4.1 - DIVISIBILITY AND MODULAR ARITHMETIC

DIVISION :

If a and b are integers, with $a \neq 0$, we say that **a divides b**, if there is an integer c such that $b = ac$.

Notation:

a divides b is denoted by $a \mid b$

> The notations $a \mid b$ and a/b are **not** same, because
> $a \mid b$: a divides b
> a/b : b divides a

When $a \mid b$, for $a, b \in \mathbb{Z}$, $a \neq 0$,
We can say that

- a divides b (or a is a divisor of b i.e., equivalently $\frac{b}{a}$ is an integer)
- b is divisible by a (i.e., $\frac{b}{a}$)
- b is a multiple of a ($\because a \mid b$ can be written as $b = ac$ for some c)
- a is a factor of b

> We can express $a \mid b$ using quantifiers as:
> $\exists c \, (b = ac)$ for $a, b \in \mathbb{Z}, a \neq 0$, $c \in \mathbb{Z}$
> domain : Set of Integers

Examples :

- $3 \mid 12$

  it can be written as 12 is a multiple of 3
  i.e $12 = 3 * 4$ (4 → some integer)

- $4 \nmid 11$

  it cannot be written as 11 is a multiple of 4
  i.e., $11 \neq 4 *$ (for some integer)

  $4 \nmid 11$ means 4 does not divide 11

- $-2 \mid 6$

  it can be written as 6 is a multiple of -2
  as $6 = -2 * (-3)$ (−3 → some integer)

But Generally we take positive integers

Example:

Let n and d be positive integers. How many positive integers not exceeding n are divisible by d.

Sol:

As given in question:

divisor = d

~~As we know~~

Suppose d divides some +ve integer i.e

$d \mid$ +ve integer , so +ve integer is a multiple of d

i.e +ve intege = d K for some K

And we have to find +ve integers not exceeding n divisible by d. So we can write it as

$$0 < \underbrace{dK}_{\text{\# of +ve integers for } K=1,2,\ldots} \leq n$$

$$\Rightarrow 0 < K \leq n/d$$

(how many K's depends on the values of d and n)

So there are $\lfloor n/d \rfloor$ positive integers not exceeding n that are divisible by d.

TEST

Suppose n=10 and d=5

$0 < K \leq n/d$ i.e $0 < K \leq 10/5$ or $0 < K \leq 2$

So there are two positive integers (one for K=1, second for K=2)

+ve integer = dK for some K

= 5 * 1 for K=1 So, There are two +ve integers not exceeding 10 that are divisible by 5,

= (5)

& = 5 * 2 for K=2

= (10)

Some basic properties of divisibility of integers are given in Theorem1.

THEOREM 1:

Let a, b and c be integers, where $a \neq 0$, then

(i) If $a|b$ and $a|c$, then $a|(b+c)$;

(ii) If $a|b$, then $a|bc$ for all integers c;

(iii) If $a|b$ and $b|c$, then $a|c$

PROOF:

(i) As $a|b$, so it can be written as $b = aC_1$ for some $C_1 \in Z$

As $a|c$, so it can be written as $c = aC_2$ for some $C_2 \in Z$

and we have to show $a|(b+c)$

$$b + c = aC_1 + aC_2$$
$$= a(C_1 + C_2)$$
$$b + c = aK \quad \text{where } K = C_1 + C_2 \in Z$$

$\Rightarrow b+c$ is a multiple of a for some K, so

$$a|(b+c)$$

(ii) As $a|b$ i.e $b = aK$

$$b = aK$$

or $bc = acK$ multiply integer on both sides

or $bc = a(cK)$

$$bc = am \quad \text{where } m = cK \in Z$$

As bc is a multiple of a, so

$$a|bc \text{ for all integers } c$$

(iii) $a|b$ i.e $b = aC_1$

$b|c$ i.e $c = bC_2$

$$c = bC_2$$
$$= aC_1C_2$$
$$c = a(C_1C_2)$$
$$\Rightarrow a|c$$

COROLLARY 1:

If a, b and c are integers, where $a \neq 0$, such that $a|b$ and $a|c$, then $a|mb+nc$ where m & n are integers.

Proof:

Hypothesis:

$a|b$ i.e $b = at$, $t \in \mathbb{Z}$

$a|c$ i.e $c = as$, $s \in \mathbb{Z}$

So $mb+nc$ can be written as:

$$mb + nc = m(at) + n(as)$$
$$= a(mt + ns)$$
$$= a\,C_3 \qquad \text{where } C_3 = mt+ns \in \mathbb{Z}$$

Conclusion:

$\Rightarrow a|mb+nc$

DIVISION ALGORITHM

Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that

$$a = dq + r$$

d: divisor
a: divident
q: quotient
r: remainder

$q = a \text{ div } d = \lfloor a/d \rfloor$

and $r = a \bmod d = a - d\lfloor a/d \rfloor$

NOTE:

Both a div d & a mod d for a fixed d are functions on set of integers.

When $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$, we have $\lfloor a/d \rfloor$ (output is also integer)

Same is the case for remainder

Example:

Find the quotient and remainder when

(i) -23 is divided by 5

(ii) 25 is divided by -5

Sol:

(i) $a = -23$ $\quad -23 \in z$

$d = 5$ $\quad 5 \in z^+$

$$5 \overline{)} \begin{array}{r} -5 \\ -23 \\ +25 \\ \hline 2 \end{array}$$

$$q = \left\lfloor a/d \right\rfloor = \left\lfloor -23/5 \right\rfloor = -5$$

$r = -23 \bmod 5 = 2$ $\quad$ (or $r = a - d * \left\lfloor a/d \right\rfloor = -23 - (5)*(-5) = -23 + 25 = 2$)

So $\quad -23 = 5 \cdot (-5) + 2 \quad 0 \leq r < d \quad (0 \leq 2 < 5)$

(ii) $a = 25$

$d = -5$

Here $a = 25 \in z$

but $d = -5 \notin z^+$

Note:

The integer a is divisible by integer d iff the remainder is zero when a is divided by d.

$a = 24$
$b = 6$

$a = dq + r$

$24 = 6 \cdot (4) + 0$

$24 = 6(4)$ → Some integer

24 is a multiple of 6, so $6 \mid 24$

$$6 \overline{)} \begin{array}{r} 4 \\ 24 \\ 24 \\ \hline 0 \end{array}$$

EXAMPLE :

What are the quotient and remainder when 101 is divided by 11 ?

Sol:-

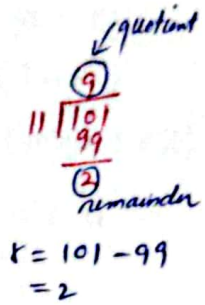
$a = 101 \quad d = 11 \qquad a \in \mathbb{Z}, d \in \mathbb{Z}^+$

and we have to find unique integers q and r with $0 \le r < d$ such that

$$a = dq + r$$

$$q = a \text{ div } d = \left\lfloor a/d \right\rfloor = \left\lfloor 101/11 \right\rfloor = 9$$

$$r = a \bmod d = 2$$



i.e.,

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

EXAMPLE :

What are the quotient and remainder when −11 is divided by 3?

Sol:

$a = -11 \quad , \quad d = 3 \qquad -11 \in \mathbb{Z}, 3 \in \mathbb{Z}^+$

To find $q = ?$ $r = ?$ with $0 \le r < 3$

$$a = dq + r$$

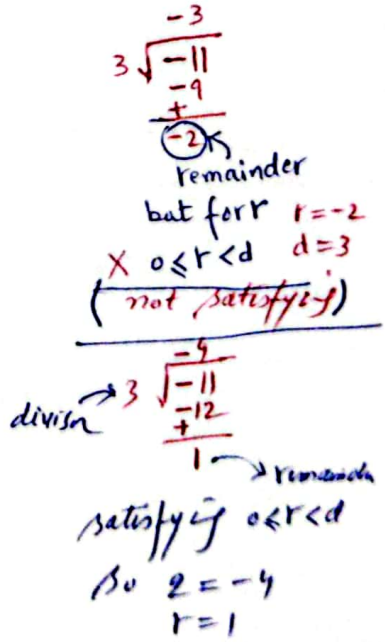
$$q = \left\lfloor a/d \right\rfloor = \left\lfloor -11/3 \right\rfloor = -4$$

$$q = -4$$

$$r = 1$$

Thus we can write it as

$$-11 = 3(-4) + 1$$



QUESTIONS REGARDING DIVISION ALGORITHMS

Q1. What are the quotients and remainder when

a. 789 is divided by 23
b. 1234567 is divided by 1001
c. 4 is divided by 1
d. 3 is divided by 5
e. 0 is divided by 19
f. −111 is divided by 11
g. −2002 is divided by 87
h. −100 is divided by 101
i. −1 is divided by 3

DIVISION ALGORITHM

$a = dq + r$

a : Divident ($a \in Z$)

d: Divisor ($d \in Z^+$)

q: Quotient (unique $q \in Z$)

$q = a \text{ div } d$

$q = \lfloor a/d \rfloor$

r: Remainder

Unique integer, with

$0 \leq r \leq d$

$r = a - d\lfloor a/d \rfloor$

Sol:a. 789 is divided by 23

$a = 789$, $d = 23$

$a = dq + r$

$789 = 23q + r$

$q = 34$ $(q = \lfloor a/d \rfloor)$

$r = 7$ $(r = a \bmod d$ or $r = a - d \cdot \lfloor a/d \rfloor)$ $:(0 \leq 7 < 23)$

So, $789 = 23 \cdot 34 + 7$ (verified)

quotient

```
   34
23 | 789
     69
     ---
     99
     92
     --
      7   → remainder
```

---

b. 1234567 is divided by 1001

$a = 1234567$, $d = 1001$

$1234567 = 1001q + r$

$q = 1233$ $\left(q = \left\lfloor \frac{1234567}{1001} \right\rfloor\right)$

$r = 334$ $(r = a - d\lfloor a/d \rfloor)$

```
      1233
1001 | 1234567
       1001
       ----
        2335
        2002
        ----
         3336
         3003
         ----
          3337
          3003
          ----
           334
```

$r = a - d\lfloor a/d \rfloor$

$= 1234567 - 1001 * 1233$

$= 1234567 - 1234233$

$= 334$

So, $1234567 = 1001 * 1233 + 334$ (verified)

---

c. 4 is divided by 1

$a = 4$, $d = 1$

$a = dq + r$

$4 = 1 \cdot q + r$

$q = 4$ $(q = \lfloor 4/1 \rfloor = 4)$

$r = 0$ $(r = 4 - 1 \cdot \lfloor 4/1 \rfloor = 4 - 4 = 0)$

```
   4
1 | 4
    4
    -
    0
```

So, $4 = 1 \cdot 4 + 0$ (verified)

d. 3 is divided by 5

$a = 3$, $d = 5$

$a = dq + r$

$3 = 5q + r$

$q = 0$ $\left(q = \left\lfloor \frac{3}{5} \right\rfloor = 0\right)$

$r = 3$ $\left(r = 3 - 5 \cdot \left\lfloor \frac{3}{5} \right\rfloor = 3 - 5 \cdot 0 = 3\right)$

$5 \overline{)\, 3}$ (0, remainder 3)

So, $3 = 5 * 0 + 3$

e. 0 is divided by 19

$a = 0$, $d = 19$

$a = dq + r$

$0 = 19 \cdot q + r$

$q = 0$

$r = 0$

$19 \overline{)\, 0}$ (0, remainder 0)

So, $0 = 19 * 0 + 0$

f. -111 is divided by 11

$a = -111$, $d = 11$

$a = dq + r$

$-111 = 11q + r$

$q = -11$

$r = 10$ (violation of r As $0 \leq r < d$)

$11 \overline{)\, -111}$ (quotient -10, $+110$, remainder -1) $\times$ $11 \overline{)\, -111}$ (quotient -11, -121, remainder 10)

So, $-111 = 11 * (-11) + 10$ (verified)

g. -2002 is divided by 87

$a = -2002$, $d = 87$

$a = dq + r$

$-2002 = 87q + r$

$q = -24$

$r = 86$

$87 \overline{)\, -2002}$ (quotient -23, $+2001$, remainder -1) $(0 \leq r < d)$

$87 \overline{)\, -2002}$ (quotient 2, -2088, remainder 86)

So, $-2002 = 87 * (-24) + 86$

h. -100 is divided by 101

$a = -100$, $d = 101$

$a = dq + r$

$-100 = 101 * q + r$

$q = -1$ $\left(q = \left\lfloor \frac{-100}{101} \right\rfloor = -1\right)$

$r = 1$ $\left(r = -100 - 101 \left\lfloor \frac{-100}{101} \right\rfloor = -100 - 101 * -1 = 1\right)$

$101 \overline{)\, -100}$ (quotient -1, $+101$, remainder 1)

So, $-100 = 101 * (-1) + 1$

(verified)

i. -1 is divided by 3

$a = -1$, $d = 3$

$a = dq + r$

$-1 = 3q + r$

$q = -1$

$r = 2$

$3 \overline{)\, -1}$ (quotient -1, $+3$, remainder 2)

So, $-1 = 3 * (-1) + 2$ (verified)

Q2. What time does a 12-hour clock read

a. 80 hours after it reads 11:00 ?

b. 100 hours after it reads 6:00?

c. 40 hours before it reads 12:00 ?

Sol:

a. 80 hours after it reads 11:00 ?

~~Current time~~

$11 + 80 = 91$

$a = 91$, $d = 12$ (12-hour clock)

$a = dq + r$

$91 = 12q + r$

$q = 7$

$r = 7 \Rightarrow 7:00$

$12 \overline{)91}$ 7, 84, 7 → current time

So, $91 = 12 * 7 + 7$ (verified)

The clock reads 7:00 (the remainder)

---

b. 100 hours after it reads 6:00 ?

$100 + 6 = 106$

$a = 106$, $d = 12$ (12 hour clock)

$a = dq + r$

$106 = 12q + r$

$q = 8$

$r = 10$

$12 \overline{)106}$ 8, 96, 10 → Current time

$106 = 12 * 8 + 10$ verified

The clock reads 10:00 (the remainder)

---

c. 40 hours before it reads 12:00 ?

$12 - 40 = -28$, $d = 12$

$a = dq + r$

$-28 = 12 * q + r$

$q = -3$

$r = 8$ $\left(r = -28 - 12 * \left\lfloor \frac{-28}{12} \right\rfloor = -28 - 12 * -3 = -28 + 36 = 8 \right)$

$12 \overline{)-28}$ -3, -36, 8 → Current time

The Clock reads 8:00 (the remainder

Q3. What time does a 24-hour clock read

a. 100 hours after it reads 2:00?
b. 188 hours after it reads 19:00?
c. 45 hours before it reads 12:00?

Sol:

a. 100 hours after it reads 2:00?

$2 + 100 = 102$

$a = 102$, $d = 24$ (24-hour clock)

$a = dq + r$

$102 = 24q + r$

$24 \overline{)\, 102}$, $q = 4$, 96, $r = 6$

$q = 4$

$r = 6 \rightarrow$ Current time

The clock reads 6:00 (the remainder)

---

b. 168 hours after it reads 19:00?

$19 + 168 = 187$

$a = 187$, $d = 24$

$a = dq + r$

$187 = 24q + r$

$24 \overline{)\, 187}$, $q = 7$, 168, $r = 19$

$q = 7$

$r = 19$

The clock reads 19:00 (the remainder)

---

c. 45 hours before it reads 12:00?

$12 - 45 = -33$

$a = -33$, $b = 24$

$-33 = 24q + r$

$24 \overline{)\, -33}$, $q = -2$, -48, $r = 15$

$q = -2$

$r = 15$

The clock reads 15:00.

MODULAR ARITHMETIC

In some situations we care only about the remainder of an integer when it is divided by some specified positive integer.

For example,

What time it will be (on a 24-hour clock) 50 hours from now?
we care only about the remainder.

$$(50 + \text{the current hour})/_{24} = \text{remainder}$$

For this we introduce a different (other than mod), but related, notion that indicates that two integers have the same remainder when they are divided by the positive integer .

Definition:

If $a, b \in Z$ and $m \in Z^+$, then a is congruent to b module m if m divides a-b.

It can be written as

$$a \equiv b \pmod m$$

$a \equiv b \pmod m$:
a relation on set of integers.

$a \bmod m = b$:
a function

THEOREM:

Let $a, b \in Z$, and $m \in Z^+$, then

$a \equiv b \pmod m$ iff $a \bmod m = b \bmod m$

CONGRUENT CLASS:

The set of all integers congruent to an integer b module m is called the Congruent class of a module m and that the union of these equivalence classes is the set of integers.

Example # :

Determine whether

- 17 is Congruent to 5 modulo 6
- 24 and 14 are Congruent to modulo 6

Sol:

- 17 is Congruent to 5 modulo 6

or we have to decide $17 \equiv 5 \pmod 6$

Check it as

$$6 \mid 17-5 \quad \text{i.e} \quad 6 \mid 12$$

as $6 \mid 12$, we can say that

$$17 \equiv 5 \mod 6$$

$\Rightarrow$ YES : 17 is Congruent

ALSo For Congruent

a and b have same remainders

17 mod 6 = 5
5 mod 6 = 5

So,
$17 \equiv 5 \mod 6$

- 24 and 14 are Congruent modulo 6 i.e. $24 \equiv 14 \pmod 6$

i.e $6 \mid 24-14$ i.e $\Rightarrow$ $6 \nmid 10$

So 24 is not Congruent

24 mod 6 = 0
14 mod 6 = 2
So,
$24 \not\equiv 14 \mod 6$

THEOREM:

Let $m \in \mathbb{Z}^+$, then integers a and b are Congruent modulo m iff there is an integer K such that $a = b + mK$

Proof: Suppose $a \equiv b \pmod m$: a and b are Congruent modulo m.

$\Rightarrow m \mid a-b$

$\Rightarrow a-b$ is a multiple of m for some $K \in \mathbb{Z}$

i.e $a-b = mK$

$a = b+mK$ (proved) : (Equation Form of Congruency)

Conversly :

Suppose we have

$a = b + Km$

$\Rightarrow a-b = Km$

$\Rightarrow m \mid a-b$ So, a is Congruent to b modulo m

$\Rightarrow a \equiv b \pmod m$

THEOREM:

Let $m \in \mathbb{Z}^+$. If $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then

- $a+c \equiv b+d \pmod m$
- $ac \equiv bd \pmod m$

PROOF:

① $a \equiv b \pmod m$

$\Rightarrow m \mid a-b$

$\Rightarrow a-b = mK_1$ (for some K_1) —Ⓐ

$c \equiv d \pmod m$

$\Rightarrow m \mid c-d$

$\Rightarrow c-d = mK_2$ (for some K_2) —Ⓑ

Adding Ⓐ and Ⓑ, we get

$(a+c)-(b+d) = mK_1 + mK_2$

$= m(K_1+K_2)$

$(a+c)-(b+d) = mK$ where $K = K_1+K_2$

$\Rightarrow m \mid (a+c)-(b+d)$: $(a+c)$ is congruent to $(b+d)$ modulo m

$\Rightarrow (a+c) \equiv (b+d) \pmod m$

Example:

$7 \equiv 2 \pmod 5$

$11 \equiv 1 \pmod 5$

$7+11 \equiv (2+1) \pmod 5$

$18 \equiv 3 \pmod 5$

② To show $ac \equiv bd \pmod m$

$a \equiv b \pmod m$

$\Rightarrow m \mid a-b \Rightarrow a-b = mK_1 \Rightarrow a = b+mK_1$ —Ⓐ

$c \equiv d \pmod m$

$\Rightarrow m \mid c-d \Rightarrow c-d = mK_2 \Rightarrow c = d+mK_2$ —Ⓑ

$ac = (b+mK_1)\cdot(d+mK_2)$

$= bd + bmK_2 + dmK_1 + mK_1 \cdot mK_2$

$ac = bd + mK$

$\Rightarrow ac - bd = mK$

$\Rightarrow m \mid ac - bd$

$ac \equiv bd \pmod m$

Example:

$7 \equiv 2 \pmod 5$

$11 \equiv 1 \pmod 5$

$7 \cdot 11 \equiv (2 \cdot 1) \pmod 5$

$77 \equiv 2 \pmod 5$

Important :

We must be careful working with CONGRUENCES.
Some properties we may expect to be true are not valid.
For example,

If $ac \equiv bc \pmod m$, then $a \equiv b \pmod m$ may be false.

① Let we take $m=4$, $c=2$ (and $a=0$, $b=2$)

$ac \equiv bc \pmod m$

$0 \equiv 4 \pmod 4$

As $0 \bmod 4 = 0$
$4 \bmod 4 = 0$

So $ac \equiv bc \bmod m$

But $a \not\equiv b \bmod m$

$0 \equiv 2 \bmod 4$

$0 \bmod 4 = 0$
$2 \bmod 4 = 2$ ($a \bmod m \neq b \bmod m$)

So $a \not\equiv b \bmod m$

It could be true i.e;

If $ac \equiv bc \pmod m$ and $GCD(m,c)=1$ (m and c are relative primes), then

$a \equiv b \pmod m$

Proof:

$ac \equiv bc \bmod m$

$\Rightarrow m \mid ac-bc \Rightarrow m \mid c(a-b)$

$m \mid c(a-b)$

if m and c are relative primes, then

$m \nmid c$, but $m \mid a-b$

$\Rightarrow a \equiv b \bmod m$

Example:
we take m & c as
$m=6$, $c=5$ (relative primes)
and $a=17$, $b=5$

So
$ac \equiv bc \bmod m$
$17 \cdot 5 \equiv 5 \cdot 5 \bmod 6$
$85 \equiv 25 \bmod 6$ (true)
$6 \mid 85-25$
$6 \mid 60$

and $a \equiv b \bmod m$
is also true as:
$17 \equiv 5 \bmod 6$
$6 \mid 17-5$ or $6 \mid 12$

COROLLARY :

Let $m \in Z^+$, and $a, b \in Z$, then

1. $(a+b) \bmod m = \big((a \bmod m) + (b \bmod m)\big) \bmod m$
2. $ab \bmod m = \big((a \bmod m) \cdot (b \bmod m)\big) \bmod m$

PROOF :

$a \equiv b \pmod m$ By Def. of Congruent, where b is remainder

or $a \equiv r \pmod m$ — (A)

Also, we know by definition of mod function

$a \bmod m = r$ (remainder

put the value of r in eq. (A), we have

$a \equiv a \bmod m \pmod m$ — (1)

Also $b \equiv b \bmod m \pmod m$ — (2)

$b \equiv a \pmod m$
$b \equiv r \pmod m$
and $r = b \bmod m$
$\Rightarrow b = b \bmod m \pmod m$

By theorem :

~~Add (1) and (2),~~

$a+b \equiv a \bmod m \pmod m + b \bmod m \pmod m$

$a+b \equiv \big((a \bmod m) + (b \bmod m)\big) \bmod m$ ~~proved.~~

By theorem

~~Multiply (1) and (2),~~

$ab \equiv (a \bmod m) \cdot (b \bmod m) \bmod m$

Testing: $(a+b) \bmod m = \big((a \bmod m) + (b \bmod m)\big) \bmod m$

$a = 177$
$b = 270$
$m = 31$

$= \big((177 \bmod 31) + (270 \bmod 31)\big) \bmod 31$

$= (22 + 22) \bmod 31$

$= 44 \bmod 31 = (13)$

$= (a+b) \bmod$
$= (177 + 270) \bmod 31$
$= 447 \bmod 31$
$= (13)$

NOTE : This Corollary shows that
How to find the values of the mod m function at the sum (and product) of the two integers using :
the values of this function at each of these integers.
We will Use this result in Section 5.4.

QUESTIONS REGARDING MODULAR ARITHMETIC (Congruency)

Q#1 Find the integer a such that

a. $a \equiv 43 \pmod{23}$ and $-22 \leq a \leq 0$

b. $a \equiv 17 \pmod{29}$ and $-14 \leq a \leq 14$

c. $a \equiv -11 \pmod{21}$ and $90 \leq a \leq 110$

d. $a \equiv -15 \pmod{27}$ and $-26 \leq a \leq 0$

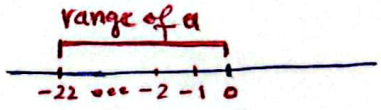
e. $a \equiv 24 \pmod{31}$ and $-15 \leq a \leq 15$

f. $a \equiv 99 \pmod{41}$ and $100 \leq a \leq 140$

(Do yourself)

Sol:-

a. $a \equiv 43 \pmod{23}$ and $-22 \leq a \leq 0$



By def., we have

$$23 \mid a-43$$

$$\frac{a-43}{23} \quad \left(\text{Required } (a-43) \bmod 23 = 0\right)$$

$a \equiv b \pmod{m}$
$\Rightarrow$
$m \mid a-b$
i.e $(a-b) \bmod m = 0$

For 23 divid $a-43$,

$(a-43)$ should be $0, 23, -23, 46, -46, \cdots$ etc.

and should be within $-22 \leq a \leq 0$

1. $a-43=0 \Rightarrow a=43$ → not within range but we are interested in $-22 \ll a \leq 0$
1. $a-43=-23 \Rightarrow a=43-23=20$ (not within range)
2. $a-43=-46 \Rightarrow a=-46+43=-3$ (yes: $-22 \leq -3 \leq 0$)

So, $\boxed{a=-3}$

and we can write it as

$$-3 \equiv 43 \pmod{23} \quad \text{with } -22 \leq a \leq 0$$

---

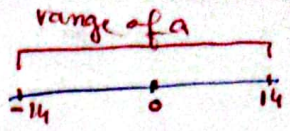
b. $a \equiv 17 \pmod{29}$ and $-14 \leq a \leq 14$

By def. we have

$$29 \mid a-17$$

$$\frac{a-17}{29} \quad \left(\text{Required: } (a-17) \bmod 29 = 0\right)$$

17



For 29 divides $a-17$,

$(a-17)$ should be $0, 29, -29, 58, -58$, etc. and maintaing the range $-14 \le a \le 14$.

1. $a-17=0 \Rightarrow a=17$ (not in range)
2. $a-17=29 \Rightarrow a=29+17=46$ (not in range)
3. $a-17=-29 \Rightarrow a=17-29=-12$ (YES)

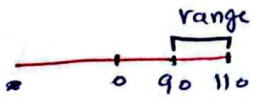
So, $\boxed{a=-12}$

and we can writ it as

$$-12 \equiv 17 \pmod{29} \quad \text{for } -14 \le a \le 14.$$

---

c. $a \equiv -11 \pmod{21}$ and $90 \le a \le 110$



By def.

$$21 \mid a+11$$

$$\frac{a+11}{21}$$

For 21 divid $a+11$, $(a+11)$ Should be $0, 21, -21, 42, -42, 63, 84, -84, 105, -105$ etc.

$a+11=105 \Rightarrow a=105-11=94$ (and it is within range $90 \le a \le 110$)

So, $\boxed{a=94}$

and $94 \equiv -11 \pmod{21}$ for $90 \le a \le 110$.

---

d. $a \equiv -15 \pmod{27}$ and $-26 \le a \le 0$

$$\frac{a+15}{27}$$

$(a+15)$ Should be $0, 27, -27$ etc.

1. $a+15=0 \Rightarrow a=-15$ (YES, in the range)

So $\boxed{a=-15}$

and

$$-15 \equiv -15 \bmod 27 \quad \text{for } -26 \le a \le 0.$$

Q#2 List five integers that are Congruent to 4 (mod 12).

Sol: $a \equiv 4 \bmod 12$, $a = ?$ (List five)

$12 \mid a-4$

$\frac{a-4}{12}$, For 12 divides $a-4$, $(a-4)$ should be $0, 12, -12, 24, -24$ etc.

1. $a-4=0 \Rightarrow \boxed{a=4}$
2. $a-4=12 \Rightarrow a=12+4=16 \Rightarrow \boxed{a=16}$
3. $a-4=-12 \Rightarrow a=-12+4=-8 \Rightarrow \boxed{a=-8}$
4. $a-4=24 \Rightarrow a=24+4=28 \Rightarrow \boxed{a=28}$
5. $a-4=-24 \Rightarrow a=-24+4=-20 \Rightarrow \boxed{a=-20}$

$a = \{-20, -8, 4, 16, 28\}$

Q#3: List all the integers between -100 and 100 that are Congruent to -1 mod 25.

Sol: $a \equiv -1 \pmod{25}$ for $-100 \leq a \leq 100$

$25 \mid a+1$

$\frac{a+1}{25}$, $a+1$ should be $0, 25, -25, 50, -50, 75, -75, 100$ etc.

1. $a+1=0 \Rightarrow \boxed{a=-1}$
2. $a+1=25 \Rightarrow \boxed{a=24}$
3. $a+1=-25 \Rightarrow \boxed{a=-26}$

$a+1=50 \Rightarrow \boxed{a=49}$

$a+1=-50 \Rightarrow \boxed{a=-51}$

$a+1=75 \Rightarrow \boxed{a=74}$

$a+1=-75 \Rightarrow \boxed{a=-76}$

$a+1=100 \Rightarrow \boxed{a=99}$

So a's are : for $-100 \leq a \leq 100$

$-76, -51, -26, -1,$
$24, 49, 74, 99$

Q#4 Describe whether each of these integers is congruent to 3 modulo 7.

a. 37
b. 66
c. -17
d. -67

Sol:

a- $37 \equiv 3 \pmod 7$

By def.

$7 \mid 37-3$ i.e $\frac{37-3}{7}$ or $\frac{30}{7}$

So, as $7 \nmid 30$, we conclude

$37 \not\equiv 3 \pmod 7$

Another way!
Here
$a \bmod m \neq b \bmod m$
$37 \bmod 7 = 2$ (remainder)
$3 \bmod 7 = 3$ (remainder)
So $37 \not\equiv 3 \pmod 7$

Another way 2

$37 \equiv 3 \pmod 7$
a, remainder, d

$a = dq + r$

$7 \overline{)37}$ (5, 35)

$q = \left\lfloor \frac{a}{d} \right\rfloor = \left\lfloor \frac{37}{7} \right\rfloor = 5$

$r = 2$

$a = dq + r$

$37 = 7 \cdot 5 + 2$

In given relation:

$37 \equiv 3 \pmod 7$

$r = 3$

but By division Algo.

$r = 2$

So, $37 \not\equiv 3 \pmod 7$

b. $66 \equiv 3 \pmod 7$

$7 \mid 66-3$

$\Rightarrow \frac{66-3}{7} \Rightarrow \frac{63}{7} = 9$ (or $63 \bmod 7 = 0$)

So, as $7 \mid 63$

$66 \equiv 3 \pmod 7$ i.e 66 is congruent to 3 with modulo 7.

c. $-17 \equiv 3 \pmod 7$

$7 \mid -17-3$

$\Rightarrow \frac{-17-3}{7} \Rightarrow \frac{-20}{7}$, So $7 \nmid -20$

$(-20 \bmod 7 \neq 0)$

So $-17 \not\equiv 3 \pmod 7$

Another way:

$-17 \equiv 3 \pmod 7$
a, r, d

Div. Alg.
$a = dq + r$

$7 \overline{)-17}$ (-3, -21, 4)

$-17 = 7 \cdot -3 + 4$

r does not match, So

$-17 \not\equiv 3 \pmod 7$

d. $-67 \equiv 3 \pmod 7$

$7 \mid -67-3$ or $\frac{-70}{7}$ or $-70 \bmod 7 = 0$

So, $7 \mid -70$

and we can say that

$-67 \equiv 3 \pmod 7$

$-66 \equiv 3 \pmod 7$
a, r, d

Div. Algo:
$a = dq + r$

$7 \overline{)-67}$ (-10, -70, 3)

$-67 = 7 \cdot -10 + 3$

r matches, So

$-66 \equiv 3 \pmod 7$

ARITHMETIC MODULO m

We can define arithmetic operations on Z_m,
where Z_m : the set of nonnegative integers less than m
: $\{0, 1, 2, \cdots, m-1\}$

We can define addition of these integers i.e $\{0,1,2,\cdots m-1\}$, denoted by $+_m$ by :

$$a +_m b = (a + b) \bmod m$$

(ordinary addition)

and
We can define multiplication of these integers denoted by $\cdot_m$ as

$$a \cdot_m b = (ab) \bmod m$$

(ordinary multiplication)

The operations
$+_m$ and $\cdot_m$ are called addition & multiplication modulo m

Example :
Use Definition of addition and multiplication in Z_m to find

- $7 +_{11} 9$
- $7 \cdot_{11} 9$

$$7 +_{11} 9 = (7 + 9) \bmod 11$$
$$= 16 \bmod 11 = 5$$

$$7 \cdot_{11} 9 = (7 \cdot 9) \bmod 11 = 63 \bmod 11 = 8$$

The operations $+_m$ and $\cdot_m$ satisfy the properties :

- Closure properties
- Associativity
- Commutativity
- Identity elements
- Additive inverse
- Distributivity