = 0$	$r = a - qb$
	$\therefore a \bmod b < \frac{a}{2}$	$r = a - b$
		$r < \frac{a}{2}$

In all cases $a \bmod b < \frac{a}{2}$