Prime Numbers: An integer $p > 1$ is called a prime number, or simply a prime, if its only positive divisors are 1 and p.

Ex: 2, 3, 5, 7, 11 etc

An integer greater than 1 that is not a prime is termed composite.

Ex: 4, 6, 8, 9, 10 etc.

Note: 2 is the only even prime.

1 is neither prime nor complete.

Theorem: If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof: If $p \mid a$, then we no need to prove.

Assume that $p \nmid a$.

$\Rightarrow \gcd(p, a) = 1$. ($\because$ the only positive divisors of p are 1 and p itself)

$\Rightarrow$ Hence, $p \mid b$, by Euclid's lemma

Ex: $3 \mid 42 = 6 \times 7$ and $3 \mid 6$ even though $3 \nmid 7$.

Whereas $4 \mid 12 = 2 \times 6$, but $4 \nmid 2$ as well as $4 \nmid 6$ (as 4 is not a prime)

Note: 1) If p is a prime and $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_i$, for some $1 \le i \le n$.

2) If $p, q_1, q_2, \cdots, q_n$ are all prime, and $p \mid q_1 q_2 \cdots q_n$, then

$p = q_i$, for some $1 \le i \le n$.

Fundamental Theorem of Arithmetic.

Every positive integer n > 1is either a prime or a product of primes; this representation is unique, apart from the order in which the factors occur.

Proof :- If n is prime, then $n = n$ is the required representation

If n is a composite number, then n has a non-trivial divisor, say a.

$\Rightarrow a|n$ or $n = ab$, for some integer b.

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

It is enough, if we prove the theorem for a and b, instead of n.

Repeating the same argument, for a, b and smaller

factors, which are all greater than 1, but less than n, we get primes, $p_1, p_2, \ldots, p_k$ such that $n = p_1 p_2 \cdots p_k$.

Uniqueness:-

let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ and

$n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$ be two distinct representations of n.

Then $p_i \mid n = q_1^{\beta_1} \cdots q_s^{\beta_s}$, $\forall i$

$\Rightarrow p_i = q_j$ for some j, $1 \le j \le s$.

Now $q_j^{\beta_j} = p_i^{\beta_j}$ and $p_i^{\alpha_i} \mid n$

$\Rightarrow p_i^{\alpha_i} \mid p_i^{\beta_j}$

$\Rightarrow \alpha_i \le \beta_j$

For the similar argument,

$\beta_j \le \alpha_i$

$\Rightarrow \alpha_i = \beta_j$ whenever $p_i = q_j$

$\Rightarrow r = s$

$\therefore n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ and

$n = q_1^{\beta_1} \cdots q_s^{\beta_s}$ are same representations, except the order of primes

$\Rightarrow$ Uniqueness.

Canonical representation:-

For $n > 1$, the representation $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, with $p_1 < p_2 < \cdots < p_r$ is a canonical representation of n as a product of prime numbers.

Ex:- $4200 = 2^3 \times 3 \times 5^2 \times 7$

$10780 = 2^2 \times 5 \times 7^2 \times 11.$

G.C.D:-

If $a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$

$b = p_1^{\beta_1} \cdots p_r^{\beta_r}$

then $g.c.d(a,b) = p_1^{\gamma_1} \cdots p_r^{\gamma_r}$

where each $\gamma_i = \min\{\alpha_i, \beta_i\}$

Ex:- $\gcd(4200, 10780)$

$= 2^2 \times 5 \times 7 = \underline{140}$

Exactly divides:-

$p^\alpha \| a$ (i.e., p^α exactly divides a)

if $p^\alpha | a$ and $p^{\alpha+1} \nmid a$

(i.e., α is the largest exponent

of p, such that $p^\alpha \mid a$)

Ex:- $2^3 \| 24$ ($\because 2^3 = 8 \mid 24$ but $2^4 = 16 \nmid 24$)

Note:- ① If $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ is the canonical representation of n, then $p_i^{\alpha_i} \| n$.

② If $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, then no. of divisors of n is equal to $(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_r+1)$.

(Infact, $p_i^{\beta_k} \mid n$, for $1 \le k \le i$, and $\forall i$.

$\Rightarrow$ there are $\alpha_i + 1$ choices for

each i, which are $p_i^0, p_i^1, p_i^2, \ldots, p_i^{k_i}$

Ex:- $24 = 2^3 \times 3$

$\Rightarrow$ There are $(3+1)(1+1) = 8$ divisors of 24.

They are: 1, 2, 3, 4, 6, 8, 12, 24

Ex:- Prove that any prime of the form $3n+1$ is also of the form $6m+1$.

Let $p = 3n+1$ is a prime.

$\Rightarrow p$ is odd. $\Rightarrow p-1 = 3n$ is even.

$\Rightarrow n$ is even, let $n = 2m$

$\Rightarrow p = 3(2m) + 1 = \underline{6m+1}$

Ex:- Each integer of the form $3n+2$ has a prime factor of this form.

Let $3n+2 = p_1 p_2 \cdots p_k$ be the factorization (allowing the repeation)

Each p_i is of the form, $3q+1$ or $3q+2$ (by division algorithm).

If <u>all</u> $p_i = 3q_i + 1$, then

$p_1 p_2 \cdots p_k = 3l + 1 \neq 3n+2$

(by uniqueness of division algorithm)

$\therefore$ there must be atleast one prime factor of the form <u>$3n+2$</u>

Ex:- Prove that only prime of the form n^3-1 is 7.

$$n^3-1=(n-1)(n^2+n+1)$$

If n^3-1 is prime either $n-1=1$ or $n^2+n+1=1$, which is not possible.

$\Rightarrow n=2$

$\Rightarrow n^3-1=7$.

Ex:- Prove that ten only prime p for which $3p+1$ is a perfect square is $p=5$.

$$3p+1=n^2 \Rightarrow 3p=n^2-1$$
$$=(n-1)(n+1)$$

If $p=5$, then $3p+1=16=4^2$.

$\Rightarrow n=4$

$3p=(n-1)(n+1) \Rightarrow n-1=3$, $n+1=p$

or

$n-1=p$, $n+1=3$

$\Rightarrow$ $\underline{n=4}$ or $\underline{n=2}$

$n=2 \Rightarrow 3p+1=2^2=4$

$\Rightarrow 3p=3 \Rightarrow p=1$ (not possible)

$p=5$ is the only case.

Ex:- The only prime of the form n^2-4 is 5

$p=n^2-4=(n-2)(n+2)$

$\Rightarrow$ $\begin{cases} n-2=1 \ \& \ n+2=p \\ \text{OR} \\ n-2=p \ \& \ n+2=1 \end{cases}$

$\Rightarrow$ $\begin{cases} n=3 \text{ and } p=5 \\ \text{OR} \\ n=-1 \text{ and } p=-3, \text{ not possible} \end{cases}$

$\therefore \underline{p=5}$ is the only prime.

Ex:- A prime $p \mid a^n \Rightarrow p^n \mid a^n$.

$$p \mid a^n = \underbrace{a \cdot a \cdot a \cdots a}_{n \text{ times}}$$

$$\Rightarrow p \mid a \Rightarrow a = p^k$$

$$\Rightarrow a^n = p^n k^n$$

$$\Rightarrow p^n \mid a^n$$

Ex:- If $n > 4$ is a composite, then $n \mid (n-1)!$

Let $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$

If $n > 1$, then $p_i^{\alpha_i} \mid n$, $\forall i$

$$\Rightarrow p_i^{\alpha_i} < n \Rightarrow p_i^{\alpha_i} \leq n-1$$

$$\Rightarrow p_i^{\alpha_i} \mid (n-1)!, \forall i$$

$$\Rightarrow \pi p_i^{\alpha_i} = n \mid (n-1)!$$

Suppose, $n = 1 \Rightarrow n = p^\alpha$

n is composite $\Rightarrow \underline{\alpha \geq 1}$

$\Rightarrow n = p \cdot p^{\alpha-1}$

$\Rightarrow n > p$ and $n > p^{\alpha-1}$

$\Rightarrow n-1 \geq p$ and $n-1 \geq p^{\alpha-1}$

If $p \neq p^{\alpha-1}$, then both p and $p^{\alpha-1}$ are in the representation of $(n-1)!$

$\therefore p \cdot p^{\alpha-1} = n \mid (n-1)!$

If $p = p^{\alpha-1}$, then $\alpha - 1 = 1$ or

$\alpha = 2$

$\Rightarrow n = p^2$

But $n > 4 \Rightarrow p \neq 2$.

$n \geq 6 \Rightarrow 2(n-1) < (n-1)!$

$\Rightarrow 2(n-1)$ is in terms of $(n-1)!$

$\because$ p and $2p$ are in terms of $(n-1)!$

$\Rightarrow p \cdot 2p \mid (n-1)!$

$\Rightarrow 2p^2 \mid (n-1)! \Rightarrow p^2 = n \mid (n-1)!$

Gaussian integers :-

$\alpha = n + mi$, (where n, m are integers) are Gaussian integers.

Ex :- Use Euclidean algorithm to find g.c.d. $(5+6i, 3-2i)$

$$|5+6i| = \sqrt{5^2+6^2} > \sqrt{3^2+(-2)^2} = |3-2i|$$

$$\frac{5+6i}{3-2i} = \frac{(5+6i)(3+2i)}{3^2+2^2}$$

$$= \frac{1}{13}(3 + 28i)$$

$$\simeq 0 + 2i$$

Note:-

$\frac{3}{13} = 0.2307 < 0.5$

$\frac{28}{13} = 2.1538 \simeq 2.$

$\frac{3}{13}$ is closer to 0 than 1

$\frac{28}{13}$ is closer to 2 than 3

$\therefore 5 + 6i = \underbrace{2i(3 - 2i)}_{4 + 6i} + 1$

$= 2i(3 - 2i) + (1)$

$\therefore$ g.c.d. $(5 + 6i, 3 - 2i) = 1$

Moreover,

$1 = (5 + 6i) \times 1 - 2i(3 - 2i)$

Ex:- Find g.c.d $(7-11i, 8-19i)$

$$8-19i = 2(7-11i) + (-6+3i)$$

$$7-11i = (-2+i)(-6+3i) + (-2+i)$$

$$-6+3i = 3(-2+i) + 0.$$

$\therefore$ g.c.d. $(7-11i, 8-19i)$

$$= \underline{\underline{-2+i}}$$

Moreover,

$$-2+i = (-3+2i)(7-11i) + (2-i)(8-19i)$$

Note:-

Gaussian integers are complex numbers with real and imaginary parts are integers.

They are the vertices of the

squares of grid.

If α and β are Gaussian integers, then $\alpha \mid \beta$ if there is a Gaussian integer γ such that $\beta = \alpha\gamma$?

g.c.d. $(\alpha, \beta) = \delta$, then δ is a Gaussian integer of maximum absolute value which divides both α and β.

Note:- g.c.d. of Gaussian integers is not unique, as by multiplying ± 1 and $\pm i$, we get Gaussian integers with same absolute value and dividing both α and β.

Ex:- If $p \mid b^6+1$, where p is a prime and b^6+1 is an integer, then p can be expressed as $p = c^2+d^2$, for some integers c and d.

Infact, $b^6+1 = (b^2+1)(b^4-b^2+1)$

If $p \mid b^6+1$, then,

$p \mid b^2+1$ or $p \mid b^4-b^2+1$

① If $p \mid b^2+1 = (b+i)(b-i)$,

but $c+di = g.c.d.(p, b+i)$.

Then $p = (c+di)(c-di)$

$\Rightarrow p = c^2+d^2$

② If $p \mid b^4-b^2+1 = (b^2-1)^2+b^2$

$\Rightarrow p \mid [(b^2-1)+bi][(b^2-1)-bi]$

Let $\gcd(p, (b^2-1)+bi) = c+di$

$\Rightarrow p = (c+di)(c-di)$

$\Rightarrow \underline{p = c^2+d^2}$

Ex:- If $12277 \mid 20^6+1$, find express the prime 12277 as a sum of two squares.

Ans: $12277 = 89^2+66^2$

Ex:- $769 \mid 196^6+1 \Rightarrow$ Express 769 as a sum of two squares.