Number Theory 1

06 August 2023 11:05

$x \mid y$ means x divides y

$1 \mid x$ and $x \mid 0$ are always true

$x \mid y$ and $y \mid z \Rightarrow x \mid z$

$x \mid y \Rightarrow y = kx$ where $k \in \mathbb{Z} - \{0\}$ → It is 0 only when y is 0

↪ $\frac{y}{x} \in \mathbb{Z} - \{0\}$

$2 \mid 0 \Rightarrow 2 \cdot 0 = 0$

$\frac{z}{x} = \frac{y}{x} \cdot \frac{z}{y} \in \mathbb{Z} \iff x \mid z$

$x \mid y$ and $x, y \in \mathbb{Z}$ then either $y = 0$ or $|x| \leq |y|$

$y = kx$

$|y| = |k||x| \Rightarrow |y| \geq |x|$

→ $|k| \geq 1$

$x \mid y$ and $x, y \in \mathbb{Z}^+$ then $x \leq y$

→ $|x| = x$, $|y| = y$ $\quad y = kx$

$|y| \geq |x| \Rightarrow y \geq x$

$S = \{\text{multiples of } 5\}$

$= \{\dots, -10, -5, 0, 5, 10, 15, \dots\}$

$k \in \mathbb{Z}$. $s \in S$ $\quad s_1, s_2 \in S$

$ks \in S$ (multiple of 5) $\quad s_1 + s_2 \in S$

$k_1 s_1 + k_2 s_2 \in S$ for all $k_1, k_2 \in \mathbb{Z}$ and $s_1, s_2 \in S$.

Properties:- $1|x$, $x|0$, $x|x$

$x|y$ and $y|x \Rightarrow |x| = |y| \Rightarrow x = \pm y$

$x|y$ and $y|z \Rightarrow x|z$

$x|y,z$ means $x|y$ and $x|z$

$x|y,z \Rightarrow x|ay+bz \ \forall a,b \in \mathbb{Z}$

$x|y \Rightarrow x|yz$

$x|y$ if and only if $xz|yz$ where $z \neq 0$

Q1. $n|2n+1 \Rightarrow n|1 \Rightarrow n = \pm 1$

Q2. For two fixed integers x, y then $(x-y) | (x^n - y^n)$ for any $n \in \mathbb{Z}$

$$x^n - y^n = (x-y)(\underbrace{x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}}_{\in \mathbb{Z}})$$

$$= x^n + x^{n-1}y + \cdots + xy^{n-1} - x^{n-1}y - xy^{n-1} - y^n$$

$$= x^n - y^n$$

---

a divisor, b dividend

$b = ka + r$; $0 \le r < a$, $k \in \mathbb{Z}$

to find the gcd of a and b

$\gcd(a,b) = g$

$gk_1 = a$ k_1, k_2 are coprime

$gk_2 = b$

$\gcd(a, b - ka)$

$= \gcd(gk_1, gk_2 - kgk_1)$

$= g[\gcd(k_1, k_2 - kk_1)]$

$= g$

Suppose $d|(k_1)$

$d|(k_2 - kk_1)$

$\Rightarrow d | k_2 - kk_1 + kk_1$

$\Rightarrow d | k_2 \Rightarrow d = 1$

$(24, 10)$

$10) 24 (2$
-20
$4) 10 (2$
-8
$(2)) 4 (2$
-4
0

$b = ka + r_1$

$a = kr_1 + r_2$

$r_1 = kr_2 + r_3$

$\vdots$

$2 \overline{)\,4\,(2}$
-4
0

$r_1 = k r_2 + r_3$
$\vdots$
$r_{n-2} = k r_{n-1} + r_n = 0$

Some numbers exist which has no divisors ⇒ primes

$\forall\, k \in \mathbb{Z}$, $k \nmid p$ Then p is prime except $|k| = p$, and $|k| = 1$

Q. Find all +ve integers n for which $3n-4$, $4n-5$, $5n-3$ are all primes.

Ans:- $3n-4+4n-5+5n-3 = 12(n-1)$ → one of them must be even

2 is the only even prime

$n = 2$

For $n=1$ we have $3n-4 = -1$ not possible

For $n=2$ we have $3n-4=2$, $4n-5=3$, $5n-3=7$

For $n \geq 3$ we have all of $3n-4$, $4n-5$, $5n-3 > 2$

So all of $n \geq 3$ not possible as one of them must be 2

$a = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$ → necessarily distinct prime factors are $p_1, p_2, \ldots, p_n$

→ not necessarily distinct prime factors are, p_1 (r_1 times), p_2 (r_2 times) ..., p_n (r_n times)

→ $r_1 + r_2 + \cdots + r_n$ numbers of factors.

Total number of factors: $(r_1+1)(r_2+1)\cdots(r_n+1)$

Fundamental Theorem of Arithmetic :-

Any natural number greater than 1 has a unique factorization upto order.

$n \in \mathbb{N}$, $n = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$ → $p_1, p_2, \ldots p_n$ are all distinct primes upto

$n \in \mathbb{N}$, $n = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$ → $p_1, p_2, \ldots p_n$ are all distinct primes

↳ this form is unique

$12 = 2^2 3^1$ → necessarily distinct prime factors 2

↳ not necessarily distinct prime 3

Total factors = 6

Q. If $a < b$ are two consecutive odd prime numbers show that $a+b$ has at least 3 prime factors not necessarily distinct.

Ans:— $b = a+2$

$a+b = 2a+2 = 2(a+1)$ → here 3.

2 ← 2 ← ↳ p