15 1729 a carzmichal numberzo

answer: -

a commichael number is a composite number nuhich satisfies the congression relution:

an = a modning of the world to the says 5 teo-1 Heru,

n=1719 = 7x13x19

let, P1=7, P2=13, P3=19 then P1=1=6, D1-1-12 and P3-1-18

a150, n-1=1729-1=1728 which is divisible JAKTER STATE by p1-1=6

therefor, n-1 is divisible by P,-1

THE PLAT SOUTH BE CONTRATED ON THE PROPERTY OF A 5tep-2.

We can show that n-1 is also divisible by Pr - 1 and P3 - 1.

Therefore, from the letinition of A LINE LEEK ! MELLY LITERAL COLOR continichael numbers and the above discussion, we can conclude that 1729 is indeed a archickael number

torns let,

3 = the set of integers from 1 to 22 under multiplication module 23

LUNG ON AND STREET

Since 23 is a praime number 12*23 = \$ \$ (23) = 22

so, a prainitive root q is an integer such thut,

9 - 7 - 12 WHT 600 gk + 1 mod 23 Poiz all K122 ists in a man - 2 of a and g22 = 1 and 23

We their forcy = 5:

-> prime factors 0 + 22 = 2,11 752212 = 911 mod 23 = 22 #1 => 522/11 = 51 = 25 mod 23 = 2 + 1

GOSTION TIMES FINANCE 50,5 is a primitive root module 23

(x) Is 12-37 +7, 12-35, x> atte abelian THEN HAVE USED IN THE WASHINGTON

group?

(237, +): is an abelian group under addition mod 37. Alwars true fare zo with addition

(239,x): is not an abelian group only the units in 235 forzm a group under multiplical

(x7 let's take p=2 and n=3 that makes the CrF(p^n) = GF(23) then solve this with polynomial arithmetic approach.

answerz:

Given, P=2, n=3

21218 WALL ELECT VELLED + 4218 145, 1 step-1: select an increducible polynomial of degree 3 over GFL2) Jasolvid Si asking series - Replement and

CIXEINY : POUR : O

f(x)=x>+x+1

5 tep-2: Define the field elements. Every elemen of GE(23) can be expressed as a polynomial with degree less than 3 and coefficient in S' I'M that were MAN STREET WELL STORES 9F(2)

step 3. Define addition and multiplication N+71=01 x2+1= x2+1

enample: 200 = 22 eno reduction medel as degree) n 1 destru 23, notcedention)