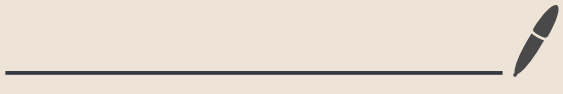
Unit 1

Number theory



Divisibility: An integer b is divisible by an integer a $(a \neq 0)$ if there is an integer k such that $b = ka$, and we write $a \mid b$.

If b is not divisible by a, we write $a \nmid b$.

Ex: $2 \mid 16$, $3 \mid 15$, $5 \nmid 16$

Note that $a \mid b$ doesnot mean that $\frac{a}{b}$ is defined.

In particular,

$0 \mid a$ is true

$a \mid 0$ is false unless $a = 0$

$2 \mid a \Rightarrow a$ is Even

Thm 1:

i) $a \mid b$ implies $a \mid bc$ for any integer c.

ii) $a \mid b$ and $b \mid c$ imply $a \mid c$.

iii) $a \mid b$ and $a \mid c$ imply $a \mid bx+cy$ for any integers x and y.

iv) $a \mid b$ and $b \mid a$ imply $a = \pm b$

v) $a \mid b$, $a > 0$, $b > 0$, imply $a \leq b$.

pf: iii) Given $a \mid b$ and $a \mid c$

$\Rightarrow b = am$ and $c = an$ for some integers m and n

$\Rightarrow bx = amx$ and $cy = any$ for any $x, y \in \mathbb{Z}$

$\Rightarrow bx + cy = a(mx+ny)$

$\Rightarrow bx + cy = ak$ where $k = mx+ny$

$\Rightarrow a \mid bx+cy$ by defn.

Thm 2: [Division algorithm]:

Given any integers a and b, $(a>0)$ there exist unique integers q and r such that

dividend — b = q (quotient) a (divisor) + r (remainder), $0 \le r < a$.

If $a \nmid b$, then $0 < r < a$. (and if $a|b$, $r=0$)

Ex: $a=11$, $b=101$

$101 = 11 \cdot 9 + 2$

$$\begin{array}{r} 9 \\ 11 \overline{)\,101} \\ \underline{99} \\ 2 \end{array}$$

Ex: $a=3$, $b=-11$

$-11 = -4 \cdot 3 + 1$

$$\begin{array}{r} -4 \\ 3 \overline{)\,-11} \\ \underline{-12} \\ 1 \end{array}$$

Greatest Common divisor (gcd)

Defn: Let b and c be integers. Then the largest integer g that divides both b and c is called gcd of b and c

OR

d is a common divisor of b and c if

$d|b$ and $d|c$.

g is called gcd of b and c

if i) $g|b$ and $g|c$

ii) If d is any common divisor, then $d|g$.

Notation: gcd of b and c is denoted by

$\gcd(b,c)$ or (b,c)

Ex: i) Let $a=5$ and $b=15$. Then $(a,b) = 5$

ii) $(12, 20) = 4$

ii) $(13, 155) = 1$

Defn: Integers a and b are said to be relatively prime or Coprime iff $\gcd(a,b)=1$

Ex: 4 and 15 are Coprime. Since $(4,15)=1$

gcd as linear combination

Thm3 [Bézout's thm]: If $(b,c)=g$, then there exist integers x_0 and y_0 such that $g = bx_0 + cy_0$

Moreover, least positive integer of the set $\{ bx+cy \mid x, y \in \mathbb{Z} \}$ is gcd of b and c

Ex: $\gcd(6, 15) = 3$

we have $x_0 = 3$ and $y_0 = -1$ such that

$6x_0 + 15y_0 = 6(3) + 15(-1) = 3$

Corollary: For any $a, b, d \in \mathbb{Z}$. A linear eqn

$$ax + by = d$$

has integer solution if and only if

$\gcd(a,b)$ divides d (d is multiple of $\gcd(a,b)$)

Ex1: $5x + 2y = 3$ has integer soln, since $(5,2)=1$ and $1 \mid 3$.

Ex2: $6x + 20y = 5$ doesnot have integer soln,

since $(6,20)=2$ and $2 \nmid 5$.

Note: If $ax+by=d$ has one solution, then it has infinitely many solutions.

For instance, if x_0 and y_0 is a soln, the for every k $x_0 - kb$ and $y_0 + ka$ is also a soln

Thm 4: For any positive integer m,

$$(ma, mb) = m(a,b)$$

pf: By Bezout's thm:

$$(ma, mb) = \text{least +ve integer of } \{max + mby \mid x, y \in \mathbb{Z}\}$$

$$= m \times \text{least +ve integer of } \{ax + by \mid x, y \in \mathbb{Z}\}$$

$$= m(a,b)$$

Corollary: If $d \mid a$ and $d \mid b$ and $d > 0$, then

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

If $(a,b) = g$, then $\left(\frac{a}{g}, \frac{b}{g}\right) = 1$.

pf: In thm 4 replace m by d, a by $\frac{a}{d}$ and b by $\frac{b}{d}$

we get $(a,b) = d\left(\frac{a}{d}, \frac{b}{d}\right)$

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

Second assertion is the special case of the first obtained by using $\gcd(a,b) = g$ in the role of d.

Ex: 1) $(48, 72) = 24$

and $\left(\frac{48}{6}, \frac{72}{6}\right) = (8, 12) = 4 = \frac{24}{6}$

2) $(12, 15) = 3$,

and $\left(\frac{12}{3}, \frac{15}{3}\right) = (4,5) = 1$

Thm 5: For any integer x, $(a,b) = (b,a) = (a,-b) = (a, b+ax)$

Pf: Denote (a,b) by d and $(a, b+ax)$ by g.

We need to S.T $d = g$.

Since $(a,b) = d$,

$\Rightarrow d|a$ and $d|b$

$\Rightarrow d|(ax+b)$, (by Thm 1 (iii))

but $(a, b+ax) = g$

$\therefore d|g$ — ① by the defn of gcd

We have $(a, b+ax) = g$

$\Rightarrow g|a$ and $g|b+ax$

$\Rightarrow g|a(-x)+b+ax$

$\Rightarrow g|b$

but $(a,b) = d$

$\therefore g|d$ — ②

From ① and ② $d = g$.

Thm 6: If $c|ab$ and $(b,c) = 1$, then $c|a$

Methods to find gcd (a,b), $a < b$

1) Let us list all no.s from 1 to a

$1, 2, 3, 4, 5, \cdots, a$.

Then we find the largest no. that divides both a and b.

# of steps in an algorithm $\approx$ Constant $\times$ a

2) Find prime factorization of a and b.

Suppose $a = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k}$

and $b = p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} \cdots p_k^{\beta_k}$

Then $$\gcd(a,b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_k^{\min(\alpha_k,\beta_k)}$$

For instance, $a = 130 = 2 \times 3^0 \times 5^1 \times 13^1$

$b = 240 = 2^4 \times 3 \times 5 \times 13^0$

$$(130, 240) = 2 \times 5 = 10$$

# of step in an algorithm $\approx$ Constant $\times \sqrt{a}$

3) Euclid's Algorithm

Thm 7 [Euclid's algorithm]

Given two integers b and $c > 0$, we make a repeated application of division algorithm,

$b = c q_1 + r_1, \quad 0 < r_1 < c$

$c = r_1 q_2 + r_2, \quad 0 < r_2 < r_1$

$r_1 = r_2 q_3 + r_3, \quad 0 < r_3 < r_2$

$\vdots$

$r_{j-2} = r_{j-1} q_j + r_j, \quad 0 < r_j < r_{j-1}$

$r_{j-1} = r_j q_{j+1} + 0$

$\gcd(c, b)$
$= (c, b - cq_1)$ (by thm 5)
$= (c, r_1)$
$= (r_2, r_1)$
$= (r_3, r_2)$
$\vdots$
$= (r_j, r_{j-1})$
$= (0, r_j) = r_j$

The $\gcd(b,c) = r_j$, the last non-zero remainder

Further, values x_0 and y_0 in the linear Eqn

$$bx + cy = \gcd(b,c)$$

is obtained by writing r_j as linear combination of b and c.

Ex: Find gcd g of 42823 and 6409 and find integers x and y to satisfy

$$42823x + 6409y = g \qquad (6409, 42823)$$

Soln:

$42823 = \underset{q_1}{6} \cdot 6409 + \underset{r_1}{4369} \quad -(1)$ $\quad = (6409, 42823 - 6 \cdot 6409)$

$6409 = \underset{q_2}{1} \cdot 4369 + \underset{r_2}{2040} \quad -(2)$ $\quad = (6409, 4369)$

$\quad = (4369, 2040)$

$4369 = \underset{q_3}{2} \cdot 2040 + \underset{r_3}{289} \quad -(3)$ $\quad = (2040, 289)$

$2040 = \underset{q_4}{7} \cdot 289 + \underset{r_4}{17} \quad -(4)$ $\quad = (289, 17)$

$289 = \underset{q_5}{17} \cdot 17 + 0 \quad -(5)$ $\quad = (17, 0) = 17$

Thus $(42823, 6409) = 17$

To find x and y that satisfy

$$42823x + 6409y = 17$$

(4) $\Rightarrow$ $17 = 2040 + 289(-7) \quad -(6)$

(3) $\Rightarrow$ $289 = 4369 + 2040(-2) \quad -(7)$

Sub (7) in (6)

$$17 = 2040 + (4369 + 2040(-2))(-7)$$

$$= 4369(-7) + 2040(15) \quad -(8)$$

(2) $\Rightarrow$ $2040 = 6409 + 4369(-1) \quad -(9)$

Sub (9) in (8),

$$17 = 4369(-7) + (6409 + 4369(-1))(15)$$

$$= 6409(15) + 4369(-22) \quad -(10)$$

(1) $\Rightarrow$ $4369 = 42823 + 6409(6)$ — (11)

Sub (11) in (10)

$$17 = 6409(15) + (42823 + 6409(6))(-22)$$

$$\Rightarrow 17 = 42823(-22) + 6409(147)$$

Thus $x = -22$ and $y = 147$ is a soln.

Defn: (least common multiple): The integers $a_1, a_2, \dots a_n$ all different from zero, have a common multiple b if $a_i | b$ for $i = 1, 2, \dots n$.

lcm

The least of the +ve common multiples is called lcm, and it is denoted by $[a_1, a_2, \dots, a_n]$.

Note: If $h = [a_1, a_2, \dots, a_n]$, then common multiples of a_i's are $0, \pm h, \pm 2h, \pm 3h, \dots$

Thm 8: Let a and b be integers. Then

$$[a,b] \cdot (a,b) = |ab|$$

pf: Suppose $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$

Then $(a,b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \dots p_k^{\min(\alpha_k, \beta_k)}$

$$[a,b] = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \dots p_k^{\max(\alpha_k, \beta_k)}$$

Thus $(a,b)\,[a,b] = |ab|$.

Primes

Defn: An integer $p > 1$ is called a prime no., or a prime, in case there is no divisor d of p satisfying $1 < d < p$.
If an integer $a > 1$ is not a prime, it is called composite no.

Note: There are infinitely many primes. (Prove)

Thm 9: [The fundamental Theorem of arithmetic]

Every integer $n > 1$ can be expressed as product of primes (with perhaps only one factor)

Ex: $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2$; $1024 = 2^{10}$
$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$; $641 = 641$

of divisors of n, $\tau(n)$

Let $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots p_k^{\alpha_k}$ Then

$$\tau(n) = (\alpha_1+1)(\alpha_2+1)\cdots(\alpha_k+1)$$

Because # of divisors of $p_k^{\alpha_1} = \alpha_k + 1$ and $\tau(mn) = \tau(m)\tau(n)$ if $(m,n)=1$

$\therefore$ the answer.

Sum of divisors of n, $\sigma(n)$

Let $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Then

$$\sigma(n) = \left(\frac{p_1^{\alpha_1+1}-1}{p_1-1}\right)\left(\frac{p_2^{\alpha_2+1}-1}{p_2-1}\right)\cdots\left(\frac{p_k^{\alpha_k+1}-1}{p_k-1}\right)$$

$$\sigma(n) = \prod_{m=1}^{k}\left(\frac{p_m^{\alpha_m+1}-1}{p_m-1}\right)$$

Because Sum of divisors of $p_1^{\alpha_1} = \left(p_1^0 + p_1^1 + p_1^2 + \cdots + p_1^{\alpha_1}\right)$

$$= \frac{\left(p_1^{\alpha_1+1}-1\right)}{p_1-1}$$

and $\sigma(mn) = \sigma(m)\sigma(n)$ if $(m,n)=1$.

Ex: Let $n = 504$. Find i) $\tau(n)$, $\sigma(n)$ and product of +ve divisors of n.

Soln: $504 = 2^3 \times 3^2 \times 7$

$$\tau(n) = (3+1)(2+1)(1+1)$$
$$= 4 \times 3 \times 2 = 24$$

$$\sigma(n) = \left(\frac{2^4-1}{2-1}\right)\left(\frac{3^3-1}{3-1}\right)\left(\frac{7^2-1}{7-1}\right)$$
$$= 15 \times \frac{26}{2} \times \frac{48}{6}$$
$$= 15 \times 13 \times 8 = 1560$$

$2 \mid 504$
$2 \mid 252$
$2 \mid 126$
$3 \mid 63$
$3 \mid 21$
7

Simple method for primality testing

Let $n \in \mathbb{Z}^+$. Then n is a prime if there is no +ve integer, $d \leq \sqrt{n}$ such that $d \mid n$.

Also, we can say that n is a prime if there is no prime $p \leq \sqrt{n}$ such that $p \mid n$.

Because if one of the factors of n is $\geq \sqrt{n}$, then other will be $\leq \sqrt{n}$, vice versa.

Ex: To check 157 is a prime or not.

Consider no.s $\leq \sqrt{157}$

No.s are 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12

primes in these no.s are

2, 3, 5, 7, 11

No numbers divide 157. $\therefore$ 157 is a prime.

we understand

i) the definition of Congruences

ii) Arithmetic operations on congruence modulo m.

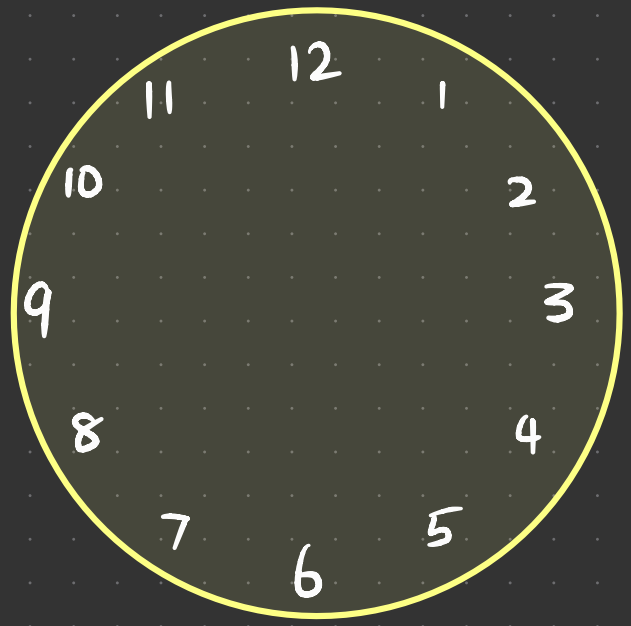
- Addition mod m
- Multiplication mod m

In the world of clocks there are only 12 no.s

0 1 2 3 4 5 6 7 8 9 10 11

This world is called

'Congruence modulo 12'.



Clock

Any integer x is same as one of these 12 no.s.

For instance,

13 is same as 1

55 is same as 7

93 is same as 9

−31 is same as 5

For instance,

13 is same as 1

we say 13 is congruent to 1 modulo 12

we write as $13 \equiv 1 \pmod{12}$

55 is same as 7, $55 \equiv 7 \pmod{12}$

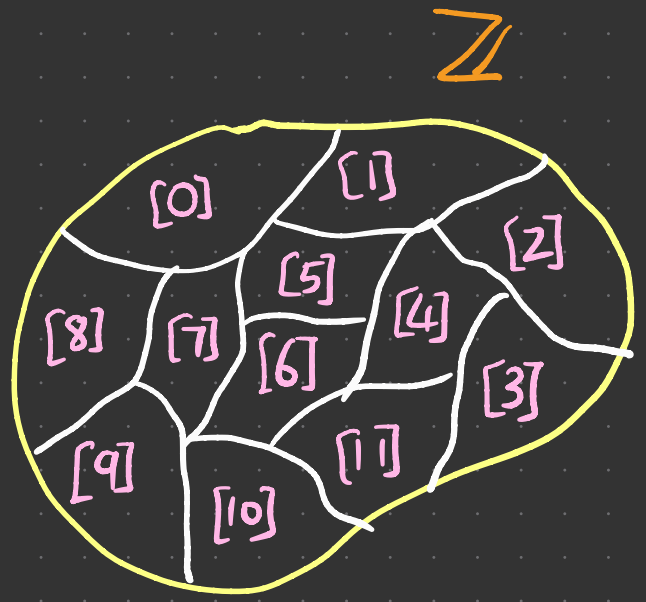
93 is same as 9, $93 \equiv 9 \pmod{12}$

-31 is same as 5, $-31 \equiv 5 \pmod{12}$

The relation congruence mod 12 partitions set of integers, $\mathbb{Z}$ into 12 parts.

i.e,

$$\mathbb{Z} = [0] \cup [1] \cup [2] \cup [3] \cup [4] \cup [5] \cup [6] \cup [7] \cup [8] \cup [9] \cup [10] \cup [11]$$



where

$[0]$ = set of integers congruent to $0 \bmod 12$

$= \{ x \mid x \equiv 0 \pmod{12} \}$

$= \{ 12k, \ k \in \mathbb{Z} \}$

We call 'the congruence class of 0 modulo 12'.

To be particular,

we also denote it by $[0]_{12}$.

Similarly

$$[1] = \{12k+1, \quad k \in \mathbb{Z}\}$$

$$[2] = \{12k+2, \quad k \in \mathbb{Z}\}$$

$$[3] = \{12k+3, \quad k \in \mathbb{Z}\}$$

$$\vdots$$

$$[11] = \{12k+11, \quad k \in \mathbb{Z}\}$$

Note that distinct congruence classes are disjoint

The set of distinct Congruences classes modulo 12 is denoted by $\mathbb{Z}_{12}$

i.e,

$$\mathbb{Z}_{12} = \{[0], [1], [2], \ldots, [11]\}$$

In general,

Set of distinct congruences classes modulo m is

$$\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\}$$

Henceforth, we can define Congruences as follow:

For $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$

$$a \equiv b \pmod{m}$$

iff both a and b belongs to same Congruence class modulo m.

Notation: For any $a \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$

$a \pmod m$ is a *remainder* when a is divided by m.

Ex:

1) $5 \pmod 4 = 1$

2) $93 \pmod 7 = 2$

3) $-14 \pmod 3 = 1$

For $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, we say

$$a \equiv b \pmod{m}$$

iff

$$a \pmod{m} = b \pmod{m}$$

Arithmetic on Congruence modulo m

Addition modulo m, $\oplus_m$

For any $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$

$$a \oplus_m b = a + b \pmod{m}$$

Ex:

1) $12 \oplus_7 14 = 12 + 14 \pmod{7} = 26 \pmod{7} = 5$

2) $41 \oplus_6 13 = 54 \pmod{6} = 0$

Arithmetic on Congruence modulo m

Multiplication modulo m, $\otimes_m$ or $\odot_m$

For any $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$

$$a \otimes_m b = a \times b \pmod{m}$$

Ex:

1) $12 \otimes_7 14 = 12 \times 14 \pmod{7} = 0$

2) $41 \otimes_6 13 = 5$

Additive and Multiplicative identity of Congruence mod m

Additive identity is 0 (any element in [0])

In general, mk, $k \in \mathbb{Z}$

Multiplicative identity is 1 (any element in [1])

In general, $mk+1$, $k \in \mathbb{Z}$

Congruences

Defn: For any $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$ we say

$$a \equiv b \pmod{m}$$

$$\Leftrightarrow \quad a - b = mk \text{ for some } k \in \mathbb{Z}$$

$$\text{or} \quad m \mid (a-b)$$

If a is not congruent to b mod m, then we write $a \not\equiv b \pmod{m}$

Ex: $15 \equiv 1 \pmod{7}$, since $7 \mid (15-1)$

$19 \not\equiv 3 \pmod{5}$, since $5 \nmid (19-3)$

Remark: For any $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$.
The following statements are Equivalent

1) $a \equiv b \pmod{m}$
2) $m \mid (a-b)$
3) Both a and b belong to same congruence class mod m.
4) $a \pmod{m} = b \pmod{m}$

Complete residue system modulo m

Defn: The set

$$x_0, x_1, x_2, \ldots, x_{m-1}$$

is said to be complete residue system modulo m if for any integer y there is one and only x_j such that $y = x_j \pmod{m}$.

Further, we see that $x_i \not\equiv x_j \pmod{m}$ when $i \neq j$.

Here each x_i is a representative from distinct Congruence classes modulo m.

Ex: For $m=7$

1) $0, 1, 2, 3, 4, 5, 6$ is complete residue system mod 7.

2) $14, 15, 16, 17, 18, 19, 20$ is complete residue sytem mod 7.

It is obvious that there are infinitely many residue system modulo m.

Modular Arithmetic

Defn: If a and b are integers and m is a +ve integer, then a is congruent to b modulo m, we write

$a \equiv b \pmod{m}$, if $m \mid (a-b)$ (m divides $(a-b)$)

if $a \not\equiv b \pmod{m}$, then $m \nmid (a-b)$

Notation: $a \bmod m$ is a remainder when a is divided by m.

Ex: i) $15 \equiv 3 \pmod{4}$, since $4 \mid (15-3)$

ii) $29 \equiv 7 \pmod{11}$

iii) $33 \not\equiv 5 \pmod{8}$

iv) $19 \pmod{3} = 1$, since 1 is the remainder when 19 is divided by 3.

Thm 10: Let a and b be integers, and m be a +ve int. Then $a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$.

Thm 11: i) $a \equiv b \pmod{m}$, $b \equiv a \pmod{m}$, and $(a-b) \equiv 0 \pmod{m}$ are equivalent st. mts

ii) If $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

iii) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m}.$$

iv) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$

v) If $a \equiv b \pmod{m}$ and $d \mid m$, $d > 0$, then

$a \equiv b \pmod{d}$

vi) If $a \equiv b \pmod{m}$ then $ac \equiv bc \pmod{mc}$ for $c > 0$.

pf iii) Let $a \equiv b \pmod m$ and $c \equiv d \pmod m$,

$\Rightarrow m \mid (a-b)$ and $m \mid (c-d)$

$\Rightarrow m \mid [(a-b)+(c-d)]$

$\Rightarrow m \mid [(a+c)-(b+d)]$

$\Rightarrow a+c \equiv b+d \pmod m$.

pf iv) Let $a \equiv b \pmod m$ and $c \equiv d \pmod m$,

$\Rightarrow m \mid (a-b)$ and $m \mid (c-d)$

$\Rightarrow m \mid [(a-b)x + (c-d)y]$ for any $x, y \in \mathbb{Z}$

put $x = c$, $y = b$

$\Rightarrow m \mid [(a-b)c + (c-d)b]$

$\Rightarrow m \mid (ac - bd)$

$\Rightarrow ac \equiv bd \pmod m$.

pf v) Given $a \equiv b \pmod m$ and $d \mid m$

$\Rightarrow m \mid (a-b)$ and $d \mid m$

$\Rightarrow d \mid m$ and $m \mid (a-b)$

$\Rightarrow d \mid (a-b)$

$\Rightarrow a \equiv b \pmod d$

Thm 12: i) $ax \equiv ay \pmod m$ iff $x \equiv y \left(\mod \frac{m}{(a,m)}\right)$

ii) if $(a, m) = 1$ and $ax \equiv ay \pmod m$, Then

$x \equiv y \pmod m$.

iii) $x \equiv y \pmod{m_i}$ for $i = 1, 2, 3, \ldots, r$ if f

$x \equiv y \pmod{[m_1, m_2, m_3, \ldots, m_r]}$

pf i) If $ax \equiv ay \pmod{m}$, then $m \mid (ax - ay)$

$\Rightarrow ax - ay = km$ for some $k \in \mathbb{Z}$.

$\Rightarrow \frac{a}{(a,m)}(x-y) = \frac{k}{(a,m)} m$

$\Rightarrow \frac{m}{(a,m)} \mid \frac{a}{(a,m)}(x-y)$

∵ If $(a,b) = g$, $\left(\frac{a}{g}, \frac{b}{g}\right) = 1$

∵ If $(a,b) = 1$ and $a \mid bc$, then $a \mid c$

But $\left(\frac{a}{(a,m)}, \frac{m}{(a,m)}\right) = 1$. Therefore $\frac{m}{(a,m)} \mid (x-y)$

That is $x \equiv y \pmod{\frac{m}{(a,m)}}$.

Conversely, If $x \equiv y \pmod{\frac{m}{(a,m)}}$, then

$ax \equiv ay \pmod{\frac{am}{(a,m)}}$ ($am = km$, $k = \frac{a}{(a,m)}$)

$\Rightarrow ax \equiv ay \pmod{m}$ (from thm 11(v))

pf ii) It is a special case of i)

pf iii) If $x \equiv y \pmod{m_i}$ for $i = 1, 2, \ldots, r$, then

$m_i \mid (x-y)$ for $i = 1, 2, \ldots r$.

That $(x-y)$ is multiple of $m_1, m_2, \ldots m_r$ and

$\therefore [m_1, m_2, \ldots, m_r] \mid (x-y)$

$\Rightarrow x \equiv y \pmod{[m_1, m_2, \ldots, m_r]}$

Conversely, if $x \equiv y \pmod{[m_1, m_2, \ldots, m_r]}$, then

$x \equiv y \pmod{m_i}$ $\quad (\because m_i \mid [m_1, m_2, \ldots m_r])$

(from thm 11 (v))

Ex: Find the remainder when 6^{100} is divided by 7.

Soln: We have $6 \equiv -1 \pmod 7$

$\Rightarrow 6^2 \equiv (-1)^2 \pmod 7$

$\Rightarrow (6^2)^{50} \equiv 1^{50} \pmod 7$

$\Rightarrow 6^{100} \equiv 1 \pmod 7$

$\therefore$ 1 is the remainder.

Ex: Compute $2^{160} \pmod 7$

Soln: We have $2^3 \equiv 1 \pmod 7$

$\Rightarrow (2^3)^{53} \equiv 1^{53} \pmod 7$

$\Rightarrow 2^{159} \equiv 1 \pmod 7$

$\Rightarrow 2 \cdot 2^{159} \equiv 2 \pmod 7$

$\Rightarrow 2^{160} \equiv 2 \pmod 7$

$\therefore$ 2 is the remainder.

Defn: If $x \equiv y \pmod m$ then y is called residue of x modulo m.

A set $x_1, x_2, \ldots, x_m$ is called complete residue system modulo m if for every integer y there is one and only x_j such that

$y \equiv x_j \pmod m$

Ex: $0, 1, 2, 3, 4$ is complete residue system modulo 5

Also, $5, 6, 7, 8, 9$ is "

$\Rightarrow$ There are infinitely many complete residue system.

Linear congruences

A congruence of the form

$$ax \equiv b \pmod{m}$$

where m is a +ve int, a and b are integers, and x is a variable, is called a linear congruence.

Thm 13: If $(a, m) = 1$, then there is an int x such that $ax \equiv 1 \pmod{m}$.

Any two such x are congruent $\pmod{m}$.

If $(a, m) > 1$ then there is no such x.

pf: If $(a, m) = 1$, then there exist x and y such that

$$ax + my = 1.$$

$$\Rightarrow ax = 1 - my$$

$$\Rightarrow ax - 1 = m(-y)$$

$$\Rightarrow m \mid (ax - 1)$$

$$\Rightarrow ax \equiv 1 \pmod{m}.$$

Conversely, if $ax \equiv 1 \pmod{m}$

$$\Rightarrow m \mid ax - 1$$

$$\Rightarrow ax - 1 = m(k) \quad \text{for some } k \in \mathbb{Z}$$

$$\Rightarrow ax + my = 1, \quad (y = -k)$$

$$\Rightarrow (a, m) = 1$$

If $ax_1 \equiv 1 \pmod m$ and $ax_2 \equiv 1 \pmod m$ $(x_1 \neq x_2)$

$\Rightarrow ax_1 \equiv 1 \pmod m$ and $1 \equiv ax_2 \pmod m$

$\Rightarrow ax_1 \equiv ax_2 \pmod m$

$\Rightarrow x_1 \equiv x_2 \pmod m$

| $a \equiv b \pmod m$
| $c \equiv d \pmod m$
| $ac \equiv bd \pmod m$

Thus, there is only one soln in complete residue system mod m.

Notation: For any $m \in \mathbb{Z}^+$,

$$\mathbb{Z}_m = \{0, 1, 2, 3, 4, \cdots, m-1\}.$$

These are distinct elements in congruence modulo m.

Multiplicative inverse

If $ab \equiv 1 \pmod m$, then b is called multiplicative inverse of a modulo m.

Further, a has multiplicative inverse in congruence modulo m iff $(a, m) = 1$.

If multiplicative inverse of a exists, then it is denoted by $\bar{a}$.

Ex: Find all elements which has multiplicative inverses in congruence mod 10 i.e, $\mathbb{Z}_{10}$.

Soln: $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

Clearly, multiplicative inverses are

1, 3, 7, 9

Since $(1, 10) = 1$, $(3, 10) = 1$, $(7, 10) = 1$, $(9, 10) = 1$

Further, $\bar{1} = 1$, $\bar{3} = 7$, $\bar{7} = 3$, $\bar{9} = 9$.

Notation: Set of all multiplicative inverses of $\mathbb{Z}_m$ is denoted by $\mathbb{Z}_m^\times$

For instance, $\mathbb{Z}_{10}^\times = \{1, 3, 7, 9\}$.

Ex: Find an inverse of 3 mod 7.

Soln: To find x such that

$$3x \equiv 1 \pmod 7.$$

Inverse exist because $(3,7)=1$

∴ Inverse of 3 mod 7 is 5. (We found it by inspection)

$x=1,\ 3 \not\equiv 1 \pmod 7$

$x=2,\ 6 \not\equiv 1 \pmod 7$

$x=3,\ 9 \not\equiv 1 \pmod 7$

$x=4,\ 12 \equiv 1 \pmod 7$

$x=5,\ 15 \equiv 1 \pmod 7$

Let us find inverse by Euclidean algorithm.

WKT $(3,7)=1$, $\exists$ x and y such that

$$3x+7y=1. \quad \text{——} (*),$$ where x is inv of 3.

Consider

$$7 = 2\cdot 3 + 1 \quad \text{——} (1)$$
$$3 = 3\cdot 1$$

$(1) \Rightarrow 1 = 7 + 3(-2)$ ——(2)

From (*) and (2), $x=-2$, $y=1$

Thus, inverse $x = -2$

In general, inverse $x \equiv 5 \pmod 7$.

Ex 2: Find an inverse of 101 modulo 4620.

Soln: We have to x such that

$$101x \equiv 1 \pmod{4620} \Rightarrow 101x - 1 = 4620k,\ k \in \mathbb{Z}$$
$$\Rightarrow 101x + 4620y = 1,\ y = -k$$

Consider

$$4620 = 101 \cdot \underset{\sim}{45} + \underset{\sim}{75} \quad (1)$$
$$\sim q_1 \quad \sim r_1$$

$$101 = 75 \cdot \underset{\sim}{1} + \underset{\sim}{26} \quad (2)$$
$$\sim q_2 \quad \sim r_2$$

$$75 = 26 \cdot \underset{\sim}{2} + \underset{\sim}{23} \quad (3)$$
$$\sim q_3 \quad \sim r_3$$

$$26 = 23 \cdot \underset{\sim}{1} + \underset{\sim}{3} \quad (4)$$
$$\sim q_4 \quad \sim r_4$$

$$23 = 3 \cdot \underset{\sim}{7} + \underset{\sim}{2} \quad (5)$$
$$\sim q_5 \quad \sim r_5$$

$$3 = 2 \cdot \underset{\sim}{1} + \underset{\sim}{1} \quad (6)$$
$$\sim q_6 \quad \sim r_6$$

$$2 = 1 \cdot \underset{\sim}{2} + 0 \quad (7)$$
$$\sim q_7$$

Thus $(101, 4620) = 1$. Hence inverse x exist.

Find x and y such that

$$101x + 4620y = 1 \quad (*)$$ where x is inv.

(6) $\Rightarrow$ $1 = 3 + 2(-1)$ — (8)

(5) $\Rightarrow$ $2 = 23 + 3(-7)$ — (9)

Sub (9) in (8)

$$1 = 3 + (23 + 3(-7))(-1)$$

$$\Rightarrow 1 = 23(-1) + 3(8) \quad (10)$$

(4) $\Rightarrow$ $3 = 26 + 23(-1)$ — (11)

Sub (11) in (10)

$$1 = 23(-1) + (26 + 23(-1))(8)$$
$$\Rightarrow 1 = 26(8) + 23(-9) \quad \text{— (12)}$$

(3) $\Rightarrow$ $23 = 75 + 26(-2)$

Sub in (12),

$$1 = 26(8) + (75 + 26(-2))(-9)$$
$$\Rightarrow 1 = 75(-9) + 26(26) \quad \text{— (13)}$$

(2) $\Rightarrow$ $26 = 101 + 75(-1)$

Sub in (13),

$$1 = 75(-9) + (101 + 75(-1))(26)$$
$$\Rightarrow 1 = 101(26) + 75(-35) \quad \text{— (14)}$$

(1) $\Rightarrow$ $75 = 4620 + 101(-45)$

Thus, $1 = 101(26) + (4620 + (101)(-45))(-35)$

$\Rightarrow 1 = 4620(26) + 101(1601)$

Hence $x \equiv 1601 \pmod{4620}$.

Thm 14: Let a, b and $m > 0$ be given integers, and put $g = (a, m)$.

The congruence $ax \equiv b \pmod{m}$ has a soln iff $g \mid b$.

If this condition is met, then the solns form an arithmetic progression with common difference $\frac{m}{g}$, giving g solns $(\text{mod } m)$.

Pf : Let $ax \equiv b \pmod m$ has a soln.

$\Rightarrow \quad m \mid (ax-b)$ for some $x \in \mathbb{Z}$

$\Rightarrow \quad ax - b = mk, \quad \exists\ k \in \mathbb{Z}$

$\Rightarrow \quad ax + m(-k) = b \quad$ — (1)

$g = (a,m) \Rightarrow g \mid a$ and $g \mid m$

$\Rightarrow g \mid (ax + m(-k))$

$\Rightarrow g \mid b.$ (from (1))

Conversely, let $g \mid b$ and $g = (a,m)$.

$\Rightarrow \quad g \mid b,\ g \mid a$ and $g \mid m$

$\Rightarrow \quad b = u_1 g,\ a = u_2 g,\ m = u_3 g$ for some $u_1, u_2, u_3 \in \mathbb{Z}$

Consider

$$ax \equiv b \pmod m$$
$$\Rightarrow u_2 g\, x \equiv u_1 g \pmod{u_3 g}$$
$$\Rightarrow u_2 x \equiv u_1 \pmod{u_3} \quad — (2)$$

(Note $(u_2, u_3) = 1$ $\because (a,m) = g \Rightarrow \left(\frac{a}{g}, \frac{m}{g}\right) = 1$)

$\because (u_2, u_3) = 1$, inverse of u_2 (i.e $\overline{u_2}$) exist.

$\therefore u_2 \overline{u_2} \equiv 1 \pmod{u_3}$

x by $\overline{u_2}$ to (2),

$$u_2 \overline{u_2}\, x \equiv u_1 \overline{u_2} \pmod{u_3}$$

($\because ax \equiv ay \pmod m \Rightarrow x \equiv y \pmod{\frac{m}{(a,m)}}$)

$$\Rightarrow \quad x \equiv \underbrace{u_1 \overline{u_2}}_{x_0} \pmod{\underbrace{u_3}_{m/g}}$$

$\therefore$ Solns are

$$x_0,\ x_0 + \frac{m}{g},\ x_0 + 2\frac{m}{g},\ \cdots\ x_0 + (g-1)\frac{m}{g} \pmod m.$$

Ex: Find all solns of the congruence

a) $15x \equiv 25 \pmod{35}$

Soln: Here $a=15$, $b=25$ and $m=35$,

$(15, 35) = 5$, and $5 \mid 25$

$\therefore$ five solns exist.

To find solns:

$$15x \equiv 25 \pmod{35}$$

$$\Rightarrow 5 \cdot 3x \equiv 5 \cdot 5 \pmod{35}$$

$$\Rightarrow 3x \equiv 5 \pmod{\frac{35}{(5,35)}}$$

$$\Rightarrow 3x \equiv 5 \pmod{7} \quad \text{——} \ (*)$$

we have

$ax \equiv ay \pmod{m}$

$\Rightarrow x \equiv y \pmod{\frac{m}{(a,m)}}$

By inspection,

$x \equiv 4 \pmod{7}$

is soln of (*)

By Euclid's alg.

Consider the Eqn $3x + 7y = 5$

$$7 = 3 \cdot 2 + 1$$

$$\Rightarrow 1 = 7 + 3(-2)$$

$$\Rightarrow 5 = 7(5) + 3(-10)$$

$$\Rightarrow x \equiv -10 \equiv 4 \pmod{7}$$

Solns of given linear congruences are

$4, \ 4+1\cdot7, \ 4+2\cdot7, \ 4+3\cdot7, \ 4+4\cdot7 \pmod{35}$

i.e, $4, 11, 18, 25, 32 \pmod{35}$.

b) $20x \equiv 4 \pmod{30}$.

Soln: Here $a=20$, $b=4$ and $m=30$

$(20, 30) = 10$. But $10 \nmid 4$. $\therefore$ it has no solns.

c) $3x \equiv 4 \pmod{7}$.

Soln: Here $(3, 7) = 1$ and $1 \mid 4$. $\therefore$ We have 1 soln.

By inspection,

$x \equiv 6 \pmod{7}$

Defn [Euler function]: The number $\phi(m)$ is the number of positive integers less than or equal to m that are relatively prime to m.

Ex: $m=8$, $\phi(8)=4$
$m=5$, $\phi(5)=4$

($\because$ No. of +ve ints ≤ 8 and relatively prime to 8 are 1, 3, 5, and 7)

Also, note that $\phi(m)$ = # multiplicative inverses in $\mathbb{Z}_m = |\mathbb{Z}_m^\times|$

Note: 1) If $(m_1, m_2)=1$, then $\phi(m_1 \cdot m_2) = \phi(m_1) \cdot \phi(m_2)$.

Ex: $m = 35 = 5 \cdot 7$

$\phi(35) = \phi(5 \cdot 7) = \phi(5)\phi(7) = 4 \cdot 6 = 24.$

2) If m is any positive integer,

$$\phi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right)$$

Ex: $m=8$. Here $8 = 2^3$

$$\therefore \phi(8) = 8 \cdot \left(1 - \frac{1}{2}\right) = 4$$

Ex: $m=100$

Here $100 = 2^2 \cdot 5^2$

$$\phi(100) = 100 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right)$$

$$= 100 \cdot \frac{1}{2} \cdot \frac{4}{5}$$

$$= 40$$

3) If p is any prime, then

$$\phi(p) = p - 1$$

Ex: $m = 101$ ($\because$ 101 is a prime)

$\phi(101) = 100$

Thm 15 [Fermat Little theorem]: Let p denote a prime. If $p \nmid a$, then

$$a^{p-1} \equiv 1 \pmod{p}$$

For every integer a,

$$a^p \equiv a \pmod{p}$$

Ex: Let $p=5$, $a=4$. Then $4^4 \equiv 1 \pmod{5}$

Ex: Let $p=101$, $a=1542$. Then $1542^{100} \equiv 1 \pmod{101}$

Thm 16 [Euler's generalisation of Fermat's Little thm]:

If $(a,m)=1$, then

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Ex: Let $m=8$, $a=15$.

$\phi(8)=4$ and $15^4 \equiv 1 \pmod{8}$

Ex: Find the remainder when 7^{222} is divided by 11.

Soln: We have to find $7^{222} \bmod 11$.

Here $m=11$

$\phi(11) = 11-1 = 10$ $\quad ((11,7)=1)$

$\therefore$ By Euler's thm,

$7^{\phi(11)} \equiv 1 \pmod{11}$

$\Rightarrow 7^{10} \equiv 1 \pmod{11}$ ——— (1)

By division algorithm

$$222 = 22.10 + 2$$

$$\therefore 7^{222} = 7^{22.10+2}$$

$$= (7^{10})^{22} \cdot 7^2$$

$$\equiv 1^{22} \cdot 49 \qquad (\text{From } ①)$$

$$\equiv 5 \pmod{11}$$

Thus $7^{222} \bmod 11 = 5$.

Ex: Find last two digits of 3333^{4444}

Soln: last two digists of $3333^{4444} = 3333^{4444} \pmod{100}$

(i.e remainder when 3333^{4444} is divided by 100)

Clearly, $(3333, 100) = 1$

$\therefore$ By Euler's thm

$$3333^{\phi(100)} \equiv 1 \pmod{100}$$

$$\Rightarrow 3333^{40} \equiv 1 \pmod{100} \qquad (\phi(100) = 40)$$

By division alg.

$$4444 = 40(111) + 4$$

$$\Rightarrow 3333^{4444} = 3333^{40(111)+4}$$

$$= (3333^{40})^{111} \cdot 3333^4$$

$$\equiv (1)^4 \cdot 3333^4 \pmod{100} \quad — ①$$

But $3333 \equiv 33 \pmod{100}$

$$\Rightarrow 3333^4 \equiv 33^4 \pmod{100} \quad — ②$$

From ① and ②

$$3333^{4444} \equiv 33^4 \pmod{100}$$

$$\equiv 21 \pmod{100}$$

$\therefore$ Last two digits of $3333^{4444} = 21$.

Cryptography

- Crytography is the science of securing data.
- It enables to store sensitive information or transmit it across insecure networks (like the internet)

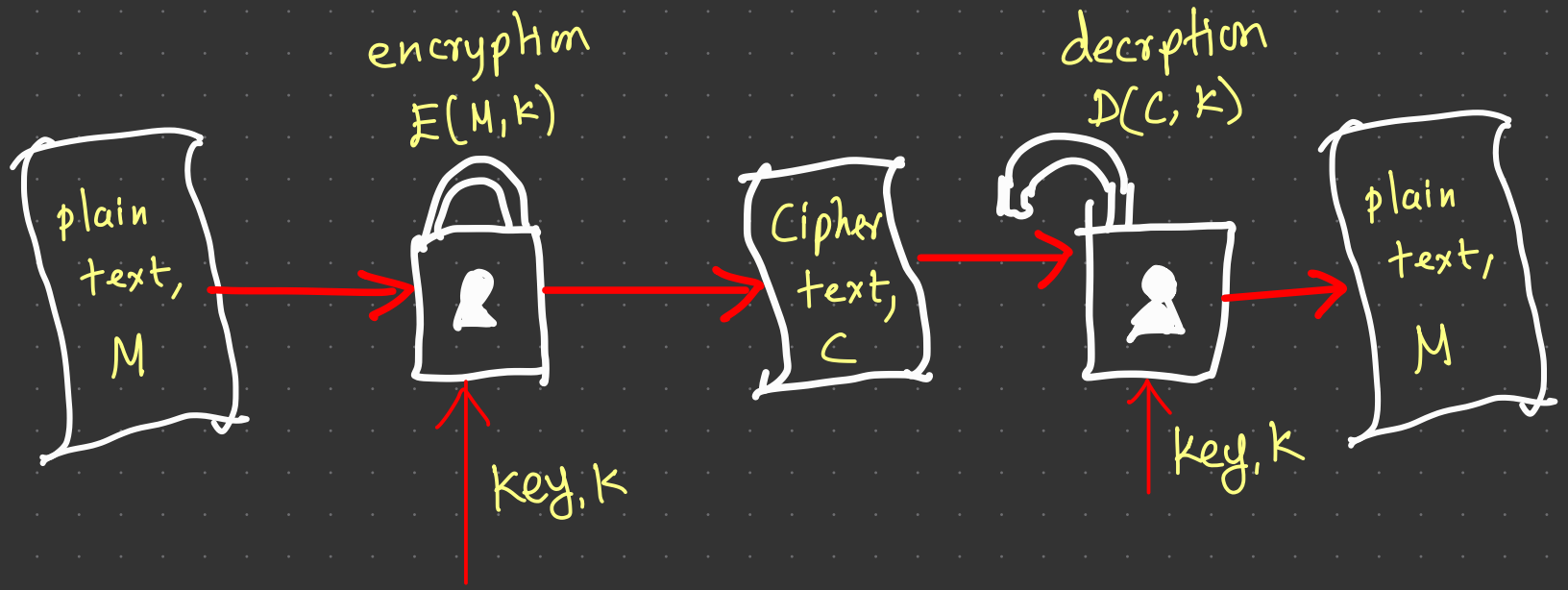
Encryption and decryption

→ The method of disguising plaintext in such a way as to hide its substance is called encryption

→ Encrypted plaintext results in unreadable gibberish called Ciphertext

→ The process of reverting ciphertext to its original plaintext is called decryption

Process


encryption
E(M,K)
decryption
D(C,K)
plain text, M
Cipher text, C
plain text, M
key, K
key, K

Shift Cipher (Caesar cipher)

Idea is to shift letters in alphabet

Suppose key, K = 3

A → D
B → e
⋮
W → Z
X → A
Z → C

Encoding of letters for the shift cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Q	R	S	T	U	V	W	X	Y	Z
16	17	18	19	20	21	22	23	24	25

Both plaintext and the ciphertext are now elements of $\mathbb{Z}_{26}$.

Definition: Shift cipher

Let $x, y, k \in \mathbb{Z}_{26}$, where k is a key.

Encryption : $E(k, x)$, $y \equiv x + k \pmod{26}$

Decryption : $D(k, y)$, $x \equiv y - k \pmod{26}$

# of keys $= 26$

Ex: What is the cipher text (secret msg) produced from the message

"STOP GLOBAL WARMING"

using shift cipher with shift $K = 11$.

Soln: First translate each letters in

STOP GLOBAL WARMING

to corresponding elements in $\mathbb{Z}_{26}$.

we get

18 19 14 15 6 11 14 1 0 11 22 0 17 12 8 13 6.

Encryption: $E(K, x)$, $y \equiv x + 11 \pmod{26}$

Applying it to each no., we get

3 4 25 0 17 22 25 12 11 22 7 11 2 23 19 24 17.

Translating back to letters, we obtain

"DEZA RWZMLW HLCXTYR"

This is cipher text.

Ex2 : Decrypt the ciphertext message

"TPSVI RKKRTB"

Affine Cipher

Key, $K = (a, b)$, $x, y \in \mathbb{Z}_{26}$

Encryption : $E(K, x)$, $y \equiv ax + b \pmod{26}$

Decryption : $D(K, y)$, $x \equiv (y - b)\,\bar{a} \pmod{26}$

($\bar{a}$ is multiplicative inv. of a)

$$\#\text{ of keys, } k = \#a \times \#b$$

$$= \phi(26) \times 26$$

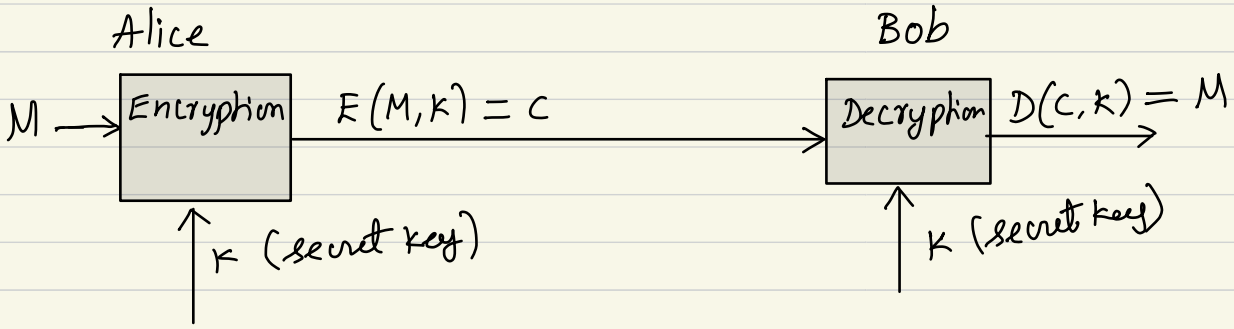
$$= 12 \times 26 = 312$$

Two possible attacks

1) Frequency analysis
2) brute-force

Cryptography

Symmetric cryptosystem.



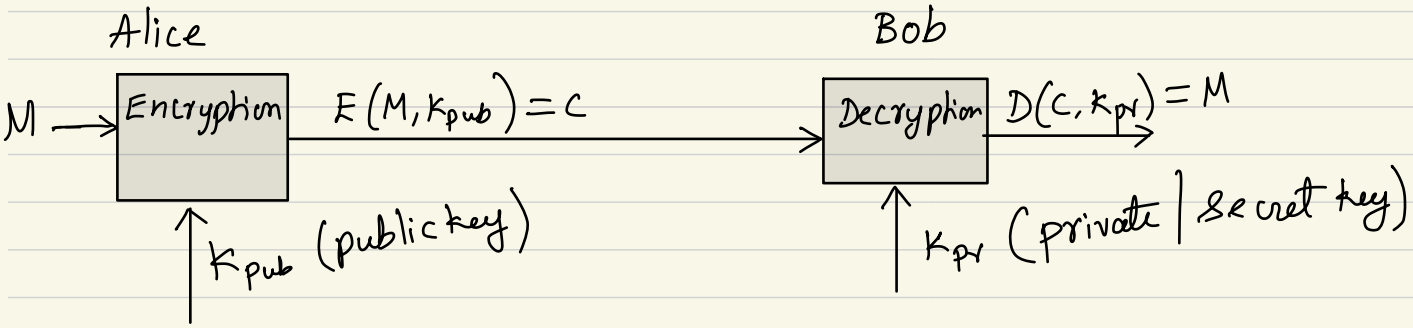
M — Message or plaintext to be sent.

C — Cipher text

K — Secret key

In symmetric cryptosystem same key K (secret key) is used to encrypt and decrypt the message M.

Asymmetric cryptosystem (Public key cryptosystem)



Here we use different keys to encrypt and decrypt messages.

The key we use to encrypt the message is called public key.

and key to decrypt msg is kept secret.

Following are the popularly used Public-key cryptosystem.

1) RSA cryptosystem (Rivest – Shamir – Adleman)

2) Elliptic curve cryptosystem

RSA cryptosystem

a) Key generation

publickey K_{pub}, privatekey K_{pr}

It require computation of the pair (K_{pub}, K_{pr})

1) Choose large primes p, q (200 digits)

2) $n = p \cdot q$

3) $\phi(n) = \phi(p \cdot q) = \phi(p) \cdot \phi(q) = (p-1)(q-1)$

4) Choose $K_{pub} = (n, e)$

where $e \in \{1, 2, 3, \cdots, \phi(n)-1\}$ $\left(\text{i.e, } e \in \mathbb{Z}_{\phi(n)}^{\times}\right)$

such that $(e, \phi(n)) = 1$.

5) Compute $K_{pr} = d$ such that

$d \cdot e \equiv 1 \pmod{\phi(n)}$

For instance
$n = 15 = 3 \cdot 5$
$\phi(15) = 2 \cdot 4 = 8$

Then $e=3$ or $e=5$, or $e=7$

b) Encryption and decryption

Enc:

Given $K_{pub} = (n, e)$, Let M be a message (plain text) (it is an integer belongs to $\mathbb{Z}_n$)

$$C = E(M, K_{pub}) = M^e \pmod{n}.$$

$\left(\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}\right)$

Dec:

Given $K_{pr} = d$, $C \in \mathbb{Z}_n$

$$M = D(C, K_{pr}) = C^d \pmod{n}.$$

Because $de \equiv 1 \pmod{\phi(n)}$

$\Rightarrow de - 1 = t\,\phi(n)$, for some int t

$\Rightarrow de = 1 + t\,\phi(n)$

and $M^{ed} = M^{1+t\phi(n)}$

$\Rightarrow (M^e)^d = M \cdot M^{t(\phi(n))}$

$\Rightarrow C^d \equiv M \cdot 1 \pmod n$ $\left(\because C \equiv M^e \pmod n,\ M^{\phi(n)} \equiv 1 \pmod n\right)$

assume $(M,n)=1$

Suppose $(M,n) \neq 1$. Then $\gcd(M, pq) = p$ or q.

Without loss of generality, we assume $\gcd(M,pq)=p$

$C^d \equiv M^{de} \pmod n$

$\equiv M^{1+t\phi(n)} \pmod n$

$\equiv M^{1+t(p-1)(q-1)} \pmod{pq}$

$\equiv M^{t(p-1)(q-1)} M \pmod{pq}$

Since $\gcd(M,q) = 1$

$\Rightarrow M^{\phi(q)} \equiv 1 \pmod q$

$\Rightarrow M^{q-1} \equiv 1 \pmod q$

$\Rightarrow (M^{(q-1)})^{t(p-1)} \equiv 1 \pmod q$

$\Rightarrow M^{t(p-1)(q-1)+1} \equiv M \pmod q$

$\Rightarrow q \mid (M^{t(p-1)(q-1)+1} - M)$ — (1)

Since $p \mid M$

$\Rightarrow p \mid (M^{t(p-1)(q-1)+1} - M)$ — (2)

From (1) and (2)

$pq = n \mid (M^{t(p-1)(q-1)+1} - M)$

Thus $C^d = M^{t(p-1)(q-1)+1} \equiv M \pmod n$

Ex: Suppose we need to send a msg

$M = 4$ (Any text msg should be first converted to an integer)

a) Key generation

1) Choose $p = 3$ and $q = 11$

2) $n = p \cdot q = 33$

3) $\phi(n) = (p-1)(q-1) = 20$

4) Choose e, let $e = 3$ ($\because 3 < 20$ and $(3, 20) = 1$)

$\therefore K_{pub} = (n, e) = (33, 3)$.

5) Compute $K_{pr} = d$, such that

$$de \equiv 1 \pmod{\phi(n)}$$
$$\Rightarrow 3d \equiv 1 \pmod{20}$$

By inspection, $d = 7$

b) Encryption:

Cipher text, $C = M^e \bmod n$

i.e $C = 4^3 \bmod 33$

$\therefore C = 31$.

The encrypted msg is now $C = 31$. The receiver can get the original msg M by below computation.

c) Decryption:

Original msg, $M = C^d \bmod n$

$= 31^7 \bmod 33$

That is M is the remainder when 31^7 is divided by 33.

The binary expansion of 7 is

$$7 = 2^2 + 2 + 1 = 4 + 2 + 1$$

To compute $31^7 \bmod 33$, we will proceed as follows:

$$31^2 = 961 \equiv 4 \pmod{33}$$

$$31^4 \equiv 4^2 \pmod{33}$$

$$\Rightarrow \quad 31^7 = 31^{4+2+1} = 31^4 \cdot 31^2 \cdot 31 \equiv 16 \cdot 4 \cdot 31 \bmod 33$$

$$\equiv 31 \cdot 31 \pmod{33}$$

$$= 4$$

Thus, $31^7 \pmod{33} = 4 = M$

In this way we can recover the original msg M from the encrypted msg C.