Problema 1

miércoles, 9 de diciembre de 2020 21:22

Problema 1 Considerem en el conjunt $\mathbb{C} = \{z = (a,b) \mid a,b \in \mathbb{R}\}$ les operacions internes següents:

$$(a,b)+(c,d) = (a+c, b+d), \quad \forall (a,b),\ (c,d) \in \mathbb{C},$$
$$(a,b)\cdot(c,d) = (ac-bd, ad+bc), \quad \forall (a,b),\ (c,d) \in \mathbb{C}.$$

i) Determineu l'element neutre de l'operació suma.

ii) Determineu el simètric d'un element (a,b) per l'operació suma.

iii) Proveu que $(\mathbb{C},+)$ té estructura de grup abelià.

iv) Sabent que l'operació producte és commutativa, proveu que l'operació producte és distributiva respecte de l'operació suma.

v) Determineu l'element neutre de l'operació producte. (1,0)

vi) Determineu quins elements són invertibles per l'operació producte, i doneu el seu invers, quan existeixi.

Es pot veure que $(\mathbb{C},+,\cdot)$ té estructura de cos commutatiu i s'anomena cos dels nombres complexos. Notem que $\mathbb{R} \subseteq \mathbb{C}$ i podem representar tot $a \in \mathbb{R}$ com l'element $(a,0) \in \mathbb{C}$. Amb aquesta representació proveu que:

vii) Si $i = (0,1)$ aleshores $i^2 = -1$.

viii) Tot número complex $z = (a,b)$ es pot expressar com $z = a + bi$.

(*Puntuació*: 2 punts: i) 0.2, ii) 0.2, iii) 0.2, iv) 0.2), v) 0.4, vi) 0.4, vii) 0.2, viii) 0.2)

i) L'element neutre és $(0,0)$ Ho demostrem:
   a. $(0,0) \in \mathbb{C}$
   b. $(a,b)+e = e+(a,b) = (a,b) \Rightarrow (a+0, b+0)$
      $= (0+b, 0+b) = (a,b)$

ii) Un element simètric a^{-1} de $(1,1)$ serà $(-1,-1)$ Ho demostrem
   a. $(-1,-1) \in \mathbb{C}$
   b. $(1,1)+(-1,-1) = (-1,-1)+(1,1) = e \Rightarrow$
      $(1-1, 1-1) = (-1+1, -1+1) = (0,0) = e$

iii) $(C,+)$ Tindrà estructura de grup abelià si:
   a. Compleix la propietat associativa:
      $a+(b+c) \stackrel{?}{=} (a+b)+c$
      $$\left.\begin{array}{l} a+(b+c) = a+\left(b_1+c_1, b_2+c_2\right) = (a_1+b_1+c_1, a_2+b_2+c_2) \\ (a+b)+c = \left(a_1+b_1, a_2+b_2\right)+c = (a_1+b_1+c_1, a_2+b_2+c_2) \end{array}\right\} \Rightarrow$$
      $a+(b+c) = (a+b)+c$
      Podem determinar doncs que compleix la propietat associativa.
   b. Existeix element neutre. L'element neutre ja l'hem trobat a l'apartat i)
   c. Tot element de C ha de tenir simètric:
      Cert, ho demostrem:
      $\forall (a,b) \in C, \exists (a,b)^{-1}$
      $(a,b)^{-1} de\ (a,b) = (-a,-b)$
   d. Compleix la propietat commutativa:
      $a+b = b+a$
      $$\left.\begin{array}{r} a+b = (a_1+b_1, a_2+b_2) \\ b+a = \left(b_1+a_1, b_2+a_2\right) \stackrel{?}{=} (a_1+b_1, a_2+b_2) \end{array}\right\} \Rightarrow a+b = b+a$$
      Sabem que la sumà algebraica compleix la propietat commutativa

      Podem determinar doncs que compleix la propietat commutativa.
   Com que compleix totes les propietats necessàries podem dir que té estructura de grup abelià.

iv) Volem demostrar que
   $a \cdot (b+c) = a \cdot b + a \cdot c \ \wedge (a+b) \cdot c = a \cdot c + b \cdot c, \forall a,b,c \in \mathbb{C}$

v) L'element neutre és $(1,0)$ Ho demostrem:
   a. $(1,0) \in \mathbb{C}$
   b. $(a,b)\cdot(1,0) = (1,0)\cdot(a,b) = (a,b) \Rightarrow$
      $(a\cdot 1 - b\cdot 0, a\cdot 0 + b\cdot 1) = (1\cdot a - 0\cdot b, 0\cdot a + 1\cdot b) = (a,b)$

vi) Els elements invertibles per l'operació producte són:
   - $(1,0) \rightarrow (1,0)^{-1} = (1,0)$
   - $(0,-1) \rightarrow (0,-1)^{-1} = (0,1)$
   - $(0,1) \rightarrow (0,1)^{-1} = (0,-1)$

Problema 2

jueves, 7 de enero de 2021 12:11

i) Per determinar els fragments, utilitzarem l'aplicació f

- Fragment Laura: $f(45) = 47 + 29 \cdot 45 + 378 \cdot 45^2 = y_2 = 766802 \equiv 413 \pmod{457}$
- Fragment Albert: $f(321) = 47 + 29 \cdot 321 + 378 \cdot 321^2 = y_4 = 38958854 \equiv 61 \pmod{457}$
- Fragment Roger: $f(54) = 47 + 29 \cdot 54 + 378 \cdot 54^2 = y_5 = 1103861 \equiv 206 \pmod{457}$

ii) Hem de calcular: $b_{24} \pmod{457} \to (x_2 - x_4)^{-1} \pmod{457} \to$

$\to (45 - 321)^{-1} \pmod{457} \to (-276)^{-1} \pmod{457}$

Calcular l'invers, es l'equivalent a calcular la congruència

$-276\, x \equiv 1 \pmod{457}$

1. Aplicant la definició de congruència, obtenim l'equació diofàntica:

$-276\, x - 457 k = 1$

2. Tindrà solució si $mcd(-276, 457) = 1$

$-457 = -276 \cdot 2 + 95 \to 95 = -457 + 276 \cdot 2$

$-276 = 95 \cdot (-3) + 9 \to 9 = -276 + 95 \cdot 3$

$95 = 9 \cdot 10 + 5 \to 5 = 95 - 9 \cdot 10$

$9 = 5 \cdot 1 + 4 \to 4 = 9 - 5$

$5 = 4 \cdot 1 + \boxed{1} \to 1 = 5 - 4$

$4 = 1 \cdot 4 + 0$

Així doncs, $mcd(-276, -457) = 1$

Per tant, podem resoldre l'equació diofàntica

2. $1 = 5 - 4 = 5 - (9 - 5) = 2 \cdot 5 - 9 =$

$= 2 \cdot (95 - 9 \cdot 10) - 9 =$

$= 2 \cdot 95 - 21 \cdot 9 =$

$= 2 \cdot 95 - 21(-276 + 95 \cdot 3) =$ Comprovo

$= 2 \cdot 95 + 21 \cdot 276 - 63 \cdot 95 =$

$= -61 \cdot 95 + 21 \cdot 276 =$

$= -61 \cdot (-457 + 276 \cdot 2) + 21 \cdot 276 =$

$= 61 \cdot 457 - 122 \cdot 276 + 21 \cdot 276 =$

$= 61 \cdot 457 - 101 \cdot 276 \leftarrow$ Comprovo

$\mathbb{Z}_{457}$ $61 \cdot 0 - 101 \cdot 276 = -276 \cdot 101$

Així doncs: $-276 \cdot 101 = 1 \; \mathbb{Z}_{457}$

Per tant, la solució és $b_{24} = 101$

iii) $b_{ij} = (x_i - x_j)^{-1}$

$b_{ji} = (x_j - x_i)^{-1}$

Sigui $s = x_i - x_j$:

$b_{ij} = s^{-1}$

$b_{ji} = (-s)^{-1} \Rightarrow (-1)^{-1} \cdot s^{-1} = -s^{-1}$

iv)

Volem calcular:

$s \equiv 321 \cdot 54 \cdot 101 \cdot 203 \cdot 413 + 45 \cdot 54 \cdot 356 \cdot 368 \cdot 61 + 45 \cdot 321 \cdot 254 \cdot 89 \cdot 206 \equiv$

$\equiv 425 \cdot 101 \cdot 203 \cdot 413 + 145 \cdot 356 \cdot 368 \cdot 61 + 278 \cdot 254 \cdot 89 \cdot 206 \equiv$

$\equiv 424 \cdot 203 \cdot 413 + 436 \cdot 368 \cdot 61 + 234 \cdot 89 \cdot 206 \equiv$

$\equiv 156 \cdot 413 + 41 \cdot 61 + 261 \cdot 206 \equiv 448 + 216 + 297 \equiv 47$

v) Volem calcular:

$K = 47^{2327} \pmod{457}$

Com que 457 és un número primer

$\phi(457) = 456$

Llavors, tenim:

$2327 = 456 \cdot 5 + 47$

Aplicant el teorema d'Euler obtenim que:

$47^{2327} \equiv 47^{47}$

Per calcular 47^{47} apliquem l'algorisme del camperol rus:

$47^{47} \equiv 47^{46} \cdot 47 \equiv (47^{23})^2 \cdot 47 \equiv (47^{22} \cdot 47)^2 \cdot 47 \equiv$

$\equiv ((47^{11})^2 \cdot 47)^2 \cdot 47 \equiv ((47^{10} \cdot 47)^2 \cdot 47)^2 \cdot 47 \equiv$

$\equiv (((47^5)^2 \cdot 47)^2 \cdot 47)^2 \cdot 47 \equiv ((((47^4 \cdot 47)^2 \cdot 47)^2 \cdot 47)^2$

$\equiv ((((47^2)^2 \cdot 47)^2 \cdot 47)^2 \cdot 47)^2 \cdot 47 \equiv$

$\equiv (((381^2 \cdot 47)^2 \cdot 47)^2 \cdot 47)^2 \cdot 47 \equiv (((292 \cdot 47)^2 \cdot 47)^2 \cdot 47)^2$

$\equiv ((14^2 \cdot 47)^2 \cdot 47)^2 \cdot 47 \equiv ((196 \cdot 47)^2 \cdot 47)^2 \cdot 47 \equiv (72^2 \cdot 47)^2 \cdot$

$\cdot 47 \equiv$

$\equiv (157 \cdot 47)^2 \cdot 47 \equiv 67^2 \cdot 47 \equiv 376 \cdot 47 \equiv 306$

Per tant, tenim que $K = 306$

$\cdot 47 \equiv$

$47 \equiv$