Numbers Theory and Abstract Algorithm 138405

(1) Is 1729, a carimichael numberi?

A caronichael number is a composit number n which satisfies the congruence relation:

à = a moden pris el quarter :

fore all integers a that are trelatively prime to n.

To prove that, 1729 is a caronichael numbers, when we need to show that it satisfies the above condition.

Step 1:

As given, n = 1729 = 7 x 13 x 19 Let, $P_1 = 7$, $P_2 = 13$ and $P_3 = 19$ Then P1 =1 =6, P2=1=12 and P3-1=18 Also, n-1 = 1729 - 1 = 1728, which is divisible by Pz-1 =6

therselone trom the definition of number. 8 -knoon ovillingions is not Similarly, we can show that not is also divisible by P2-1 and P3-1 therefore, not is divisible by op-1 discussion were agan conclude that Step 02:00 of by atmospher of the most mark carmichael numbers and the above is indeed a carrinichael

es obstromodado 20) iare element que zas such @ Primitive roof (Grenerator) of z_23? such that every non-zaro element -> Delinition: A primitive intent modulo we want to find a primitive most of zp is a power of no a prime : Pis an integers to in zp · Hort Abus

this with polynomial arcithmetic approthe GF(Pn) = GF (2), then solve 6) Let's take P=2 and n=3 that makes ナスナック ニ (x)+

> Given, (10) horro = 0x P=2, n=3

we want to construct the finite
hield c-(F(53)) which has 23 = 8 elements step 1: choose an immediale polynomial of degree , e over corf(2)

mold 8 MIA. common choice 15 months of 15 months of 15 123 to the condition of 15 months of 15 m 5tep 2: Define of the of tield claments, every as a polynomial with degree less element of GF(23) can be expiress

step 3: Define addition and multiplication 10,1,x,x+1,x~,x~+1,x~+x,x~+x+主 than a and co-efficients in GF(2):

· Addition is performed by adding corresponding co-efficients modulo 2

(3) Is <2-11,+, x> a Ring? Ring because and multiplication modulo 11 is a Yes, Z== 10,1,2,--10) with addition

· (zst) is an abelian group. · Multiplication is associative and

distributes over addition.

since 11 is prime 7 714 is also a worder muttiplication. But block

505 (211,+ 1/2) 116 Lan Ring ...

So, 19 10 year of stock JOST - HANCEL-PIPLES.

Strong ? (1) Is <2-37)+>, 12-35, x> Otre abelian

addition mod 37. Always true for zni with addition; This is an abolian group woder

this is not land abelian group. non-invertibles. under multiplication, includes o, under multiplication. But full Zas only the units in 235 trom a group

So, it's not a group.

2311- boon and are multiplication modul that the powers of generator all tell, touth works ross so throughouse 2 23 = the set of integers from non-zero elements of z_23.

since 23 is a prime number; 123 = 0 (23) = 22 at BEFF So, a primitive root of is an integer

such that:

we checker fote g=6: ming of hold = 2 mil 1 11 529/14 = 52 mod 23 = 2 # 1 to and 192 = 4 mod 28 11110 gh # 1 mod 23 for all 4<22 52% = 5 = mod 23 = 22 7 1

2 Proper

50, 5 is a primitive tood modulo 23

6 Johnson of CIE (Pa) God po externs and multiplication. exclose a choose takes existing a poly Governce & board and Go-off of early a 1910 Example railoutations: hygolythan is tenforance of so Filt-Lune bress modelion and smul-life KI-アメ、ドナガメ、マス、ドアメ、ス、にの ANON S and co-officients in as a boldwornigh might godinas 10100 01 x 4 12 = x? (x+x). · x.x = xx (no treduction needed) Thus, GR(2) is a Hold with 8 nts and well defined addition x+x =0 , x~+1 = x+1 ·Hulliplication is polynomial multiplif(x) = x3+x+1 contion followed by treduction modules x3 = x+= (mod fcx)