Escola Politècnica Superior **Universitat de Lleida**
Grau en Enginyeria Informàtica

Àlgebra

Gener de 2019

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

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

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.

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)

Problema 2 La comissió de tresoreria del Consell de l'Estudiantat de l'EPS està formada per cinc membres: la Marta, la Laura, el Pere, l'Albert i el Roger. Per evitar sospites han decidit no poder tocar els diners que tenen en una caixa forta si no hi són almenys tres dels cinc. A tal fi, han decidit utilitzar un *esquema per a compartir secrets de Shamir* (*secret sharing scheme SSS*, en anglès). En un SSS de Shamir, el distribuïdor escull un secret de $\mathbb{Z}_p$, i assigna a cada participant un element, també de $\mathbb{Z}_p$, anomenat fragment. En el nostre cas, quan tres dels participants col·laborin, podran recuperar el valor del secret original.

El procediment a seguir és:

- Cada participant (la Marta, la Laura, el Pere, l'Albert i el Roger) escull un valor de $\mathbb{Z}_p$, diferent de zero i diferents entre ells. Aquests valors x_i, $i = 1, \ldots, 5$ es fan públics.

- La *distribuïdora* D (que en aquest cas és la Secretària Acadèmica de l'EPS) escull una aplicació $f : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ de la forma

$$f(x) = s + a_1 x + a_2 x^2,$$

on $a_i \in \mathbb{Z}_p$ i de manera que s és el secret que vol compartir. Els valors a_i només els coneix D.

- Finalment, D assigna, de forma privada, el *fragment de secret* $y_i = f(x_i)$ a cada participant.

En el cas de l'EPS, la distribuïdora ha escollit $p = 457$ i cada partipant ha escollit el valor públic següent:

$$\begin{array}{lll} \text{Marta} : x_1 = 100, & \text{Laura} : x_2 = 45, & \text{Pere} : x_3 = 230, \\ \text{Albert} : x_4 = 321, & \text{Roger} : x_5 = 54 & \end{array}$$

De forma secreta D escull $a_1 = 29, a_2 = 378$ i $s = 47$.

i) Determineu els fragments que la distribuïdora donarà a la Laura, l'Albert i el Roger.

Quan aquests tres estudiants es reuneixen i volen trobar el secret compartit s, han de fer un seguit de càlculs, coneguts amb el nom de *mètode d'interpolació de Lagrange.*

ii) En primer lloc han de calcular els inversos modulars a $\mathbb{Z}_p$ següents: $b_{ij} = (x_i - x_j)^{-1}$. Calculeu b_{24}.

iii) Determineu com es pot calcular b_{ji} a partir de b_{ij}.

iv) Els tres amics poden trobar el valor de s de la forma següent:

$$s \equiv x_4 \cdot x_5 \cdot b_{24} \cdot b_{25} \cdot y_2 + x_2 \cdot x_5 \cdot b_{42} \cdot b_{45} \cdot y_4 + x_2 \cdot x_4 \cdot b_{52} \cdot b_{54} \cdot y_5 \pmod{457}.$$

Trobeu el valor de s sabent que $b_{25} = 203, b_{42} = 356, b_{45} = 368, b_{52} = 254, b_{54} = 89$.

v) Determineu el valor de la combinació secreta de la caixa forta $K \equiv s^{2327} \pmod{457}$, utilitzant el teorema d'Euler i l'algorisme del camperol rus.

(*Puntuació*: 2 punts: i) 0.2, ii) 0.7, iii) 0.2, iv) 0.2), v) 0.7)