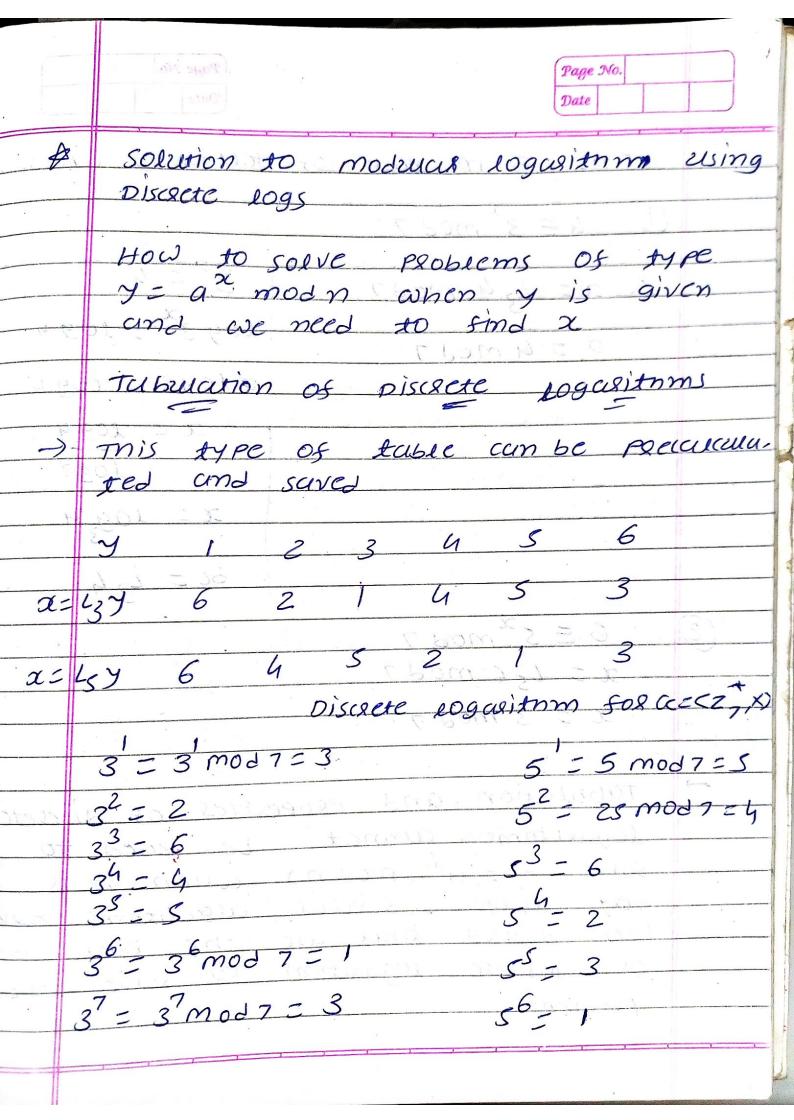
P	Discrete jogarithm		
	# 1 1 1 CO 100 1 1		
	The gloup & = <zp*, 7="" hus="" sevelu<="" th="" x=""></zp*,>		
	Properties		
	The state of the s		
1.	Its elements include all integers from		
Sugar	1 to P-1 3055		
. 5 5			
2.	2. It always has primitive 200ts		
3.			
4.	me primitive 200ts cen be thought		
did	as the base of logarithm. It group		
5			
	Y= 9 mod n eulculation can be done in		
	: x = 109 y k disterent bases		
seto'il.	1000000 10 10 10 10 10 10 10 10 10 10 10		
(· · ·			
	-) sol any element y in the set		
	there is another element & thus		
	is the log of y in base g		
	-) This type of logarithm is cauld		
	discrete logarithm		
1	we use notation Lg to show that but		



Page No.

Date

pind a in each of following cuscus O $4 = 3^{x} \mod 7$ $2 = 4 \mod 7$ $3 = 4$ $4 = 4$		Page No.	Date
1. $\alpha = 134 \mod 7$ $\alpha = 4 \mod 9$ $\alpha = 4 \mod 9$ $\alpha = 4 \mod 9$ Tabulation and properties of discrete logalithms cannot be used to solve $y = \alpha^2 \pmod n$ when n is been devised that use the basic ideal of pisaete logalithm $\alpha = 4 \mod n$		Find & in each of	sollowing cuses
OLE L34 (2) 6 = 5 mod 7 A = 136 mod 7 A = 3 mod 7 Tabulation and properties of discrete logalithms cannot be used to very large several algorithms have been devised that use the basic idea of pisalte logalithm to		2. x = 134 mod 7 x = 4 mod 7	$1093^{2} = 1094$ $21093 = 1094$ $2 = 1094$ 1093
Tabulation and properties of discrete logalithms cannot be used to solve year (modn) when n is very lurge several algorithms have been devised that use the basic idea of pisaete logalithm to	<u></u>		3
Solve y = ax (mod n) when n is very large several algorithms have been devised that use the basic idea of pisaete logarithm to		25 6 mod 7	3 73 5
	→	Solve y = ax (mod n) very large several been devised that use of pisaete logalitum	when n is culgorithms have the busic idea