Modular Division

→ For modular division we require multiplicative inverse.

→ Modular multiplicative inverse can be found by greatest common divisor (GCD).

→ Multiplicative inverse exists iff their GCD is 1.

e.g:

* $Z_6 = \{0, 1, 2, 3, 4, 5\}$

$a \in Z_6$

$a^{-1} \bmod 6$ exists iff

$GCD(a, 6) = 1$

So

$5^{-1} \bmod 6$ only exists

* $Z_5 = \{0, 1, 2, 3, 4\}$

$2^{-1} \bmod 5$ exists

$3^{-1} \bmod 5$ exists

$4^{-1} \bmod 5$ exists

If n is a prime number than the maximum members have multiplicative inverse.

→ ~~Two~~ Multiplicative inverse also exists when the number and mod n are relatively prime to each other.

→ Two integers are relatively prime to each other iff their GCD = 1.

Eucledeon Algorithm

It is a way to find GCD.

Lets have an example:

(85 , 34)

$85 = (34 \times 2) + 17$

$34 = (17 \times 2) + 0$

Now,

GCD = 17

(1331 , 1001)

$1331 = (1001 \times 1) + 330$

$1001 = (330 \times 3) + 11$

$330 = (11 \times 30) + 0$

Now GCD = 11

(9888 , 6060)

9888 = 6060 + 3828

6060 = 3828 + 2232

3828 = 2232 + 1596

2232 = 1596 + 636

1596 = 636(2) + 324

636 = 324 + 312

324 = 312 + 12

312 = 12 (26) + 0

GCD = 12 .

Find the values of unknown:

$1331x + 1001y = 11$ extended eucledeon method

$11 = 1001 - 330(3)$

$11 = 1001 - [1331 - 1001]3$

$11 = 1001 - 1331(3) + 1001(3)$

$11 = 1001(4) + 1331(-3)$

So

$x = -3$

$y = 4$

$$213x + 117y = 3$$

Eucledean Algorithrm

$213 = 117 + 96$

$117 = 96(1) + 21$

$96 = 21(4) + 12$

$21 = 12 + 9$

$12 = 9 + 3$

$9 = 3(3) + 0$

$GCD = 3$

Extended eucledean Algorithm

$3 = 12 - 9$

$3 = 12 - (21 - 12)$

$3 = 12 - 21 + 12$

$3 = 12(2) + 21(-1)$

$3 = [96 - 21(4)]2 + 21(-1)$

$3 = 96(2) - 21(8) + 21(-1)$

$3 = 96(2) + 21(-9)$

$3 = 96(2) + [117 - 96](-9)$

$3 = 96(2) + 117(-9) + 96(9)$

$3 = 96(11) + 117(-9)$

$3 = (213 - 117)(11) + 117(-9)$

Scanned with CamScanner

$$3 = 213(11) + 117(-11) + 117(-9)$$
$$3 = 213(11) + 117(-20)$$

Now

$$x = 11$$
$$y = -20$$

$252x + 198y = 18$

Eucledean Algorithm

$$252 = 198(1) + 54$$
$$198 = 54(3) + 36$$
$$54 = 36 + 18$$
$$36 = 18(2) + 0$$
$$GCD = 18$$

Extended Eucledean Algorithm

$$18 = 54 - 36$$
$$18 = 54 - [198 - 54(3)]$$
$$18 = 54 - 198 + 54(3)$$
$$18 = 54(4) + 198(-1)$$
$$18 = (252 - 198)4 + 198(-1)$$
$$18 = 252(4) + 198(-4) + 198(-1)$$
$$18 = 252(4) + 198(-5)$$

Now

$x = 4$

$y = -5$

Calculate multiplicative inverse using eucledean method:

1- Calaulate $5^{-1} \bmod 7$.

$7 = 5(1) + 2$

$5 = 2(2) + 1$

Now:

$1 = 5 - 2(2)$

$1 = 5 - (7-5)2$

$1 = 5 + 7(-2) + 5(2)$

$1 = 5(3) + 7(-2)$

Now

$5^{-1} \bmod 7 = 3 \bmod 7$

Verification:

$= (5 \cdot 3) \bmod 7$

$= 15 \bmod 7$

$= 1 \bmod 7$

Hence verified that

$5^{-1} \bmod 7 = 3 \bmod 7$

2- $8^{-1} \bmod 11 = ?$

$11 = 8(1) + 3$

$8 = 3(2) + 2$

$3 = 2 + 1$

Now:

$1 = 3 - 2$

$1 = 3 - [8 - 3(2)]$

$1 = 3 - 8 + 3(2)$

$1 = 3(3) + 8(-1)$

$1 = (11-8)3 + 8(-1)$

$1 = 11(3) + 8(-3) + 8(-1)$

$1 = 11(3) + 8(-4)$

$-4 \bmod 11 = 7 \bmod 11$

The inverse is $7 \bmod 11$

Verification:

$8^{-1} \bmod 11 = 7 \bmod 11$

$= (8 \cdot 7) \bmod 11$

$= 56 \bmod 11$

$= 1 \bmod 11$

Hence verified that

$8^{-1} \bmod 11 = 7 \bmod 11$

3- $6^{-1} \bmod 9 = ?$

$6^{-1} \bmod 9$ does not exist as they are not relatively prime to each other.

4- $7^{-1} \bmod 9 = ?$

$9 = 7(1) + 2$

$7 = 2(3) + 1$

Now,

$1 = 7 - 2(3)$

$1 = 7 - [9 - 7]3$

$1 = 7 - 9(3) + 7(3)$

$1 = 7(4) + 9(-3)$

$7^{-1} \bmod 9 = 4 \bmod 9$

Verification:

$(7 \cdot 4) \bmod 9$

$= 28 \bmod 9$

$= 1 \bmod 9$

Hence verified

$7^{-1} \bmod 9 = 4 \bmod 9$

5- $9^{-1} \bmod 10 = ?$

$10 = 9(1) + 1$

Extended eucledian method

$1 = 10 - 9$

$1 = 10 + 9(-1)$

$-1 \bmod 10 = 9 \bmod 10$

So

$9^{-1} \bmod 10 = 9 \bmod 10$

verification:

$(9 \cdot 9) \bmod 10$

$= 81 \bmod 10$

$= 1 \bmod 10$

Hence verified that

$9^{-1} \bmod 10 = 9 \bmod 10$

* It also shows that an integer can be an inverse of itself.

Scanned with CamScanner

Affine Cipher

- key k (a, b)

a should be that number whose multiplicative inverse exists.

- It operates on $Z_{26} = \{A, B, .. Z\}$

A	F	K	P	U	Z
0	5	10	15	20	25

- **Encrypit:**

$$y = (ax+b) \bmod 26$$

- **Decrypit:**

$$x = a^{-1}(y-b) \bmod 26$$

Example:

VOTE k(5, 7)

V	O	T	E
↓	↓	↓	↓
21	14	19	4
x_1	x_2	x_3	x_4

$$y_1 = (ax_1+b) \bmod 26$$

$$y_1 = [5(21)+7] \bmod 26$$

$$y_1 = 112 \bmod 26$$

$y_1 = 8 \bmod 26$

$y_1 = I$

$y_2 = [5(14) + 7] \bmod 26$

$y_2 = 77 \bmod 26$

$y_2 = 25 \bmod 26$

$y_2 = Z$

$y_3 = [5(19) + 7] \bmod 26$

$y_3 = 102 \bmod 26$

$y_3 = 24 \bmod 26$

$y_3 = Y$

$y_4 = [5(4) + 7] \bmod 26$

$y_4 = 27 \bmod 26$

$y_4 = 1 \bmod 26$

$y_4 = B$

Now VOTE is encrypted into

I Z Y B

Decryption:-

I	Z	Y	B
↓	↓	↓	↓
8	25	24	1
y_1	y_2	y_3	y_4

$a = 5$

$5^{-1} \bmod 26$

$26 = 5(5) + 1$

extended eucledean method

$1 = 26 - 5(5)$

$1 = 26 + 5(-5)$

$-5 \bmod 26 = 21 \bmod 26$

So $a^{-1} = 21$

$x = a^{-1}(y - b) \bmod 26$

$x_1 = 21(8 - 7) \bmod 26$

$x_1 = 21 \bmod 26$

$x_1 = V$

$x_2 = 21(25 - 7) \bmod 26$

$x_2 = 21(18) \bmod 26$

$x_2 = 378 \bmod 26$

$x_2 = 14 \bmod 26$

$x_2 = O$

$x_3 = 21(24-7) \bmod 26$

$x_3 = 21(17) \bmod 26$

$x_3 = 357 \bmod 26$

$x_3 = 19 \bmod 26$

$x_3 = T$

$x_4 = 21(1-7) \bmod 26$

$x_4 = 21(-6) \bmod 26$

$x_4 = -126 \bmod 26$

$x_4 = 4 \bmod 26$

$x_4 = E$

The decrypted message is VOTE.

ii- SKY key (11, 2)

S	K	Y
↓	↓	↓
18	10	24
x_1	x_2	x_3

$y_1 = (ax_1 + b) \bmod 26$

$y_1 = [11(18) + 2] \bmod 26$

$y_1 = 200 \bmod 26$

$y_1 = 18 \bmod 26$

$y_1 = S$

$y_2 = [11(10)+2] \bmod 26$

$y_2 = 112 \bmod 26$

$y_2 = 8 \bmod 26$

$y_2 = I$

$y_3 = [11(24)+2] \bmod 26$

$y_3 = 266 \bmod 26$

$y_3 = 6 \bmod 26$

$y_3 = G$

The SKY is encrypted into SIG.

$a = 11$; $a^{-1} = ?$

$26 = 11(2) + 4$

$11 = 4(2) + 3$

$4 = 3 + 1$

Extended Eucledean Method.

$1 = 4 - 3$

$1 = 4 - [11 - 4(2)]$

$1 = 4 + 11(-1) + 4(2)$

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

$1 = [26 - 11(2)]3 + 11(-1)$

$1 = 26(3) + 11(-6) + 11(-1)$

$1 = 26(3) + 11(-7)$

$-7 \bmod 26 = 19 \bmod 26$

So

$a^{-1} = 19$

Decryption:-

S	I	G
↓	↓	↓
18	8	6
y_1	y_2	y_3

$x_1 = a^{-1}(y - b) \bmod 26$

$x_1 = 19(18 - 2) \bmod 26$

$x_1 = 304 \bmod 26$

$x_1 = 18 \bmod 26$

$x_1 = S$

$x_2 = 19(8-2) \bmod 26$

$x_2 = 114 \bmod 26$

$x_2 = 10 \bmod 26$

$x_2 = K$

$x_3 = 19(6-2) \bmod 26$

$x_3 = 76 \bmod 26$

$x_3 = 24 \bmod 26$

$x_3 = Y$

Decrypted message is SKY.

Probability

Random Processes:

Those processes whose outcome can be predicted but not gauranted are called random processes.

e.g:

- Rolling a die
- Rolling a coin
- Choosing a card from a deck.

Sample Space:

→ All possible outcomes of a random process are called sample space.

→ It is written in the form of a set.

- **Rolling a coin:**

  S = { H, T }

- **Rolling a die :**

  S = { 1, 2, 3, 4, 5, 6 }

- **Choosing a card**

  S = { 52 cards }

- **Rolling two dice**

  S = { HH, HT, TH, TT }

Event :

A subset of a sample space is called an event.

Equally likely event :

Events having equal chances to occurr.

Probability: (Naive definition)

$$\text{Probability} = \frac{\text{No. of favorable outcomes}}{\text{No. of total outcomes}}$$

$$P = \frac{N(E)}{N(S)}$$

Probability of choosing a face card.

$N(E) = 12$

$N(S) = 52$

$$P = \frac{N(E)}{N(S)}$$

$$P = \frac{12}{52} = \frac{3}{13}$$

Heart → Red

Spade → Black

Diamond → Red

Club → Black

Probability of getting only black face card.

$N(E) = 6$

$N(S) = 52$

$$P = \frac{N[E]}{N[S]} = \frac{6}{52} = \frac{3}{26}$$

Two dice are rolled. What is the probability that their sum is 8.

S = {(1,1), (1,2), (1,3), (1,4), (1,5), (1,6),
(2,1), (2,2), (2,3), (2,4), (2,5), (2,6),
(3,1), (3,2), (3,3), (3,4), (3,5), (3,6),
(4,1), (4,2), (4,3), (4,4), (4,5), (4,6),
(5,1), (5,2), (5,3), (5,4), (5,5), (5,6),
(6,1), (6,2), (6,3), (6,4), (6,5), (6,6)}

$N(S) = 36$

$E = \{(2,6), (3,5), (4,4), (5,3), (6,2)\}$

$N(E) = 5$

$$P = \frac{N(E)}{N(S)} = \frac{5}{36}$$

Finite countable

Infinite Uncountable

Countably finite: One to one correspondence with natural numbers.

Counting:

What is the probability of getting two digit numbers that are divisible by 3?

$$S = \{10, 11, \underset{\substack{\downarrow \\ 4}}{12}, 13, 14, \underset{\substack{\downarrow \\ 5}}{15}, \ldots \underset{\substack{\downarrow \\ 33}}{99}\}$$

$$N(S) = n - m + 1$$
$$= 99 - 10 + 1$$
$$= 90$$

$$E = \{4, 5, \ldots 33\}$$

$$N(E) = n - m + 1$$
$$= 33 - 4 + 1$$
$$= 30$$

$$P = \frac{N(E)}{N(S)}$$

$$P = \frac{30}{90}$$

$$P = \frac{1}{3}$$

What is the probability of getting a three digit number that are divisible by 5.

$S = \{100, 101, 102, \ldots 999\}$

$N(S) = n - m + 1$

$= 999 - 100 + 1$

$= 900$

$E = \{20, \ldots 199\}$

$N(E) = 199 - 20 + 1$

$= 180$

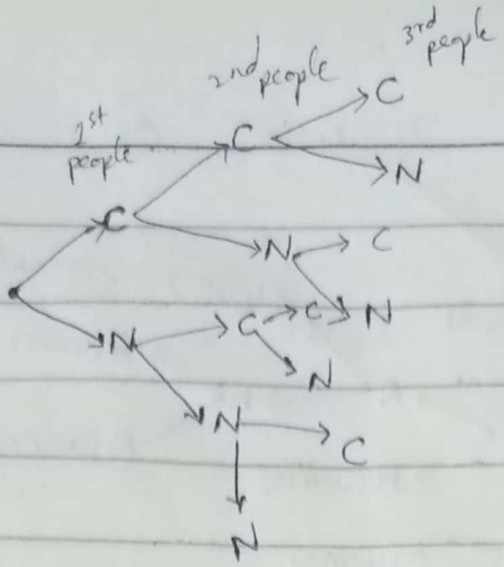
$$P = \frac{N(E)}{N(S)}$$

$$P = \frac{18\cancel{0}}{90\cancel{0}}$$

$$P = \frac{1}{5}.$$

Possibility Tree:

Three people went to meet covid patient. Probability of getting covid.



$S = \{CCC, CCN, CNC, CNN, NCC, NCN, NNC, NNN\}$

$N(S) = 8$

Find the probability that at least one people get covid.

$E = \{CCC, CCN, CNC, CNN, NCC, NCN, NNC,\}$

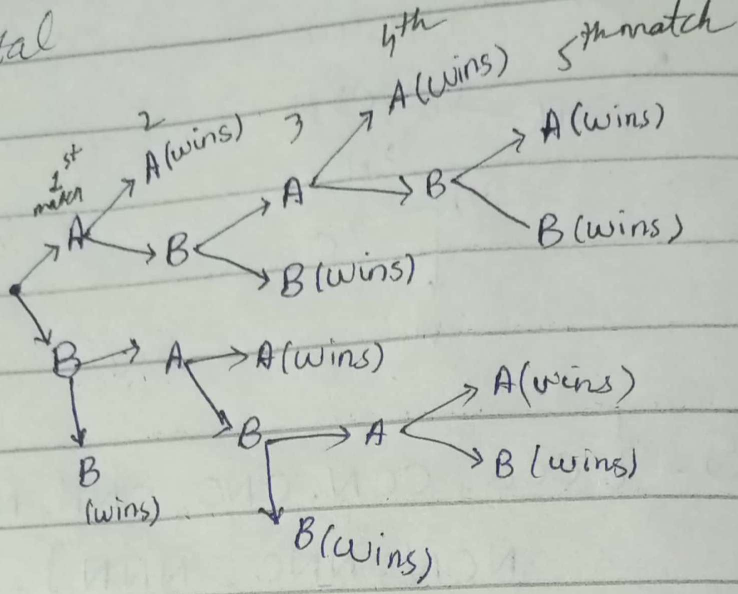
$N(E) = 7$

$$P = \frac{N(E)}{N(S)}$$

$$P = \frac{7}{8}$$

Scanned with CamScanner

Consective 2 wins or 3 wins total



Winning total possible outcomes are 10.