Number Theory 2

13 August 2023 12:17

Numbers as Multiset

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} \equiv \{\underbrace{p_1, p_1, \ldots p_1}_{\alpha_1 \text{ times}}, \underbrace{p_2, p_2, \ldots, p_2}_{\alpha_2 \text{ times}}, \ldots, \underbrace{p_n, p_n, \ldots, p_n}_{\alpha_n \text{ times}}\}$$

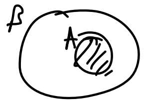
$$4 = \{2, 2\} = 2^2$$

$$24 = \{2, 2, 2, 3\} = 2^3 \cdot 3$$

Lemma

Divisibility in Sets :- If a, b are integers then $a | b \iff A \subset B$

$b = ka \quad k = 1, b = a \Rightarrow A = B$ for $k = 1$ case



GCD :-

GCD or the Greatest Common Divisor of two numbers is the number obtained by the set of common prime factors. For two numbers m, n it is denoted by $\gcd(m, n)$.

$$n = 2^3 \cdot 3^2 \cdot 5 \Rightarrow N = \{2, 2, 2, 3, 3, 5\}$$

$$m = 2^2 \cdot 5^3$$

$$\hookrightarrow M = \{2, 2, 5, 5, 5\}$$

$$\gcd(m, n) = M \cap N = \{2, 2, 5\} = 2^2 \cdot 5$$

Lemma: Let a and b be integers. Then $\gcd(a, b) \leq a$ and $\gcd(a, b) \leq b$

Proof:- $|A \cap B| \leq |A|, |A \cap B| \leq |B| \Rightarrow \gcd(a, b) \leq a, b$

$d = \gcd(a, b)$, $\quad d | a \Rightarrow d \leq a$, $d | b \Rightarrow d \leq b \quad \Rightarrow d \leq a, b$

Lemma:- Let $a, b, c \in \mathbb{Z}$. Then

$$c | a, \; c | b \Rightarrow c | \gcd(a, b)$$

Proof:- $d = \gcd(a, b)$ $\quad a = dk_1, b = dk_2 \Rightarrow \gcd(k_1, k_2) = 1$ or k_1 and k_2 are coprime

$\Rightarrow d | a, b \Rightarrow$

$k_2 = q k_1$

Proof:- $d = \gcd(a,b)$

$\Rightarrow d \mid a, b \Rightarrow a = dk_1,\ b = dk_2 \Rightarrow \gcd(k_1, k_2) = 1$ [illegible]

$c \mid dk_1,\ c \mid dk_2$

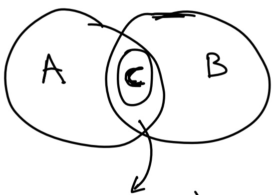
$dk_1 = ck_3$
$dk_2 = ck_4$

$\frac{k_1}{k_2} = \frac{k_3}{k_4} \Rightarrow k_3 = qk_1,\ k_4 = qk_2$

↳ most simplified form

$dk_1 = cqk_1$
$dk_2 = cqk_2$
$\Rightarrow d = cq$

$c \mid d \Rightarrow c \mid \gcd(a,b)$



gcd(a, b)

$C \subset \{\gcd(a,b)\} \Rightarrow C \mid \gcd(a,b)$

Lemma:- (The Prime Factorization of GCD)

Let $a, b \in \mathbb{Z}$ with prime factorization,

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$$

where α_i, β_i are non-negative integers (possibly 0)

Then $\gcd(a,b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_n^{\min(\alpha_n,\beta_n)}$

LCM:-

Let $a, b \in \mathbb{Z}$ and prime multisets are A, B

$\operatorname{lcm}(a,b) = A \cup B$

LCM of a, b is the least number divisible by both a and b

Then $\operatorname{lcm}(a,b) \geq a, b$

Prime Factorization of LCM :-

$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ where α_i, β_i are non-negative

$b = p_1^{\beta_1} \cdots p_n^{\beta_n}$ numbers (possibly 0)

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$$

where α_i, β_i are non-negative numbers (possibly 0)

$$\text{lcm}(a,b) = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \cdots p_n^{\max(\alpha_n,\beta_n)}$$

Lemma :- $a, b, c \in \mathbb{Z}$. Then $a|c,\ b|c \Rightarrow \text{lcm}(a,b)|c$

Proof :- H.W. (both set theoritic and algebraic)

Lemma :- (Product of GCD and LCM).

$a, b \in \mathbb{Z}$, then $\gcd(a,b)\,\text{lcm}(a,b) = ab$

Proof :- H.W. (both set theoretic and algebraic)

$$\boxed{\begin{aligned} &|A\cup B| = |A| + |B| - |A\cap B| \\ \Rightarrow\ &|A\cup B| + |A\cap B| = |A| + |B| \end{aligned}} \longrightarrow \text{Cardinality of relation of } A, B, A\cup B, A\cap B$$

---

a and b are coprime $\Leftrightarrow \gcd(a,b) = 1$

Q:- Prove that $\gcd(a,b) = a$ if and only if $a|b$

Ans:- $a|b \Rightarrow b = ak_1,\ k_1 \in \mathbb{Z}$

$\gcd(a,b) = \gcd(a, ak_1) = a$

$\gcd(a,b) = a \Rightarrow a|b$

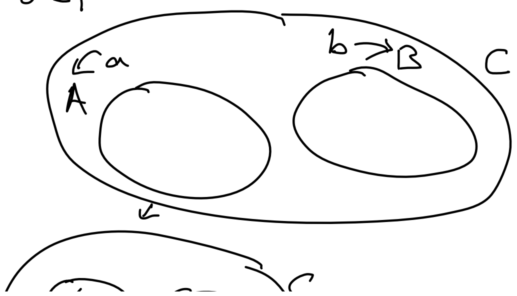
Q:- Let a, b be relatively prime. Show that if $a|c,\ b|c$ then $ab|c$

→ means coprime

Ans:- $\gcd(a,b) = 1$

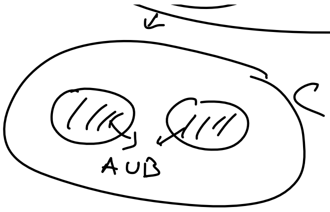
$ab = A + B = A\cup B$

$A\cap B = \phi$



$ab = A+B = A \cup B$

$A \cap B = \phi$



$A \cup B \subset C$

$\Rightarrow ab \mid c$

H.W. :- Algebraically prove this

Lemma :- (Product of GCD and LCM).

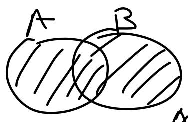
$a, b \in \mathbb{Z}$, then $\gcd(a,b)\,\mathrm{lcm}(a,b) = ab$

Proof :- H.W. (both set theoretic and algebraic)

Sol :- Alg :- $a = dk_1 \quad b = dk_2 \qquad \gcd(a,b) = d \Rightarrow k_1, k_2$ are coprime

$\mathrm{lcm}(a,b) = d k_1 k_2$

$\gcd(a,b)\,\mathrm{lcm}(a,b) = dk_1 dk_2 = ab$



$A \cup B + (A\cap B) = A+B$

$A+B = A\cup B + A \cap B$

Set :- A = set for $a \qquad \gcd = A \cap B$

B = set for $b \qquad \mathrm{lcm} = A \cup B$

set for $ab = A + B = (A \cup B) + (A \cap B)$

$= \mathrm{lcm}(a,b)\gcd(a,b)$

$a \times b = A+B$

$\gcd \times \mathrm{lcm} = A\cup B + A \cap B$

$A = \{P_1 P_1 P\}$

$B = \{P_1, P_2\}$

$ab = P_1^3 P_1 P_2$

$\ \ |||$

$A+B = \{P_1 P_1 P_1 P_1 P_2\}$

Lemma :- $a, b, c \in \mathbb{Z}$. Then $a \mid c,\ b \mid c \Rightarrow \mathrm{lcm}(a,b) \mid c$

Proof :- H.W. (both set theoritic and algebraic)

Sol :- Alg :- $a \mid c,\ b \mid c \qquad \gcd(a,b) = d$

$a = dk_1 \quad b = dk_2 \qquad \mathrm{lcm}(a,b) = dk_1k_2$

$dk_1 \mid c \qquad dk_2 \mid c \qquad c = (\text{const})\, d k_1 k_2$

$= (\text{const})\ \mathrm{lcm}(a,b)$

$\Rightarrow \mathrm{lcm}(a,b) \mid c$

Q :- Let a, b be relatively prime. Show that if

$\Rightarrow$ ... coprime

Q :- Let a, b be relatively prime. Show that if $a | c$, $b | c$ then $ab | c$ → means coprime

Sol :- Algebraic :- $\gcd(a, b) = 1 \Rightarrow a \nmid b, b \nmid a$

Using above lemma $\text{lcm}(a, b) | c \Rightarrow ab | c$