Number Theory

(i) Divisibility of integers :-

let 'a' and 'b' are two integers where $a \neq 0$.

We can say a divides b (a/b) if there exists an integer c such that,

$b = ac$ ...(i)

b is multiple of 'a', dividend ; a → divisor ; a is factor of b.

$\forall a \forall b \exists c [b = ac]$

Theorem 1:

using proof

(a) If a/b and a/c then $a/(b+c)$

(b) if a/b then a/bc

(c) if a/b and b/c then a/c.

(*) If a/b and b/a then $a = b$ or $a = -b$ where a and b are integers.

Solution

let a/b is true → a divides b.

$b/a = c$; where c is integer

$b = ac$ ...(i)

let b/a is true, → b divides a

$a/b = k$; where k is integer ...(ii)

From (i) and (ii)

$a = ack$

$ck = 1$.

Theorem 2: The Division Algorithm:

Let 'a' be an integer and 'd' be a positive integer ~~and b~~ then there are unique integers 'q' and 'r' ($0 \le r < d$) such that.

$$a = dq + r$$

Here, d = divisor

a = dividend.

q = quotient

r = remainder.

* Find quotient and remainder when 101 is divided by 11.

Solution

$d = 11$

$a = 101 / 11 = 9$

$r = 101 \% 11 = 2$

$$101 = 11 \times 9 + 2$$

(*) Quotient and remainder when -11 is divisible by 3?

$a = -11$

$b = 3$

$q = -11/3 = -4$

$r = -11/3 = +1$

$-11 = -4 * 3 + 1$.

$$\begin{array}{r|l} & -4 \\ 3 & -11 \\ \hline & -12 \\ \hline & +1 \end{array}$$

222·
8, 11, 12, (28), 34, (40) (28)

* congruent modulo

let a and b are two integers then the integers a and b are said to be congruent modulo to integer m ($a \equiv b \pmod{m}$) if and only if they have same remainder when divided by m.

i.e a mod m = b mod m.

if a and b are integers then a is congruent modulo to (a ≡ b mod m) mod m if and only if m divides (a−b)

* Is 17 congruent modulo to 5 modulo 6

Solution

$17 \equiv 5 \pmod{6}$

a b m

$a - b = 17 - 5$

$\Rightarrow 12$.

~~now (a-b) is~~

~~12/6 = 2~~

now '6' divides '12'

$12/6 \Rightarrow 2$.

(5) Is 18 congruent modulo to 14 modulo 5

Solution

$18 \equiv 14 \pmod{5}$

$a - b = 18 - 14$

$= 4$

now: 5 ✗ 4

Theorem 3: let 'm' be a positive integer then the integers a and b are congruent modulo to m if and only if there is an integer k such that $\boxed{a = b + km}$

(*) let 'm' be a positive integer if $a \equiv b \pmod m$ and $c \equiv d \pmod m$ then $(a+c) \equiv (b+d) \pmod m$ and $ac \equiv bd \pmod m$.

Solution

Since $a \equiv b \pmod m$, then,

$a = b + km$ - (i)

$c \equiv d \pmod m$

$c = d + lm$ - (ii)

$a + c \equiv (b+d) \bmod m$

(a) (b)

Then, $(a+c) - (b+d)$ is divisible by 'm':

Substituting the value of a and b.

$(b + km) + d + lm = -b - d$

$= km + lm$

$= (k+l)m$ which is divisible by 'm'

$\therefore (a+c) \equiv (b+d) \bmod m$.

b) $ac \equiv bd \pmod m$

$ac - bd =$

$(b + km)(d + lm) - bd$

~~bd~~ $+ blm + dkm + klm^2 - bd$

$(bl + dk + klm) \cdot m$

$ac = bd \pmod m$

prime number

A positive integer p is greater than 1 is called prime if it has only two factors p and 1. else it is called compositive number.

Theorem 1:- Every integer greater than 1 can be represented as a prime or as product of two or more prime numbers where the prime factors are written in order a non decreasing sides.

prime factorization

a) 100 = 2*2*5*5
= $2^2 * 5^2$

b) 1024 = 2^{10}

c) 999 = 3*3*3*37
= $3^3 * 37$

Theorem 2: If n is a composite integer then 'n' has a prime divisor less than or equal to $\sqrt{n}$.

ex $\sqrt{25} \rightarrow 5$ prime number

Solution

let n = composite integer

Then, $\frac{n}{a} = b$; when, $1 < a < n$

$n = ab$ - (1) $1 < b < n$.

let suppose,

$a > \sqrt{n}$ and $b > \sqrt{n}$

$a \cdot b > \sqrt{n} \cdot \sqrt{n}$

$a \cdot b > n$ .. (ii).

since,

$n = ab$,

eqn(ii) is a contradiction.

Therefore, either

$a \leq \sqrt{n}$ or $b \leq \sqrt{n}$

Since 'a' and 'b' are both divisor of 'n' we see that 'n' has a positive divisor not exceeding $\sqrt{n}$.

This divisor is either prime or by fundamental theorem of arithmetic (Theorem 1 has a prime divisor less than itself).

(*) Show that 101 is prime number.

Solution

$\sqrt{n} = \sqrt{101} \approx 10.04$

$\approx 10.$

prime number less than or equal to 10

2, 3, 5, 7.

Since 101 doesnot have any prime factor less than or equal to $\sqrt{101}$. It is not compositie number ie 101 is prime number.

6, 27, 30, 54, 28, 26.

GCD (Greatest Common Divisor) / HCF:
let a and b be the two integers then the greatest integer that divides both a and b is known as greatest common division or highest common factor

GCD (a, b) = d

(Q) Find GCD of 12 and 36 using prime factorization
solution

$12 = 2 \cdot 3 \cdot 2 = 2^2 \cdot 3$

$36 = 2 \cdot 2 \cdot 3 \cdot 3 = 2^2 \cdot 3^2$.

$GCD(12, 36) = 2^{\min(2,2)} \cdot 3^{\min(1,2)}$

$= 2^2 \cdot 3^1$

$= 12$.

(Q) Find GCD of 24 and 36 using prime factorization
Solution

Here

$24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3$

$36 = 2 \cdot 2 \cdot 3 \cdot 3 = 2^2 \cdot 3^2$

$GCD(24, 36) = 2^{\min(3,2)} \cdot 3^{\min(1,2)}$

$= 2^2 \cdot 3^1$

$= 12$.

(Q) Find GCD of 120 and 500 using prime factorization ?

Solution

Here,

$120 = 2^3 \cdot 3 \cdot 5$

$500 = 2^2 \cdot 3^0 \cdot 5^3$

$GCD(120, 500) = 2^2 \cdot 3^0 \cdot 5^1$

$= 10$

* Relative prime ⇒
Two integers a and b are said to be relatively prime if their GCD is equals to 1. GCD(17, 22) = 1

* Pairwise Relative prime ⇒
The integers $a_1, a_2, a_3, \ldots a_n$ are known as pairwise relative prime

$$GCD(a_i, a_j) = 1$$
$$1 \le i \le j \le n$$

a 10, 17, 21
GCD(10, 17) = 1
GCD(17, 21) = 1
GCD(10, 21) = 1.

Euclidean Algorithm.
1) Given two integers 'a' and 'b' where ($a \ge b$).
compute $r = a \% b$
2) If $r == 0$ then, GCD(a, b) = b
3) If $r != 0$, then Set
$a = b$
$b = r$
4) Repeat Step 1 and 2.

Ex: 414, 662

a = 414

b = 662.

a	b	r = a % b
662	414	248
414	248	166
248	166	82
166	82	2
82	2	0

GCD (a,b) = GCD (662, 414)

= 2

(Q) 252, 198

a = 252

b = 198

a	b	r = a % b
252	198	

Bezout's Theorem: (linear combinations)

If a and b are two integers then the GCD of a and b can be written as GCD(a,b): d = sa + tb;

where s and t are integers also known as Bezout's coefficient.

Extended Euclidean Algorithm.

Step 1:- Initialize two pairs of number

$(r_0, s_0, t_0) = (a, 1, 0)$

$(r_1, s_1, t_1) = (b, 0, 1)$

Step 2: compute

$r_2 = r_0 \% r_1$

$q = r_0 / r_1$

Step-3:

compute new pair

$r_2 = r_0 \% r_1$

$s_2 = s_0 - q * s_1$

$t_2 = t_0 - q * t_1$

step 4:- set

$(r_0, s_0, t_0) = (r_1, s_1, t_2)$

$(r_1, s_1, t_2) = (r_2, s_2, t_2)$

Step 5:- Repeat step 2, 3 and 4 until $r_2 = 0$

Step 6:- The GCD of a and b is r_1 and

$s = s_1$

$t = t_1$

Q Find the GCD of 56 and 15 also express it as a linear combination of 56 and 15

$q = r_0/r_1$	r_0	s_0	t_0	r_1	s_1	t_1	$r_2 = r_0 - q*r_1$	$s_2 = s_0 - q*s_1$	$t_2 = t_0 - q*t_1$
$q = 56/15 = 3$	56	1	0	15	0	1	$56 - 3*15 = 11$	$1 - 3*0 = 1$	$0 - 3*1 = -3$
$q = 15/11 = 1$	15	0	1	11	1	-3	4	-1	4
$q = 11/4 = 2$	11	1	-3	4	-1	4	3	3	-11
	4	-1	4	3	3	-11	1	-4	15
	3	3	-11	1	-4	15	0		

GCD(56, 15) = 1

$s = s_1 = -4$

$t = t_1 = 15$

$1 = sa + tb$

$1 = -4(56) + 15(15)$

GCD(56, 15) = 1 = $sa + tb$

$s = s_1 = -4 = (-4)56 + 15(15)$

$t = t_1 = 15$

Q GCD(252, 198) =