O dis 1729 a comichael numbers? 30 910 Argueria in both words men and ofconting A commichael on number is a composit numbers in which of satisfies the congruence relation: . apporte discussion, en comerciale deprison it is independ a commissionel for all integers a that are relatively Primitive most (q. of oto smith or olubions tocor : solitioning A : mitinfied Swilling stepoor: que mi er competarino si q As given in = 1729 = 7 x13×19 +01 Letin PET monuncy o 21 avillming po= 15 mits at time ins. second readule 28, m. cols Then P=1=6, P2-1,1=12 and B-1=18 n-1= 1729-1= 1428, which is divisible Therefore, n-10 is divisible by p,-1

1) ils men or commichael number 20 9048 similarly, we can show that not not A commen so si madmin to Dandomores A Thornetone from the definition of - commichael numbers and the above discussion, une com conclude Ahost 1729 is indeed a cammichael Mumbers.

Claritalises such forth a surjection to infile

Primitive most for of otra 23091 - Definition: A proimitive rosof modulo or begine to is on integers is in == isochts that levery nonzero clement of ab is a boness total N' +37. - cue wont to find or primitive sooof modulo 23, an element of 223 generator all non-zero elements of 13-23 sidisivily store complants in

をかって、丁二

J 1-21038

Let 2-23 = the set of integers of from.

The 1 to 22 under multiplication

modulo 23

Since y 23175 8 00 prome u mimber : = 15

12/20 1 = 100 (23) = 2120 Bord mollybbo

such that:

out of the floor and 23 for all kcc2

out of green and 23

out of green and 23

not confident.

for 9 = 5; mod 23 = 2 7 1 3000 527 = 52711 - 5.2 mod 23 = 2 7 1 30000

50, 2 13, 19 beautifilities troopy magnile 53

35015-1I

yes

addition and multiplication modules

11 is a Ring toom. authorized on as pecause.

(ZII, +) is an abelian grotop

· multiplication is associative and · distributes over addition.

Since it sis prime The is labor a field to bom the prime of the sister o

210:38 (4) Is ZZ-37, 47, KZ-35, x ame abelian group? (c) = (c) = (c) = (c)

Soln: Duimonulair Million elite antia modela (7 37 1+): Nonsangera offernationa

This is an abelian group under addition mod 97. Always theme for 20 with · addition

(232)*) Think sale from the sale of of This is not an abelian governo.

Onto: Anterior conits in 732 forom or genous unden multiplication includes o, non-inventible 30 its not a group 10 blied of

> Dichon common A (1. 16) Ex = (10)]

Then solve this with polynomial arothmetic appropriach.

son. Son.

Given pearly extends for hours

To construct the finite field.

To build $GF(2^3)$, select on immediable Polynomial of degree 3 over GF(2),

A common choice is $A(n) = x^3 + x + 1$

This polynomial comnot be: factored to over GF (2). so it is suitable for defining multiplecation in the field is (1)

Step 32 Define other field elements. Every element of GF(23), com be expents ous a responsion primits degree less then 3 and coefficients in GF(z): (There page elements.

ster :03 990 196) 4+4 : 4. (1+10)

petine addition and multiplication Addition is pentonmed log by odding commes ponding acefficients a modulo 2, x+x=0, x+1=x+1

Hollowed why weducation module in 100 from the first on the module in 100 from the first of the

Since, Since, Since, Since, Since, Since, Since, 239245 Cele meplace, no by rett whenever it orppeans during multiplication . them 3 and coefficients informations. (1) MOREN (187) => N· u2= N3= N+1 (meduc n3

?troms/3 > modulo fous) => (m+1) . n = 22+x (degree 43; 95) motheritation and mother reduction Thus GE(23) rist field with commesponding as & remains & Bodulo 2. 14N =14N O= NHX