NT 1

- Roles of Prime Numbers
- GCD, LCM
- Parities.
- Divisiblity.
- Problem Solving & Rigorous Proof Writing.

– by Hsu Wutt Yee Lin
(IMO 2023 - HM
IMO 2024 - HM)

We will begin at 8:05 p.m.

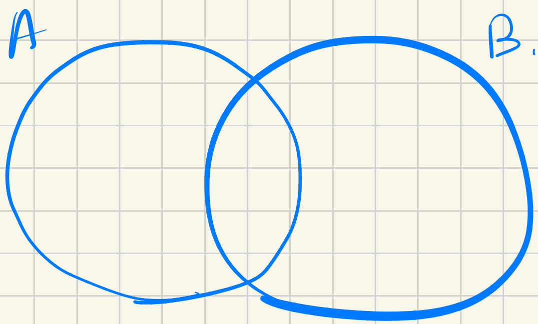
In the meantime, please try this question.

Venn Diagram w/ GCD, LCM.

Firstly, imagine the numbers as sets of prime factors.

Eg. $20 = \{2, 2, 5\}$, $75 = \{3, 5, 5\}$.

Then,



Why does this prove that

$$GCD(A,B) \times LCM(A,B) = AB \ ?$$

Ans: $GCD(A,B) = A \cap B$.
$LCM(A,B) = A \cup B$.
$\therefore GCD(A,B) \times LCM(A,B) = A \cap B + A \cup B$
$= [A] + [B] = AB$

A) Roles of Prime numbers

Prime: " A number that can be divided exactly only by 1 and itself "

> #1 tip to solving NT problems →
>
> Any number n can be written as:
>
> $$\text{"} \; n = p_1^{\alpha_1} \, p_2^{\alpha_2} \, p_3^{\alpha_2} \cdots p_k^{\alpha_k} \; \text{"}$$

any natural number

prime numbers.

B) GCD, LCM

$$a = p_1^{\alpha_1} \, p_2^{\alpha_2} \, p_3^{\alpha_3} \cdots p_k^{\alpha_k}.$$

$$b = p_1^{\beta_1} \, p_2^{\beta_2} \, p_3^{\beta_3} \cdots p_k^{\beta_k}$$

- $GCD(a,b) = p_1^{\min(\alpha_1, \beta_1)} \, p_2^{\min(\alpha_2, \beta_2)} \, p_3^{\min(\alpha_3, \beta_2)} \cdots p_k^{\min(\alpha_k, \beta_k)}$
- $LCM(a,b) = p_1^{\max(\alpha_1, \beta_1)} \, p_2^{\max(\alpha_2, \beta_2)} \, p_3^{\max(\alpha_3, \beta_2)} \cdots p_k^{\max(\alpha_k, \beta_k)}$

* See how it instantly get easy to spot that

$$\boxed{GCD(a,b) \times LCM(a,b) = ab.} \;?$$

Euclid's division algorithm.

let $a > b$.

To find $\gcd(a,b)$, we can use the following algorithm.

$$a = bq_1 + r_1$$
$$b = r_1 q_2 + r_2$$
$$r_1 = r_2 q_3 + r_3$$
$$\vdots$$
$$r_{n-2} = r_{n-1} q_n + r_n$$
$$r_{n-1} = r_n q_{n+1}$$

$$\gcd(a,b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-1}, r_n)$$
$$= r_n$$

Eg. Find $\gcd(126, 210)$.

Ans: $\gcd(126, 210) = \gcd(126, 84) = \gcd(84, 42) = 42$

Eg. (IMO 1959 P1)

Prove that for any $n \in \mathbb{N}$, the fraction $\dfrac{21n+4}{14n+3}$ is irreducible.

Ans: $\gcd(21n+4, 14n+3) = \gcd(7n+1, 14n+3)$
$$= \gcd(7n+1, 7n+2)$$
$$= \gcd(7n+1, 1)$$
$$= 1$$

C) Parities

Some basic ideas:

1. even numbers can be expressed as $2k$.
2. odd numbers can be expressed as $2k+1$.
3. $o+o=e$. $\quad o\times o=o$
   $o+e=o$ $\quad o\times e=e$
   $e+e=e$. $\quad e\times e=e$.
4. A product of integers is even if and only if one of them is even.

D) Divisibility

Basic Divisibility Tests

- $2|n$ if n is even.
- $3|n$ if sum of the digits of n is divisible by 3.
- $4|n$ if last two digits of n is divisible by 4. $\leftarrow 25$
- $5|n$ if unit digit is either 0 or 5.
- $8|n$ if last three digits of n is divisible by 8. $\leftarrow 125$
- $9|n$ if sum of the digits of n is divisible by 9.
- $11|n$ if (sum of digits in odd places) $-$ (sum of digits in even places) is divisible by 11.

Some Divisibility Rules

- if $z|x,y$, then
  $z|ax+by$
- if $x|y$, then
  $y=0$ (OR) $|x|\leq|y|$.

Q1. Let $m, n \in \mathbb{N}$ such that.

$$\gcd(m,n) + \operatorname{lcm}(m,n) = m+n.$$

Show that one of the two numbers is divisible by the other.

(i.e $m \mid n$ or $n \mid m$). {All Russia Mathematics Olympiad - 1995}

Ans:

Let $\gcd(m,n) = g$.

$$\operatorname{lcm}(m,n) = \frac{mn}{g}.$$

$$g + \frac{mn}{g} = m+n$$

$$g^2 + mn = g(m+n)$$

$$g^2 - g(m+n) + mn = 0.$$

$$(g-m)(g-n) = 0.$$

$g = m$ or $g = n$.

$\gcd(m,n) = m$ $\therefore n \mid m$. } $\gcd(m,n) = n$ $\therefore m \mid n$.

$\therefore$ QED.

Made with Goodnotes

Q2. Let a, b be positive integers such that there exists a prime p with the property $\operatorname{lcm}(a, a+p) = \operatorname{lcm}(b, b+p)$. Prove that $a=b$.

[Romania Mathematics Olympiad]

Ans: $$\operatorname{lcm}(a, a+p) = \frac{a(a+p)}{\gcd(a, a+p)}$$

$$\operatorname{lcm}(b, b+p) = \frac{b(b+p)}{\gcd(b, b+p)}$$

$$\therefore \frac{a(a+p)}{\gcd(a, a+p)} = \frac{b(b+p)}{\gcd(b, b+p)}$$

$$\gcd(a, a+p) = \gcd(a, p) = 1 \text{ or } p.$$
$$\gcd(b, b+p) = \gcd(b, p) = 1 \text{ or } p.$$

Case ①: $[\gcd(a, a+p), \gcd(b, b+p)] = \{1, 1\}$.

$$\frac{a(a+p)}{1} = \frac{b(b+p)}{1}$$

$$\therefore a^2 + ap = b^2 + bp$$
$$a^2 - b^2 = bp - ap.$$
$$(a-b)(a+b) = -p(a-b)$$
$$a = b \quad \text{or} \quad a+b = -p$$
(impossible)

$$\therefore a = b$$

Case ②: $\{\gcd(a, a+p), \gcd(b, b+p)\} = \{p, p\}$

$$\frac{a(a+p)}{\cancel{p}} = \frac{b(b+p)}{\cancel{p}}$$

goes back to Case ①.

$$\therefore a = b.$$

Case 3: $\{\gcd(a, a+p), \gcd(b, b+p)\} = \{1, p\}$ or $\{p, 1\}$.

WLOG, Assume that

$\{\gcd(a, a+p), \gcd(b, b+p)\} = \{1, p\}$.

$\gcd(a, a+p) = \gcd(a, p) = 1$.

This implies that $p \nmid a$.

$\therefore p \nmid \operatorname{lcm}(a, a+p)$. — 1

$\gcd(b, b+p) = \gcd(b, p) = p$.

This implies that $p \mid b$.

$\therefore p \mid \operatorname{lcm}(b, b+p)$. — 2

1 & 2 implies that $\operatorname{lcm}(a, a+p) \neq \operatorname{lcm}(b, b+p)$

$\therefore$ impossible

$\therefore$ According to case 1 & 2, $a = b$.

$\therefore$ QED.

Q3. Find all pairs (a,b) of positive integers such that "$a^{2017}+b$" is a multiple of ab.

{Harvard-MIT Math Tournament 2017}

$ab \mid a^{2017}+b \Rightarrow a \mid a^{2017}+b. \Rightarrow a \mid b.$

$\therefore b = ak$ for some positive integer k.

$ab \mid a^{2017}+b \Rightarrow a^2k \mid a^{2017}+ak \Rightarrow ak \mid a^{2016}+k$

Given: $ab \mid a^{2017}+b$.

What we got: $ak \mid a^{2016}+k$. $\Rightarrow$ We get $a \mid k$

$\therefore k = ak_1 \Rightarrow ak_1 \mid a^{2015}+k_1$

$ak_2 \mid a^{2014}+k_2$

$\vdots$

$ak_{2015} \mid a+k_{2015}$

$ak_{2016} \mid 1+k_{2016}$

let $l = k_{2016}$

$\therefore al \mid 1+l$

This implies $l \mid 1+l \Rightarrow l = 1$.

$a \mid 1+l \Rightarrow a \mid 2 \Rightarrow a = 1$ or $a = 2$.

If $a=1$,

$$ab \mid a^{2017}+b.$$

$$b \mid 1+b$$

$$\therefore b=1.$$

If $a=2$,

$$2b \mid 2^{2017}+b$$

$$b \mid 2^{2017}+b \quad \& \quad 2 \mid 2^{2017}+b.$$

$$\downarrow \qquad\qquad\qquad \downarrow$$

$$b \mid 2^{2017} \qquad\qquad 2 \mid b.$$

$$\therefore b=2^{q} \text{ for } 1 \leq q \leq 2017.$$

$$\therefore (a,b)=(1,1)$$

$$(a,b)=(2,2)$$
$$(2,2^{2})$$
$$(2,2^{3})$$
$$\vdots$$
$$(2,2^{2017})$$

24. Let n be a positive integer and let $d_1, d_2, \dots, d_k$ be all its positive divisors such that $1 = d_1 < d_2 < \dots < d_k$. Find all values of n for which $k \geq 4$ & $n = d_1^2 + d_2^2 + d_3^2 + d_4^2$.

Ans: {Balkan MO 1989}

If n was odd,

d_1, d_2, d_3 and d_4 would be odd.

$n = d_1^2 + d_2^2 + d_3^2 + d_4^2 =$ even.

$\therefore$ n is surely not odd.

n must be even.

$d_1 = 1$, $d_2 = 2$.

$n = 1 + 2^2 + d_3^2 + d_4^2$

$n = 5 + \boxed{d_3^2 + d_4^2} \leftarrow$ odd,

$\underset{\text{even}}{n}$ $\quad$ $\underset{\text{odd}}{5}$

$\therefore$ $d_3^2 + d_4^2$ is odd.

This imply that one of d_3^2 and d_4^2 is odd while the other is even.

Since one of them is odd, we should know that one of d_3 and d_4 will be a prime number "p". {if it was not a prime, that number would be breaking the $1 = d_1 < d_2 < \dots < d_k$ statement.}

So far, we know that three of d_1, d_2, d_3, d_4 is 1, 2 and p. The other number must be even. That even number must be 4 or 2p.

Case ①: 2p.

$n = d_1^2 + d_2^2 + d_3^2 + d_4^2$

$n = 1 + 2^2 + p^2 + (2p)^2$

$n = 5 + 5p^2$

$n = 5(1+p^2)$

$\therefore 5 \mid n$

if $p = 3$

$(d_1, d_2, d_3, d_4) = (1, 2, 3, 6)$

But $5 < 6$, so d_4 should be 5.

$\therefore p \neq 3$.

then $p = 5$.

$\therefore (d_1, d_2, d_3, d_4) = (1, 2, 5, 10)$

Case ②: 4

$n = d_1^2 + d_2^2 + d_3^2 + d_4^2$

$n = 1 + 2^2 + p^2 + 4^2$

$n = 21 + p^2$

$p \mid n$ (p is a divisor)

$\therefore p \mid 21 + p^2 \Rightarrow p \mid 21$.

$p = 3$ or $p = 7$.

$(d_1, d_2, d_3, d_4) = (1, 2, 3, 4)$

$(1, 2, 4, 7)$

$(d_1, d_2, d_3, d_4) = (1, 2, 5, 10)$ or — A

$= (1, 2, 3, 4)$ or — B

$= (1, 2, 4, 7)$ — C

Case (A):

$$n = d_1^2 + d_2^2 + d_3^2 + d_4^2 = 1^2 + 2^2 + 5^2 + 10^2$$
$$= 130.$$

$\therefore$ Case (A) is valid.

Case (B):

$$n = d_1^2 + d_2^2 + d_3^2 + d_4^2 = 1^2 + 2^2 + 3^2 + 4^2$$
$$= 30.$$

But $4 \nmid 30$.

$\therefore$ Case (B) is invalid.

Case (C):

$$n = d_1^2 + d_2^2 + d_3^2 + d_4^2 = 1^2 + 2^2 + 4^2 + 7^2$$
$$= 70.$$

But $4 \nmid 70$.

$\therefore$ Case (C) is invalid.

25. The sum of two smallest positive divisors of N is 8 and the sum of two largest positive divisors of N is 968. What is N? {MMO 2016}

sum of 2 smallest positive divisors $= d_1 + d_2$

$d_1 = 1$, so $\quad 1 + d_2 = 8.$

$d_2 = 7.$

$$N = 1 \times N$$
$$= 7 \times \frac{N}{7}$$
$$= \vdots \times \vdots$$

sum of 2 largest positive divisors $= d_{k-1} + d_k$

$$\frac{N}{7} + N = 968$$

$$\frac{8N}{7} = 968$$

$$N = \cancel{968}^{121} \times \frac{7}{\cancel{8}}$$

$$\boxed{N = 847.}$$

Made with Goodnotes