Polinomis i codis

Competències que s'avaluen: C6 i C7.

En la teoria moderna de codis es fan servir polinomis per xifrar. Qualsevol transferència bancària, identificació amb password (com per exemple instagram, twitter, facebook, google, etc) o connexió a una xarxa wifi passa pel xifratge relacionat amb la divisió de polinomis. És un procés complicat i que té una base teòrica molt abstracta. No obstant, en aquest exercici veurem una versió simplificada dels conceptes més elementals que hi intervenen.

Qualsevol missatge es pot traduir a una seqüència de nombres, i qualsevol seqüència de nombres es pot interpretar com els coeficients d'un polinomi. Per exemple, els nombres 12301 es poden interpretar com els coeficients d'un polinomi de grau 4:

$$x^4 + 2x^3 + 3x^2 + 1$$

Fixeu-vos que el terme de grau 1 no hi apareix perquè el coeficient corresponent és 0.
Per tal de xifrar s'estableix una clau, per exemple la clau 11, que correspondria al polinomi $x + 1$. Aquesta clau ens permet xifrar un nombre simplement multiplicant els dos polinomis corresponents. Per exemple, el missatge 1320 en la clau 11 esdevé

$$\underbrace{(x^3 + 3x^2 + 2x)}_{1320} \cdot \underbrace{(x + 1)}_{11} = \underbrace{x^4 + 4x^3 + 5x^2 + 2x}_{14520}$$

I el missatge xifrat corresponent a 1320 és 14520.
I com podem desxifrar un missatge? Evidentment necessitarem saber la clau, i l'únic que haurem de fer és passar el missatge xifrat a polinomi i dividir entre el polinomi corresponent a la clau. Per exemple, si la clau és 11 i el missatge xifrat és 132, només caldrà dividir el polinomi $x^2 + 3x + 2$ entre $x + 1$, cosa que podem fer per Ruffini

	1	3	2
-1		-1	-2
	1	2	0

i el missatge sense xifrar és 12.
Ara ens podem preguntar, i què passa si en desxifrar un missatge obtenim un residu que no és 0? Doncs diem que el residu és l'error que s'ha comès en el procés de xifratge.

1) Codifiqueu els següents missatges segons la clau 11
   a) 1032
   b) 11111
   c) 1034
2) Descodifiqueu els següents missatges segons la clau 11
   a) 1441
   b) 1111
   c) 12320
3) Digueu l'error que s'ha comès en xifrar els següents missatges segons la clau 12.
   (a) 13441
   (b) 121575
4) Esbrineu la clau que s'ha utilitzat en xifrar el missatge 1234 si el missatge xifrat ha estat 124634.