stall into a for Number Theory and Abstract Algebra Assignment -04
Abida Sultana 1-19 pd aldir i 21032, 1-17, 1900 3 3 3 11

1) Is 1729 a Carmichael number ?

si I-re book mode non our plantimis Answer :-

A cannichael number is a composit number n which satisties the congruence relation?

success and a mod reducer.

for all integers of that are relatively primed to milosuloimas

To prove that, 1729 is a Carmichael number, we need to show that it satisties the avove condition. Step 010 mole mole of oming

As given, n=1729 = 7x13x19

Let, P1 = 7, P2 = 13 and P3 = 19.

Then,  $P_1 = 1 \pm 6$ ,  $P_2 - 1 = 12$ , and  $P_3 - 1 = 18$ . madula 23. an element graza sen

Also, n-1=1729-1=1728, which is divisible. by  $P_1-1=6$ .

Theretone, n-I is divisible by P1-1

## Step 02 min landiment to our

Similarly, we can show that n-1 is also divisible by P2-1 and P3-1.

Therebore, brom the detinition of Carmichael numbers and the above discussion, we can conclude that 1729 is indeed a carmichael number.

2) Primitive Root (Generator) of 2,23?

Detinition: A primitive root modulo a prime p is an integer n in 2p such that every nonzero element of 2p is a power of n.

We want to find a primitive root modulo 23, an element  $g \in \mathbb{Z}_{23}$  such that

the powers of g generate all non-zero elements of Z-23.

Let, it obstant nottonil githum the

2.23 = the set of integers from 1 to 22 Under multiplication modulo 23. Since 23 is a prime number,  $|2^{4}23| = 0(23) = 22$ 

so, a primitive root g is an integer such that:

 $g^{\frac{1}{2}}$  1 mod 23 for all  $\frac{1}{2}$ , and  $g^{\frac{2}{2}}$  = 1 and 23

weicheck ton g = 5:

prime tractors of 22 = 2, 11

, 522/2 = 511 mod 23 = 22 + 1

.52/11 = 52 = 25 mod 23 = 2 \$1

So, 5 is a primitive root modulo 23

3) Is ZZ-11,+,\*>a Ring ? 109

Yes, 211 = <01,2, -- , 10% with addition

and multiplication modulo 11 /2 a

Ring Abecause:

· (ZII, +) is an abelian group.

- Multiplication is associative and

distributes over addition.

. . It has a multiplicative identity: 1

Since 11 is prime, 12,1 is also a

Field. 89 borner 1: 93 borns

So, (Z11,+,\*) Is a Ring.

, prime tenter 16 22 = 2, 11 1 + 12 = 52 hood 23 = 21 + 1

1 to e - Es tony de - ea . 11/665.

es eluboration primition pret module es

1 Is (2-37, +>, 42-35, xx are abelian

Answer:

(Z<sub>37</sub>, +):

This is an obelian group under addition mod 37. Always true ton In with addition

(735, \*): 2 = 82 201 Holes (80) 10

This is not an abelian, group.

only the unite in 235 tonm a group under multiplication. But tull 235 under multiplication includes 0, non-inventibles -

so It's not a group.

This poolgaranion corned by horters

the little of the solution of the province of

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

Answer group moiledo no si sutt

Glven, p=2, n=3.

We want to construct the binite bield

We want to construct the binite bield

GF (2<sup>3</sup>) which has  $2^3=8$  elements.

Step 1: Choose an inneducible polynomial

To build GF (2<sup>3</sup>), select an inneducible

polynomial of degree 3 over GF(2). A

common choice is:

This polynomial cannot be tactored over GF(2). So it is suitable tor detining multiplication in the tield.

Step 2: Define the field elements

Every element of GF(23) can be expressions as a polynomial with degree less than 3 and coeklicients in GF(2):

3 and coekticients in GF(2): x.

Y0,1,x, x+1,x,x+1,x+x,x+x+1?

There are exactly 8 elements as expected.

Step 3: Detine addition and multiplication

. Addition is performed by adding corresponding coefficients modulo 2.

21+x=0, 21+1 =21+1

· Multiplication is polynomial multiplication to the lowed by reduction modulo  $t(x) = x^3 + x + 1$ 

Since  $x^3 = x+1 \pmod{t(x)}$ ,

We replace 23 by 241 whenever it appear

during multiplication, Example calculations: · x · x = 21. (no reduction needed as degree (3) · x.x² = x³ = x+1 (reduce as modulo · (x+1). x=x2+x (degree <3, no preduction) Thus, GF (23) is a field with 8 elements and well detined addition and multiplication: 2 11 11 21032 int, o publica I enth-. Depthon . In warry by it mother it fillers. stated referrators plantage transitate contra Langue Cours

(100) to the stand of the gray of the

many to the amount of the street and another ment