77 21006

Number Theory and Abortractoring of Algorithm

Plant bord Classignment -04

Assignment -04

Shubmita Ghosh Shoili

Thereis is doing IT-21006

1.) In 1729, at cardinichael number 25001950017

A carmichael number is a composit number no which satisfies the congruence relation:

an= a mod no 1 29 god sidisivily frame ton all sintegens a sithad and relatively prime

ton.

To prove that, 1729 is a chanmichael number,

To prove that, 1729 is a chanmichael number,

we need to show that it satisfies the

above condition.

An given in 21 29 = 7x13x19 Let, P1=7, P2=13 and P3=19 Assignment-04 Then P1 = 1 = 6; P2 - 1 = 12 and P3 - 1 = 18 Also, n-1-1729-1300728 which is divisi by P1-1=6 Therefore introvins bedivisibles by Pa-1. at A carmichael number is a composit getteren 3 imilanty, were can och out that inst is also divisible by P2-1 and of 3-1. eming 17219 leip san corinie had lemulaitents Prumitive root of 2237 that, 1729 is a charmic Definition: A primitive 200+ modulo a prime p is an integer re in zpsuc above condition.

that every non-zerro element obzp is a power sactors of 22. 2, 23 or to nowoq

We want to find a spruimitive croot modulo 23, an element gezzamuch that the

powers obser generations all non-zero? elements of Z23.

Let, Spring D(+,+, LL=S) AI (C)

223 - the set of integers from 11 to 20

under multiplication modulo, 23.

Since 23 ls a prûme number pris

12,3 = \$ (23) = 22 ai (+, 15) ~

50,000 primitives rootrogitsis joins integer

such that gk \$1 mod 23 tonal kc2

1. Photosilation of pod \$1.

and $9^{22} \equiv 1 \mod 23$

77.57006

I7-21006

Me epeck pour 3=2: nou Buss. pout

-> preime factors of 22 = 2,11 m de nouver

alubom +00 = 5 3 vinnod +23 1 22 it I mow sw

>522/11/575 mods 230-2420 on :62

50, 5 isora primitive roof modulo 2309

3) In <Z=11, +, +.> a Ring?

and multiplication modulo 11 is a Ring, because:

> (211, t) is a abelian group

> multiplication is associative and

distrubutes over addition;

> It has a multiplicative identity:1

Since 111 is prime 1212 is also a held. 5011(CZ+102+0*)116(EQ) Ring (110) 100 soll-

(237,+): Simonyling dimension dimens

This is an abelian group under addition

mod Bx malways true ton 2n with addition

Rep 1: choose an inneducible politiques.

side This mis nort and abelian grouplied of

only there units simples form agrioup under multiplication, includes sois monto rinevitables, so

1/3 not du group. Loimonylog ENT over art(2). 30 it is suitable for

defining multiplication in the field.

(5) Let so take p=2 and n=3 that makes the GF (p^n) + GF (23) athent solve this with polynomial aruthmatic approach (quong rolledo 3710 (x (zes) (+, xes) (+, xes) We want to construct the finite Held addition notibbe d'in as not sunt 3 = 8 sue ments. bon Step 1: choose an inreducible polymomial. To build of (23), select and irrneducable) sobre polymonial of degnée Biover GF(12). oz as Anteominon ochoice and who fexy of x3 fix 1 m This polynomial cannot be to ctoned over GF(2). 30 it is suitable for

defining multiplication in the field.

JODES - T. T. 2100C stèpli Define the field elements . Eveny elements of GIF (23) can be expents as a polynomial with degree less than 3 and inothopily thum privile armaggo co-efficients in GF(2):

50,1,x, x+1,x2+1,x2+1,x2+x, x2+x+13, x=

There are exactly & elements as expected:

Step3: N= N'12 (degree <3, noneductop)

Define additional and multiplication.

Addition bis perstoremed by by adding connerponding co-efficients modulo 2-

x+x=0, x2+1: x2+1

-> Multiplication in polynomial multiplication followed by reduction modulo fex)-x3+x+1

IT-21000 Since: 25 = x+1 (mod f(x)) we replace x3 by not 1, wherever it olynomial with degree less than 3 and appears during multiplication: Example calculation: -> n. 2 2 x2 cho reduction néedlet as degnee Bar. K2 = 23 = 2x + 1 (reduce 1/3) modulo f(x) -> (x+1), x = x2+x (degree <3, no reduction) Thus, " Cot E(23) His ab field row tho & glements and defined board dittion and multiplian connerponding co-efficients modulo 2. Ctox: Ctox, O:X+X

-> Multiplication in polynomial multiplication