LCM of two integers

Let a and b be two integers.

We say m is the lcm of a and b

if i) $m > 0$

ii) $a \mid m$, $b \mid m$

iii) If $a \mid c$ & $b \mid c$ then

$m \mid c$.

THU JAN 12, 2023

Qun: What is lcm of $(0, a)$?

Qun: Can you express $\text{lcm}(a,b)$ as a linear Combination of a & b?

Yes, because $\text{GCD}(a,b)$ divides $\text{lcm}(a,b)$.

Linear Diophantine equation

$ax + by = c$ Assume $a \neq 0$, $b \neq 0$

Let us think about

$ax + by = 0$

Suppose there is a non-zero solution

$ax = -by$

multiple of a — multiple of b

$$ax = lcm(a,b)\,n \Rightarrow x = \frac{lcm(a,b)}{a}\,n$$

$$by = -lcm(a,b)\,n \Rightarrow y = -\frac{lcm(a,b)}{b}\,n$$

$$ax_1 + by_1 = c$$

$$ax_0 + by_0 = c$$

$$a(x_1 - x_0) + b(y_1 - y_0) = 0$$

$$\Rightarrow x_1 - x_0 = \frac{lcm(a,b)}{a}\,n$$

$$y_1 - y_0 = -\frac{lcm(a,b)}{b}\,n$$

THU JAN 12, 2023

$$x_1 = x_0 + \frac{\text{lcm}(a,b)}{a} n$$

$$y_1 = y_0 - \frac{\text{lcm}(a,b)}{b} n$$

All the solutions to

$$ax + by = c$$

→ Show that if $GCD(a,b) = LCM(a,b)$

then $a = b$.

$GCD(a,b) \leq a \leq LCM(a,b) \Rightarrow a = b = GCD = LCM$

→ Show that $GCD(GCD(a,b),c) = GCD(a, GCD(b,c))$.

What about LCM?

It is true!

How would you solve

$$a_1x + a_2y + a_3z = c \; ?$$

Solve for $a_1x + a_2y = w$

& $a_4w + a_3z = c$

$3x + 15y + 7z = 10$

$3x + 15y = 3u$ — — (1)

$3u + 7z = 10$ — — — (2)

We solve 2nd equation first

A particular solution is $u = z = 1$

General Soln is $u = 1 + 7t \quad z = 1 - 3t$

Eq (1) can be rewritten as

$x + 5y = u$

A particular sol'n is $x = -4u \quad y = u$

$$X = -4ut + 5m$$

$$y = 4 - m$$

$$x = -4(1+7t) + 5m$$

$$y = 1+7t - m$$

$$z = 1-3t$$

Prime numbers

Defn: We say p $(\neq 1)$ is a prime number if & only if only divisors of p are 1 & p.

Example: $2, 3, 5, 7, 11, 13, 17, \ldots$

Q: How many even prime numbers are there? Only one, 2

Q: How many odd prime numbers are there? Infinitely many

Q: What do they look like?

$4k+1$ or $4k+3$

Qn: If $a \mid bc$ & $(a,b) = 1$ then $a \mid c$.

Qn: If $p \mid ab$, then $p \mid a$ or $p \mid b$.

Soln: If $(a,b) = 1$, then $ax + by = 1$

$$acx + bcy = c \Rightarrow a \mid c.$$

Soln: If $p \nmid a$, then $(p,a) = 1 \Rightarrow p \mid b$.

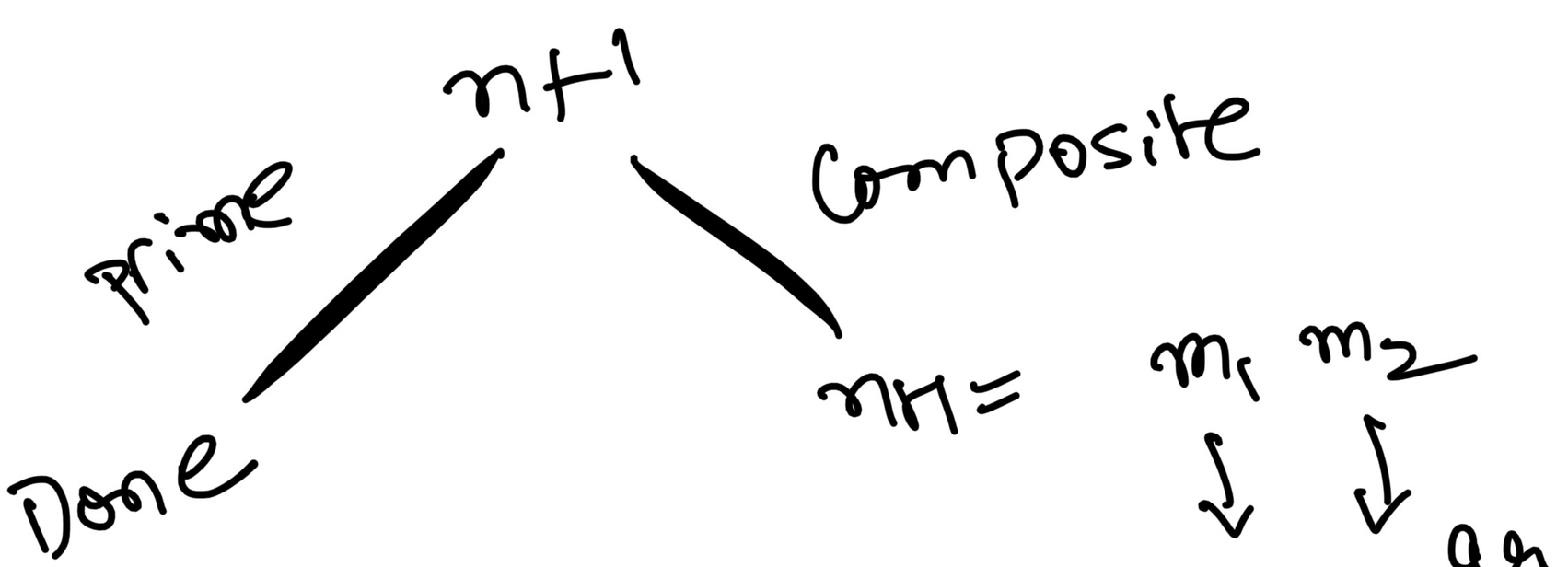
Prime factorization

Thm: Every non-zero integer can be written uniquely as product of primes (upto sign & reordering.)

Pf: We will show it for positive integers.

Nothing to show for $n=1$

Assume it holds for all integers from 1 to n.



Uniqueness will follow from property of prime numbers.

$$a = p_1^{a_1} \cdots p_r^{a_r}$$

$$b = p_1^{c_1} \cdots p_r^{c_r} q_1^{b_1} \cdots q_s^{b_s}$$

$$GCD(a,b) = p_1^{\min(a_1,c_1)} \cdots p_r^{\min(a_r,c_r)}$$

$$LCM(a,b) = p_1^{\max(a_1,c_1)} \cdots p_r^{\max(a_r,c_r)}$$

$$(GCD)(LCM) = ?$$

$$= a \cdot b$$

Propn: If $N > 1$ is composite, then N has a prime factor between 1 and $\lfloor \sqrt{N} \rfloor$.

Pf: If $d_1 d_2 = N$, then either $d_1 \leq \sqrt{N}$ or $d_2 \leq \sqrt{N}$.