[Number Theory and Abotract Algorithm] TT-21010 (Shafinddinseram)

\$ In 1729 a Carmichael number?

Am: A carmichael number is a composit rembon n which satisfies the congruence relation! an = a moder of concertor of the mind to

Son all integers athat are relatively prime to n to prove that 1729 is a camichael number we need to show that it natisfies the above condition of

Step 01:

Angiven n= 1729 = 7x13x10 - times on ES

Let, P, =7, P2 = 13 and P3 = 10

Then P_= 1 = 6, P2= 1= 12 and P3-1=185

Alno, n-1 = 1729-1 = 1728, which in divisible

b7 P1-1=6

Therefore, n-1 is divisible by Pit 85 sovie

Step 02:

Est = 6 (23) = 77 Similarly we can show that not in also divisible

by P2-1 and P3-1

Therefore from the defination of commohael numbers and the above dincumbin are can corolude that 1720 in indeed a comi-

17-21010 (shafieddinge Jam)

in outinhier the congruence me lation! # Primitive Root (Generator of 2 = 23? Defination: A primitive root modulo aprime Pin an integer To in 2p nuch that every non zero element of Zp in a power of n. we want to find a primitive nost modulo 23, an element of 223 nuch that the powers of a generator all non-zero elements of Z-23. Let Z-23 = the net of integers from 1 to 22 un der multiplication modulo 23. Since 23 in a prime number Z23 1 = 0 (23) = 22 So a primitive nost q in an integer nuch

that gk #1 mod 23 for all KKZ.

and agree = 1 med 23 it be avoident

(0195-TE)

(clos-TE)

we shear for 9=3: <+ , +8=5 \ 1:# prome factors of 22 = 2 / lbn moder 522/2 = 5 mod 23 = 22 \$ 1 (+ 505) 5011002 507 mod 23 72 2 1 mo ci aid sion 5 for a preimitive troot modulo 2300 (Ess +): This is not an abelian group # Fasas II to the Ring on Ping Yen Zu = 6001/2 monto jo with addition and multiplication modulo 11 in a Ring (ZII, +) is an abelian group Multiplication in annoeiative and distributes over addition It has a multiplicative identity: I Sircell in prime, ZII in also a field. So (211, 7, 7) in a Ring. Hollo (8) 70 Stept: chare on inneducible pargraphical to build FE(2) select on includible polynomial of degree 3 over (F(2). A common chaine in!

(IT-21010)

common choine in!

(0195-TE)

#In (2-37, +), L235, 27 are abelian group? = 55 40 cnotost ening P(237,+)! + 55= ES bom' = = 5155 This is an abelian group under addition mod 37. Always trace for In with addition (235, 4): This is not an abelian group Only the units in 235 forem a group under noits not a group. 7 Letis take P= 2 and n=3 that makes the GP(PIN) = GF(23) then nelve thin with polynomial anithmetic approach. are want to construct the finite stell af(29) which has 2 = 8 elements Stept chone an inneducible polynomial to build ap (23) select an imedacible polynomial of degree 3 over GF (2). A

This polynomial connect be factored over arcz) so
It is suitable for defining multiplication in the

Step2: De fine the field elements. Frenze element of at 1=(23) combe expents as a potnomial with degree lens than 3 and coefficient in aF(2);

8 0,1,7,2+1,2,2+1,2+2,2+2+1

There are exactly 8 elements as expected

Aten3

Define addition and multiplication, Addition in performed log by adding corresponding coefficient modulo 2.

スナモ=0メナー=ガナー

multiplication in polynomial multiplication followed by reduction modulo $f(x) = x^2 + x + 1$ Since $x^3 = x + 1 \pmod{f(x)}$ we replace x^3 by x + 1 where ver it appears durning multiplication!

(2T-21010)

10015-TI)

Example calculation! 2.22 in (no reduction reeded un degral3) 2.22=2322+1 (neduce 23 modulo 5(3)) bet) 2 = 2 +2 (degree (3, 20 neducation) Thun, aF(23) in a field with 8 elements and well defined addition and maltiplication. poloseles as yours and soloseled of Act 66 to a condition of actions of actions of the lotte to reputation in post of tel puriodie controligithme Inimarches, or authority Allowed by neduction instead of Do 27724 (18) 2 bor) 1 to E SE 2001 Constant of 20 20th Contents to the constant of ! Authority 1+ Lur petano