Modular Division we readular division we require multiplicative inverse.

Modular multiplicative inverse

can be found by greatest

common divisor (GCD). Multiplicative inverse exists

it their GCD is 1. at mod 6 exists igt GCD(a, 6) = 15 mod 6 only exists  $Z_5 = \{0,1,2,3,4\}$ than the maximum member

have multiplicative inverse. -> Few Multiplicative inverse also exists when the number and mad n are relatively prime to each other. -> Two integers are relatively prime to each other ist their GCD = 1. Eucledeon Algorithm
It is a way to find Lets have an example: (85, 34)  $85 = (34x^2) + 17$ 34 = (17X2) + Q Now, Marian Look GCD = 17 (1331, 1001)  $1331 = (1001 \times 1) + 330$  $1001 = (330 \times 3) + 11$  $330 = (11 \times 30) + 0$ 

ADIV $GCD = 11$
(9988, 6060)
- 6060 + 3828
10/0 = 3828 + 2232
2028 = 2232 + 1516
= 1596 + 636
1596 = 636(2) + 329
636 = 324 + 312
324 = 312 + 12
312 = 12 (26) + 0
The state of the s
GCD = 12.
Find the values of unknown
1331x + 1001y = 11 extended eviledeon
method
11 = 1001 - 330(3)
11 = 1001 - [1331-1001]3
11 = 1001 - 1331(3) + 1001(3)
11 = 1001(4) + 1331(-3)
50
2 = -3
4 5 4

213x + 117y = 3
Evcledean Algorithm
213 = 117 + 96
 117 = 96 (1)+21
96 = 21(4) + 12
12 = 9 + 3
9 = 3(3) + 0
GCD = 3
E 1 1 1 2 0 1 10 :44
Extended eveledean 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)

	1.71
-	3 = 213(11) + 117(-11) + 117(-9)
	213(11) + 11
	3 = 210
	Now
	$\gamma = 11$
60 S	y=-20
Ch	
	252x + 198y = 18
	runalian Algorithm
	(25) = 100
	198 = 54(3) + 36
	54 = 36 + 18
	36 = 18(2) + 0
	GCD = 18
	Extended Eveledean Algorithm
	19 - 54 - 36
	18 = 54 - [198 - 54(3)]
,	18 = 54 - 198 + 54(3)
- 10	18 = 54(4)+198(-1)
(8)	18 = 1252-198)4 + 198(-1)
	18 = 252 (4) + 198(-4)+198(-1)
	18 = 252 (4) + 198(-5)

Now	S a 12 have the
	C = 4
y	= -5
Calcul	late multiplicative in evcledean method:
using	evcledean method:
Calaula	ate 5 <sup>1</sup> mod 7.
	7 = 5(1) + 2
	5 = 2(2) + 1
Now:	- 17 4 (8) 68
	1 = 5-2(2)
	1 = 5 - (7-5)2
100	1 = 5 + 7(-2) + 5(2)
	1 = 5(3) + 7(-2)
Now	veripication:
5	$\frac{1}{1}$ mod $7 = 3$ mod $7$
Verificat	tion:
3	(5.3) mod 7
5	15 mod 7
	1 mod 7
	verified that  5 mod 7 = 3 mod 7

		1
	$8^{-1} \mod 11 = ?$	1
	11 = 8(1) + 3	
-	8 = 3(2) + 2	
	3 = 2 + 1	
-	The state of the s	
00P 1:-	Now:	
, f 410.	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 mod 11 = 7 mod 11	
	The inverse is 7 mod 11	
1 -		
	verification: 8 mod 11 = 7 mod 11	
	= (8.7) mod 11	
-	= 56 mod 11	
	= 1 mod 11	
	Hence verified that	
	8- mod 11 = 7 mod 11	
	· · · · · · · · · · · · · · · · · · ·	

3-	$6^{-1} \mod 9 = ?$	- 5 -
	6 mod 9 does not	
	exist as they are not.	
	relatively prime to each	
	other.	
,		
4-	7' mod 9 = ?	
	9 = 7(1) + 2	
	7 = 2(3) + 1	
	Now:	
	1 = 7-2(3)	
	1 = 7-19-7]3	
	1 = 7 - 9(3) + 7(3)	
	1 = 7(4) + 9(-3)	
	7 mod 9 = 4 mod 9	
	Verification:	
	(7-4) mod 9 p	
	= 28 mod 9	
	= 1 mod 9	
	Hence verified 7 mod 9 = 4 mod 9	

1 1 10 = ?	
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	
Extended evoledian method	
$     \begin{array}{ccccccccccccccccccccccccccccccccc$	
-1 mod 10 = 9 mod 10	
50 9 mod 10 = 9 mod 10	
verification:	
(9.4) mod 20	
= 81 mod 10	1
= 1 mod 10	
Hence verified that  9' mod 10 = 9 mod 10	
* It also shows that	
an integer can be an inverse of itself.	
P born 12	

و	Assine Ciph	2A.
Lou	Hyine Ciphe (a,b)	
a constant	nould be the	at 1
a was	multiplication	icu number
exists.	- surfactive	unverse
existo.	xerates on Z2	, - {A.B 7}
• 00 0.	2500	6 = (,0,
_A	FKPI	JZ
0	5 10 15 5	20 25
. Encry	pit.	
	y = (ax+b)m	rad 26
. Deci	upit.	
	OI .	
	$x = a^{-1}(y-b)$	mod 26
Example	- 101	
	VOTE	k(5,7)
V	0 T	
21	O T 14 19	4
		x4
	10	
y	= (ax,+b)mod	126
y	= [5(21)+7] mod	d 26
01	= 112 mod	

```
= 8 mod 26
      = [5(14) + 7] mod 26
       77 mod 26
      = 25 mod 26
      = [5(19)+7] mod 26
       102 mad 26
        24 mod 26
       [5(4)+7] mod 26
        27 mod 26
       1 mod 26
Now NOTE is encrypted into
     IZYB
```

Decryption	
OI .	
I Z Y B	
8 25 24 1 u y y y	
y y, y, y,	
01 02 03 04	
a = 5	
5-1 mod 26	
26 = 5(5) + 1	
extended eviledean method	
1 = 26 - 5(5)	
	#
1 = 26 + 5(-5)	+
$-5 \mod 26 = 21 \mod 26$	-
So $a^{-1} = 21$	
$x = a^{-2}(y-b) \mod 26$	
$\chi_1 = 21(8-7) \mod 26$	-
$\chi_1 = 21 \mod 2.6$	
X1 = V	
$\chi_2 = 21(25-7) \mod 26$	
$\chi_2 = 21(18) \mod 26$	
$x_2 = 378 \mod 26$	

		13
	126	
	$\chi_2 = 14 \mod 26$	
	x 2 = 0	
	21 (24-7) mod 26	1
	$x_3 = 21 (29^2) \mod 26$	
1	$\chi_3 = 21 (17) \text{ Wiba 20}$	
	$\chi_3 = 35.7 \mod 26$	
Ch.	$\chi_3 = 19 \mod 26$	
	$\chi_3 = T$	-
-!-		_
	$x_4 = 21(1-7) \mod 26$	
-,7	$\chi_4 = 21(-6) \mod 26$	
-	$x_4 = -126 \mod 26$	_
	$\chi_4 = 4 \mod 26$	
104	74 = E	_
-	The decrypted message is	
**	VOTE:	
	The second secon	
ii-	SKY key (11,2)	
	SK	
	1 1	
	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	
	73	

```
y = (ax,+b) mod 26
      =[11(18)+2]mod 26
      200 mod 26
       18 mod 26.
      S
      = [11(10)+2] mod 26
      = 112 mod 26
       8 mod 26
     = [11(24)+2] mod 26
        266 mod 26
  43
       6 mad 26
  43
  43
The SKY is encrypted into
       SIG.
a = 11; a^{-1} = ?
26 = 11(2) + 4
 11 = 4(2) + 3
 4 = 3+1
```

```
Extended Eucledean Method.
           4-[11-4(2)]
        = 4+11(-1)+4(2)
          4(3)+11(-1)
          [26-11(2)] 3+11(-1)
          26(3)+11(-6)+11(-1)
          26(3) + 11(-7)
   -7 mod 26 = 19 mod 26
                  43
            42
       = a (y-b) mod 26
      = 19 (18-2) mod 26
   X1
   x1 = 304 mod 26
        = 18 mod 26
   XI
```

X2 = 19(8-2) mod 26 - 114 mod 26 = 10 mod 26 x3 = 19(6-2)mod26 x3 = 76 mod 26 xs = 24 mod 26 and y Decrypted message is SKY. Probability Random Processes + Those processes whose outcome can be predicted but not gaurantted 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 Rolling a coin:

S = { H, T} Rolling a die: S = {1,2,3,4,5,6} · Choosing a card  $S = \{52 \text{ cards}\}$ · Rolling two dice S= { HH, HT, TH, TT} Events A subset of a sample space is called an event. Equally likely events Events having equal chances to occur.

Probability =	La company la contre
	No. of favorable outcor
nananis.	N. ( C. E ( B. E. ) . ( B. E. ) . [2
P = N(E)	
N(S.	
Probability of card.	choosing a jac
N(E) = 12	Heart -> 1
N(S) = 52	Spade → B
P = NE)	Diamond > K
N(S)	club > 8
P = 12 = 52	13
Probability of face card.	getting only bla
N(E) = 6	6
N(S) =	
P = NCE] N(S)	= 6 = 3

Two dice are rolled what is the probability that their sun is  $S = \{(1,1), (1,2), (1,3), (1,4), (1,5), (1,6), (2,2), (2,4), (2,5), (2,6), (2$ (2,1), (2,2), (2,3), (2,4), (2,5), (2,6)(2,1), (2,2), (3,3), (3,4), (3,5), (3,6), (3,1), (3,2), (3,3), (4,1), (1,1), (3,5), (3,6), (3,1), (3,2), (3,2), (3,3), (3,4), (3,5), (3,6),(3,1), (3,2), (4,3), (4,4), (4,5), (4,6)(5,1), (5,2), (5,3), (5,4), (5,5), (5,5)(6,1), (6,2), (6,3), (6,4), (6,5), (6,6)N(S) = 36 $E = \{(2,6), (3,5), (4,4), (5,3), (6,1)\}$ N(E) = 5= N(E) = 5 N(S) = 36Finite countable Injinite uncountable

Countably finite: One to one

Correspondence with natural

Counting:  What is the probability of getting two digit numbers the are divisible by 3?  S=\{10,11,12,13,14,15,99\}  N(S) = n-m+1  = 90  E=\{4,5,33\}  N(E) = n-m+1  = 33-4+1  = 30  P=N(E)  N(S)  P=30  90  P=1  3  What is the probability of getting three digit number that	What is the probability of ing two digit numbers the divisible by 3? $10,11,12,13,14,15,,99$ $10,11,12,13,14,15,15,,99$ $10,11,12,13,14,15,15,,99$ $10,11,12,13,14,15,15,15,15,15,15,15,15,15,15,15,15,15,$
are divisible by 3? $S=\{10,11,12,13,14,15,,99\}$ $N(S) = n-m+1$ $= 99-10+1$ $= 90$ $E=\{4,5,,33\}$ $N(E) = n-m+1$ $= 33-4+1$ $= 30$ $P=N(E)$ $N(S)$ $P=30$ $P=1$ $= 30$ $= 3$	divisible by 3?  10,11,12,13,14,15, 99}  S) = $n-m+1$ = 99-10+1 = 90  = $\{4,5,33\}$ (E) = $n-m+1$ = 33-4+1 = 30  P = $N(E)$ $N(S)$
are divisible by 3? $S=\{10,11,12,13,14,15,,99\}$ $N(S) = n-m+1$ $= 99-10+1$ $= 90$ $E=\{4,5,,33\}$ $N(E) = n-m+1$ $= 33-4+1$ $= 30$ $P=N(E)$ $N(S)$ $P=30$ $P=1$ $= 30$ $= 3$	divisible by 3?  10,11,12,13,14,15, 99}  S) = $n-m+1$ = 99-10+1 = 90  = $\{4,5,33\}$ (E) = $n-m+1$ = 33-4+1 = 30  P = $N(E)$ $N(S)$
$N(S) = n-m+1$ $= 90$ $E = \{4, 5, \dots 33\}$ $N(E) = n-m+1$ $= 33-4+1$ $= 30$ $P = N(E)$ $N(S)$ $P = 30$ $90$ $P = 1$ $3$ What is the probability of getting set of the probability set of the probabi	S) = $n-m+1$ = $99-10+1$ = $90$ = $\{4,5,,33\}$ (E) = $n-m+1$ = $33-4+1$ = $30$ P = $N(E)$ N(S)
$N(S) = n-m+1$ $= 99-10+1$ $= 90$ $E = \{4,5,33\}$ $N(E) = n-m+1$ $= 33-4+1$ $= 30$ $P = N(E)$ $N(S)$ $P = 30$ $90$ $P = 1$ $3$ Nhat is the probability of getting and solutions are significant.	S) = $n-m+1$ = $99-10+1$ = $90$ =
$= 99 - 10 + 1$ $= 90$ $E = \{4, 5, \dots 33\}$ $N(E) = n - m + 1$ $= 33 - 4 + 1$ $= 30$ $P = N(E)$ $N(S)$ $P = 30$ $90$ $P = 1$ $3$ What is the probability of getting and getting	$= 99 - 10 + 1$ $= 90$ $= \{4, 5, \dots 33\}$ $(E) = n - m + 1$ $= 33 - 4 + 1$ $= 30$ $P = N(E)$ $N(S)$
$E = \{4, 5, \dots 33\}$ $N(E) = n - m + 1$ $= 33 - 4 + 1$ $= 30$ $P = N(E)$ $N(S)$ $P = 30$ $90$ $P = 1$ $3$ What is the probability of getting the second secon	$= 90$ $= \{4, 5, \dots 33\}$ $(E) = n - m + 1$ $= 33 - 4 + 1$ $= 30$ $P = N(E)$ $N(S)$
$E = \{4, 5, \dots 33\}$ $N(E) = n - m + 1$ $= 33 - 4 + 1$ $= 30$ $P = N(E)$ $N(S)$ $P = 30$ $90$ $P = 1$ $3$ What is the probability of getting and getting and getting and getting and getting are getting as a getting and getting and getting are getting as a getting and getting are getting as a getting and getting are getting and getting are getting as a getting and getting are getting as a getting are getting as a getting are getting as a getting and getting are getting as a getting are getting as a getting and getting are getting as a getting are getting are getting as a getting are getting are getting as a getting are getting as a getting a	$= \{4, 5, \dots 33\}$ $(E) = n - m + 1$ $= 33 - 4 + 1$ $= 30$ $P = N(E)$ $N(S)$
N(E) = n-m+1 $= 33-4+1$ $= 30$ $P = N(E)$ $N(S)$ $P = 30$ $90$ $P = 1$ $3$ What is the probability of getting	(E) = n-m+1 = 33-4+1 = 30 P = N(E) N(S)
N(E) = n-m+1 $= 33-4+1$ $= 30$ $P = N(E)$ $N(S)$ $P = 30$ $90$ $P = 1$ $3$ What is the probability of getting	(E) = n-m+1 = 33-4+1 = 30 P = N(E) N(S)
= 33 - 4 + 1 $= 30$ $P = N(E)$ $N(S)$ $P = 30$ $90$ $P = 1$ $3$ What is the probability of getting	= 33 - 4 + 1 $= 30$ $P = N(E)$ $N(S)$
P = N(E) $N(S)$ $P = 30$ $90$ $P = 1$ $3$ What is the probability of getting the probability of get	P = N(E) $N(S)$
P = N(E) $N(S)$ $P = 30$ $90$ $P = 1$ $3$ What is the probability of getting	P = N(E) N(S)
N(S) $P = 30$ $90$ $P = 1$ $3$ What is the probability of getting t	N(S)
P = 30 90 P = 1 3 What is the probability of getting	
90 P = 1 3 What is the probability of getting	P = 30
P = 1 3 What is the probability of getting	
What is the probability of getting	
What is the probability of getting	Post 1
What is the probability of getting three digit number that	3
a three digit number that	is the probability of getti
/	three digit number that

$S = \begin{cases} 100, 101, 102, \dots, 999 \end{cases}$ $S = \begin{cases} 100, 101, 102, \dots, 999 \end{cases}$ $N(S) = n - m + 1$ $999 - 100 + 1$ $900$ $E = \begin{cases} 20, \dots, 199 \end{cases}$ $N(E) = 199 - 20 + 1$ $= 180$ $P = N(E)$
$N(S) = n - m + 1$ $999 - 100 + 1$ $900$ $E = \{20,, 1993$ $N(E) = 199 - 20 + 1$ $= 180$
$N(S) = n - m + 1$ $999 - 100 + 1$ $900$ $E = \{20,, 1993$ $N(E) = 199 - 20 + 1$ $= 180$
900 E = {20, 1993 N(E) = 199-20+1 180
900 E = {20, 1993 N(E) = 199-20+1 180
$E = \{20,, 199\}$ $N(E) = 199 - 20 + 1$ $= 180$
$E = \{20, 1993\}$ $N(E) = 199 - 20 + 1$ $= 180$
N(E) = 199-20 = 180
N(E) = 199-20 = 180
180
P N(E)
P N(E)
P = N(E) $N(S)$
P = 180
900
P = 1.
Possibility Tree .
Three people went to
meet covid patient Probability
of getting covid.
- I will be a middle of the state of the sta
- White remains that the state of the state
The state of the s

3rd note	
2nd people 3rpeque	
people IC >N	
× N→ C	
IN AGRESIN	
NA SA	-
C	-
The state of the s	-
	-
S- ¿ ccc, ccn, cnc, cnn, ncc,	-
NCN, NNC, NNN3	
N(S) = 8	
Find the probability that at least one people get could.	
least one people get covid.	
E= { ccc, ccn, cnc, cnn, ncc,	
NCN, NNC, 3	
N(E) = 7	
P = N(E)	
N(S)	
P 7	
P = 7 8	

