Product of 2 or more prime numbers gives a composite number.

eg $2 \times 3 \rightarrow 6$ (composite No.)

If 1 was defined as prime number then it could be added as many times we want to the list of factors & then theorem would not be true.

↳ fundamental theorem of arithmetic

It states that every number > 1 can be written as product of primes

* PRIME FACTORISATION :

for eg $60 \rightarrow \underbrace{2 \times 2 \times 3 \times 5}_{\text{prime numbers}}$

steps to find prime factorisation of 60

① we have $7 < \sqrt{60} < 11$ $\left(\underbrace{7^2 = 49}_{\text{closest}} < 60 < 11^2 = 121 \right)$

② divide it by primes in decending order

③ $7 \nmid 60$

④ $60 = 5 \times 12$ and $5 \nmid 12$

⑤ $12 = 3 \times 4$ and $3 \nmid 4$

⑥ $4 = 2 \times 2$ $\Rightarrow$ $60 = 5 \times 3 \times 2 \times 2$.

exercise : prime factorization of 135

(1) $11 < \sqrt{135} < 13$

(2) $\underline{121} < 135 < 169$

closest

(3) $121 \nmid 135$

(4) $49 \nmid 135$

(5) $135 = 5 \times 27$

(6) $27 = 3 \times 9$

(7) $9 = 3 \times 3$

so $\boxed{\rightarrow\ 135 = 5 \times 3 \times 3 \times 3}$

DISCRETE MATHEMATICS

(*1) Prime factorization and the Euclidean algorithm:-

* Division of Integers:-

If a and b are integers, with $a \neq 0$, a divides b if there is an integer K such that $(b = aK)$ this is denoted by $a|b$

eg $3|12$ means 3 divide 12 & $12 = 3 \times 4$

so in the language of logic : $a|b \equiv \exists K : b = a \times K$

Properties of division :- Given integers (a, b & c)

(1) a is always factor of itself.
eg. 4 is a factor of 4 $(4 = 4 \times 1)$

(2) a is always a multiple of 1
$4 = (4 \times 1)$

(3) if $a|b$ & $a|c$ then $a|(b+c)$

eg $4|8$ & $4|12$ ie $4|(8+12) = 4/20$ ✓

(4) if $a|b$ then $a|bc$ {c any number}

(5) if $a|b$ & $b|c$ then $a|c$

_/_/_

* Prime Numbers

a number is prime when (P)

① $P > 1$
② it is only divisible by itself & 1

* Composite Number

① $P > 1$
② if it has other positive factors instead of itself & 1.

Examples

prime numbers → 3, 5, 7, 19

even prime number → only 2

composite number → 6, 9, 35
6 → 3×2 , 9 = 3×3.

1 is not a prime number

_/_/_

* LCM & GCD (Greatest Common divisor)

eg 10845

~~5~~	~~10845~~
~~3~~	~~2169~~
~~3~~	~~723~~
~~9~~	~~241~~

5	108045
3	21609
3	7203
7	2401
7	343
7	49
7	7
	1

$108045 \rightarrow 5 \times 3 \times 3 \times 7 \times 7 \times 7 \times 7 \times 2^0$

$120 \rightarrow 2 \times 2 \times 2 \times 3 \times 5 \times 7^0$

$\Downarrow$

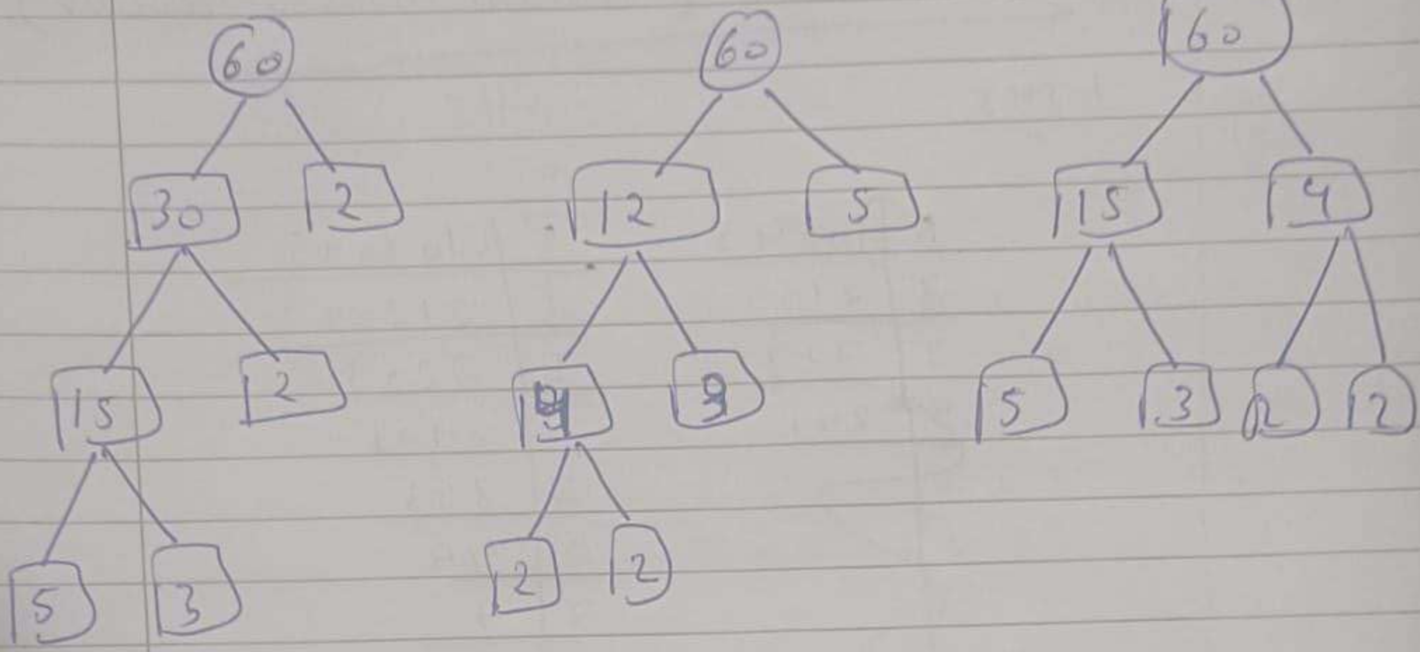
$\boxed{G.C.D} \rightarrow$ $5^1 \times 3^2 \times 7^4 \times 2^0$ - 108045

$2^3 \times 3^1 \times 5^1 \times 7^0$ - 120

(Take no. with small power) $\rightarrow$ $G.C.D = 2^0 \times 3^1 \times 5^1 \times 7^0 = 15$

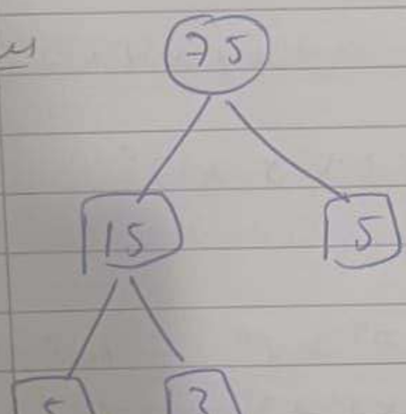
(Take no. with high power) $L.C.M = 2^3 \times 3^2 \times 5^1 \times 7^4 =$

* FACTOR TREE

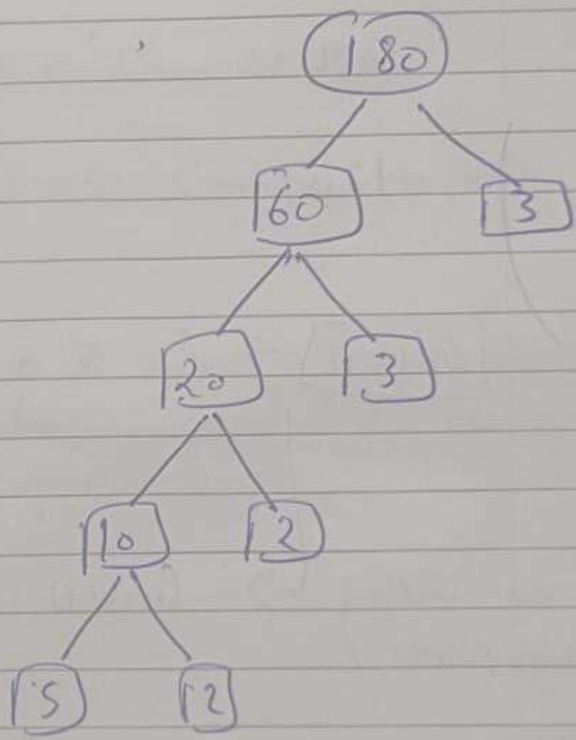


60 → 5×3×2×2

exercises



→ 75 = 5×5×3



180 = 5×2×2×3×3

\# if $a \mid b$ then $\gcd(b, a) = a$.

* BASE CONVERSION

- Our numeral system is base 10 system.

eg $837 = 8 \times 10^2 + 3 \times 10^1 + 7 \times 10^0$

- computers use base 2 (binary)
  base 8 (octal)
  base 16 (hexadecimal)

* Base 10

{ we express numbers in increasing powers of 10 from right to left.

eg 2017

$2 \times 10^3 + 0 \times 10^2 + 1 \times 10^1 + 7 \times 10^0$

Base 5

{ we represent numbers of powers of 5.

eg 1432_5

$\Downarrow$

$(1 \times 5^3) + (4 \times 5^2) + (3 \times 5^1) + (2 \times 5^0)$

in order to express it in base 10 multiply it out.

$\boxed{240_{10}}$

___/___/___

excercise 12 & 140

2	12
2	6
3	3
	1

2	140
2	70
5	35
7	7
	1

$$12 = 2^2 \times 3^1 \times 7^0 \times 5^0$$
$$140 = 2^2 \times 5^1 \times 7^1 \times 3^0$$

$$gcd(12,140) = 4$$

$$LCM(12,140) = 420$$

* EUCLIDEAN ALGORITHM:

Consider 2 integer a, b where b > a
when we divide b by a

$$b = m_0 \times a + r_0$$

{ m_0 - multiplier, r_0 - remainder }

so $gcd(b,a) = gcd(a,r_0)$

& $a = m_1 \times r_0 + r_1$

eg GCD (120, 18)

$$120 = 18 \times 6 + 12$$
$$18 = 12 \times 1 + 6$$
$$12 = 6 \times 2 + 0$$

So GCD(120, 18) => 6

$(2017)_{10}$

⇓

$\frac{3}{5^4}$ $\frac{1}{5^3}$ $\frac{0}{5^2}$ $\frac{3}{5^1}$ $\frac{2}{5^0}$

$2017 = 3 \times 625 + 142$
$142 = 1 \times 125 + 17$
$17 = 0 \times 25 + 17$
$17 = 3 \times 5 + 2$
$2 = 2 \times 1 + 0$

$(2017)_{10} = (31023)_5$

Method 2 eg 2473

$2473 \div 10 = 247 R 3$
$247 \div 10 = 24 R 7$
$24 \div 10 = 2 R 4$
$2 \div 10 = 0 R 2.$

Rough

$$
\begin{array}{r}
22 \\
16\overline{)353} \\
\underline{32} \\
33 \\
\underline{32} \\
1
\end{array}
\qquad
\begin{array}{r}
43 \\
2\overline{)87} \\
\underline{8} \\
07 \\
\underline{6} \\
1
\end{array}
$$

$$
\begin{array}{r}
16 \\
7\overline{)113} \\
\underline{7} \\
43 \\
\underline{42} \\
1
\end{array}
\qquad
\begin{array}{r}
16 \\
7\overline{)115} \\
\underline{7} \\
45 \\
\underline{42} \\
3
\end{array}
$$

$4800 = 930 + 150$

$930 = 150 \times 6 + 30$

$150 = 30 \times 5 + 0$

3887

$a = 1$

$a \mod 6 =$

$a = k6 + r$

$323 = k6 + 17$

$323 - 17$

$306 = k6$

$3887 = 759 + 92$

$759 = 92 \times 8 + 23$

$92 = 23 \times 4 + 0$

$\boxed{\text{Base 2}}$

In base 2 we only use 0 and 1.

for eg 100101_2 is

$$(1\times2^5)+(0\times2^4)+(0\times2^3)+(1\times2^2)+(0\times2^1)+(1\times2^0)$$

to express it in base 10 multiply it.

Converting from base 10 to base 5

2017

$$(2\times10^3)+(0\times10^2)+(1\times10^1)+(7\times10^0)$$

$$\Downarrow$$

$$(2\times5^3)+(0\times5^2)+(1\times5^1)+(7\times5^0)$$

$$=(2\times125)+0+5+7$$

$$250+12$$

$$\Rightarrow 262$$

$$(2017)_{10}=(262)_5$$

1^{13}, 65

~~2017~~

~~2017 ÷ 5 = 403.4~~

2017 ÷ 5 =

MODULAR ARTHIMETIC

If an integer A divided by another integer B & has remainder ≥ 0 Then,

$$r = a \bmod b$$

$$\Downarrow$$

$$a = kb + r \qquad \{k \to \text{integer}\}$$

eg

$17 \bmod 2 = 1$ (as $17 = 8 \times 2 + 1$)

$17 \bmod 7 = 3$ ($17 = 7 \times 2 + 3$)

Question

$(10821793 \times 27228955) \bmod 2$

as both are odd no.s

So it is $\boxed{1}$

* Modular exponential

$$\left.\begin{aligned} 2^{4n} \bmod 10 &= 6 \\ 2^{4n+1} \bmod 10 &= 2 \\ 2^{4n+2} \bmod 10 &= 4 \\ 2^{4n+3} \bmod 10 &= 8 \end{aligned}\right\} \quad \{n > 1\}$$

$1585_{10} = \quad _5$

$\cancel{(2 \times 625) + (\quad \times 5^3}$

$1585 = 2 \times 625 + 335$
$335 = 2 \times 125 + 85$
$85 = 3 \times 25 + 10$
$10 = 2 \times 5 + 0$

2	252
2	126
3	63
3	21
7	7
	1

5	90
2	16
2	8
2	4
2	2
	1

$1177 = 1 \times 9^3 + 448$
$448 = 5 \times 9^2 + 43$
$43 = 4 \times 9^1 + 7$
$7 = 7 \times 9^0 + 0$

2060 =	206	0
	20	6
	2	

__/__/__

2	4800
2	2400
2	1200
2	600
2	
2	300
2	150
5	75
5	15
3	3
	1

$2^6 \times 5^2 \times 3^2 \times 93^0$

$2^1 \times 5^1 \times 3^0 \times 93^1$

$2^6 \times 5^2 \times 3^1 \times 93$

2	930
5	465
93	93
3	3/1
	1

5	990
2	198
3	99
3	33
11	11
	1

2	96
2	48
2	24
2	12
2	6
3	3
	1

$5^1 \times 2 \times 3^2 \times 11^1$

$5 \times 2 \times 3^2 \times 11$

$5^0 \times 2^5 \times 3^1 \times 11^0$

$Gcd = 5^0 \times 2 \times 3 \times 11^0$

6

$5^1 \times 2^5 \times 3^2 \times 11$