Number theory

Even and odd number

- An integer a is said to be even number if there exists a natural number k such that a = 2k.
- An integer a is said to be odd number if there exists a natural number k such that a = 2k + 1.

Properties of even and odd number

- The sum of two even numbers is an even number.
- The sum of two odd numbers is an even number.
- The sum of an even and an odd numbers is an odd number.
- An even number ends with 0, 2, 4, 6, and 8.
- An odd number ends with 1, 3, 5, 7 and 9.
- The even number is divisible by 2 and leaves remainder 0.
- The odd number is not divisible by 2 and leaves the remainder 1.

Divisibility of integer:

An integer b is said to be divisible by an integer a $\neq 0$, if there exists an integer c such that b = a·c. It is denoted by a|b. If b is not divisible by a then we can write a†b.

Properties:

- a|o, 1|a and a|a
- a|b and b|a iff a = $\pm$ b
- If a|b and c|d then ac|bd
- If a|b and a|c then a|bx + cy for some x, yϵ
- If a|b and a|c then a|bc
- If a|b and b $\neq$ 0 then |a| $\leq$ |b|

Theorem: For a, b, c ϵ Z, a|b and a|c then a|bx + cy ∀ x, y ϵ Z

Proof: since a|b then ∃ p ϵ Z such that b = pa

and **a**|c then ∃ q ϵ Z such that c = qa

Now, bx +cy = pax + qay = a(px + qy)

Since, px + qy ϵ z, so, a|bx + cy ∀ x, y ϵZ. Proved

Theorem: a, b ϵ Z if a|b and b $\neq$ 0 then |a| ≤ |b|

Proof: Given that a|b then for some x ϵ Z, b = ax and since b $\neq$ 0, we have x $\neq$ 0, hence |x| ≥ 1

Now, b = ax ⇒ |b| = |ax| ⇒ |b| = |a||x| ……….. (i)

Again, |a| ≤ |a||x| because |x| ≥ 1 …….. (ii)

From (i) and (ii), we get

|a| ≤ |b| Proved

Division algorithm: Given integers a and b with b $>$ 0, there exists unique q and r satisfying a = qb + r, 0 ≤ r $<$ b. The integers q and r respectively called quotient and reminder in the division of a by b.

Proof: Let a and b are any two integers such that b $\neq$ 0, let us consider the set of integers are { ……. -3b, -2b, -b, 0, b, 2b, 3b, ……. }.

By Archimedean property, bq ≤ a≤ b(q +1) …….. (i)

Subtract bq on both sides of (i), we get

0 ≤ a –bq ≤ b

⇒ 0 ≤ r≤ b where r = a –bq ⇒ a = bq + r

Again, q, q_1, r and r_1 are integers such that a = bq + r and a = bq_1 + r_1

Then, a = bq + r = bq_1 + r_1 for 0 ≤ r, r_1 < b

⇒ bq -bq_1= r_1- r

⇒ b(q - q_1)= r_1-r

⇒ (q - q_1) = $\frac{r_1 - r}{b}$

⇒ b|$(r_1 - r)$

Since r and r_1 are less than b but b|(r_1 - r). So, the number (r_1 - r) must be zero.

⇒ r_1- r = 0 ⇒ r = r_1

By this, bq + r = bq_1 + r_1

⇒ bq + r = bq_1 + r

⇒ bq = bq_1

⇒ q = q_1

Hence, q and r are unique integers. This completes the proof of the theorem.

Common divisor:

If a and b be two arbitrary integers then an integer d is said to be a common divisor of integers a and b if d|a and d|b.

Greatest common divisor (GCD)

A positive integer d is said to be greatest common divisor of given two integers a and b if d satisfies the following:

1. d|a and d|b
2. If c|a and c|b then c ≤ d.

Examples: Find the GCD of 12 and 18.

Solution: The positive divisors of 12 are 1, 2, 3, 4, 6, 12 and the positive divisors of 18 are 1, 2, 3, 6, 9, 18. Hence the positive common divisors of 12 and 18 are 1, 2, 3 and 6.

So, gcd(12, 18) = 6

Theorem: given integer a and b both of which are non zero, ∃ x, y ϵ Z such that gcd(a, b) = ax + by.

Proof: consider the non empty set of all positive linear combination of a and b such that S = { ax_0 + by_0: ax_0 + by_0> 0 where x_0, y_0 ∈ Z}

Let us choose x and y such that ax + by will give a least positive integer d in the set s. thus ax + by = d. Now, we can write gcd(a, b) = d for this we have to show that d|a and d|b.

If possible, suppose that d†a. Thus by division algorithm ∃ q, r ∈ Z such that a = dq + r, 0≤ r< d.

Thus r = a – dq = a –q(ax + by) =a(1-qx) +b(-qy)

Hence r ∈ S, s0 d cannot be a least positive integer since r < d. which is contradiction so we must have d|a. By same process, we can show d|b.

Now, if c is an arbitrary common positive divisor of a and b. Then we can write, c|a and c|b. It follows that c|ax + by, i.e. c|d. where d = ax +by and we know that c ≤ d. so that d is greater than every positive common divisor of a and b.

So, gcd(a, b) = d= ax + by . Proved

Relatively prime integers:

If a and b are any two integers such that at least one of which is non-zero, then a and b are said to be relatively prime if gcd(a, b) = 1.

Theorem: let a and b be integers not both zero. Then a and b are relatively prime iff ∃ x, y ∈ Z such that ax + by = 1.

Proof: let a and b are relatively prime, then gcd(a, b) = 1 and for the given integer a and b ∃ x, y ∈ Z such that gcd(a, b) = ax + by.

Which implies that ax + by = 1.

Conversely, if ax + by = 1, then we have to show that a and b are relatively prime. Let gcd(a, b) = d

⇒ d|a and d|b ⇒ d| ax +by for x,y ∈ Z ⇒ d|1 ⇒ d = 1

Hence, gcd(a, b) = 1, therefore a and b are relatively prime.

Theorem: if gcd(a, b) = d then gcd($\frac{a}{d}$, $\frac{b}{d}$) = 1.

Proof: since gcd(a, b) = d it can expressed as the linear combination of a and b such that d = ax + by for any x, y ∈ Z.

Dividing both sides by d, we get 1 = $\frac{a}{d}$x + $\frac{b}{d}$y

Since $\frac{a}{d}$ and $\frac{b}{d}$ are integer with gcd(a, b) = d then for any a, b ∈ Z and a ≠ 0, b ≠ 0.

If 1 = $\frac{a}{d}$x + $\frac{b}{d}$y, then we can write gcd($\frac{a}{d}$, $\frac{b}{d}$) = 1.

∴ gcd($\frac{a}{d}$, $\frac{b}{d}$) = 1

Euclid lemma: If a|bc with gcd(a, b) = 1 then a|c.

Proof: since a|ac and a|bc. Then we can write a| acx + bcy

⇒ a| c(ax + by) …… (i)

Since gcd(a, b) = 1 so there exists x, y ∈ Z such that ax + by = 1 …. (ii)

From (i) and (ii),

We get a|c proved

Theorem: Let a, b be integers not both zero for a positive integer d, d = gcd(a, b) iff (i) d|a and d|b (ii) whenever c|a and c|b then c|d.

Proof: since gcd(a, b) = d then d|a and d|b

If a and b are integers, a ≠ 0, b ≠ 0 then ∃x, y ∈ Z such that gcd(a, b) = ax + by. Thus, if c|a and c|b then c|ax + by ⇒ c|d

Conversely, let d|a and d|b. Let c|a and c|b then c|d implies that c ≤ d because d > 0. Hence gcd(a, b) = d proved

Lemma: If a = qb + r then gcd(a, b) = gcd(b, r).

Proof: Let gcd(a, b) = d

⇒ d|a and d|b ⇒ d|a – qb ⇒ d|r

So, we have d|b and d|r.

Hence d is a common divisor of both b and r.

If c is an arbitrary common divisor of b and r. then c|b and c|r

⇒ c|qb + r ⇒ c|a This shows that c is common divisor of a and b. Hence c ≤ d. Then by definition it follows that d = gcd(b, r)

∴ gcd(a, b) = gcd(b, r) proved

Euclidean algorithm:

Given integers b and c > 0, we have a repeated application of division algorithm, we obtain a series of equations

b = q_1c + r_1 , 0 ≤ r_1<c …… (1)

c = q_2r_1 + r_2 , 0 ≤ r_2<r_1 …… (2)

r_1 = q_3r_2 + r_3 , 0 ≤ r_3< r_2 …… (3)

………………………………

…………………………………

r_{n-2} = q_nr_{n-1} + r_n , 0 ≤ r_n<r_{n-1} …… (n-1) and

r_{n-1} = $q_{n+1}r_n$ + 0 ……………. (n)

The greatest common divisor of b and c is r_n. The least non-zero remainder in the division process is equal to the gcd(b, c) and can be expressed as the linear combination of x_0 and y_0 i.e. gcd(b, c) = bx_0 +cy_0.

Proof: The chain of equation is obtained by dividing b by c, c by r_1; r_1 by r_2; ….. ; r_{n-1} by r_n. This process ends when the remainder becomes zero if the division is exact. If not exact we write 0 < r_1<c in stead of 0 ≤ r_1<c.

If r_1 = 0 the chain stop and c becomes gcd of b and c.

We have to prove that gcd(b, c) = gcd(c, r) for c =qb + r

So, gcd(b, c) = gcd(c, r_1) = gcd(r_1, r_2) = ……. = gcd(r_n, 0) = r_n

We have to show that r_n is a linear combination of b and c.

From given equation, r_n = r_{n-2} - q_nr_{n-1}

Also from algorithm, r_{n-1} = r_{n-3} - $q_{n-1}r_{n-2}$

∴ r_n = r_{n-2} - $q_n(r_{n-3}$ - $q_{n-1}r_{n-2})$

= $(\mathbf{1}+\boldsymbol{q_nq_{n-1}})\boldsymbol{r_{n-2}}$ +(- $\boldsymbol{q_n})\boldsymbol{r_{n-3}}$

This represents r_n as linear combination of r_{n-2} and r_{n-3}.

Continuing backward through system of equations, we eliminate remainders r_{n-1}, r_{n-2}, …. , $r_1$until we reached to the stage r_n = gcd(b, c) is expressed as a linear combination of b and c . so we can write

r_n = bx_0 +cy_0

Theorem: If k > 0, then gcd(ka, kb) = |k| gcd(a, b).

Proof: we know that the equation of Euclidean algorithm multiplying by k, then we get,

ak = q_1bk + r_1k , 0 ≤ r_1k < bk …… (1)

bk = q_2r_1k + r_2k , 0 ≤ r_2k<r_1k …… (2)

………………………………

…………………………………

r_{n-2}k = q_nr_{n-1}k + r_n k, 0 ≤ r_nk<r_{n-1}k …… (n-1) and

r_{n-1}k = $q_{n+1}r_n$ k+ 0 ……………. (n)

By Euclidean algorithm, gcd(ak, bk) = $\boldsymbol{r_n}$ k = k$\boldsymbol{r_n}$ = k gcd(a, b).

Examples: **find the gcd(427, 616) and express it in terms of 427x + 616y.**

Solution: we have, by using division algorithm,

616 = 1. 427 + 189

427 = 2. 189 + 49

189 = 3.49 + 42

49 = 1. 42 + 7

42 = 7. 6 + 0

We have, r_n = 7 (least / last non-zero remainder)

∴ gcd(616, 427) = 7

Now, we can express 7 on linear combination of 616 and 427.

We have,

7 = 49 – 1. 42

= 49 –[189 – 3. 49]

= 4. 49 – 189

= 4.[427 – 2. 189] – 189

= 4. 427 -9. 189

= 4. 427 – 9. [616 – 1.427]

= 13 . 427 – 9. 616

= 427x + 616y where x= 13 and y = -9

∴ gcd(616, 427) = 7 = 427x + 616y ans

Examples: **find the gcd(24, 138) and express it in terms of 24x + 138y.**

Solution: we have, by using division algorithm,

138 = 5. 24 + 18

24 = 1. 18 + 6

18 = 6. 3

We have, r_n = 6 (least / last non-zero remainder)

∴ gcd(24, 138) = 6

Now, we can express 6 on linear combination of 24 and 138.

We have,

6 = 24 – 1. 18

=24 – 1. (138 – 5. 24)

= 6. 24 – 1.138

= 24x + 138y where x = 6 and y = -1

∴ gcd(24, 138) = 6 = 24x + 138y ans

Least common multiple (LCM):

The positive integer m is said to be the LCM of integer a and b if it satisfies the following.

1. a|m and b|m
2. If a|c and b|c wuth c > 0 then m ≤ c

Examples: Find the LCM of 6 and 8.

Solution:

The multiples of 6 is M_6 = {6, 12, 18, 24, 30, 36, 42, 48, ……}

The multiples of 8 is M_8 = {8, 16, 24, 32, 40, 48, ……}

The common multiples of 6 and 8 are = $M_6 \cap M_8$ = {24, 48, ….. }

The least common multiple of 6 and 8 is 24.

LCM = 24 ans

Theorem: For positive integers a and b; gcd(a, b).LCM(a, b) = a.b

Proof: Let gcd(a, b) = d ⇒ d|a and d|b

⇒ a = dr and b = ds for some r, s ∈ Z

If m = $\frac{ab}{d}$ then m = $\frac{a.ds}{d}$ = a.s and m = $\frac{dr.b}{d}$ = b.r ⇒ a|m and b|m

Let, c be any positive integer and is common multiple of a and b

i.e. c = av and c = bu

since gcd(a, b) = d then ∃ x, y ∈ Zsuch that d = ax + by

Now, $\frac{c}{m} = \frac{c}{ab/_{d}} = \frac{cd}{ab} = \frac{c(ax+by)}{ab} = \frac{acx+bcy}{ab} = \frac{c}{b}x + \frac{c}{a}y$ = ux + vy

i.e. $\frac{c}{m}$ = ux + vy ⇒ m|c

so, we conclude that m ≤ c.

Then by definition, LCM(a, b) = m = $\frac{ab}{d} = \frac{ab}{\gcd(a,b)}$

∴ LCM(a, b).gcd(a, b) = a.b

a is congruent to b modulo n

let n ∈ Z^{+}be an integer. Two integers a and b are said to be congruent modulo n (a is congruent to b modulo n) if n|a-b and denoted by a ≡b(modn).

If n† $a - b$ then a is incongruent to b modulo n and denoted by a≢b.

Examples:

- 3≡27(mod8) because 8|27-3 i.e. 8|24
- 2≢19(mod9) because 9†19-2 i.e. 9† 17.

Note:

- Since 1|a-b then a and b are congruent modulo 1.
- If any two integer are modulo 2 then either both odd or even.

Theorem: Let n ∈ Z^{+}be non-zero integer then a ≡b(modn) iff a and b have the same non negative remainder when divided by n.

Proof: since a ≡b(modn) ⇒ n|a-b ⇒ a – b = kn, k ∈ Z ⇒ a = b + kn. Dividing b by n, b leaves a certain remainder r, i.e. b = qn + r, 0≤ r < n

Therefore, a = b + kn

= qn + r + kn

= (q + k)n + r

This shows that a leaves same remainder r when divided by n.

Conversely, if a and b have the same non negative remainder when divided by n. Then, a = q_1n + r and b = q_2n + r, 0≤ r < n.

Now, a – b = (q_1n + r) – (q_2n + r) = q_1n – q_2n = (q_1 – q_2)n ⇒ n|a-b

⇒ a ≡b(modn)

Properties of congruence

Let n > 0 be fixed and a, b, c, d be arbitrary integers. Then the following properties hold.

1. **If a ≡a(modn) [reflective]**
2. **If a ≡b(modn) then b ≡a(modn) [symmetric]**
3. **If a ≡b(modn) and b ≡c(modn) then a ≡c(modn) [transitive]**
4. **If a ≡b(modn) and c ≡ d(modn) then a + c ≡b + d(modn) and ac ≡bd(modn)**
5. **If a ≡b(modn) then a + c ≡b + c(modn) and ac ≡bd(modn)**
6. **If a ≡b(modn) then $a^k \equiv b^k$(modn), for any k ∈ Z^{+}**

Proof:

1. For any integer a, we have, a – a = 0 = 0.n ⇒ n|a - a

   ⇒ a ≡ a(modn)
2. Since a ≡b(modn) ⇒ n|a - b ⇒ a – b = kn, k ∈ Z

   Now, b – a = - (a – b) = - (kn) = (-k)n ⇒ n|b - a

   Then by definition, b ≡ a(modn)
3. Since, a ≡b(modn) ⇒ n|a- b ⇒ a – b = k_1n, k_1 ∈ Z

   Again, b ≡ c(modn) ⇒ n|b - c ⇒ b – c = k_2n, k_2 ∈ Z

   Now, a – c = (a – b) + (b – c) = k_1n + k_2n =(k_1 + k_2)n

   ⇒ n|a- c, k_1 + k_2 ∈ Z ⇒ a ≡ c(modn)

4. Since, a ≡b(modn) ⇒ n|a- b ⇒ a – b = k_1n, k_1 ∈ Z

   And c ≡ d(modn) ⇒ n|c - d ⇒ c – d = k_2n, k_2 ∈ Z

   Now, (a – b) + (c – d) = k_1n + k_2n =(k_1 + k_2)n

   ⇒ (a + c) - (b + d) = (k_1 + k_2)n

   ⇒ n|(a + c) – (b + d), k_1 + k_2 ∈ Z ⇒ a + c ≡ $b + d$(modn)

   Again, a ≡b(modn) ⇒ n|a- b ⇒ a – b = k_1n, k_1 ∈ Z ⇒ a = b + k_1n

   And c ≡ d(modn) ⇒ n|c - d ⇒ c – d = k_2n, k_2 ∈ Z ⇒ c = d + k_2n

   Now, ac = (b + k_1n)(d + k_2n) = bd + bk_2n + dk_1n + $k_1 k_2 n^2$

   ⇒ ac – bd = n(bk_2 + dk_1 + $k_1 k_2 n$) ⇒ n|ac – bd ⇒ ac ≡bd(modn)

5. Since, a ≡b(modn) ⇒ n|a- b ⇒ a – b = kn, k ∈ Z

   Now, a – b + c – c = kn, k ∈ Z

   ⇒ (a + c) - (b + c) = kn

   ⇒ n|(a + c) – (b + c), k ∈ Z ⇒ a + c ≡ $b + c$(modn)

   Again, a ≡b(modn) ⇒ n|a- b ⇒ a – b = kn, k∈ Z

   Now, (a – b)c = kn.c, k∈ Z

   ⇒ n|ac – bd ⇒ ac ≡bc(modn)

6. We use induction on k.

   If k = 1, then obviously a ≡b(modn) …… (i)

   By induction hypothesis suppose $a^{k-1} \equiv b^{k-1}$(modn) ….. (ii) is for the k = k-1

   Now, $a.a^{k-1} \equiv b.b^{k-1}$(modn)

   ⇒ $a^k \equiv b^k$(modn) which is true for all k.

Theorem: Let n∈ Z be an integer and n ≠ 0 then a ≡b(modn) iff a ≡ r(modn)where r is remainder when n divides b.

Proof: Let n∈ Z^+ and a ≡b(modn) then we have to show that a ≡r(modn)

We have a ≡b(modn) ⇒ n|a- b ⇒ a – b = $q^{|}$n ⇒ a = b + $q^{|}$n, $q^{|}$ ∈ Z ….. (i)

By division algorithm, for b and n there exists q, r ∈ Z such that b = nq + r….. (ii)

From (i) and (ii),

a = nq + $q^{|}$n + r ⇒ a – r = (q + $q^{|}$)n ⇒ n|a- r ⇒ a ≡ r(modn)

conversely, suppose a ≡ r(modn), where r is the remainder upon division by n then we have to show that a ≡ b(modn). Since r is remainder upon division b by n then b = qn + r with quotient q. i.e. r = b – qn and a ≡ r(modn) ⇒ a ≡ $(b - qn)$(modn) ⇒ a - b ≡0(modn) ⇒ n|a- b ⇒ a ≡b(modn)

Divisibility Rules for the Numbers 2 to 12.

1. **The Divisibility Rule for 2:** Check whether the last digit of a given number is zero or even number. If yes, then the given number is divisible by 2.
2. **The Divisibility Rule for 3:** Check whether the sum of the digits of a given number is divisible by 3 or not. If so, then the given number is divisible by 3.
3. **The Divisibility Rule for 4:** Check whether the last two digits of a given number are divisible by 4 or not. If yes, then the given number is divisible by 4.
4. **The Divisibility Rule for 5:** If the last digits of a number are 0 or 5, then the number is divisible by 5, otherwise not.
5. **The Divisibility Rule for 6:** Check whether the given number is divisible by 2 and 3 both or not. If yes, then the given number is divisible by 6.
6. **The Divisibility Rule for 7:** To check whether the given number is divisible by 7, one must multiply the last digit by 2, and then subtract the product from the number being left. Finally, if the difference obtained is 0 or a multiple of 7, then the given number is divisible by 7.
7. **The Divisibility Rule for 8:** Check whether the last three digits of the given number are divisible by 8 or not. If yes, then the given number is divisible by 8.
8. **The Divisibility Rule for 9:** Check whether the sum of the digits of a given number is divisible by 9 or not. If yes, then the given number is divisible by 9.

9. **The Divisibility Rule for 10:** If the last digit of a number is zero, then the given number is divisible by 10, otherwise not.
10. **The divisibility rules for 11:** if the difference of the sum of the alternative digits of a number is divisible by 11.
11. **The divisibility rules for 12:** if the number is divisible by both 3 and 4, then it is divisible by 12.