3

Basic Arithmetic Foundations (Part 3)

Mathematics-1

Today’s Agenda

- LCM
- GCD
- Euclidean Algorithm on Numbers
- Co-prime numbers

Final Thought on Fundamental Theorem of Arithmetic

“What seems obvious to the child becomes awe-inspiring to the philosopher.”

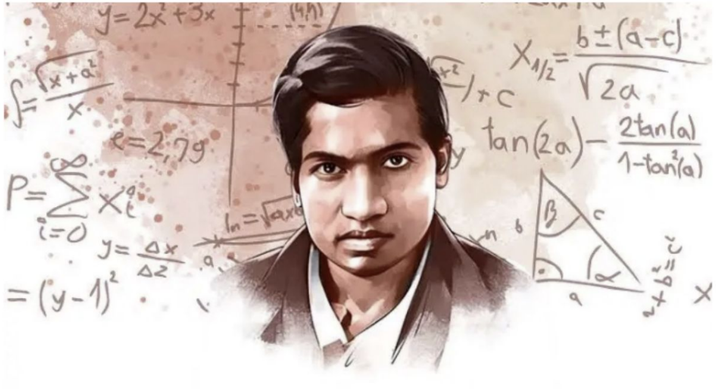
Uniqueness of prime factorization is not trivial.

It is a miracle of structure — and we must pause to appreciate it.

Newton School of Technology

Srinivasa Ramanujan

- Hardy Said: **“Every positive integer is Ramanujan’s personal friend.”**
- This quote highlights the deep and often unexpected connections between numbers.
- There’s even a movie on the life of Ramanujan, focusing on Hardy & Ramanujan’s collaboration - **“The Man Who Knew Infinity”**



Perfect Number

- A Perfect Number is a positive integer where the sum of its proper divisors (divisors other than itself) adds back to itself.

Example 1: Consider 6

- Divisors of 6 are 1, 2, 3, 6.
- Proper divisors are 1, 2, 3.
- Sum of proper divisors:
  1 + 2 + 3 = 6
- Therefore, 6 is a perfect number.

Example 2: Consider 28

- Divisors of 28 are 1, 2, 4, 7, 14, 28.
- Proper divisors are 1, 2, 4, 7, 14.
- Sum of proper divisors:
  1 + 2 + 4 + 7 + 14 = 28
- Therefore, 28 is a perfect number.

Twin Prime Conjecture

- In the list of primes, it is sometimes true that consecutive odd numbers are prime (Twin Primes).

- **Examples:** (3,5), (5,7), (11,13), (17,19), (29,31), (41,43), (59,61), (71,73),...

- **Question:** Are there infinitely many twin primes?

Goldbach Conjecture

- Every even integer greater than 2 can be expressed as the sum of two prime numbers.
- **Examples:**
    - $4 = 2 + 2$
    - $6 = 3 + 3$
    - $8 = 3 + 5$
    - $10 = 3 + 7 = 5 + 5$
    - $12 = 5 + 7, \ldots$

Can you prove it?

Do you want to earn millions? Solve!

- While mathematicians have found very large twin primes, no proof exists that the number of twin primes is infinite.

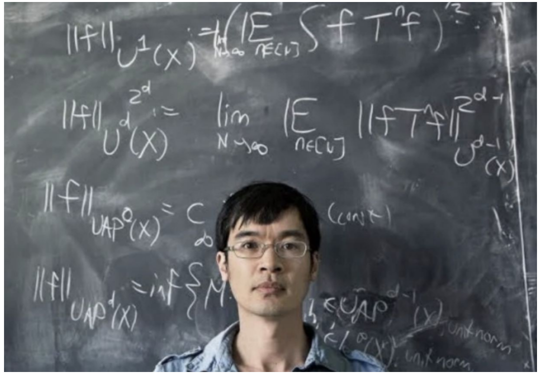
- Goldbach Conjecture has been verified for extremely large numbers (up to 4×10^{18}), but no general proof exists according to Wikipedia.

- So, **Twin Prime Conjecture** and **Goldbach Conjecture** both are **unsolved** [with prize money in millions!].

- Terence Tao is working on these!

Terence Tao’s Strategy

- **STEP 1:** Collect data — write down numbers (by hand or on computer).
- **STEP 2:** Look for patterns and relationships.
- **STEP 3:** Make a guess, formulate a conjecture.
- **STEP 4:** Test your conjecture on more examples.
- **STEP 5:** Try to prove it!



Voila! 🎉

💡 It takes patience, practice, and perseverance to follow these 5 steps — but the reward is deep mathematical insight.

Division Algorithm

Introduction to Division

- Among integers, we can perform addition, multiplication, subtraction, and division.
- Division gives birth to interesting pattern hunting tools!
- Let's learn the **Division Algorithm**.
- **Why call it an Algorithm?**
  - An Algorithm is a "finite" set of rules or steps to solve a problem or to achieve a certain task.
  - So, while dividing an integer 'a' with an integer 'b' (assuming $a > b$), we need a "finite" set of "rules" to achieve Division.

- Consider dividing 7 by 3.
- We can take two groups of 3 from 7:

$$7 = 2 \times 3 + 1$$

- Here, 1 is the remainder.
- Why algorithm? I could have done $7 = 3 \times \mathbf{3} - 2$ or $7 = 0 \times \mathbf{3} + 7$ nobody stops me!
- We need to fix the copies of b.How much it leaves behind.One rule we impose is;
- **The remainder 'r' should be greater than or equal to 0 and less than 'b' (the divisor)**.

The Division Algorithm

- Given integers a and b, with $b \neq 0$, there exist **unique** integers q (quotient) and r (remainder) such that:
$$a = q \cdot b + r$$
- where $0 \leq r < |b|$.
- This ensures a unique remainder.
- Examples:
  - Single digit: $7 = 2 \cdot 3 + 1$
  - Two digits: $15 = 4 \cdot 3 + 3$
  - Three digits: $125 = 10 \cdot 12 + 5$
  - Seven digits: $1234567 = 123456 \cdot 10 + 7$

Rapid fire

Can the remainder ever be negative?

Rapid fire

Can the remainder ever be negative?

Answer: No

- ➔ If we allow negative remainder, then we lose the uniqueness property of division algorithm.
- ➔ Remainder is defined to be non-negative in math because we want the remainder to represent a "leftover" quantity. So, it should always be a small, clean, and positive offset.

Divisibility and Notation

- Now when remainder is Zero i.e. $r = 0$, we record that situation with a notation.
- **English:** "d divides a"
- **Notation:** $d \mid a$
- **Examples:**
  - English: "2 divides 6" $\rightarrow$ Notation: $2 \mid 6$ (since $6 = 2 \times 3 + 0$)
  - English: "5 divides 15" $\rightarrow$ Notation: $5 \mid 15$ (since $15 = 5 \times 3 + 0$)
  - English: "2 does not divide 7" $\rightarrow$ Notation: $2 \nmid 7$ (since $7 = 2 \times 3 + 1$)
- A divisor d of an integer a means $d \mid a$.

Common Divisors and Properties

- If a, b are arbitrary integers, then d is said to be a **common divisor** if d divides both a and b.
  - i.e., $d \mid a$ and $d \mid b$.
- **Definition of Divisibility:** $d \mid a$ means there exists an integer k such that $a = k \cdot d$.
- **Properties of Divisibility:** If $d \mid a$ and $d \mid b$, then:
  - $d \mid (a + b)$ ✓
  - $d \mid (a - b)$ ✓
  - $d \mid (ab)$ ✓

Properties of Divisibility

If $d \mid a$ and $d \mid b$, then:

1. $d \mid (a+b)$:

$$a = dk,\ b = dl \implies a + b = d(k + l).$$

2. $d \mid (a-b)$:

$$a - b = d(k - l).$$

3. $d \mid (ab)$:

$$ab = (dk)(dl) = d^2(kl).$$

👉 Hence, d divides $a+b$, $a-b$, and ab.

Problems on Divisibility

- **Problem 1:** Show that:
  - The product of any 3 consecutive integers is divisible by 6.
  - The product of any 4 consecutive integers is divisible by 24.
  - The product of any 5 consecutive integers is divisible by 120.

Do you see a pattern?

Problems on Divisibility

- **Problem 1:** Show that:
  - The product of any 3 consecutive integers is divisible by 6.
  - The product of any 4 consecutive integers is divisible by 24.
  - The product of any 5 consecutive integers is divisible by 120.

Do you see a pattern?

3 consecutive ⇒ divisible by 6

Among any 3 consecutive integers, one is a multiple of 3, and at least one is even.

So the product has a factor $3 \times 2 = 6$.

4 consecutive ⇒ divisible by 24

In any 4 consecutive integers:

- Exactly two are even, and among them one is a multiple of 4 ⇒ even part contributes $4 \times 2 = 8$.
- One is a multiple of 3.

  Thus the product has $8 \times 3 = 24$.

5 consecutive ⇒ divisible by 120

In any 5 consecutive integers:

- There are at least two evens, one of which is a multiple of 4 ⇒ even part gives $4 \times 2 = 8$.
- One is a multiple of 3.
- One is a multiple of 5.

  Hence the product has $8 \times 3 \times 5 = 120$.

Problems on Divisibility

Observed Pattern:

The product of any k consecutive integers is divisible by k!.

Problems on Divisibility

- **Problem 2:** Check if $2^{35} - 1$ is divisible by 3.

Problems on Divisibility

- **Problem 2:** Check if $2^{35} - 1$ is divisible by 3.

  - If the exponent is **odd**, 2^n leaves remainder **2** when divided by 3.
  - If the exponent is **even**, 2^n leaves remainder **1** when divided by 3.

So the remainders alternate:

$$2, 1, 2, 1, 2, 1, \ldots$$

- 2^{35} leaves remainder 2 when divided by 3.
- So, 2^{35} - 1 leaves remainder 2 - 1 = **1** when divided by 3.

Least Common Multiple

25

Least Common Multiple (LCM)

- We can define the Least Common Multiple (LCM) of a and b.
- Let m be a positive integer satisfying:

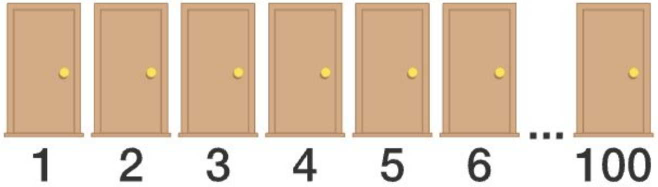
  (i) $a \mid m$ and $b \mid m$

  (ii) If $a \mid c$ and $b \mid c$ with $c > 0$, then $m \leq c$.

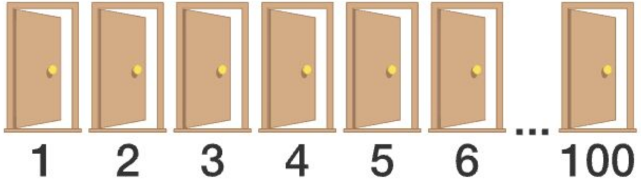
- The condition (ii) emphasizes the “least” aspect of the LCM.

100 Doors Problem

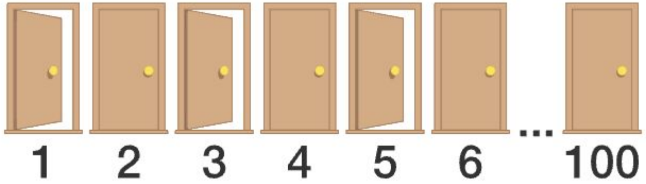
- Let's take a look at the hallway of 100 doors.
- In the hallway of 100 doors, 100 people numbered 1 to 100 are standing in a long hallway that has 100 closed doors also numbered 1 to 100:



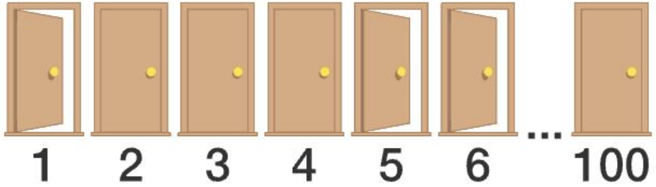
- Person 1 walks down the hallway and opens every door:



- Person 2 walks down the hallway and closes every door that is a multiple of 2:



- Person 3 walks down the hallway and changes every door that is a multiple of 3. That is, if the door is open, they close it, and if it is closed, they open it:



- Person 4 changes every door that is a multiple of 4, Person 5 every door that is a multiple of 5, etc. This continues until all 100 people have walked down the hallway and changed their doors.

Question:

What is the number of the first door changed by both Person 6 and Person 8?

Lowest Common Multiple

- **Person 6** changes the doors that are **multiples of 6**:
  6, 12, 18, 24, 30, 36……….

- **Person 8** changes the doors that are **multiples of 8**:
  8, 16, 24, 32, 40………..

Question:

What is the number of the first door changed by both Person 6 and Person 8?

→ **24**

Lowest Common Multiple

Can you compute LCM using Prime Factorisation?

$$294 = 2^1 \times 3^1 \times 7^2$$

$$364 = 2^2 \times 7^1 \times 13^1$$

Lowest Common Multiple

Can you compute LCM using Prime Factorisation?

$$294 = 2^1 \times 3^1 \times 7^2 \times 13^0$$

$$364 = 2^2 \times 3^0 \times 7^1 \times 13^1$$

Finding LCM using Prime Factorization

$$294 \qquad\qquad\qquad\qquad 364$$

$$2^1 \times 3^1 \times 7^2 \times 13^0 \qquad\qquad 2^2 \times 3^0 \times 7^1 \times 13^1$$

$$2^2 \times 3^1 \times 7^2 \times 13^1$$

$$\mathrm{lcm}(294, 364)$$

Logic behind taking highest exponent while computing LCM

Suppose:

$$a = 2^1 \times 3^2, \quad b = 2^3 \times 3^1$$

- For prime 2: a needs at least one 2, b needs three.

  → To cover both, we need **three 2′s** → 2^3.
- For prime 3: a needs two 3′s, b needs one.

  → To cover both, we need **two 3′s** → 3^2.

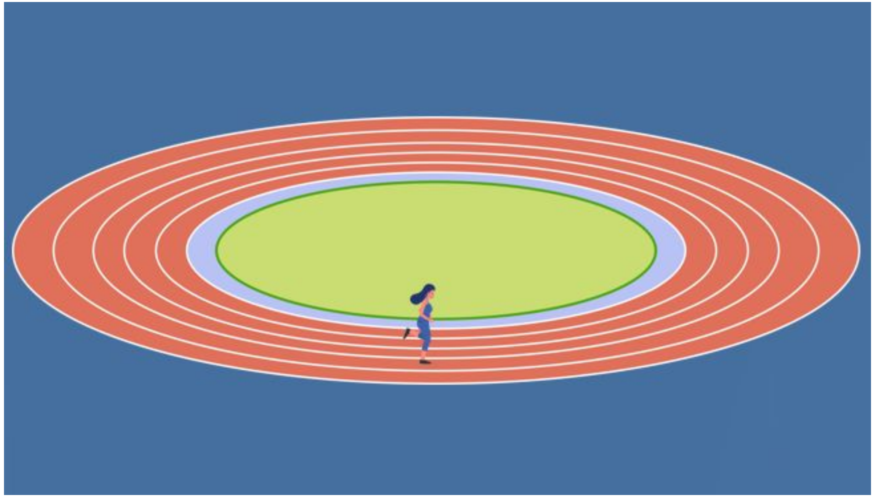
So LCM = $2^3 \times 3^2$.

This works because:

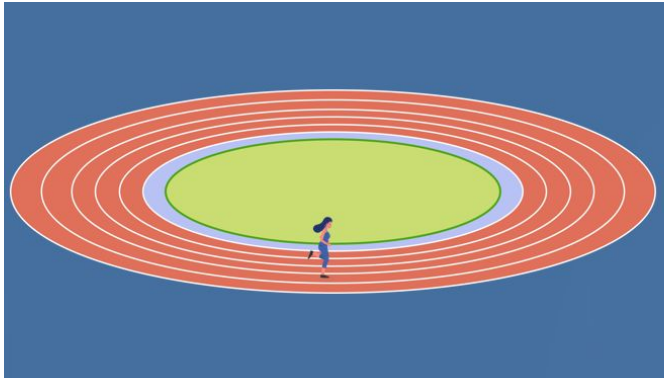
- If we took **lower exponents**, the number would fail to be divisible by one of them.
- Taking the **highest exponent** ensures divisibility by *both*.

Example:

Q. Three runners Manshu, Pintu, and Dally who are running around a circular track can complete one lap in 250, 400, and 600 seconds, respectively. After how long will they meet at the starting point next if they start together?



Example:



2	250
5	125
5	25
5	5
	1

$250 = 2^1 \times 5^3$

2	400
2	200
2	100
2	50
5	25
5	5
	1

$400 = 2^4 * 5^2$

2	600
2	300
2	150
3	75
5	25
5	5
	1

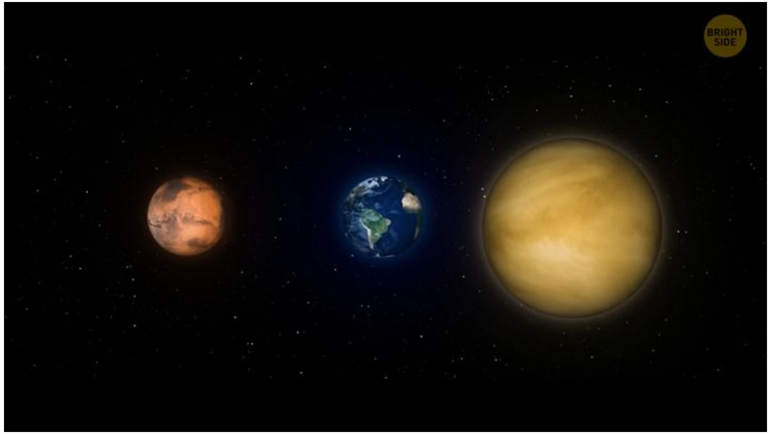
$600 = 2^3 * 3^1 * 5^2$

$$LCM(250, 400, 600) = 2^4 * 3^1 * 5^3 = 16 * 3 * 125 = \underline{6000}$$

$$\underline{6000\,s} = \frac{6000}{60} = \underline{100\,min}$$

Example:

Earth rotates around the sun in 365 days and Venus rotates around the sun in 730 days. Whenever Earth and Venus cross each other, a unique phenomenon occurs due to which the population of the Olive Ridley turtle reduces to half. Considering the initial population of Olive Ridley turtle is 10000, what will their population after 10 years?



Newton School of Technology

E → 365

V → 730

$LCM(365, 730) = 730$ days

10 years

$365 * 10 = 3650$ days

$\frac{3650}{730} = 5$ times

1^{st} time $\longrightarrow \frac{10000}{2} = 5000$

2^{nd} time $\longrightarrow \frac{5000}{2} = 2500$

3^{rd} time $\longrightarrow \frac{2500}{2} = 1250$

4^{th} time $\longrightarrow \frac{1250}{2} = 625$

5^{th} time $\longrightarrow \frac{625}{2} = 312.5 \longrightarrow \lfloor 312.5 \rfloor = 312$ ✓

$\left\lfloor \frac{3}{2} \right\rfloor = \lfloor 1.5 \rfloor = 1$

floor

$\left\lceil \frac{3}{2} \right\rceil = \lceil 1.5 \rceil = 2$

ceil

When to use LCM?

- **Scheduling problems**: Aligning events that occur at different intervals (e.g., bus schedules, maintenance cycles).
- **Adding/subtracting fractions**: Finding a common denominator to combine fractions.
- **Aligning cycles**: Matching frequencies of repeating patterns (e.g., gears, traffic lights).
- **LCM of polynomials**: Finding the least common multiple in algebraic expressions.
- **Least number divisible by all numbers**: Determining the smallest number that is divisible by several numbers.
- **Solving work rate problems**: Handling tasks with workers at different rates.
- **Finding common time intervals**: For combined events with different schedules.

Greatest Common Divisor

Greatest Common Divisor (GCD)

- If a and b are arbitrary integers, and if d is a common divisor, and when one of the integers is non-zero, then there will be a “finite” number of positive common divisors for a and b. The greatest among them is the **GCD**.

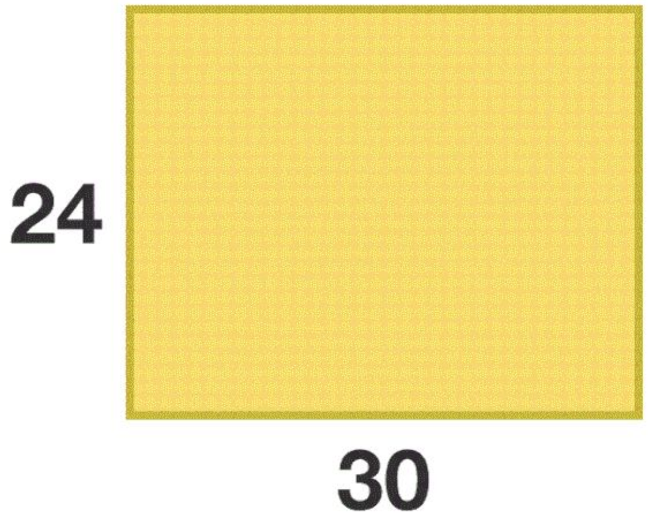
- **Mathematical Definition:** Let a and b be given integers, with at least one of them different from 0. An integer d is the Greatest Common Divisor of a and b, denoted as gcd(a, b), if:
    - 1. $d \mid a$ and $d \mid b$ (i.e., d is a common divisor)
    - 2. If $c \mid a$ and $c \mid b$ for any integer c, then $c \leq d$. (i.e., d is the greatest among common divisors)

- **GCD is also called as Highest Common Factor (HCF).**

Example:

Q. If you want to tile a 24×30 rectangle with square tiles that are all the same size, what are the largest square tiles you can use?

Ans:



Example:

Q. If you want to tile a 24×30 rectangle with square tiles that are all the same size, what are the largest square tiles you can use?

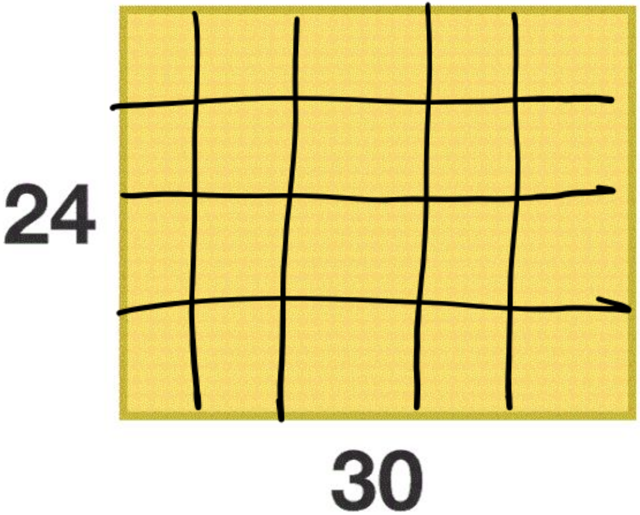
Ans:

GCD(24,30) = 6

24 → 1, 2, 3, 4, 6, 8, 12, 24

30 → 1, 2, 3, 5, 6, 10, 15, 30

HCF



Finding GCD using prime factorization

$$294 \qquad\qquad 364$$

$$2^1 \times 3^1 \times 7^2 \times 13^0 \qquad\qquad 2^2 \times 3^0 \times 7^1 \times 13^1$$

$$2^1 \times 3^0 \times 7^1 \times 13^0$$

$$\gcd(294, 364)$$

Therefore, we have

$$\begin{aligned} \gcd(294, 364) &= 2^1 \times 3^0 \times 7^1 \times 13^0 \\ &= 2^1 \times 1 \times 7^1 \times 1 \\ &= 2^1 \times 7^1. \end{aligned}$$

Logic behind taking lowest exponent while computing GCD

Suppose:

$$a = 2^1 \times 3^2, \quad b = 2^3 \times 3^1$$

- For prime 2:

  a needs one 2, b needs three.

  → Common factor = one 2 → 2^1.
- For prime 3:

  a needs two 3's, b needs one.

  → Common factor = one 3 → 3^1.

So:

$$\mathrm{GCD} = 2^1 \times 3^1$$

This works because:

- If we took **higher exponents**, the number would fail to divide one of them.
- Taking the **lowest exponent** ensures divisibility into **both** numbers.

Example:

Q. If you want to reduce the fraction 30/24 to lowest terms, what number should you divide the numerator and denominator by?

Ans: 2 / 3 / 6 / 12 ???

Newton School of Technology

Example:

Q. If you want to reduce the fraction 30/24 to lowest terms, what number should you divide the numerator and denominator by?

Ans: 6

$$\begin{array}{r|l} 2 & 30 \\ \hline 3 & 15 \\ \hline 5 & 5 \\ \hline & 1 \end{array} \qquad \begin{array}{r|l} 2 & 24 \\ \hline 2 & 12 \\ \hline 2 & 6 \\ \hline 3 & 3 \\ \hline & 1 \end{array}$$

$30 = 2^1 * 3^1 * 5^1$

$24 = 2^3 * 3^1 * 5^0$

$HCF(30, 24)$

$= 2^1 * 3^1 * 5^0$

$= 2 \times 3$

$= 6$

How to Find GCD? (School Days Method)

- **Method 1:** Listing Divisors
    1. Find all divisors of a.
    2. Find all divisors of b.
    3. List their common divisors.
    4. Find the greatest among the common divisors.
- **Limitation:** It is cumbersome for big a and b.

How to Find GCD?

$$a = 60 = 2^2 \times 3^1 \times 5^1$$

$$b = 48 = 2^4 \times 3^1$$

GCD = $2^{\min(2,4)} \times 3^{\min(1,1)} = 2^2 \times 3^1 = 12$

- **Method 2:** Using Prime Factorisation

1. Write the prime factorisation of a.
2. Write the prime factorisation of b.
3. Select the common prime factors with their smallest power.
4. Multiply them together → This gives the **GCD**.

- **Limitation:** Not practical for very large numbers.

Euclidean Algorithm

51

Efficient Way to Find GCD: Euclidean Algorithm

- The idea is to use the repeated application of the Division Algorithm.
- Euclid wrote about this in his 7th book, ”Elements”.

Euclidean Algorithm

- Given a and b, with $b \neq 0$, assuming $a \geq b > 0$.
- First apply Division Algorithm (DA) on a and b, which gives unique q_1 and r_1:

$$a = q_1 b + r_1; \quad 0 \leq r_1 < b$$

- Apply DA repeatedly:

$$\begin{aligned} b &= q_2 r_1 + r_2; & 0 \leq r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3; & 0 \leq r_3 < r_2 \\ &\vdots & \vdots \end{aligned}$$

Euclidean Algorithm

- The process continues until the remainder is zero:

$$r_{n-2} = q_n r_{n-1} + r_n; \quad 0 < r_n < r_{n-1}$$
$$r_{n-1} = q_{n+1} r_n + 0 \quad \rightarrow \text{STOPPING CONDITION}$$

- The **Greatest Common Divisor (GCD)** is the last non-zero remainder, r_n.

Finding GCD using Euclidean Algorithm

Let's compute **GCD(1160718174, 316258250)**

- 1160718174 = 3 ×316258250 + 211943424
- 316258250 = 1 ×211943424 + 104314826
- 211943424 = 2 × 104314826 + 3313772
- 104314826 = 31 × 3313772 + 1587814
- 3313772 = 2 × 1587814 + 137944
- 1587884 = 11 ×137984 + 20070
- 137984 = 1 ×20070 + 67914
- 20070= 1 ×67914 + 2156
- 67914 = 31 ×2156 + **1078**
- 2156 = 2 ×1078 + 0 (STOP!, **GCD = 1078**)

Imagine, how much time method 1 will take? (Computational Thinking)

Euclidean Algorithm for finding GCD of 2 numbers

Question: Find the GCD of 48 and 18.

Euclidean Algorithm for finding GCD of 2 numbers

Question: Find the GCD of 48 and 18.

Solution:

Apply Division Algorithm:

- **Step 1:** 48 = 2 x 18 + 12
- **Step 2:** 18 = 1 x 12 + **6**
- **Step 3:** 12 = 2 x 6 + 0

So, gcd(48, 18) = 6

When to use GCD?

- **Simplifying fractions**: Reducing fractions to their simplest form.
- **Dividing into equal groups**: Splitting items into the largest possible equal groups.
- **Finding common factors**: Identifying shared factors for optimization.
- **Modular arithmetic**: Important in number theory and cryptography for calculating inverses.
- **Minimizing waste**: Splitting things (e.g., cutting a ribbon) with minimal leftover.
- **Rationalizing ratios**: Simplifying ratios or proportions to their smallest form.

Relation between LCM and GCD

The product of the LCM and GCD of two numbers equals the product of the numbers themselves: **gcd(a, b) × lcm(a, b) = a × b**

- LCM(12,15) × GCD(12,15) = 12×15
- 60×3 = 180, and 12×15 = 180

Question:

- **Is it true for three numbers?**

60 × 3 = 180 ✓

12 × 15 = 180 ✓

12	15
24	30
36	45
48	60
60	75
72	⋮
⋮	

Example:

Q. Find sum of two positive integers x and y such that the LCM of x and y is 360 and their GCD is 15.

Example:

Q. Find sum of two positive integers x and y such that the LCM of x and y is 360 and their GCD is 15.

$$LCM(x,y) * GCD(x,y) = x*y$$

$$360 \quad * \quad 15 \quad = xy$$

$$\therefore \boxed{xy = 5400}$$

$$GCD(x,y) = 15$$

$$GCD(15a, 15b) = 15 \Rightarrow$$

$$LCM(x,y) = 360$$

$$LCM(15a, 15b) = 360$$

$$\therefore \boxed{LCM(a,b) = 24}$$

$xy = 5400$

$15a * 15b = 5400$

$\boxed{ab = 24}$

1. $a * b = 24$
2. $LCM(a,b) = 24$
3. $GCD(a,b) = 1$

$a = \underline{\underline{8}}$, $b = \underline{\underline{3}}$

$a = \underline{\underline{24}}$, $b = \underline{\underline{1}}$

So, you will get 2 different answers.

Newton School of Technology

$$x = 15a = 15 \times 8 = 120$$

$$y = 15b = 15 \times 3 = 45$$

$$\underline{\underline{165}}$$ ✓

$$x = 15a = 15 \times 24 = 360$$

$$y = 15b = 15 \times 1 = 15$$

$$\underline{\underline{375}}$$ ✓

Co-prime Numbers

Co-prime (Relatively prime) Numbers

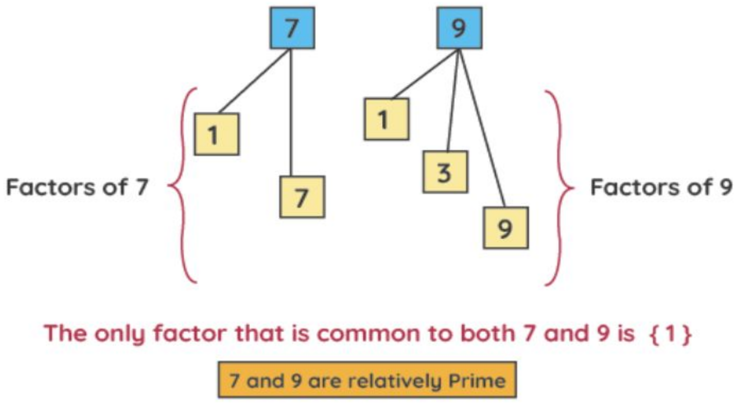
- Two numbers are called co-prime (or relatively prime) if they have no common positive integer factor other than 1.
- a and b are relatively prime if **gcd(a,b) = 1**.
- The LCM of two co-prime numbers is their product: lcm(a, b) = ab.
- Two prime numbers are always coprime.
- Consecutive integers are always coprime.
- A prime number and any number not divisible by it are co-prime.

Interesting Fact: 8 and 15 are co-prime but nether 8 nor 15 are prime.

Relatively prime

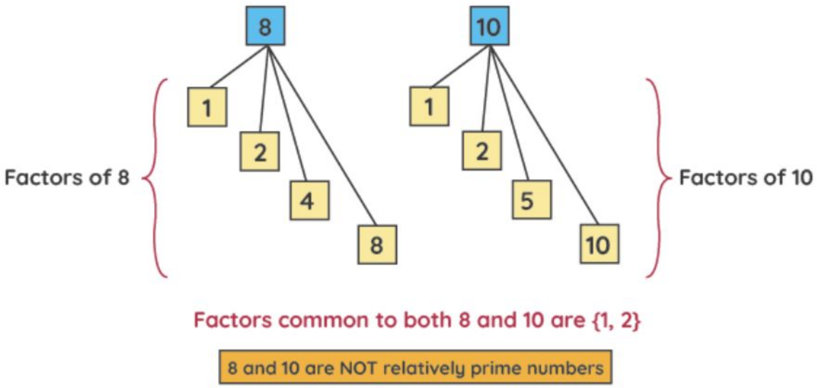
Example 1: gcd(7,9) = 1

So, 7 and 9 are relatively prime numbers.



Example 2: gcd(8,10) = 2

So, 8 and 10 are not relatively prime numbers.



Example:

Q. How many of the numbers 1, 2, 3 ,…, 100 are relatively prime to 101?

Ans:

Example:

Q. How many of the numbers 1, 2, 3 ,…, 100 are relatively prime to 101?

Ans: 100

$$\left.\begin{array}{l} GCD(1, 101) = 1 \\ GCD(2, 101) = 1 \\ \vdots \qquad\qquad\quad \vdots \\ GCD(100, 101) = 1 \end{array}\right\} \text{Total } 100 \text{ numbers}$$

Quiz Quiz Quiz

Key Takeaways

Today we learnt :

- LCM
- GCD
- Euclidean Algorithm on Numbers
- Co-prime numbers


Feedback Time

See You Guys in Next Session :)