Pràctica 1: Aritmètica

Funcions útils per a realitzar la pràctica:

- digits (base=10, digits=None, padto=0)
- degree (x=None, std_grading=False)
- polynomials (of_degree=None, max_degree=None)

1. Criteris de Divisibilitat (**2 punts**)

   (a) Criteri del 7. Per saber si un nombre és divisible per 7, eliminem la xifra de les unitats (u) i, al nombre resultant, li restem el doble de la unitat eliminada ($2 \cdot u$). Repetim aquest procés fins que el nombre resultant sigui igual o inferior a 70. En aquest punt, mirem si el resultat és divisible per 7. Podeu utilitzar la taula del 7 fins al 10 per saber si un nombre inferior a 70 és divisible per 7.
   Escriviu una funció que retorni True si un nombre és divisible per 7 utilitzant aquest mètode. Per a implementar aquesta funció, no podeu utilitzar cap altre criteri o funció que indiqui la divisibilitat (e.g. mòdul).

   (b) Criteri del 13. Per saber si un nombre és divisible per 13, eliminem la xifra de les unitats (u) i, al nombre resultant, li restem 9 vegades la unitat eliminada ($9 \cdot u$). Repetim aquest procés fins que el resultat sigui un nombre de dos xifres. En aquest punt, mirem si el resultat és divisible per 13. Podeu utilitzar la taula del 13 fins al 7 per saber si un nombre de dues xifres és divisible per 13.
   Escriviu una funció que retorni True si un nombre és divisible per 13 utilitzant aquest mètode. Per implementar aquesta funció, no podeu utilitzar cap altre criteri o funció que indiqui la divisibilitat (e.g. mòdul).

2. Identitat de Bézout (**4 punts**)

   (a) Implementeu la funció `UAB_extended_gcd(m,n)` que calculi el màxim comú divisor (d) i els coeficients de la identitat de Bézout (a,b) tals que

   $$mcd(m,n) = d = am + bn$$

   El resultat d'aquesta funció ha de ser la llista `[d,a,b]`. Per exemple:

   $$[13,-54,65] = \texttt{UAB\_extended\_gcd}\,(2613,2171)$$

   Per a implementar aquesta funció, heu d'utilitzar l'algorisme estès d'Euclides. No podeu utilitzar la funció *xgcd* ni la *gcd*.

   (b) Utilitzant la funció `UAB_extended_gcd(m,n)`, creeu la funció `UAB_inverse_modulo(a,p)` que retorni l'invers de a a $\mathbb{Z}_p$ (assumint que p és primer).

3. L'anell quocient de $\mathbb{Z}_3[x]/m(x)$ (**4 punts**)

   (a) Utilitzeu la funció `UAB_extended_gcd(m,n)` per crear la funció `UAB_zero_divisors(mx)`, la qual ha de retornar la llista amb tots els divisors de zero a $\mathbb{Z}_3[x]/m(x)$. Per implementar aquesta funció, podeu utilitzar la funció `polynomials`.

   (b) Implementeu la funció `UAB_is_field(mx)` que retorni `True` o `False` en funció de si $\mathbb{Z}_3[x]/m(x)$ és o no un cos. Per implementar aquesta funció, heu d'utilitzar la funció `UAB_zero_divisors(mx)`.
   Comproveu que el resultat de la vostra implementació és correcte mitjançant la funció `is_irreducible`.