to provide with both days

Name: Md. shahidul Islam ID: IT-21024

A summittee rout of 7 , is in integer * Assignment;

1) Is 1729 a carmichael number?

Ans:

Yes, 1729 is a carmichael number. Because, A caremichael number is a composite number n such that,

$$a = 1 \pmod{n}$$

where ged (a,n) = 1.

1729 = 7×13×19 (product of distincts prime). It satisfies korcselt's criterian, hence it's a cannichael number.

2) Preimitive Root Generator of Z23?

Ans:

A primitive root of Z₂₃ is an integer g such that the powers of g mod 23 generate all non-zero elements of Z₂₃, where

A number g is a primitive root modulo 23 if (9.1.23, 9.1.23, --- g.1.23) gives all values from 1 to 22.

All primitive roots of Z_{23} = $\{5, 7, 10, 11, 14, 15, 17, 19, 20, 21\}$

commiched numbers.

IT-210245-TI (3) Is < Z114, *> a Ring? + ... Ans: Zi means the set of integer modulo 11: General assignis. we define, + = Addition modulo 11,0000 = multiplication modulo 11. > (Zu, +) is an abelian group. - (ZII) +) is a semigritup. > Left distribution: a (b+c) = ab+ac mod 11 Right distribution: (a+b) c= ac+bc mod 11

since it satisfy the condition.

.. (Z11,+,*) is a Ring(x 1,5)

{ hs ... 1512/107 = 2 Hence ged (s, us) = s = 1 (LZGGIX) is not an abelian griging.

(4) Is Z_{32} , +>, Z_{35} , x> and abelian group? Ans: <239,+> Ans: Set : 737 = (011,2,3,--- 36) opercation: Addition modulo 37. General axioms: 1. closurie: a + b mod 32 EZJ2 2. Associativity: (a+b)+c=a+(b+c) mod 32 3. Identity: 0 is the additive identity. 4. Inverse: Every a has an inverse-a such that a+(-a)=0 mod 37 5. commutativety: at be b+a mod >2 .: (Zz,1+) is an abelian group.

Hene ged (5,35) = 5 \ 1

(1. (Z35,X) is not an abelian annual

(5) Let's take p=2 and n=3 that makes the $Grf(p^n) = Gr(2^3)$ then solve this with polynomial arithmetic approach.

(Es) no air e si fluenn adr.

Ans:

Base field: Z=20,1}

field size: 23 = 8

Inneducible polynomial: f(x) = x3+x+1

All polynomial of degree <3 over Z2:

= (0,1,x,x+1,x,x+1,x+x,----)

Let a = x mod f(x) then

$$\alpha^3 = \alpha + 1$$

Arcithmetic:

Addition: XOR of coefficients

multiplication: multiply polynomials then

then reduce mod f(x) so over toll (3) orf(60) - arr(68) thin solve t Example: $(n+1)(n+21)=21^3+21=(n+1)+21=1$.. The nesult is 1 in GF(23) Reld size: 07 = 8 I to kt. Pre- (1217 - lower orking aldoub ann I All polymorals of degree es avou 25: Louis, and a significant states. Holle (all- burn x - x to) -1 HX - 3" 6 · sitemalina, thisisitions to 40x: noitible multiplication: multiply polynomials then