Unit-III

Divisibility Theory and Canonical Decompositions

Defn [Prime]

A +ve integer is called a prime number if its only divisors are 1 and itself.

Defn [composite number]

A +ve integer is called a composite number if it is not a prime.

Examples

(1) 2 is a prime.

∵ Its divisors are 1 and 2.

2 is the only even prime.

(2) 3, 5, 7, 11 are prime numbers.

(3) 6, 18, 100 are not primes.

∵ Divisors of 6 are 1, 2, 3, 6.

Divisors of 18 are 1, 2, 3, 6, 18.

Divisors of 100 are 1, 2, 4, 5, 10, 20, 25, 50, 100.

∴ 6, 18, 100 are composite number.

Theorem: ① Every integer $n \geq 2$ has a prime factor.

Proof: We prove this theorem by mathematical induction.

When $n = 2$, 2 divides 2

$\Rightarrow$ n has a prime factor 2.

$\therefore$ The result is true for $n = 2$.

Induction hypothesis: Assume that the result is true for integer $k \geq 2$.

It is enough to prove this result for $k+1$

case(i) Suppose $k+1$ is prime.

Then $(k+1)$ divides $(k+1)$.

case(ii) Suppose $(k+1)$ is not a prime.

Then $(k+1)$ is a composite number.

Then $(k+1)$ has a divisor 'd'

By induction hypothesis, d has a prime factor say 'p'.

This p divides $(k+1)$ also.

$\therefore$ $(k+1)$ has a prime factor p.

$\therefore$ By induction the result is true for any integer $n \geq 2$.

Theorem ② There are infinitely many primes.

[Euclid's Theorem]

Proof:-

Suppose there are only finite number of primes.

List them by $p_1, p_2, \ldots, p_n$.

Take $N = p_1 p_2 \ldots p_n + 1$.

Then $N \geq 2$.

We know that every integer ≥ 2 has a prime factor.

$\therefore$ N has a prime factor.

Since $p_1, p_2, \ldots, p_n$ are only primes, N has a prime factor p_i where $1 \leq i \leq n$.

$\Rightarrow p_i$ divides N.

$\Rightarrow p_i$ divides $(p_1 p_2 \ldots p_n + 1)$ $\longrightarrow$ ①.

Also p_i divides $(p_1 p_2 \ldots p_n)$ $\longrightarrow$ ②.

$\Rightarrow p_i$ divides $(p_1 p_2 \ldots p_n + 1 - p_1 p_2 \ldots p_n)$

Result. If a divides b and a divides c then a divides $(bl + cm)$ where $l, m \in Z$

$\Rightarrow p_i$ divides 1 ③

Which is impossible.

$\therefore$ There are infinitely many prime numbers.

Procedure For finding prime number

Suppose we want to find a given number 'n' is prime or not.

Step ① Find $\sqrt{n}$.

Step ② List out all primes $\leq \sqrt{n}$.

Step ③ Suppose any prime listed in step ② divides n then n is not a prime.

Otherwise n is prime.

Example Determine whether 1601 is a prime

Soln

$$\sqrt{1601} = 40.012$$

Prime numbers which are $\leq \sqrt{1601}$ listed by 2, 3, 5, 7, 11, 13, 17, 19, 23 and 29.

None of these above listed primes divides 1601.

∴ 1601 is a prime number.

Homework

① Determine whether 1487 is a prime.

② Determine whether 1597 is a prime.

The Sieve of Eratosthenes

To find the prime numbers $\leq$ given positive integer.

This method was introduced by a Greek mathematician Eratosthenes.

We illustrate by an example for finding prime numbers ≤ 100.

~~1~~	(2)	(3)	~~4~~	(5)	~~6~~	(7)	~~8~~	~~9~~	~~10~~
(11)	~~12~~	(13)	~~14~~	~~15~~	~~16~~	(17)	~~18~~	(19)	~~20~~
~~21~~	~~22~~	(23)	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	(29)	~~30~~
(31)	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	(37)	~~38~~	~~39~~	~~40~~
(41)	~~42~~	(43)	~~44~~	~~45~~	~~46~~	(47)	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	(53)	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	(59)	~~60~~
(61)	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	(67)	~~68~~	~~69~~	~~70~~
(71)	~~72~~	(73)	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	(79)	~~80~~
~~81~~	~~82~~	(83)	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	(89)	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	(97)	~~98~~	~~99~~	~~100~~

Steps

① Find prime numbers $\sqrt{100} = 10$.

a) 2, 3, 5, 7.

② cut 1 and multiples of 2, 3, 5, 7 but not 2, 3, 5, 7.

③ Numbers remaining as non-cut are required primes.

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Theorem ③: Prove that there is no polynomial with integer coefficients that will produce primes for all integers 'n'.

Proof:

Suppose there is a polynomial

$$f(n) = a_k n^k + a_{k-1} n^{k-1} + \cdots + a_1 n + a_0 \quad \text{where } a_k \neq 0$$

that gives primes for all integer 'n'.

i) $f(n)$ = always prime.

Let $b \in Z$.

Then $f(b) = p$ where p is prime.

$$\Rightarrow a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0 = p. \longrightarrow ①$$

Take $t \in Z$ arbitrarily.

Then $b + tp \in Z$.

$$f(b+tp) = a_k (b+tp)^k + a_{k-1} (b+tp)^{k-1} + \cdots + a_1 (b+tp) + a_0$$

$$= \left[a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0 \right] + p \cdot g(t)$$

where $g(t)$ is polynomial in t.

$\therefore f(b+tp) = p + p \cdot g(t)$

$f(b+tp) = p\left[1 + g(t)\right]$

$\Rightarrow p$ divides $f(b+tp)$.

By our assumption, $f(b+tp)$ is a prime

$\Rightarrow f(b+tp) = p$.

$\therefore$ We have $f(b) = p = f(b+tp)$

This is true for every integer t.

$\Rightarrow$ f takes the same value 'p' at infinitely many times.

But $f(n)$ is a polynomial of degree k.

$\therefore$ It cannot have the same value infinitely many times.

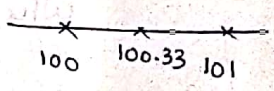
$\therefore$ We get a $\Rightarrow\Leftarrow$.

$\therefore$ There is no such polynomial.

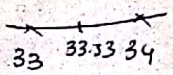
Defn [Lowest integral part].

For any number 'n', lowest integral part of n is denoted by $\lfloor n \rfloor$ and defined by the lowest integer contained in n.

Example

① $\lfloor 100.33 \rfloor = 100$ ($\because$ 

)

② $\left\lfloor \frac{100}{3} \right\rfloor = \lfloor 33.33 \rfloor = 33$ ($\because$ 

)

To find number of primes $\leq$ given +ve integer.

Let n be a +ve real number.

$\pi(n)$ denote number of primes $\leq n$.

Steps

① Find $\sqrt{n}$

② List the primes $\leq \sqrt{n}$.

③ Suppose the primes are

$P_1, P_2, P_3, \ldots, P_K$.

Then $\pi(n) = n - 1 + \pi(\sqrt{n}) - \sum \left\lfloor \frac{n}{P_i} \right\rfloor$

$+ \sum_{i<j} \left\lfloor \frac{n}{P_i P_j} \right\rfloor - \sum_{i<j<k} \left\lfloor \frac{n}{P_i P_j P_k} \right\rfloor + \cdots$

$+ (-1)^K \left\lfloor \frac{n}{P_1 P_2 \cdots P_K} \right\rfloor$

Here $\lfloor b \rfloor$ denote lowest integral part.

Problem Find the number of primes ≤ 100.

Soln.

$n = 100$.

$\sqrt{n} = \sqrt{100} = 10$.

Primes $\leq \sqrt{n} = 10$ are $2, 3, 5, 7$.

$\therefore \pi(100) = 100 - 1 + \pi(10) - \left[\left\lfloor \frac{100}{2} \right\rfloor + \left\lfloor \frac{100}{3} \right\rfloor + \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{7} \right\rfloor \right]$

$+ \left[\left\lfloor \frac{100}{2 \cdot 3} \right\rfloor + \left\lfloor \frac{100}{2 \cdot 5} \right\rfloor + \left\lfloor \frac{100}{2 \cdot 7} \right\rfloor + \left\lfloor \frac{100}{3 \cdot 5} \right\rfloor + \left\lfloor \frac{100}{3 \cdot 7} \right\rfloor + \left\lfloor \frac{100}{5 \cdot 7} \right\rfloor \right]$

$- \left[\left\lfloor \frac{100}{2 \cdot 3 \cdot 5} \right\rfloor + \left\lfloor \frac{100}{2 \cdot 3 \cdot 7} \right\rfloor + \left\lfloor \frac{100}{3 \cdot 5 \cdot 7} \right\rfloor \right] + \left\lfloor \frac{100}{2 \cdot 5 \cdot 7} \right\rfloor$

$+ \frac{100}{2 \cdot 3 \cdot 5 \cdot 7}$.

$= 99 + 4 - (50 + 33 + 20 + 14) + (16 + 10 + 7 + 6 + 4 + 2) - (3 + 2 + 1 + 0) + 0 = 25$

∴ There are 25 primes which are ≤ 100.

Homework

(1) Find the number of primes ≤ 50

(2) Find the number of primes ≤ 75.

Important Result

For every +ve integer n, there are n consecutive integers that are composite numbers.

They are

$$(n+1)! + 2,\ (n+1)! + 3,\ (n+1)! + 4,\ \ldots,\ (n+1)! + (n+1)$$

Proof:-

Let n be any +ve integer.

Consider $(n+1)! + 2,\ (n+1)! + 3,\ (n+1)! + 4,\ \ldots,\ (n+1)! + (n+1)$.

Clearly the above numbers are consecutive.

It is enough to prove they are composites.

2 divides $(n+1)! + 2$

3 divides $(n+1)! + 3$

4 divides $(n+1)! + 4$

$\vdots$

$(n+1)$ divides $(n+1)! + (n+1)$.

∴ They are composite numbers.

H/p.

Problem Find six consecutive integers that are composites.

Soln $n = 6$.

$\therefore (6+1)! + 2,\ (6+1)! + 3,\ (6+1)! + 4,$

$(6+1)! + 5,\ (6+1)! + 6,\ (6+1)! + 7$

are required numbers.

$$(6+1)! = 7! = 1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7$$

$$= 5040.$$

$\therefore$ 5042, 5043, 5044, 5045, 5046, 5047 are six consecutive integers which are composites.

Homework

① Find five consecutive integers which are composites.

② Find seven consecutive integers which are composites.

Division Algorithm

Theorem ④ (U.Q): Let 'a' be any integer and 'b' a positive integer. Then there exist unique integers q and r such that

$$a = b \cdot q + r \quad \text{where} \quad 0 \le r < b.$$

Here $b \rightarrow$ divisor

$q \rightarrow$ quotient

$r \rightarrow$ remainder.

Proof :-

Let 'a' be any integer and 'b' a +ve integer.

Consider $S = \{ a - xb \;/\; x \text{ is an integer}, \; a - xb \geq 0 \}$

Claim ①: S is non-empty.

Consider $x = -|a|$.

Clearly x is an integer.

$$a - xb = a + |a|b$$
$$\geq a + |a|$$
$$\geq 0.$$

By the choice of $x = -|a|$, $a - xb \in S$.

$\therefore$ S is non-empty.

Hence the claim ①.

Let 'r' be the least element of S.

Then $r = a - qb$ where q is an integer and $a - qb \geq 0$.

$\therefore \quad r = a - qb$ where $0 \le r$ ~~<b~~.

Claim ②: $r < b$.

Suppose $r \geq b$.

Consider $a-(q+1)b = a-qb-b$

$= r-b$

≥ 0. ($\because r \geq b \Rightarrow r-b \geq 0$)

$\Rightarrow a-(q+1)b \in S$

But $a-(q+1)b = a-qb-b = r-b < r$.

This is a $\Rightarrow\Leftarrow$ to r is the least element of S.

$\therefore r < b$.

$\therefore \exists$ q and r such that $a = bq+r$ where $0 \leq r < b$.

To prove the uniqueness:

Suppose $\exists$ 2 representations

$a = bq+r$, $0 \leq r < b$ and

$a = bq_1+r_1$, $0 \leq r_1 < b$.

Then $bq+r = bq_1+r_1$

$\Rightarrow b(q-q_1) = r-r_1$

Take modulus both sides

$|b(q-q_1)| = |r-r_1|$.

$\Rightarrow b|(q-q_1)| = |(r-r_1)|$ ⟶ ①.

Now $0 \le r_1 < b$

$\Rightarrow -b \le -r_1 \le 0$.

Also $0 \le r < b$.

Adding above two inequalities

$$-b \le r - r_1 \le b.$$

$$\Rightarrow |r - r_1| \le b \quad (\because -a \le x \le a \Rightarrow |x| \le a).$$

From ①, $b|q - q_1| \le b$.

$$\Rightarrow |q - q_1| \le 1.$$

$$\Rightarrow |q - q_1| = 0 \quad (\because q \text{ and } q_1 \text{ are integers}).$$

$$\Rightarrow q - q_1 = 0$$

$$\Rightarrow \boxed{q = q_1}$$

Sub $q = q_1$ in eqn ①

$$b(0) = |r - r_1|.$$

$$\Rightarrow 0 = |r - r_1|$$

$$\Rightarrow 0 = (r - r_1)$$

$$\Rightarrow \boxed{r = r_1}$$

$\therefore$ The representation is unique.

Problem Find the quotient 'q' and the remainder 'r' when

(i) 207 is divided by 15

(ii) -23 is divided by 5.

Soln (i) $207 = 15 \cdot (13) + 12$.

$\therefore q = 13, r = 12$.

(ii) $-23 = 5(-5) + 2$.

$\therefore q = -5, r = 2$.

Theorem ⑤: Pigeonhole Principle

If m pigeons are assigned to n pigeonholes, where $m > n$ then atleast two pigeons must occupy the same pigeonhole.

Proof:

Suppose no two pigeons occupy the same pigeonhole.

Then every pigeon must occupy the distinct pigeonhole.

$\Rightarrow n \not> m$.

Which is a $\Rightarrow \Leftarrow$ to $m > n$.

$\therefore$ At least two pigeons must occupy Same pigeonhole.

Defn [Divides]

Using division algorithm $a = bq + r$.

If $r = 0$, $a = bq$.

$\Rightarrow$ a is divided by b.

Also b divides a.

In other words, a is a multiple of b.

We denote b/a if b divides a.

$b \not/ a$ if b does not divide a.

Problem [Application of Pigeonhole principle].

Let b be an integer ≥ 2. Suppose $b+1$ integers are randomly selected. Prove that the difference of two of them is divisible by 'b'.

Soln:-

Let a be any integer and 'b' a +ve integer with $b \geq 2$.

Then by division algorithm,

$$a = b.q + r \quad ; \quad 0 \leq r < b.$$

Select any $(b+1)$ integers randomly.

These $(b+1)$ integers yield $(b+1)$ remainders when divided by b.

But there are only 'b' possible remainders.

Take $(b+1)$ remainders as pigeons

b possible remainders as pigeonhole.

∴ By pigeonhole principle, two of the remainders are equal.

Let x and y be corresponding integers.

Then $x = bq_1 + r$ and

$$y = bq_2 + r$$

$$x - y = b(q_1 - q_2).$$

$\Rightarrow$ $x - y$ is divided by.

Theorem ⑥ Let a and b be +ve integers such that a/b and b/a then $a = b$.

Proof

Let a and b be any +ve integers such that a/b & b/a.

$a/b \Rightarrow b = a \cdot q_1 \longrightarrow ①$

$b/a \Rightarrow a = b \cdot q_2 \longrightarrow ②$.

Sub ② in ①, $b = b \cdot q_2 \cdot q_1$.

$\Rightarrow 1 = q_1 \cdot q_2$.

Since q_1 and q_2 are integers, Both q_1 and q_2 may be equal to 1

(or)

both q_1 and q_2 may be equal to -1.

From ①, ② $a = b$.

Theorem ⑦: Let a, b, c, α and β be any integers.

Then (i) If a/b and b/c, then a/c. [Transitive property]

(ii) If a/b and a/c, then $a/(\alpha b + \beta c)$

(iii) If a/b, then a/bc.

Proof:

(i) If a/b and b/c

Then $b = a \cdot q_1$ and $c = b \cdot q_2$.

$c = a \cdot q_1 q_2$

$\Rightarrow a/c$.

(ii) If a/b and a/c

Then $b = a \cdot q_1$ and $c = a \cdot q_2$.

$\alpha b = a \cdot \alpha q_1$ and $\beta c = a \cdot \beta q_2$.

$\alpha b + \beta c = a\alpha q_1 + a \cdot \beta q_2$.

$\alpha b + \beta c = a[\alpha q_1 + \beta q_2]$.

$\Rightarrow a / \alpha b + \beta c$.

(iii) If a/b then $b = a \cdot q$

$\Rightarrow bc = a \cdot cq$.

$\Rightarrow a / bc$.

Hence the proof.

Union, Intersection and Complement.

Let A, B be any sets.

$A \cup B = \{ x / x \in A \text{ (or) } x \in B \}$.

$A \cap B = \{ x / x \in A \text{ and } x \in B \}$.

$A^c = \{ x / x \notin A \}$.

$A \cup B$ is union of A and B.

$A \cap B$ is intersection of A and B.

A^c is complement of A.

Important result

① $|A \cup B| = |A| + |B| - |A \cap B|$.

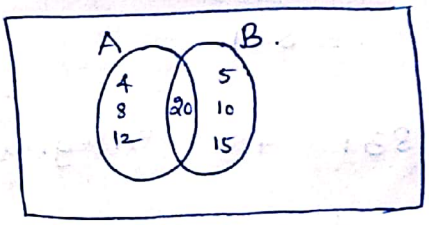
Here $|x|$ means number of element in the set X.

~~② $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$~~

② $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|$.

Problem Find the number of positive integers ≤ 2076 and divisible by neither 4 nor 5.

Soln.



Let A be the set of positive integers ≤ 2076 and divisible by 4.

i.e. $A = \{x / x \leq 2076, x \text{ is divisible by } 4\}$.

$$|A| = \left\lfloor \frac{2076}{4} \right\rfloor = 519$$

Let B be the set of +ve integers ≤ 2076 and divisible by 5.

i.e. $B = \{y / y \leq 2076, y \text{ is divisible by } 5\}$.

$$|B| = \left\lfloor \frac{2076}{5} \right\rfloor = 415.$$

$\therefore A \cup B = \{x \mid x \leq 2076,\ x \text{ is divisible by } 4$ (or) $x \text{ is divisible by } 5\}$.

$A \cap B = \{x \mid x \leq 2076,\ x \text{ is divisible by } 4$ and $x \text{ is divisible by } 5$

$$A \cap B = \left\lfloor \frac{2076}{4 \times 5} \right\rfloor = \left\lfloor \frac{2076}{20} \right\rfloor = 103$$

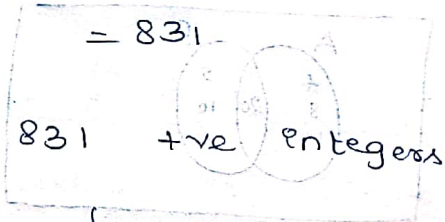
Formula

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

$\therefore |A \cup B| = 519 + 415 - 103$

$= 934 - 103$

$= 831$



$\therefore$ There are 831 +ve integers ≤ 2076 which are either divisible by 4 or by 5.

$\therefore$ Number of +ve integers ≤ 2076 and divisible by neither 4 nor 5

$= 2076 - 831$

$= 1245$.

Problem: Find the number of positive integers ≤ 3000 and divisible by 3, 5 or 7.

Soln: Let A, B, C denote the set of +ve integers ≤ 3000 and divisible by 3, 5, 7 respectively.

$\Rightarrow |A| = \left\lfloor \frac{3000}{3} \right\rfloor = 1000$

$|B| = \left\lfloor \frac{3000}{5} \right\rfloor = 600$

$|C| = \left\lfloor \frac{3000}{7} \right\rfloor = 428$

$|A \cap B| = \left\lfloor \frac{3000}{3 \times 5} \right\rfloor = 200$

$|B \cap C| = \left\lfloor \frac{3000}{5 \times 7} \right\rfloor = 85$

$|A \cap C| = \left\lfloor \frac{3000}{7 \times 3} \right\rfloor = 142.$

$|A \cap B \cap C| = \left\lfloor \frac{3000}{3 \times 5 \times 7} \right\rfloor = 28.$

Number of +ve integers ≤ 3000 and divisible by 3, 5 or 7 $\Big\} = |A \cup B \cup C|$

$= |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|$

$= 1000 + 600 + 428 - 200 - 85 - 142 + 28$

$= 1629.$

Defn [Even and Odd integer].

Even integer is of the form $2n$.

Odd integer is of the form $(2n+1)$.

Note

* zero is even
* even + even = even
* even · even = even
* odd + odd = even
* odd · odd = odd
* even + odd = odd
* even · odd = even.
* $(\text{even})^2 = \text{even}$
* $(\text{odd})^2 = \text{odd}$

Base - b Representation

Let 'b' be a positive integer ≥ 2.

Take $N \in Z^+$.

Then N can be written as

$$N = a_k b^k + a_{k-1} b^{k-1} + a_{k-2} b^{k-2} + \cdots + a_1 b + a_0.$$

Where $a_0, a_1, a_2, \ldots, a_k$ are non negative integers $< b$.

$a_k \neq 0$ and $k \geq 0$.

We write $N = (a_k a_{k-1} \cdots a_1 a_0)_b$ in base 'b'.

Example

Take $b = 2$.

$N = 57$.

Method ①

$57 = 2(28) + 1$

$28 = 2(14) + 0$

$14 = 2(7) + 0$

$7 = 2(3) + 1$

$3 = 2(1) + 1$

$1 = 2(0) + 1$

Write from down to up.

$57 = (111001)_2$

$57 = (1 \times 2^5) + (1 \times 2^4) + (1 \times 2^3) + (0 \times 2^2) + (0 \times 2^1) + (1 \times 2^0)$

$= 32 + 16 + 8 + 1$

$= 57.$

Method ② Easy

2	57
2	28 – 1
2	14 – 0
2	7 – 0
2	3 – 1
	1 – 1

$57 = (111001)_2$

ⓐ $57 = (1 \times 2^5) + (1 \times 2^4) + (1 \times 2^3) + (0 \times 2^2) + (0 \times 2^1) + (1 \times 2^0)$

$= 32 + 16 + 8 + 0 + 0 + 1$

Special Number Patterns :

① **Binary Expansion**

If $b = 2$, the Base-b representation is called binary expansion.

In binary expansion each coefficient is either 0 or 1.

② If $b = 10$, then Base-b representation is called decimal system.

Decimal system is ordinary number system.

Example $(234)_{10} = 234$

③ When $b > 10$.

We use letters $A = 10$

$B = 11$

$C = 12$

$D = 13$

⋮

to avoid confusions.

④. If $b = 16$ then Base b-representation is called Hexa-decimal number system.

⑤ If $b = 8$ then Base b-representation is called Octal numbers.

Problems

① Express $(10110)_{two}$ in base ten.

Soln.

$$(10110)_{two} = (1\times2^4) + (0\times2^3) + (1\times2^2) + (1\times2^1) + (0\times2^0)$$

$$= 16 + 0 + 4 + 2 + 0$$

$$= 22$$

$$= (22)_{10}.$$

---

② Express $3ABC_{Sixteen}$ in base ten.

A = 10
B = 11
C = 12

Soln.

$$(3ABC)_{16} = 3(16^3) + A(16^2) + B(16^1) + C(16^0)$$

$$= 3(16^3) + 10(16^2) + 11(16^1) + 12(16^0)$$

$$= 12,288 + 2560 + 176 + 12$$

$$= 15,036$$

$$= (15036)_{10}.$$

---

③ Express 3014 in base eight.

Soln

8	3014	
8	376	— 6
8	47	— 0
	5	— 7

$\therefore$ $3014 = (5706)_8.$

---

④ Represent 15,036 in hexadecimal number system.

Soln

16	15036	
16	939	— 12 = C
16	58	— 11 = B
	3	— 10 = A

$\therefore$ $15036 = (3ABC)_{16}.$

Operations in Non decimal Bases

Suppose you want to add the numbers 58 and 67.
in decimal base (a base 10)

First we add $8+7=15$

Then we will write 5 and write 1 on up for 5 and 6.

If we note this carefully $15 = 1(10) + 5$.

1 → quotient

5 → remainder.

∴ we write remainder in one's place and carry the quotient on top of 10'th place.

Then similar operation will be done in 100'th place.

$$\begin{array}{r} \overset{1}{} \\ 58 \\ 67 \\ \hline 125 \end{array}$$

Similarly we can operate on Non-decimal patterns.

Adding

Addition in Base-b

Problems

① Add the binary integers 10110_{two} and 1011_{two}.

Soln

$$\begin{array}{r} {\scriptstyle ①\ \ ①\ \ ①} \\ 1\ 0\ 1\ 1\ 0 \\ (+)\quad 1\ 0\ 1\ 1 \\ \hline 1\ 0\ 0\ 0\ 0\ 1 \\ \hline \end{array}$$

$0+1=1 = 0(2)+1$

$1+1=2 = 1(2)+0.$

---

② Add $A58B_{twele}$ and $9A3_{twele}$.

Soln

$$\begin{array}{r} {\scriptstyle ①\ \ ①\ \ ①} \\ A\ 5\ 8\ B \\ (+)\quad 9\ A\ 3 \\ \hline B\ 3\ 7\ 2 \\ \hline \end{array}$$

A = 10
B = 11

$B+3 = 14 = 1(12)+2.$

$1+8+A = 19 = 1(12)+7.$

$1+5+9 = 15 = 1(12)+3$

Answer : $B372_{twele}$.

---

③ Add $ABC_{Sixteen}$ & $CBA_{Sixteen}$.

$$\begin{array}{r} {\scriptstyle ①\ \ ①} \\ A\ B\ C \\ (+)\quad C\ B\ A \\ \hline 1\ 7\ 7\ 6 \\ \hline \end{array}$$

A = 10
B = 11
C = 12

$C+A = 12+10 = 22 = 1(16)+6.$

$①+B+B = 1+11+11 = 23 = 1(16)+7.$

$①+A+C = 1+10+12 = 23 = 1(16)+7.$

Answer : $(1776)_{Sixteen}$.

Subtraction in Base - b

Problems

① Evaluate $(2354)_{seven} - (463)_{seven}$.

Soln

$$\begin{array}{r} \overset{}{\overset{(12)}{\overset{(1)}{\overset{(2)}{\overset{(15)}{}}}}} \\ 2\ 3\ 5\ 4 \\ (-)\quad 4\ 6\ 3 \\ \hline 1\ 5\ 6\ 1 \end{array}$$

*. Not necessary to write in exam.

$15 - 6 = x$. (say)

$\Rightarrow x + 6 = 15$.

So x is the number, when it is added with 6 gives y. $\Rightarrow \boxed{x + 6 = y}$

When y is divided by '7' it gives 5 as the remainder and 1 as quotient.

$\therefore y = 1(7) + 5$

$\therefore \boxed{y = 12}$

$\therefore \boxed{x = 12 - 6 = 6}$

Checking $(2354)_7 - (463)_7 = (1561)_7$.

$\Rightarrow (1561)_7 + (463)_7 = (2354)_7$.

$$\begin{array}{r} \overset{}{\overset{(1)}{\overset{(1)}{}}} \\ 1\ 5\ 6\ 1 \\ (+)\quad 4\ 6\ 3 \\ \hline 2\ 3\ 5\ 4 \end{array}$$

Problem ② Evaluate $(A74)_{12} - (39B)_{12}$

A = 10
B = 11

Soln

$$\begin{array}{r} \overset{(16)}{(9)}\ \overset{(6)}{(6)}\ \overset{(14)}{(14)} \\ A\ 7\ 4 \\ (-)\quad 3\ 9\ B \\ \hline 6\ 9\ 5 \end{array}$$

$14 - B$ = number which leaves remainder 4 and quotient 1 when added with $B = 10$.

$14 - B = 5$.

Answer : $(695)_{12}$.

Problem ③ Evaluate $2076_{\text{sixteen}} - 177_{\text{sixteen}}$.

A = 10
B = 11
C = 12
D = 13
E = 14
F = 15

Soln

$$\begin{array}{r} \overset{(1)}{(1)}\ \overset{(F)}{(F)}\ \overset{(16)}{(6)}\ \overset{(16)}{(16)} \\ 2\ 0\ 7\ 6 \\ (-)\quad 1\ 7\ 7\ 7 \\ \hline 8\ F\ F \end{array}$$

Answer : $(8FF)_{\text{sixteen}}$.

Steps

① $16 - 7 = F$.

$(\because 7 + F = 7 + 15 = 22 = 1(16) + 6.)$

② $F - 7 = 8$

$(\because F = 15 > 7)$.

(A) Subtract $(1011)_{two}$ from $(100001)_{two}$.

Soln.

$$\begin{array}{r} 0\ \overset{1}{\not 1}\ \overset{1}{\not 0}\ \overset{1}{\not 0}\ \overset{10}{\not 0}\ 1 \\ (-)\quad 1\ 0\ 1\ 1 \\ \hline 0\ 1\ 0\ 1\ 1\ 0 \end{array}$$

$10 - 1 = 1$ $\quad (\because 1+1 = 2 = 1_{(2)} + 0)$

Answer: $(010110)_{two}$.

Multiplication in Base-b.

Problems

① Evaluate $(1011)_{two} \times (101)_{two}$.

$$\begin{array}{r} 1\ 0\ 1\ 1 \\ (\times)\quad 1\ 0\ 1 \\ \hline 1\ 0\ 1\ 1 \\ (+)\ 0\ 0\ 0\ 0 \\ 1\ 0\ 1\ 1 \\ \hline 1\ 1\ 0\ 1\ 1\ 1 \end{array}$$ adding.

Answer: $(110111)_{two}$.

Problem: ② Evaluate $(1024)_{eight} \times (2776)_{eight}$.

Soln.

$$
\begin{array}{r}
1024 \\
(\times)\ 2776 \\
\hline
\textcircled{1} \\
\textcircled{1}\ 6170 \\
\textcircled{1}\ 7\ 2\ 8\ 4 \\
(+)\ \textcircled{1}\ 7\ 2\ 1\ 4 \\
2\ 0\ 5\ 0 \\
\hline
3\ 0\ 7\ 1\ 7\ 3\ 0
\end{array}
\quad \text{adding}
$$

Answer : $(3071730)_{eight}$.

Homework

① Evaluate $(1076)_{eight} + (2076)_{eight}$.

② $(3076)_{sixteen} + (5776)_{sixteen}$.

③ $(11000)_{two} - (100)_{two}$

④ $(A89B)_{twele} - (65A6)_{twele}$.

⑤ $(CBA)_{Sixteen} \times (ABC)_{sixteen}$.

Greatest common Divisor [G.C.d]

Let a and b be integers not both zero.

A positive integer 'd' is called the g.c.d of a and b if it satisfies the following.

(i) d/a and d/b.

(ii) Suppose another m/a and m/b then m/d.

Here d = g.c.d of a and b.

Denoted by $d = (a, b)$.

Examples

① G.C.d of $(12, 18) = 6$.

or $(12, 8) = 6$.

② $(11, 19) = 1$.

③ $(-15, 25) = 5$.

④ $(3, 0) = 3$.

Defn [Relatively prime]

Two positive integers a and b are relatively prime if their g.c.d is 1.

Examples

① 6 and 35 are relatively prime. $(\because (6, 35) = 1)$

② 11 and 24 are relatively prime $(\because (11, 24) = 1$

③ 2 and 18 are not relatively prime $(\because (2, 18) = 2)$

Theorem 8: Let $(a,b) = d$. Then

(i) $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

(ii) $(a, a-b) = d$.

Proof

Let $(a,b) = d$.

(i) Let $\left(\frac{a}{d}, \frac{b}{d}\right) = d'$.

To prove $d' = 1$.

Since d' is g.c.d of $\left\{\frac{a}{d} \text{ & } \frac{b}{d}\right.$, $\frac{a}{d} = \ell d'$ and $\frac{b}{d} = md'$

for some integers ℓ and m.

$\Rightarrow a = \ell d d'$ and $b = m d d'$.

$\Rightarrow dd'$ is common divisor of a and b.

But $d = (a,b)$.

$\therefore$ dd' must divide d.

$\Rightarrow d' = 1$.

(ii) Let $d' = (a, a-b)$.

It is enough to prove $d' = d$.

First we prove $d \leq d'$.

Since d is a common divisor of a and b,

$a = md$ and $b = nd$ for some integers m & n.

$a - b = (m-n)d$.

$\Rightarrow d \,/_{(a-b)}$.

$\therefore$ d is a common divisor of a and $(a-b)$.

But d' is a g.c.d of a and $(a-b)$

$\Rightarrow d \leq d' \longrightarrow (1)$

Now we prove $d' \leq d$.

Since d' is a common divisor of a and $a-b$,

$a = \alpha d'$ and $(a-b) = \beta d'$ for some integers α and β.

$\Rightarrow a - (a-b) = (\alpha d' - \beta d')$

$b = (\alpha - \beta) d'$.

$\Rightarrow d'$ is a common divisor of a and b.

But d = g.c.d of a and b.

$\Rightarrow d' \leq d$ ⟶ (2)

From (1) and (2), $d = d'$.

Hence the proof.

Theorem: 9 **Euler Theorem**

The g.c.d of the positive integers a and b is a linear combination of a and b.

Proof:

Let $S = \{ma + nb \,/\, ma+nb > 0, m \text{ and } n \in Z\}$

Consider $a = 1.a + 0.b \in S$.

$\Rightarrow S$ is non-empty.

$\therefore S$ has a least +ve element say d.

$\Rightarrow d = \alpha a + \beta b$, $\alpha, \beta \in Z$

Claim: $d = (a,b)$

(i) First we will prove d/a and d/b.

By division algorithm, $\exists$ integers q and r such that $a = dq + r$ where $0 \leq r < d$.

$\Rightarrow r = a - dq$.

$= a - (\alpha a + \beta b) q$

$= a - \alpha a q - \beta b q$

$r = a(1 - \alpha q) + b(-\beta q)$

$\Rightarrow r \in S.$

Also $r < d.$

Which is a $\Rightarrow\Leftarrow$ to d is the smallest element in S.

$\therefore r = 0.$

$\therefore d/a.$

Similarly, $d/b.$

(ii) Suppose another +ve common devisor say m.

i) m/a and m/b.

It is enough to prove $m \leq d$.

m/a and $m/b \Rightarrow m/(\alpha a + \beta b)$ [using Thm: 7]

$\Rightarrow m/d.$

$\Rightarrow m \leq d.$

$\therefore d$ is the g.c.d of a and b.

Hence the proof.

Theorem: 10 Two positive integers a and b are relatively prime if and only if there are integers α and β such that $\alpha a + \beta b = 1$.

Proof: Assume that a and b are relatively prime

$\Rightarrow$ gcd of a and $b = 1$.

$\Rightarrow 1 = \alpha a + \beta b$ for some integers α and β.

[using Euler thm].

Conversely, assume that $\alpha a + \beta b = 1$.

claim: a and b are relatively prime.

Let $d = (a, b)$.

It is enough to prove $d = 1$

Since $d = (a, b)$, d/a and d/b.

$\Rightarrow d/_{\alpha a + \beta b}$, $\alpha, \beta \in Z$.

$\Rightarrow d/_1$.

$\therefore \boxed{d = 1}$

Hence the proof.

Corollary ①: If $(a, b) = 1 = (a, c)$ then $(a, bc) = 1$.

Proof:

If $(a, b) = 1$ and $(a, c) = 1$.

Then by thm: 10, a and b are relatively prime

and a and c are relatively prime

$\Rightarrow$ a and bc are relatively prime.

By thm 10, $(a, bc) = 1$.

Corollary ②: If a/c and b/c and $(a, b) = 1$ then ab/c.

Proof

$a/c \Rightarrow c = ma$, $m \in Z \longrightarrow ①$

$b/c \Rightarrow c = nb$, $n \in Z \longrightarrow ②$

Since $(a, b) = 1$, $1 = \alpha a + \beta b$. , $\alpha, \beta \in Z$

Multiply both sides by c

$c = \alpha ac + \beta bc$.

$c = \alpha a(nb) + \beta b(ma)$ (using ①, ②)

$c = ab(\alpha n + \beta m)$

$\Rightarrow ab/c$.

Theorem (11) : Euclid's Theorem

If a and b are relatively prime and if $a \mid bc$ then $a \mid c$.

Proof:

Since a and b are relatively prime, $(a,b)=1$.

$\therefore \quad 1 = \alpha a + \beta b$ where $\alpha, \beta \in Z$.

$\Rightarrow \quad c = \alpha ac + \beta bc. \longrightarrow (1)$

If $a \mid bc$ then $a \mid \beta bc$.

Clearly $a \mid \alpha ac$

$\therefore \quad a \mid \alpha ac + \beta bc$

$\Rightarrow a \mid c$ (using (1))

Hence the proof.

Theorem (12): Let a and b be any positive integers, and r the remainder, when a is divided by b. Then $(a,b) = (b,r)$.

Proof: Let a and b be any +ve integers.

Let 'r' be the remainder when a is divided by b.

Claim: $(a,b) = (b,r)$.

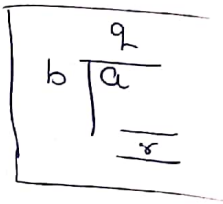
Take $(a,b) = d$ and

$(b,r) = d'$.

It is enough to prove $d = d'$.

We will prove this by $d \mid d'$ and $d' \mid d$.

Using division algorithm $\exists$ unique quotient q such that $a = bq + r$



To prove d/d'

Since $d = (a, b)$, d/a and d/b.

$\Rightarrow d/a$ and d/bq

$\Rightarrow d/(a - bq)$

$\Rightarrow d/r$.

We have d/b and d/r.

But d' is the gcd of b and r.

$\Rightarrow d/d'$.

To prove d'/d

Since $d' = (b, r)$, d'/b and d'/r

$\Rightarrow d'/bq$ and d'/r.

$\Rightarrow d'/bq + r$

$\Rightarrow d'/a$.

$\therefore$ we have d'/a and d'/b.

But $d = (a, b)$.

$\therefore d'/d$.

$\therefore d' = d$.

Hence the proof.

The Euclidean Algorithm

Aim: (i) To find gcd of given two +ve integers a and b.

(ii) To write gcd as linear combination of a and b.

Let a and b be any two +ve integers.

If $a = b$, $(a, b) = a$.

If $a > b$, apply division algorithm for a and b.

$$a = bq_0 + r_0 \quad \text{where} \quad 0 \leq r_0 < b.$$

Suppose $r_0 = 0$ then b = g.c.d of a and b.

Otherwise apply division algorithm for b and r_0.

$$b = r_0 q_1 + r_1 \quad \text{where} \quad 0 \leq r_1 \leq r_0.$$

Suppose $r_1 = 0$, $r_0 = (a, b)$.

Otherwise apply division algorithm for r_0 and r_1.

$$r_0 = r_1 q_2 + r_2$$

⋮

Proceed in this manner.

At some stage remainder must be zero.

The last non zero remainder = (a, b).

Problem ① Using euclidean algorithm find gcd of 4076, 1024 and write gcd as linear combination of 4076 & 1024.

Soln

Given 4076, 1024.

Divide 4076 by 1024, $4076 = 3(1024) + 1004$, $0 < 1004 < 1024$

Divide 1024 by 1004 $1024 = 1(1004) + 20$, $0 < 20 < 1004$.

Divide 1004 by 20 $1004 = 50(20) + 4$, $0 < 4 < 20$

Divide 20 by 4 $20 = 5(4) + 0$.

Stop the process.

The last non zero remainder = 4.

∴ gcd (4076, 1024) = 4.

From the above eqns,

$$4 = 1004 - 50(20)$$
$$= (1024 - 20) - 50(20)$$
$$= 1024 - 51(20).$$
$$= 1024 - 51(1024 - 1004)$$
$$= 1024 - 51(1024) + 51(1004)$$
$$= -50(1024) + 51(1004)$$
$$= -50(1024) + 51(4076 - 3(1024))$$
$$= 51(4076) - 50(1024) - 153(1024)$$

$$\boxed{4 = 51(4076) - 203(1024)}$$ is

required linear combination.

Problem ② Apply Euclidean algorithm to express the gcd of 1976 and 1776 as a linear combination of themselves.

(V.Q)

Soln: Given 1976 and 1776.

Divide 1976 by 1776 } $1976 = 1(1776) + 200$, $0 < 200 < 1776$.

Divide 1776 by 200, $1776 = 8(200) + 176$., $0 < 176 < 200$.

Divide 200 by 176, $200 = 1(176) + 24$., $0 < 24 < 176$.

Divide 176 by 24, $176 = 7(24) + 8$, $0 < 8 < 24$.

Divide 24 by 8, $24 = 3(8) + 0$.

Stop the process.

The last non zero remainder = 8

∴ Gcd of 1976 and 1776 = 8.

From the above eqns,

$$8 = 176 - 7(24)$$
$$= 176 - 7(200 - 176)$$
$$= 176 - 7(200) + 7(176)$$
$$= 8(176) - 7(200)$$
$$= 8(1776 - 8(200)) - 7(200)$$
$$= 8(1776) - 64(200) - 7(200)$$
$$= 8(1776) - 71(200)$$
$$= 8(1776) - 71(1976 - 1776)$$
$$= 8(1776) - 71(1976) + 71(1776)$$

$$\boxed{8 = 79(1776) - 71(1976)}$$ as required linear combination.

Problem ③ Using Euclidean algorithm find the gcd of 2076 and 1776 and express gcd as linear combination of themselves.

Soln Given 2076, 1776.

Divide 2076 by 1776, $2076 = 1(1776) + 300$, $0 < 300 < 1776$.

Divide 1776 by 300, $1776 = 5(300) + 276$, $0 < 276 < 300$.

Divide 300 by 276, $300 = 1(276) + 24$, $0 < 24 < 276$

Divide 276 by 24, $276 = 11(24) + 12$, $0 < 12 < 24$.

Divide 24 by 12, $24 = 2(12) + 0$.

Stop the process.

The last non zero remainder = 12.

∴ Gcd of 2076 and 1776 = 12.

$$12 = 276 - 11(24)$$

$$= 276 - 11[300 - 276]$$

$$= 276 - 11(300) + 11(276)$$

$$= 12(276) - 11(300)$$

$$= 12(1776 - 5(300)) - 11(300)$$

$$= 12(1776) - 60(300) - 11(300)$$

$$= 12(1776) - 71(300)$$

$$= 12(1776) - 71(2076 - 1776)$$

$$= 12(1776) - 71(2076) + 71(1776)$$

$$\boxed{12 = 83(1776) - 71(2076)}$$ is required linear combination.

Theorem (13): Euclid's Lemma

If p is a prime and $p \mid ab$ then $p \mid a$ or $p \mid b$.

Proof:-

Let p be a prime with $p \mid ab$.

Suppose $p \nmid a$

Then $(a, p) = 1$.

$\Rightarrow$ a and p are relatively prime

$\therefore$ $\exists$ integers α and β such that $1 = \alpha a + \beta p$.

Multiply both sides by b, $b = \alpha ab + \beta pb \longrightarrow (1)$

Now $p \mid ab \Rightarrow p \mid \alpha ab$.

Clearly $p \mid \beta pb$.

$\Rightarrow p \mid \alpha ab + \beta pb$.

$\Rightarrow p \mid b$ ($\because$ By (1), $b = \alpha ab + \beta pb$).

Hence the proof.

Theorem (14): Let p be a prime and $p \mid a_1 a_2 \ldots a_n$ where $a_1, a_2, \ldots, a_n$ are positive integers, then $p \mid a_i$ for some i, where $1 \le i \le n$.

Proof:- We prove this theorem by induction on 'n'.

When $n = 1$, $p \mid a_1 \Rightarrow p \mid a_1$. The result is true.

When $n = 2$, $p \mid a_1 a_2 \Rightarrow p \mid a_1$ or $p \mid a_2$. The result is true.

Induction hypothesis: Assume that the result is true for k.

i) $p \mid a_1 a_2 \ldots a_k \Rightarrow p \mid a_i$; $1 \le i \le k$.

To prove the result for $(k+1)$

Suppose $p \mid a_1 a_2 \ldots a_k a_{k+1}$

$\Rightarrow p \mid (a_1 a_2 \ldots a_k) \cdot a_{k+1}$

Take $A = a_1 a_2 \ldots a_k$ and

$B = a_{k+1}$.

$\Rightarrow p \mid AB$

$\therefore$ By Euclid's lemma, $p \mid A$ (or) $p \mid B$.

i) $p \mid a_1 a_2 \ldots a_k$ or $p \mid a_{k+1}$ $\longrightarrow$ ①

By induction hypothesis,

$p \mid a_1 a_2 \ldots a_k \Rightarrow p \mid a_i$; $1 \le i \le k$.

$\therefore$ From ①, $p \mid a_i$ (or) $p \mid a_{k+1}$; $1 \le i \le k$.

$\Rightarrow p \mid a_i$; $1 \le i \le k+1$.

$\therefore$ The result is true for $(k+1)$.

$\therefore$ By Induction method, the result is true for any +ve integer n.

Theorem (15): If $p, q_1, q_2, \ldots, q_n$ are primes such that

$p \mid q_1 \cdot q_2 \cdots q_n$ then $p = q_i$ for some i, $1 \le i \le n$.

Proof

If $p, q_1, q_2, \ldots, q_n$ are primes such that

$p \mid q_1 \cdot q_2 \cdots q_n$

Then $p \mid q_i$ for some i, $1 \le i \le n$ (using thm (14))

Since p and q_i's are primes $p \mid q_i \Rightarrow p = q_i$.

Hence the proof.

Theorem (16): Fundamental Theorem of Arithmetic

Every integer $n \geq 2$ is either a prime or can be expressed as a product of primes. The factorization into primes is unique except for the order of the factors.

Proof:

If n is prime then there is nothing to prove.

Suppose n is composite.

Then n has a divisor say d.

$\Rightarrow d \mid n$ where $1 < d < n$.

Among all such divisors of n, let p_1 be the smallest.

Claim: p_1 is prime.

Suppose not.

$\exists$ an integer d_1 such that $d_1 \mid p_1$, $1 < d_1 < p_1$.

Since d_1/p_1 and p_1/n, d_1/n.

Which is a $\Rightarrow\Leftarrow$ to p_1 is smallest.

$\therefore$ p_1 is prime.

If $n = p_1 \times n_1$ where p_1 is prime,

Suppose n_1 is prime then the proof is over.

Suppose n_1 is not a prime $\exists$ a prime p_2 such that

$$n_1 = p_2 n_2 \,, \quad 1 < n_2 < n,$$

$$\therefore n = p_1 p_2 n_2 \quad \text{where} \quad 1 < n_2 < n_1 < n.$$

If n_2 is prime then the proof is over.

Suppose n_2 is not a prime, $\exists$ a prime p_3 such that $n_2 = p_3 n_3 \,; \quad 1 < n_3 < n_2.$

$$\therefore n = p_1 p_2 p_3 n_3 \,, \quad 1 < n_3 < n_2 < n_1 < n.$$

The decreasing sequence $n > n_1 > n_2 > n_3 > \dots > 1$ cannot continue infinitely

After a few steps, n_k is prime say p_k.

$$\therefore n = p_1 p_2 \dots p_k.$$

Uniqueness:

Suppose there are two expressions

$$n = p_1 p_2 \dots p_k \,, \quad p_1 \le p_2 \le \dots \le p_k$$

and

$$n = q_1 q_2 \dots q_s \,, \quad q_1 \le q_2 \le \dots \le q_s.$$

Assume $k \leq s$.

$p_1 p_2 \ldots p_k = q_1 q_2 \ldots q_s$. $\longrightarrow$ ①

We know that $p_1 \mid p_1 p_2 \ldots p_k$.

$\Rightarrow p_1 \mid q_1 q_2 \ldots q_s$ (using ①)

$\Rightarrow p_1 = q_i$, $1 \leq i \leq s$.

∵ From ①, $p_1 p_2 \ldots p_k = q_1 q_2 \ldots q_{i-1}\, p_1\, q_{i+1} \ldots q_s$

Cancel p_1 both sides.

$p_2 \ldots p_k = q_1 q_2 \ldots q_{i-1}\, q_{i+1} \ldots q_s$. $\longrightarrow$ ②

Since $p_2 \mid p_2 \ldots p_k = q_1 q_2 \ldots q_{i-1} q_{i+1} \ldots q_s$, $p_2 = q_j$ for some j.

Cancell p_2 both sides on ②.

$p_3 \ldots p_k = q_1 q_2 \ldots q_{i-1} q_{i+1} \ldots q_{j-1} q_{j+1} \ldots q_s$.

Since $k \leq s$, continuing in this manner, we get

1 = product of q_i's.

But q_i's are primes.

∵ Product of q_i's $\neq 1$.

We get a $\Rightarrow\Leftarrow$.

$\{p_1, p_2, \ldots p_k\} = \{q_1, q_2, \ldots q_s\}$.

Also $k = s$.

H/p.

Canonical Decomposition

The canonical decomposition of a positive integer n is of the form $n = p_1^{a_1} \times p_2^{a_2} \times \dots \times p_k^{a_k}$ where $p_1, p_2, \dots p_k$ are distinct primes with $p_1 < p_2 < \dots < p_k$

Here $a_1, a_2 \dots, a_k$ are +ve integers.

Example

Find the canonical decomposition of 2520.

Soln

2	2520
2	1260
2	630
3	315
3	105
5	35
	7.

$\therefore 2520 = (2 \times 2 \times 2) \times (3 \times 3) \times (5) \times (7)$

$= 2^3 \times 3^2 \times 5^1 \times 7^1$ is required canonical decomposition.

Problem Using the canonical decompositions of 168 and 180, find their gcd.

Soln Given 168 and 180.

2	168
2	84
2	42
3	21
	7

∴ Canonical decomposition of $168 = (2 \times 2 \times 2) \times 3 \times 7$

$= 2^3 \times 3 \times 7.$

2	180
2	90
3	45
3	15
	5

∴ Canonical decomposition of $180 = (2 \times 2) \times (3 \times 3) \times 5.$

$= 2^2 \times 3^2 \times 5.$

$168 = 2^3 \times 3 \times 7.$

$180 = 2^2 \times 3^2 \times 5.$

Gcd can be taken by common primes with lowest power.

Gcd of $168, 180 = 2^2 \times 3$

$= 12.$

Defn [Least Common Multiple]

A least common multiple (lcm) of two non zero integers a and b denoted by $\text{lcm}(a,b)$ is the least +ve integer m satisfying the following

(i) a/m and b/m

(ii) Suppose a/c and b/c with $c>0$ then $m \leq c$.

Example

① $\text{lcm}(3,6) = 6$

② $\text{lcm}(25,30) = 150$.

Theorem (17) U.Q

For the +ve integers a and b,

$$\gcd(a,b) \times \text{lcm}(a,b) = ab.$$

Proof:

Let $\gcd(a,b) = d$.

Consider $\frac{ab}{d} = m$

Claim: $\text{lcm}(a,b) = \frac{ab}{d} = m$.

$$m = \frac{ab}{d} = \frac{b}{d}(a) \longrightarrow ①$$

Since d/b, $\frac{b}{d}$ is an integer.

$\therefore$ From ①, a/m.

Also $m = \frac{ab}{d} = \frac{a}{d}(b) \Rightarrow b/m$.

$\therefore$ a/m and b/m.

Suppose a/c and b/c with $c>0$.

$a/c \Rightarrow c = ar$

$b/c \Rightarrow c = bs$ where $r, s \in Z^+$

$$\frac{c}{m} = \frac{c}{(ab/d)} = \frac{cd}{ab}.$$

$$\frac{c}{m} = \frac{c \times d}{ab.} \longrightarrow (2)$$

Since $d = gcd(a,b)$, $d = ax + by$ where $x, y \in Z$

From (2), $\frac{c}{m} = \frac{c(ax+by)}{ab} = \frac{cax+cby}{ab}$

$$= \frac{bs(ax) + ar(by)}{ab} \quad (\because c = ar,\ c = bs)$$

$$\frac{c}{m} = ab\left(\frac{sx + ry}{ab}\right)$$

$$\frac{c}{m} = sx + ry.$$

$\Rightarrow m \leq c.$

$\therefore$ $lcm(a,b) = m = \frac{ab}{d}$

$\Rightarrow lcm(a,b) = \frac{ab}{gcd(a,b)}$

$\Rightarrow lcm(a,b) \times gcd(a,b) = ab.$

Hence the proof.

Theorem (18): Given +ve integers a and b, $lcm(a,b) = ab$ if and only if $gcd(a,b) = 1$.

Proof:-

W.K.T $lcm(a,b) \times gcd(a,b) = ab$. ⟶ ①

Assume that $lcm(a,b) = ab$.

Claim: $gcd(a,b) = 1$.

From ① $$gcd(a,b) = \frac{ab}{lcm(a,b)}$$

$$= \frac{ab}{ab}$$

$$= 1.$$

Conversely, assume that $gcd(a,b) = 1$.

Claim: $lcm(a,b) = ab$.

From ①, $$lcm(a,b) = \frac{ab}{gcd(a,b)}$$

$$= \frac{ab}{1}$$

$$= ab.$$

Hence the proof.

Problem: Find the lcm(3054, 12378).

Soln:

$$\boxed{lcm(a,b) \times gcd(a,b) = ab.}$$

$a = 3054$, $b = 12378$.

We will find gcd(a,b) using Euclidean algorithm.

Divide 12378 by 3054, $12378 = 4(3054) + 162$, $0 < 162 < 3054$

Divide 3054 by 162, $3054 = 18(162) + 138$, $0 < 138 < 162$.

Divide 162 by 138, $162 = 1(138) + 24$, $0 < 24 < 138$.

Divide 138 by 24, $138 = 5(24) + 18$, $0 < 18 < 24$.

Divide 24 by 18, $24 = 1(18) + 6$, $0 < 6 < 18$.

Divide 18 by 6, $18 = 3(6) + 0$.

Stop the process.

$$\text{Gcd}(3054, 12378) = \text{last non zero remainder}$$

$$= 6.$$

$$\therefore \quad \text{lcm}(3054, 12378) \times 6 = 3054 \times 12378.$$

$$\text{lcm}(3054, 12378) = \frac{3054 \times 12378}{6}$$

$$= 63000402.$$

Homeworks

(I) Express the gcd of the following as a linear combination of themselves.

(i) 3076, 1976

(ii) 2076, 1076

(iii) 1024, 1000.

(II) Find the cannonical decomposition of following

(i) 1947 (ii) 1863 (iii) 1661.

(III) Find the lcm of the following

(i) 48, 162

(ii) 175, 192

(iii) 294, 450.