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

~~$\therefore p$ and $2p$ are in terms of~~

~~$(n-1)!$~~

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

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

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

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

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

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

Moreover,

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

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

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

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

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

$$\therefore \text{g.c.d.}(7-11i, 8-19i) = -2+i$$

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 $\alpha | \beta$ 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 $p \mid b^2+1 = (b+i)(b-i)$,

let $c+di = \gcd(p, b+i)$.

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

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

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

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

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

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

Ans: $12277 = \underline{\underline{89^2+66^2}}$

Ex:- $769 \mid 19^6+1 \Rightarrow$ Express 769 as a sum of two squares.