Prime numbers

Defn: A positive integer $p>1$ is called prime if the only (+)ve factors of p are 1 and p. If a positive integer $n>1$ is not prime, then n is called Composite.

Note: (i) The (+)ve integer 1 is neither prime nor composite.

(ii) The only even prime integer is 2, rest all other primes are odd integers.

Ex: The integers 2, 3, 5, 7 etc are prime, where as 4, 6, 9, 10 etc are composite since $4=2\times 2$, $6=3\times 2$, $9=3\times 3$ & $10=5\times 2$.

Th-(2) Euclid's theorem

The number of prime numbers is infinite.

Division algorithm

Given any two integers a & b, with $b>0$, there exist unique integers q and r such that $a=bq+r$, $0\leq r<b$.

Note: In $a=bq+r$, q is called the quotient and r is called the remainder in the division of a by b. $(b\neq 0)$

Common divisor

Defn: If a & b are integers then an integer d is said to be a common divisor of a & b if $d|a$ & $d|b$.

Note: 1) Since 1 is a divisor of every integer, so, 1 is a common divisor of a and b. So, for an arbitrary pair of integers a and b there exists always a common divisor.

2) If both of a and b be zero then each integer is a common divisor of a and b. But if atleast one of a and b is non-zero, then there is only a finite no. of (+)ve common divisors. Of these (+)ve common divisors, there is a greatest one, which is called the greatest common divisors. and it is denoted by gcd (a,b)

Greatest Common divisors

Defn: If a and b are integers, not both zero, the greatest common divisors of a and b, denoted by $\gcd(a,b)$ is the (+)ve integer d satisfying

(i) $d|a$ & $d|b$.

(ii) If $c|a$ & $c|b$ then $c|d$

Ex: 1) Let $a=12$, $b=-18$, then the (+)ve divisors of 12 are 1, 2, 3, 4, 6, 12. & those of -18 are 1, 2, 3, 6, 9, 18. So, the (+)ve common divisors of 12 & -18 are 1, 2, 3, 6.

So $\gcd(12,-18)=6$

Note (i) $\gcd(a,b)\geq 1$

(ii) If $\gcd(a,b)=1$, then a & b are said to be relatively prime or coprime

(iii) If $\gcd(a_1,a_2,\dots a_n)=1$, then the integers $a_1,a_2,\dots a_n$ are said to be pairwise relatively prime.

(iv) $\gcd(a,-b)=\gcd(-a,b)=\gcd(-a,-b)=\gcd(a,b)$, where a and b are integers not both zero.

Ex 2) The divisors of 8 are $\pm1,\pm2,\pm4,\pm8$ and the divisors of 36 are $\pm1,\pm2,\pm3,\pm4,\pm6,\pm9,\pm12,\pm18,\pm36$.

So the Common divisors of 8 & 36 are $\pm1,\pm2,\pm4$.

Hence the $\gcd(8,36)=4$

3) The divisors of 15 are $\pm1,\pm3,\pm5,\pm15$ & the divisors of 44 are $\pm1,\pm2,\pm4,\pm11,\pm22,\pm44$.

So, $\gcd(15,44)=1$

So, 15 & 44 are relatively prime

4) Consider the integers 8, 17, 35. Since $\gcd(8,17)=1$, $\gcd(8,35)=1$ & $\gcd(17,35)=1$.

So the integers 8, 17, 35 are pairwise relatively prime.

Th-3 If a and b are integers, not both zero, then there exist integers u & v s.t $\gcd(a,b) = au+bv$

Th-4 If $c|ab$ and b, c are coprime, then prove that $c|a$.

Proof Since b, c are co-prime $\therefore \gcd(b,c)=1$

So there exist two integers m & n s.t

$mb+nc = \gcd(b,c)$

or $mb+nc=1$ $(\because \gcd(b,c)=1)$

or $a(mb+nc)=a$

or $mab+nac=a$ —— (1)

Now, $c|ab$ $\therefore c|mab$

Also, $c|nac$ $\therefore c|(mab+nac)$

i.e $c|a$ [by (1)]

Th-5 If a and b are coprime and a and c are coprime, then a and bc are coprime.

Proof Since a, b are coprime so, $\gcd(a,b)=1$

So, there exists two integers m & n such that

$ma+nb=1$ —— (1)

Also, since a and c are coprime so $\gcd(a,c)=1$

So there exist two integers x & y such that

$xa+yc=1$ —— (2)

From (1) & (2), we get $(ma+nb)(xa+yc)=1$

or $ma^2x+nabx+acmy+bcny=1$

or $(mxa+myc+nbx)a+(ny)bc=1$

or $pa+qbc=1$ (say) where

$p = mxa+myc+nbx$ & $q=ny$ are both integers.

Hence $\gcd(a,bc)=1$

So, a & bc are coprime.

687

Thm (6) For any (+)ve integer m, then
$\gcd(ma, mb) = m \gcd(a,b)$

Thm (7) If $d|a$ & $d|b$ & $d>0$, then
$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}\gcd(a,b)$

Note: If $\gcd(a,b) = d$, then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

Thm (8) If $\gcd(a,b) = 1$, then for any integer n,
$\gcd(an, b) = \gcd(n, b)$, holds

Thm (9) If $a|c$ & $b|c$ with $\gcd(a,b) = 1$, then
$ab|c$.

Ex-① If $\gcd(a,b)=1$, then prove that
(i) $\gcd(a+b, a-b) = 1$ or 2
(ii) $\gcd(2a+b, a+2b) = 1$ or 3.

Sol (i) Let $\gcd(a+b, a-b) = d$

$\therefore d \mid (a+b)$ & $d \mid (a-b)$

$\therefore d \mid \{(a+b)+(a-b)\}$ & $d \mid \{(a+b)-(a-b)\}$

$\therefore d \mid 2a$ & $d \mid 2b$

So, d is a common divisor of 2a & 2b —(1)

Since $\gcd(a,b)=1$ $\therefore \gcd(2a,2b)=2$ —(2)

So from (1) & (2) we have, $d \mid 2$ $\therefore d = 1$ or 2

$\therefore \gcd(a+b, a-b) = 1$ or 2

(ii) Let $\gcd(2a+b, a+2b) = d$

$\therefore d \mid (2a+b)$ & $d \mid (a+2b)$

$\therefore d \mid \{2(2a+b)-(a+2b)\}$ & $d \mid \{-(2a+b)+2(a+2b)\}$

or $d \mid 3a$ & $d \mid 3b$

So d is a common divisor of 3a & 3b —(1)

Since $\gcd(a,b)=1$ $\therefore \gcd(3a,3b)=3$ —(2)

So from (1) & (2) we have, $d \mid 3$ $\therefore d = 1$ or 3

$\therefore \gcd(2a+b, a+2b) = 1$ or 3

(2) If $\gcd(a,4) = \gcd(b,4) = 2$ then prove that $\gcd(a+b,4)=4$

Sol We have $\gcd(a,4) = \gcd(b,4) = 2$

$\therefore a = 2m$ & $b = 2n$ for some odd integers m & n.

$\therefore a+b = 2(m+n) = 2 \times 2r = 4r$ for some integer r
($\because m+n$ is even)

Now $\gcd(a+b, 4) = \gcd(4r, 4) = 4$. [Proved]

*3) If $\gcd(a,b)=1$ then prove that $\gcd(a^2,b^2)=1$ p-9

Sol Let $\gcd(a^2,b^2)=d$

If $d=1$ then $\gcd(a^2,b^2)=1$

If $d>1$ then d has a prime factor p (say)

$\therefore$ $p \mid d$ and $d=\gcd(a^2,b^2)$

$\therefore$ $p \mid d$ and $d \mid a^2$, $d \mid b^2$

$\therefore$ $p \mid a^2$ and $p \mid b^2$

$\therefore$ $p \mid a$ & $p \mid b$ since p is a prime no.

$\therefore$ $p \mid \gcd(a,b)$ $\therefore$ $p \mid 1$, which is impossible

$\therefore$ $d>1$ is not possible.

$\therefore$ $d=1$ $\therefore$ $\gcd(a^2,b^2)=1$ [Proved]

5. If $\gcd(a, bc) = 1$ then show that $g(a,b) = 1$ & $\gcd(a, c) = 1$

Sol: Since $\gcd(a, bc) = 1$, so there exist two integers u, v s.t. $au + (bc)v = \gcd(a, bc)$

$\therefore au + (bc)v = 1$ ——(1)

$\Rightarrow ua + (cv)b = 1$

$\therefore \underline{\gcd(a,b) = 1}$ (Proved) $(\because u, cv \in \mathbb{Z})$

(1) $\rightarrow$ $au + (bv)c = 1$

$\therefore \underline{\gcd(a,c) = 1}$ (Proved) $(\because u, bv \in \mathbb{Z})$

Least common multiple

Def^n: Let a & b be two (+)ve integers. Then the smallest (+)ve integer that is divisible by both a and b is called the least common multiple of a and b and it is denoted by $\text{lcm}(a,b)$. or $[a,b]$

~~Note~~: $\text{lcm}(a,b)$ is always (+)ve even if either or both a and b are negative.

Ex: $\text{lcm}(8,20) = \text{lcm}(-8,20) = \text{lcm}(8,-20) = \text{lcm}(-8,-20) = 40$.

Alternative def^n: Let the prime factorisation (decomposition) of two integers a & b be

$a = n_1^{a_1} n_2^{a_2} \cdots n_p^{a_p}$

& $b = n_1^{b_1} n_2^{b_2} \cdots n_p^{b_p}$, where each component is a non-negative integer.

$\text{lcm}(a,b) = n_1^{\max(a_1,b_1)} \cdot n_2^{\max(a_2,b_2)} \cdots n_p^{\max(a_p,b_p)}$

where $\max(a_i, b_i)$ means the maximum of two number a_i & b_i

Ex: Find $\text{lcm}(8,20)$

Sol: Here $8 = 2^3 \times 5^0$, $20 = 2^2 \times 5^1$

$\therefore \text{lcm}(8,20) = 2^{\max(3,2)} \cdot 5^{\max(0,1)} = 2^3 \cdot 5^1 = 40$.

Th If a & b are any two (+)ve integers, then $\boxed{\gcd(a,b)\cdot \text{lcm}(a,b) = ab}$

6) Using prime factorisation, find gcd & lcm of 1300, 3575. Also verify that $\gcd(a,b)\cdot \text{lcm}(a,b) = ab$

Sol We have, $1300 = 2^2\cdot 5^2\cdot 11^0\cdot 13^1$

$3575 = 2^0\cdot 5^2\cdot 11^1\cdot 13^1$

$\therefore \gcd(1300, 3575) = 2^{\min(2,0)}\cdot 5^{\min(2,2)}\cdot 11^{\min(0,1)}\cdot 13^{\min(1,1)}$

$= 2^0\cdot 5^2\cdot 11^0\cdot 13^1 = \underline{325}$

$\text{lcm}(1300, 3575) = 2^{\max(2,0)}\cdot 5^{\max(2,2)}\cdot 11^{\max(0,1)}\cdot 13^{\max(1,1)}$

$= 2^2\cdot 5^2\cdot 11^1\cdot 13^1 = \underline{14300}$

$\therefore \gcd(1300, 3575)\cdot \text{lcm}(1300, 3575)$

$= 325 \times 14300 = 4647500 = 1300 \times 3575$

Hence $\gcd(a,b)\cdot \text{lcm}(a,b) = ab$

7) Find the gcd of 252 & 595 and express it in the form $252m + 595y$

Sol By division algorithm, we have,

$595 = 2\times 252 + 91$ — (i)

$252 = 2\times 91 + 70$ — (ii)

$91 = 1\times 70 + 21$ — (iii)

$70 = 3\times 21 + 7$ — (iv)

$21 = 3\times 7 + 0$ — (v)

$$\begin{array}{r} 252)\,595\,(2 \\ 504 \\ \hline 91)\,252\,(2 \\ 182 \\ \hline 70)\,91\,(1 \\ 70 \\ \hline 21)\,70\,(3 \\ 63 \\ \hline 7)\,21\,(3 \\ 21 \\ \hline \times \end{array}$$

Since the last non-zero remainder is 7 so,

$\gcd(252, 595) = 7$

Second part : To express the gcd in the form $252x+595y$, we have from (iv)

$$7 = 70 - 3\times 21$$
$$= 70 - 3(91 - 1\times 70) \quad [\text{from (iii)}]$$
$$= 4\cdot 70 - 3\cdot 91$$
$$= 4(252 - 2\times 91) - 3\cdot 91 \quad [\text{from (ii)}]$$
$$= 4\cdot 252 - 11\cdot 91$$
$$= 4\cdot 252 - 11\cdot(595 - 2\times 252) \quad [\text{from (i)}]$$

$\therefore$ $\underline{7 = 26\times 252 - 11\times 595}$

$\therefore$ $7 = 252x + 595y$, where $\underline{x = 26}$, $\underline{y = -11}$

Linear Diophantine equations

The general form of a linear Diophantine eqn in two variables having integral coefficients is

$\underline{ax+by=c}$ — (1), where a & b are not both zero.

If there exists two integers x_0, y_0 such that $\underline{ax_0+by_0=c}$, then (x_0, y_0) is called an integral soln of (1).

Th: If a, b, c be three integers where a and b are not both zero, then the eqn $\underline{ax+by=c}$ has an integral soln if and only if $\underline{d \text{ divides } c}$, where $\underline{d = \gcd(a,b)}$.

Ex-1 Solve: $9x+6y=2$ — (1)

Comparing the eqn with $ax+by=c$, we get,

$a=9$, $b=6$, $c=2$. Now, $\gcd(9,6)=3$,

but 3 does not divide 2.

Hence the given eqn(1) has no integral soln.

(2) Solve: $\underline{3x+2y=6}$ — (2)

$\therefore$ $a=3$, $b=2$, $c=6$ $\quad\therefore$ $\gcd(3,2)=1$ and 1 divides 6

Hence the given eqn(2) has ~~a~~ integral solns.