

Aritmètica polinomial i cossos finits

Maria Bras-Amorós, Oriol Farràs Ventura

29 de novembre de 2023

Aritmètica polinomial

Congruències de polinomis i anells quocient $\mathbb{Z}_p/f(x)$

Cossos finits

Exercicis

Solucions

Aritmètica polinomial

Polinomis a \mathbb{Z}_m

Divisió de polinomis

Algoritme d'Euclides i identitat de Bézout

Arrels de polinomis

Polinomis irreductibles

Factorització de polinomis

Congruències de polinomis i anells quocient $\mathbb{Z}_p/f(x)$

Congruències de polinomis

Anells quocient $\mathbb{Z}_p/f(x)$

Aritmètica dels anells quocient $\mathbb{Z}_p/f(x)$

Cossos finits

Elements invertibles

Construcció de cossos finits

Ordre i elements primitius

Representació d'elements

Resum

Exercicis

Solucions

Polinomis amb coeficients a \mathbb{Z}_m

Anomenem $\mathbb{Z}_m[x]$ al conjunt de polinomis amb coeficients a \mathbb{Z}_m

Exemple

$$a(x) = 4x^7 + 3x^4 + x + 3 \in \mathbb{Z}_5[x],$$

$$b(x) = 2x^4 + 3 \in \mathbb{Z}_5[x].$$

Els elements de \mathbb{Z}_m s'anomenen les **constants** o els **escalars** de $\mathbb{Z}_m[x]$.

El **grau**, els **coeficients**, el **termes**, etc., es defineixen de manera anàloga als polinomis de $\mathbb{R}[x]$.

Direm que un polinomi és **mònic** si el seu coeficient de grau màxim és 1.

Les sumes a $\mathbb{Z}_m[x]$ es fan coeficient a coeficient segons la suma a \mathbb{Z}_m .

Exemple

$$\begin{aligned}a(x) + b(x) &= (4x^7 + 3x^4 + x + 3) + (2x^4 + 3) \\&= 4x^7 + (3 + 2)x^4 + x + (3 + 3) \\&= 4x^7 + x + 1.\end{aligned}$$

Aritmètica polinomial

El producte de polinomis es fa utilitzant la propietat distributiva i el producte i la suma dels coeficients segons la suma i el producte a \mathbb{Z}_m .

Exemple

$$\begin{aligned}a(x) \cdot b(x) &= (4x^7 + 3x^4 + x + 3)(2x^4 + 3) \\&= 4x^7(2x^4 + 3) + 3x^4(2x^4 + 3) + x(2x^4 + 3) + 3(2x^4 + 3) \\&= (3x^{11} + 2x^7) + (x^8 + 4x^4) + (2x^5 + 3x) + (x^4 + 4) \\&= 3x^{11} + x^8 + 2x^7 + 2x^5 + 3x + 4.\end{aligned}$$

Exercici 1

- ▶ Doneu un exemple en que $\text{grau}(a(x)b(x)) \neq \text{grau}(a(x)) + \text{grau}(b(x))$.
- ▶ Proveu que si m és primer, aleshores $\text{grau}(a(x)b(x)) = \text{grau}(a(x)) + \text{grau}(b(x))$.

Llevat que no s'especifiqui el contrari, **a partir d'ara només considerarem polinomis de $\mathbb{Z}_p[x]$ amb p primer.**

En general emprarem p per denotar un primer.

Aritmètica polinomial

Polinomis a \mathbb{Z}_m

Divisió de polinomis

Algoritme d'Euclides i identitat de Bézout

Arrels de polinomis

Polinomis irreductibles

Factorització de polinomis

Congruències de polinomis i anells quocient $\mathbb{Z}_p/f(x)$

Congruències de polinomis

Anells quocient $\mathbb{Z}_p/f(x)$

Aritmètica dels anells quocient $\mathbb{Z}_p/f(x)$

Cossos finits

Elements invertibles

Construcció de cossos finits

Ordre i elements primitius

Representació d'elements

Resum

Exercicis

Solucions

Divisió de polinomis

Teorema 1: Divisió de polinomis

Donats dos polinomis qualssevol $a(x), b(x) \in \mathbb{Z}_p[x]$ existeixen dos altres polinomis únics $q(x), r(x) \in \mathbb{Z}_p[x]$ tals que

$$a(x) = b(x)q(x) + r(x)$$

amb $0 \leq \text{grau}(r(x)) < \text{grau}(b(x))$.

Dividend, divisor, quocient, residu

Els polinomis $a(x)$ i $b(x)$ són, respectivament, el **dividend** i el **divisor** de la divisió. El polinomi $q(x)$ és el **quocient**. El polinomi $r(x)$ és el **residu**.

Divisió de polinomis

Podem dividir de la manera habitual construint el polinomi quocient $q(x)$ dels termes de grau més gran als de grau més petit.

Exemple

Vegeu-ho amb els polinomis anteriors.

El primer terme de $q(x)$ haurà de ser $2x^3$:

$$\begin{array}{r} 4x^7 + 3x^4 + x + 3 \\ - (4x^7 + x^3) \\ \hline 3x^4 + 4x^3 + x + 3 \end{array} \quad \begin{array}{r} 2x^4 + 3 \\ 2x^3 + \end{array}$$

i continuem pel terme 4:

$$\begin{array}{r} 4x^7 + 3x^4 + x + 3 \\ - (4x^7 + x^3) \\ \hline 3x^4 + 4x^3 + x + 3 \\ - (3x^4 + 2) \\ \hline 4x^3 + x + 1 \end{array} \quad \begin{array}{r} 2x^4 + 3 \\ 2x^3 + 4 \end{array}$$

Divisió de polinomis

Exemple

En notació anglosaxona és

$$\begin{array}{r} 2x^4 + 3 \overline{) \begin{array}{r} 2x^3 + 4x^7 + 3x^4 + x + 3 \\ - (4x^7 + x^3) \\ \hline 3x^4 + 4x^3 + x + 3 \end{array}} \end{array}$$

i continuem pel terme 4:

$$\begin{array}{r} 2x^4 + 3 \overline{) \begin{array}{r} 2x^3 + 4x^7 + 3x^4 + x + 3 \\ - (4x^7 + x^3) \\ \hline 3x^4 + 4x^3 + x + 3 \\ - (3x^4 + 2) \\ \hline 4x^3 + x + 1 \end{array}} \end{array}$$

Divisió de polinomis

Exemple

Deduïm que

$$q(x) = 2x^3 + 4,$$

$$r(x) = 4x^3 + x + 1.$$

Observem que el grau de $r(x)$ és més petit que el de $b(x)$ i que $a(x) = b(x)q(x) + r(x)$.

Divisors

Si $r(x) = 0$, aleshores diem que $b(x)$ és un **divisor** de $a(x)$ i que $a(x)$ és un **múltiple** de $b(x)$.

Observem que si $b(x)$ és un divisor de $a(x)$, aleshores per a qualsevol element no nul $k \in \mathbb{Z}_p$, també tenim que $kb(x)$ és un divisor de $a(x)$. Diem que $kb(x)$ és un **múltiple escalar** de $b(x)$.

Definim l'estructura (anell) dels polinomis sobre un anell \mathbb{Z}_m de la manera següent:

```
Z5=Integers(5)  
P.<x>=PolynomialRing(Z5)
```

En fer aquesta definició també estem definint la indeterminada x . Aleshores podem escriure els polinomis de la manera habitual.

```
a=4*x^7+3*x^4+x+3  
b=2*x^3+1
```

o en forma de llista:

```
a=P([3,1,0,0,3,0,0,4])  
b=P([1,0,0,2])
```

Podem operar els polinomis de la manera habitual:

$a+b$

$a*b$

El quocient i el residu d'una divisió s'escriuen com hem vist pels enters

$a // b$

$a \% b$

Podem avaluar-los en una constant:

$a(3)$

$b(4)$

Aritmètica polinomial

Polinomis a \mathbb{Z}_m

Divisió de polinomis

Algoritme d'Euclides i identitat de Bézout

Arrels de polinomis

Polinomis irreductibles

Factorització de polinomis

Congruències de polinomis i anells quocient $\mathbb{Z}_p/f(x)$

Congruències de polinomis

Anells quocient $\mathbb{Z}_p/f(x)$

Aritmètica dels anells quocient $\mathbb{Z}_p/f(x)$

Cossos finits

Elements invertibles

Construcció de cossos finits

Ordre i elements primitius

Representació d'elements

Resum

Exercicis

Solucions

Algoritme d'Euclides i identitat de Bézout

El màxim comú divisor, l'algoritme d'Euclides i la identitat de Bézout per a polinomis es poden definir de forma anàloga a com ho hem fet per als enters.

Ara, quan diem el màxim dels divisors comuns, ens referim al de màxim grau.

Exercici 2

Demostreu que el màxim comú divisor de dos polinomis és unívocament definit llevat del producte per constants no nul·les.

Solució (p.96)

Si p és primer, tot parell de polinomis no nuls de $\mathbb{Z}_p[x]$ tindrà un mcd mònic i aquest és únic. Si diem “ e/mcd ” ens estarem referint a aquest.

Algoritme d'Euclides i identitat de Bézout

Exemple

Volem calcular a $\mathbb{Z}_5[x]$ el màxim comú divisor i els coeficients de la identitat de Bézout corresponent als polinomis $a = x^5 + x + 1$ i $b = x^3 + x^2$.

I completem la taula:

λ	1	0				
μ	0	1				
quocients						
residus	$x^5 + x + 1$	$x^3 + x^2$				

Algoritme d'Euclides i identitat de Bézout

Exemple

Volem calcular a $\mathbb{Z}_5[x]$ el màxim comú divisor i els coeficients de la identitat de Bézout corresponent als polinomis $a = x^5 + x + 1$ i $b = x^3 + x^2$. Fem les divisions successives:

$$\begin{array}{r}
 \begin{array}{r}
 x^5 \qquad \qquad \qquad + x + 1 \\
 -(x^5 + x^4) \qquad \qquad \qquad) \\
 \hline
 4x^4 \qquad \qquad \qquad + x + 1 \\
 -(4x^4 + 4x^3) \qquad \qquad \qquad) \\
 \hline
 x^3 \qquad \qquad \qquad + x + 1 \\
 -(x^3 + x^2) \qquad \qquad \qquad) \\
 \hline
 4x^2 + x + 1
 \end{array}
 \qquad
 \begin{array}{r}
 x^3 + x^2 \\
 \overline{x^2 + 4x + 1}
 \end{array}
 \end{array}$$

I completem la taula:

λ	1	0	1			
μ	0	1	$4x^2 + x + 4$			
quocients			$x^2 + 4x + 1$			
residus	$x^5 + x + 1$	$x^3 + x^2$	$4x^2 + x + 1$			

Algoritme d'Euclides i identitat de Bézout

Exemple

Volem calcular a $\mathbb{Z}_5[x]$ el màxim comú divisor i els coeficients de la identitat de Bézout corresponent als polinomis $a = x^5 + x + 1$ i $b = x^3 + x^2$. Fem les divisions successives:

$$\begin{array}{r}
 x^3 + x^2 \\
 -(x^3 + 4x^2 + 4x) \\
 \hline
 2x^2 + x \\
 -(2x^2 + 3x + 3) \\
 \hline
 3x + 2
 \end{array}
 \quad
 \begin{array}{r}
 4x^2 + x + 1 \\
 4x + 3
 \end{array}$$

I completem la taula:

λ	1	0	1	$x + 2$		
μ	0	1	$4x^2 + x + 4$	$4x^3 + 4x^2 + x + 4$		
quocients			$x^2 + 4x + 1$	$4x + 3$		
residus	$x^5 + x + 1$	$x^3 + x^2$	$4x^2 + x + 1$	$3x + 2$		

Algoritme d'Euclides i identitat de Bézout

Exemple

Volem calcular a $\mathbb{Z}_5[x]$ el màxim comú divisor i els coeficients de la identitat de Bézout corresponent als polinomis $a = x^5 + x + 1$ i $b = x^3 + x^2$. Fem les divisions successives:

$$\begin{array}{r} 4x^2 + x + 1 \quad \bigg| 3x + 2 \\ -(4x^2 + x) \quad \quad \quad 3x \\ \hline 1 \end{array}$$

I completem la taula:

λ	1	0	1	$x + 2$	$2x^2 + 4x + 1$	
μ	0	1	$4x^2 + x + 4$	$4x^3 + 4x^2 + x + 4$	$3x^4 + 3x^3 + x^2 + 4x + 4$	
quocients			$x^2 + 4x + 1$	$4x + 3$	$3x$	
residus	$x^5 + x + 1$	$x^3 + x^2$	$4x^2 + x + 1$	$3x + 2$	1	

Algoritme d'Euclides i identitat de Bézout

Exemple

Volem calcular a $\mathbb{Z}_5[x]$ el màxim comú divisor i els coeficients de la identitat de Bézout corresponent als polinomis $a = x^5 + x + 1$ i $b = x^3 + x^2$. Fem les divisions successives:

$$\begin{array}{r}
 3x + 2 \quad \bigg| 1 \\
 -(3x \quad \quad) \\
 \hline
 2 \\
 -(2) \\
 \hline
 0
 \end{array}$$

I completem la taula:

λ	1	0	1	$x + 2$	$2x^2 + 4x + 1$	
μ	0	1	$4x^2 + x + 4$	$4x^3 + 4x^2 + x + 4$	$3x^4 + 3x^3 + x^2 + 4x + 4$	
quocients			$x^2 + 4x + 1$	$4x + 3$	$3x$	$3x + 2$
residus	$x^5 + x + 1$	$x^3 + x^2$	$4x^2 + x + 1$	$3x + 2$	1	0

Algorisme d'Euclides i identitat de Bézout

Exemple

Volem calcular a $\mathbb{Z}_5[x]$ el màxim comú divisor i els coeficients de la identitat de Bézout corresponent als polinomis $a = x^5 + x + 1$ i $b = x^3 + x^2$.

Deduïm que el màxim comú divisor és 1 i que els coeficients de la identitat de Bézout són $2x^2 + 4x + 1$ i $3x^4 + 3x^3 + x^2 + 4x + 4$.

Per tant, la identitat de Bézout queda de la forma

$$(2x^2 + 4x + 1)(x^5 + x + 1) + (3x^4 + 3x^3 + x^2 + 4x + 4)(x^3 + x^2) = 1.$$

Aritmètica polinomial

Polinomis a \mathbb{Z}_m

Divisió de polinomis

Algoritme d'Euclides i identitat de Bézout

Arrels de polinomis

Polinomis irreductibles

Factorització de polinomis

Congruències de polinomis i anells quocient $\mathbb{Z}_p/f(x)$

Congruències de polinomis

Anells quocient $\mathbb{Z}_p/f(x)$

Aritmètica dels anells quocient $\mathbb{Z}_p/f(x)$

Cossos finits

Elements invertibles

Construcció de cossos finits

Ordre i elements primitius

Representació d'elements

Resum

Exercicis

Solucions

Arrels de polinomis

Lema 1: Arrels

Donat un polinomi $f(x) \in \mathbb{Z}_p[x]$ i $a \in \mathbb{Z}_p$, són equivalents:

- ▶ $x - a$ divideix $f(x)$,
- ▶ $f(a) = 0$.

En aquest cas, diem que a és una **arrel** de $f(x)$.

Demostració

Si $x - a$ divideix $f(x)$, aleshores existeix $q(x)$ tal que $f(x) = (x - a)q(x)$, i en aquest cas és clar que $f(a) = 0$.



Arrels de polinomis

Lema 1: Arrels

Donat un polinomi $f(x) \in \mathbb{Z}_p[x]$ i $a \in \mathbb{Z}_p$, són equivalents:

- ▶ $x - a$ divideix $f(x)$,
- ▶ $f(a) = 0$.

En aquest cas, diem que a és una **arrel** de $f(x)$.

Demostració

Suposem ara que $f(a) = 0$. Dividim $f(x)$ entre $(x - a)$ i obtindrem un quocient $q(x)$ i un residu r de grau més petit que 1 (i, per tant, constant) tal que $f(x) = (x - a)q(x) + r$. Si ara utilitzem que $f(a) = 0$, i ho substituïm a la igualtat anterior obtenim $f(a) = 0 + r = 0$ i, per tant, $r = 0$.

Això vol dir que $f(x) = (x - a)q(x)$.

□

Exercici 3

És $x - 3$ un divisor de $x^5 + 2x^3 + 3x^2 + 1$ a $\mathbb{Z}_7[x]$? I a $\mathbb{Z}_5[x]$?
I a $\mathbb{Z}_3[x]$? I a $\mathbb{Z}_2[x]$?

Solució (p.97)

Exercici 4

Demostreu que un polinomi de $\mathbb{Z}_2[x]$,

- ▶ és divisible per x si i només si no té terme constant;
- ▶ és divisible per $x + 1$ si i només si té un nombre parell de termes.

Solució (p.98)

Arrels de polinomis

Exercici 5: Mètode per trobar les arrels d'un polinomi de grau dos a \mathbb{Z}_p , en cas de p primer senar.

1. Per què podem afirmar que 2 és un element invertible de \mathbb{Z}_p ?
2. En general, qui és l'element 2^{-1} , invers de 2 a \mathbb{Z}_p , en funció de p ?
3. Considerem la taula dels quadrats de tots els elements de \mathbb{Z}_p . Per exemple, la taula dels quadrats de \mathbb{Z}_5 seria:

a	a^2
0	0
1	1
2	4
3	4
4	1

Doneu la taula dels quadrats de \mathbb{Z}_7 .

Solució (p.99)

Arrels de polinomis

Exercici 5: Mètode per trobar les arrels d'un polinomi de grau dos a \mathbb{Z}_p , en cas de p primer senar.

4. Si $a \in \mathbb{Z}_p$, aleshores definim el **conjunt d'arrels quadrades** $\sqrt{a}^{\mathbb{Z}_p}$ com el conjunt de tots els elements $b \in \mathbb{Z}_p$ tals que $b^2 = a$. Així, per exemple, els conjunts d'arrels quadrades de tots els elements de \mathbb{Z}_5 són els següents:

$$\begin{aligned}\sqrt{0}^{\mathbb{Z}_5} &= \{0\} \\ \sqrt{1}^{\mathbb{Z}_5} &= \{1, 4\} \\ \sqrt{2}^{\mathbb{Z}_5} &= \emptyset = \{\} \\ \sqrt{3}^{\mathbb{Z}_5} &= \emptyset = \{\} \\ \sqrt{4}^{\mathbb{Z}_5} &= \{2, 3\}\end{aligned}$$

Doneu els conjunts d'arrels quadrades de tots els elements de \mathbb{Z}_7 .

Solució (p.99)

Arrels de polinomis

Exercici 5: Mètode per trobar les arrels d'un polinomi de grau dos a \mathbb{Z}_p , en cas de p primer senar.

5. Si $b, c \in \mathbb{Z}_p$ són tals que $\sqrt{b^2 - 4c}^{\mathbb{Z}_p}$ té un o més valors diferents, aleshores les arrels de $x^2 + bx + c$ són

$$(-b + \sqrt{b^2 - 4c}^{\mathbb{Z}_p}) \frac{p+1}{2} \mod p$$

o, dit d'altra manera, són els valors $(-b + y) \frac{p+1}{2} \mod p$ on y agafa tots els valors de $\sqrt{b^2 - 4c}^{\mathbb{Z}_p}$.

Per exemple, les arrels de $x^2 + 3x + 2 \in \mathbb{Z}_5[x]$ són

$$\begin{aligned} (-b + \sqrt{b^2 - 4c}^{\mathbb{Z}_p}) \frac{p+1}{2} \mod 5 &= (-3 + \sqrt{4 - 3}^{\mathbb{Z}_p}) \frac{5+1}{2} \mod 5 \\ &= (2 + \sqrt{1}^{\mathbb{Z}_p}) 3 \mod 5 \\ &= 1 + 3\{1, 4\} \mod 5 \\ &= \begin{cases} 1 + 3 \cdot 1 \mod 5 = 4 \\ 1 + 3 \cdot 4 \mod 5 = 3 \end{cases} \end{aligned}$$

Comproveu que 4 i 5 són, en efecte, arrels de $x^2 + 3x + 2 \in \mathbb{Z}_5[x]$.

Arrels de polinomis

Exercici 5: Mètode per trobar les arrels d'un polinomi de grau dos a \mathbb{Z}_p , en cas de p primer senar.

6. A $\mathbb{Z}_7[x]$ trobeu les arrels dels següents polinomis:

- ▶ $x^2 + 5x + 1$,
- ▶ $x^2 + 6$,
- ▶ $x^2 + 5x + 4$.

7. Comproveu les arrels obtingudes en l'apartat anterior.

Solució (p.99)

Lema 2

El nombre d'arrels d'un polinomi $f(x) \in \mathbb{Z}_p[x]$ és com a molt el seu grau.

Exercici 6

Demostreu el lema anterior.

Solució (p.102)

Per trobar les arrels de a podem escriure

```
[a(y) for y in Z5]
```

o, més precisament,

```
[y for y in Z5 if a(y)==0]
```

Sage té la seva pròpia funció per trobar les arrels (amb multiplicitat)

```
print("roots(a)=",a.roots())
```

Aritmètica polinomial

Polinomis a \mathbb{Z}_m

Divisió de polinomis

Algoritme d'Euclides i identitat de Bézout

Arrels de polinomis

Polinomis irreductibles

Factorització de polinomis

Congruències de polinomis i anells quocient $\mathbb{Z}_p/f(x)$

Congruències de polinomis

Anells quocient $\mathbb{Z}_p/f(x)$

Aritmètica dels anells quocient $\mathbb{Z}_p/f(x)$

Cossos finits

Elements invertibles

Construcció de cossos finits

Ordre i elements primitius

Representació d'elements

Resum

Exercicis

Solucions

Polinomis irreductibles

Polinomis irreductibles

Un polinomi és **irreductible** si els seus únics divisors són 1 i ell mateix i tots els seus múltiples escalars possibles.

Observem que tots els escalars no nuls i tots els polinomis de grau 1 són irreductibles.

Polinomis irreductibles

Si un polinomi de grau més gran que 1 és irreductible, aleshores no té arrels.

Perquè, si tingués una arrel a , aleshores tindria un factor de la forma $x - a$.

Exemple

El polinomi $f(x) = x^2 + x + 1$ és irreductible a $\mathbb{Z}_2[x]$ i no té arrels. En efecte, $f(0) = 1 \neq 0$ i $f(1) = 3 = 1 \neq 0$.

El recíproc no és cert.

Exemple

A $\mathbb{Z}_2[x]$, el polinomi $g(x) = x^4 + x^2 + 1$ no té arrels perquè $g(0) = 1 \neq 0$ i $g(1) = 3 = 1 \neq 0$. Però, en canvi,
$$(x^2 + x + 1)(x^2 + x + 1) = x^4 + x^3 + x^2 + x^3 + x^2 + x + x^2 + x + 1 =$$
$$x^4 + 2x^3 + 3x^2 + 2x + 1 = x^4 + x^2 + 1 = g(x), \text{ és a dir, } g(x) \text{ no és irreductible.}$$

Polinomis irreductibles

Exemple

Considerem el polinomi

$$f(x) = x^4 + x^3 + 2x^2 + 2x + 1 \in \mathbb{Z}_3[x].$$

Comproveu que no té arrels.

I, tanmateix, $f(x)$ no és irreductible perquè

$$f(x) = (x^2 + 2x + 2)^2.$$

Exercici 7

Demostreu que, si un polinomi té grau 2 o 3, aleshores el polinomi és irreductible si i només si no té arrels.

Solució (p.103)

Polinomis irreductibles

Exercici 8

Trobeu tots els polinomis irreductibles de grau més petit o igual que 4 de $\mathbb{Z}_2[x]$.

Solució (p.104)

Exercici 9

Considerem els polinomis de $\mathbb{Z}_2[x]$

$$\begin{aligned}f &= x^5 + x^2 + 1, \\g &= x^2 + x + 1.\end{aligned}$$

1. Quins són el quocient i el residu de dividir f entre g ?
2. Demostreu que f i g són irreductibles a $\mathbb{Z}_2[x]$.

Solució (p.106)

Exercici 10

1. Quants polinomis mònicos hi ha a $\mathbb{Z}_3[x]$ de grau 2?
2. Quins són els polinomis irreductibles mònicos de $\mathbb{Z}_3[x]$ de grau 2?

Solució (p.107)

Exercici 11

1. Considerem el conjunt P de polinomis amb coeficients a \mathbb{Z}_3 que tenen exactament un monomi de grau senar i coeficient 1 i la resta de monomis de grau parell. Poseu-ne un exemple.
2. Demostreu que un polinomi $p \in P$ que sigui irreductible ha de complir:
 - 2.1 La suma dels seus coeficients no és múltiple de 3.
 - 2.2 La suma dels seus coeficients no és congruent amb 2 mòdul 3.
3. Doneu una altra condició que ha de complir un polinomi de P que sigui irreductible.

Solució (p.108)

Aritmètica polinomial

Polinomis a \mathbb{Z}_m

Divisió de polinomis

Algoritme d'Euclides i identitat de Bézout

Arrels de polinomis

Polinomis irreductibles

Factorització de polinomis

Congruències de polinomis i anells quocient $\mathbb{Z}_p/\mathbf{f}(x)$

Congruències de polinomis

Anells quocient $\mathbb{Z}_p/\mathbf{f}(x)$

Aritmètica dels anells quocient $\mathbb{Z}_p/\mathbf{f}(x)$

Cossos finits

Elements invertibles

Construcció de cossos finits

Ordre i elements primitius

Representació d'elements

Resum

Exercicis

Solucions

Factorització de polinomis

Factorització

Tot polinomi es pot descompondre en producte de polinomis irreductibles.

Aquí la descomposició és única llevat del producte per escalars.

Exemple

Per exemple, a $\mathbb{Z}_5[x]$

$$2x^2 + 3 = (x + 1)(2x + 3).$$

Però també

$$2x^2 + 3 = (2x + 2)(x + 4).$$

I també podem separar amb una constant i un producte de polinomis irreductibles mòncics:

$$2x^2 + 3 = 2(x + 1)(x + 4).$$

Factorització de polinomis

Factorització

Si p és primer, tot polinomi de $\mathbb{Z}_p[x]$ es pot descompondre de manera única en el producte d'una constant per un producte de polinomis irreductibles mòncics.

Aquí és important que p sigui primer. Per exemple, a $\mathbb{Z}_4[x]$, el polinomi $2x + 3$ no es pot escriure com una constant per un polinomi mònic perquè 2 no té invers a \mathbb{Z}_4 .

De la mateixa manera, a \mathbb{Z}_8 , el polinomi $x^2 + 7$ admet dues descomposicions diferents: $x^2 + 7 = (x + 1)(x + 7) = (x + 3)(x + 5)$.

Factorització de polinomis

La demostració de la unicitat de la factorització en irreductibles és equivalent a la vista pel cas dels enters. En el cas dels enters, a partir de la Identitat de Bézout hem deduït que, si p és primer i $p \mid ab$, aleshores $p \mid a$ o $p \mid b$. D'aquí se segueix la demostració de la factorització en primers.

En el cas de polinomis podem demostrar, també a partir de la identitat de Bézout, que si $c(x)$ és irreductible i $c(x) \mid a(x)b(x)$, aleshores $c(x) \mid a(x)$ o $c(x) \mid b(x)$. I ara aquest resultat el podem utilitzar per demostrar la unicitat de la factorització en irreductibles.

Factorització de polinomis

Exercici 12

Factoritzeu completament el polinomi $2x^4 + 4x^2 + 3x + 1$ a $\mathbb{Z}_5[x]$.

Solució (p.109)

Podem coprovar si un polinomi és irreducible

```
a.is_irreducible()
```

O mirar de factoritzar-lo

```
factor(a)
```

Aritmètica polinomial

Congruències de polinomis i anells quocient $\mathbb{Z}_p/\mathbf{f}(x)$

Cossos finits

Exercicis

Solucions

Aritmètica polinomial

Polinomis a \mathbb{Z}_m

Divisió de polinomis

Algoritme d'Euclides i identitat de Bézout

Arrels de polinomis

Polinomis irreductibles

Factorització de polinomis

Congruències de polinomis i anells quocient $\mathbb{Z}_p/f(x)$

Congruències de polinomis

Anells quocient $\mathbb{Z}_p/f(x)$

Aritmètica dels anells quocient $\mathbb{Z}_p/f(x)$

Cossos finits

Elements invertibles

Construcció de cossos finits

Ordre i elements primitius

Representació d'elements

Resum

Exercicis

Solucions

Congruències de polinomis

Definició

Si $r(x)$ és el residu de dividir $a(x)$ per $m(x)$, aleshores diem que $r(x)$ és la **reducció de $a(x)$ mòdul $m(x)$** . Escriurem

$$a(x) = r(x) \mod m(x).$$

Exemple

Considerem els polinomis del principi de la secció,

$$a(x) = 4x^7 + 3x^4 + x + 3 \text{ i } b(x) = 2x^4 + 3 \in \mathbb{Z}_5.$$

En fer la divisió euclidiana de $a(x)$ entre $b(x)$ hem vist que el seu quocient i residu són, respectivament, $q(x) = 2x^3 + 4$ i $r(x) = 4x^3 + x + 1$.

En aquest cas, diem que la reducció de $4x^7 + 3x^4 + x + 3$ mòdul $2x^4 + 3$ és $4x^3 + x + 1$ o que

$$4x^7 + 3x^4 + x + 3 = 4x^3 + x + 1 \mod 2x^4 + 3$$

Congruències de polinomis

Congruències

Donats tres polinomis $a(x), b(x), f(x) \in \mathbb{Z}_p[x]$, diem que $a(x)$ i $b(x)$ són **congruents** mòdul $f(x)$ si, equivalentment,

- ▶ els residus de dividir $a(x)$ i $b(x)$ entre $f(x)$ coincideixen,
- ▶ la diferència $b(x) - a(x)$ és un múltiple de $f(x)$.

Escrivim

$$a(x) \equiv b(x) \pmod{f(x)}$$

Exercici 13

Comproveu que, efectivament, les dues condicions de la definició són equivalents. Vegeu el resultat anàleg de les congruències d'enters.

Aritmètica polinomial

Polinomis a \mathbb{Z}_m

Divisió de polinomis

Algoritme d'Euclides i identitat de Bézout

Arrels de polinomis

Polinomis irreductibles

Factorització de polinomis

Congruències de polinomis i anells quocient $\mathbb{Z}_p/\mathbf{f}(\mathbf{x})$

Congruències de polinomis

Anells quocient $\mathbb{Z}_p/\mathbf{f}(\mathbf{x})$

Aritmètica dels anells quocient $\mathbb{Z}_p/\mathbf{f}(\mathbf{x})$

Cossos finits

Elements invertibles

Construcció de cossos finits

Ordre i elements primitius

Representació d'elements

Resum

Exercicis

Solucions

Anells quocient $\mathbb{Z}_p/f(x)$

Com en el cas dels enters, la relació de congruència és una relació d'equivalència i per això les classes de congruència queden ben definides.

$$\mathbb{Z}_p/f(x)$$

Anomenem $\mathbb{Z}_p/f(x)$ al conjunt de classes de congruència mòdul $f(x)$.

Si $\text{grau}(r(x)) < \text{grau}(f(x))$, $[r(x)]_f$ representa la classe de tots els polinomis que dividits entre $f(x)$ tenen residu $r(x)$.

Per extensió, escriurem $[a(x)]_f = [r(x)]_f$ si $a(x) = q(x)f(x) + r(x)$ amb $\text{grau}(r(x)) < \text{grau}(f(x))$.

En particular, tindrem que $[a(x)]_f = [a(x) + k(x)f(x)]_f$ per a qualsevol polinomi $k(x) \in \mathbb{Z}_p[x]$.

Anells quocient $\mathbb{Z}_p/f(x)$

Exemple

Considerem l'anell $\mathbb{Z}_3[x]$ i el polinomi

$$f(x) = x^2 + 2x + 2 \in \mathbb{Z}_3[x].$$

Si dividim un polinomi de $\mathbb{Z}_3[x]$ entre $f(x)$, quin pot ser el residu?

Anells quocient $\mathbb{Z}_p/f(x)$

Exemple

Considerem l'anell $\mathbb{Z}_3[x]$ i el polinomi

$$f(x) = x^2 + 2x + 2 \in \mathbb{Z}_3[x].$$

*Si dividim un polinomi de $\mathbb{Z}_3[x]$ entre $f(x)$, quin pot ser el residu?
Haurà de ser un polinomi de grau més petit que 2 i amb coeficients dins de \mathbb{Z}_3 .*

Anells quocient $\mathbb{Z}_p/f(x)$

Exemple

Considerem l'anell $\mathbb{Z}_3[x]$ i el polinomi

$$f(x) = x^2 + 2x + 2 \in \mathbb{Z}_3[x].$$

*Si dividim un polinomi de $\mathbb{Z}_3[x]$ entre $f(x)$, quin pot ser el residu?
Haurà de ser un polinomi de grau més petit que 2 i amb coeficients dins de \mathbb{Z}_3 .*

Només hi ha un nombre finit de possibilitats:

0	1	2
x	$x + 1$	$x + 2$
$2x$	$2x + 1$	$2x + 2$

Anells quocient $\mathbb{Z}_p/f(x)$

Exemple

Considerem l'anell $\mathbb{Z}_3[x]$ i el polinomi

$$f(x) = x^2 + 2x + 2 \in \mathbb{Z}_3[x].$$

Si dividim un polinomi de $\mathbb{Z}_3[x]$ entre $f(x)$, quin pot ser el residu?
Haurà de ser un polinomi de grau més petit que 2 i amb coeficients dins de \mathbb{Z}_3 .

Només hi ha un nombre finit de possibilitats:

0	1	2
x	$x + 1$	$x + 2$
$2x$	$2x + 1$	$2x + 2$

Això ens està dient que només hi ha 9 classes de congruència mòdul $f(x)$ i que $\mathbb{Z}_3[x]/f(x)$ té 9 elements:

$$\mathbb{Z}_3[x]/f(x) = \{[0]_f, [1]_f, [2]_f, [x]_f, [x+1]_f, [x+2]_f, [2x]_f, [2x+1]_f, [2x+2]_f\}$$

Anells quocient $\mathbb{Z}_p/f(x)$

Exercici 14

Seguint el mateix procediment, llisteu totes les classes de congruència de $\mathbb{Z}_2[x]/x^3 + x + 1$.

Solució (p.110)

Deduïm el següent:

L'anell $\mathbb{Z}_p[x]/f(x)$ està format per $p^{\text{grau}(f)}$ classes d'equivalència.

Exercici 15

1. Quants elements tindrà $\mathbb{Z}_2[x]/x^3 + x + 1$?
2. Quants elements tindrà $\mathbb{Z}_3[x]/x^3 + x + 1$?

Solució (p.111)

Aritmètica polinomial

Polinomis a \mathbb{Z}_m

Divisió de polinomis

Algoritme d'Euclides i identitat de Bézout

Arrels de polinomis

Polinomis irreductibles

Factorització de polinomis

Congruències de polinomis i anells quocient $\mathbb{Z}_p/\mathbf{f}(\mathbf{x})$

Congruències de polinomis

Anells quocient $\mathbb{Z}_p/\mathbf{f}(\mathbf{x})$

Aritmètica dels anells quocient $\mathbb{Z}_p/\mathbf{f}(\mathbf{x})$

Cossos finits

Elements invertibles

Construcció de cossos finits

Ordre i elements primitius

Representació d'elements

Resum

Exercicis

Solucions

Aritmètica dels anells quocient $\mathbb{Z}_p/f(x)$

Dins de $\mathbb{Z}_p[x]/f(x)$ tenim dues operacions ben definides

$$[r_1(x)]_f + [r_2(x)]_f = [r_1(x) + r_2(x)]_f,$$

$$[r_1(x)]_f \cdot [r_2(x)]_f = [r_1(x) \cdot r_2(x)]_f.$$

Aquestes operacions doten $\mathbb{Z}_p/f(x)$ de l'estructura d'anell.

Aritmètica dels anells quocient $\mathbb{Z}_p/f(x)$

Exemple

Hem vist que per $f(x) = x^2 + 2x + 2$,

$$\mathbb{Z}_3[x]/f(x) = \{[0]_f, [1]_f, [2]_f, [x]_f, [x+1]_f, [x+2]_f, [2x]_f, [2x+1]_f, [2x+2]_f\}$$

Podem operar amb les classes d'equivalència fent reduccions mòdul 3 i reduccions mòdul f . Per exemple,

$$\begin{aligned}[2x+1]_f + [x+1]_f &= [3x+2]_f \\ &= [2]_f\end{aligned}$$

o bé

$$\begin{aligned}[2x+1]_f \cdot [x+1]_f &= [2x^2 + 3x + 1]_f \\ &= [2x^2 + 1]_f \\ &= [2x^2 + 1 + f(x)]_f \\ &= [2x^2 + 1 + (x^2 + 2x + 2)]_f \\ &= [3x^2 + 2x + 3]_f \\ &= [2x]_f\end{aligned}$$

Aritmètica polinomial

Congruències de polinomis i anells quocient $\mathbb{Z}_p/f(x)$

Cossos finits

Exercicis

Solucions

Aritmètica polinomial

Polinomis a \mathbb{Z}_m

Divisió de polinomis

Algoritme d'Euclides i identitat de Bézout

Arrels de polinomis

Polinomis irreductibles

Factorització de polinomis

Congruències de polinomis i anells quocient $\mathbb{Z}_p/f(x)$

Congruències de polinomis

Anells quocient $\mathbb{Z}_p/f(x)$

Aritmètica dels anells quocient $\mathbb{Z}_p/f(x)$

Cossos finits

Elements invertibles

Construcció de cossos finits

Ordre i elements primitius

Representació d'elements

Resum

Exercicis

Solucions

Elements invertibles

Exemple

Tornem a l'exemple anterior

$$\mathbb{Z}_3[x]/x^2+2x+2 = \{[0]_f, [1]_f, [2]_f, [x]_f, [x+1]_f, [x+2]_f, [2x]_f, [2x+1]_f, [2x+2]_f\}.$$

Volem saber si la classe $[x+1]_f$ té invers a $\mathbb{Z}_3[x]/f(x)$, és a dir, si hi ha alguna classe que multiplicada per $[x+1]_f$ doni $[1]_f$.

Opció 1: *Podem provar-ho per cerca exhaustiva.*

$[1]_f \cdot [x+1]_f$	$= [x+1]_f$					$\neq [1]_f$
$[2]_f \cdot [x+1]_f$	$= [2x+2]_f$					$\neq [1]_f$
$[x]_f \cdot [x+1]_f$	$= [x^2+x]_f$	$= [x^2+x+2f]_f$	$= [x^2+x+2(x^2+2x+2)]_f$	$= [2x+1]_f$	$\neq [1]_f$	
$[x+1]_f \cdot [x+1]_f$	$= [x^2+2x+1]_f$	$= [x^2+2x+1+2f]_f$	$= [x^2+2x+1+2(x^2+2x+2)]_f$	$= [2]_f$	$\neq [1]_f$	
$[x+2]_f \cdot [x+1]_f$	$= [x^2+2]_f$	$= [x^2+2+2f]_f$	$= [x^2+2+2(x^2+2x+2)]_f$	$= [x]_f$	$\neq [1]_f$	
$[2x]_f \cdot [x+1]_f$	$= [2x^2+2x]_f$	$= [2x^2+2x+f]_f$	$= [2x^2+2x+(x^2+2x+2)]_f$	$= [x+2]_f$	$\neq [1]_f$	
$[2x+1]_f \cdot [x+1]_f$	$= [2x^2+1]_f$	$= [2x^2+1+f]_f$	$= [2x^2+1+(x^2+2x+2)]_f$	$= [2x]_f$	$\neq [1]_f$	
$[2x+2]_f \cdot [x+1]_f$	$= [2x^2+x+2]_f$	$= [2x^2+x+2+f]_f$	$= [2x^2+x+2+(x^2+2x+2)]_f$	$= [1]_f$		

Trobem, doncs, que $([x+1]_f)^{-1} = [2x+2]_f$.

Elements invertibles

Exemple

Opció 2:

Podem utilitzar la identitat de Bézout de $x + 1$ i $x^2 + 2x + 2$.

En aquest cas, la taula de l'algoritme d'Euclides és

1	0	1	
0	1	$2x + 2$	
		$x + 1$	
$x^2 + 2x + 2$	$x + 1$	1	0

Per tant, la identitat de Bézout és

$$1 \cdot (x^2 + 2x + 2) + (2x + 2) \cdot (x + 1) = 1.$$

Si reduïm mòdul $f(x)$ a les dues bandes de la identitat obtenim que

$$[2x + 2]_f \cdot [x + 1]_f = [1]_f,$$

deduint de nou que $([x + 1]_f)^{-1} = [2x + 2]_f$.

Identitat de Bézout i l'invers d'un element

En general, si $\text{mcd}(f(x), a(x)) = 1$, aleshores, per la identitat de Bézout, existiran polinomis $\lambda(x)$ i $\mu(x)$ tals que

$$\lambda(x)f(x) + \mu(x)a(x) = 1$$

Això significa que $\mu(x)a(x) = 1 - \lambda(x)f(x)$ i, per tant,

$$\mu(x)a(x) \equiv 1 \pmod{f(x)}.$$

Deduïm, doncs, que $[a(x)]_f^{-1} = [\mu(x)]_f$.

Exercici 16

1. Calculeu a $\mathbb{Z}_3[x]$ el màxim comú divisor del polinomi $a = x^2 + 2x + 2$ i el polinomi $b = 2x + 1$ i expresseu-lo com a combinació lineal de a i b .
2. Podem deduir si $2x + 1$ és invertible a $\mathbb{Z}_3[x]/x^2 + 2x + 2$? En cas afirmatiu calculeu-ne l'invers.
3. Podem deduir si $x + 2$ és invertible a $\mathbb{Z}_3[x]/x^2 + 2x + 2$? En cas afirmatiu calculeu-ne invers.
4. Comproveu que tots els inversos que heu trobat són, en efecte, inversos.

Solució (p.112)

Aritmètica polinomial

Polinomis a \mathbb{Z}_m

Divisió de polinomis

Algoritme d'Euclides i identitat de Bézout

Arrels de polinomis

Polinomis irreductibles

Factorització de polinomis

Congruències de polinomis i anells quocient $\mathbb{Z}_p/f(x)$

Congruències de polinomis

Anells quocient $\mathbb{Z}_p/f(x)$

Aritmètica dels anells quocient $\mathbb{Z}_p/f(x)$

Cossos finits

Elements invertibles

Construcció de cossos finits

Ordre i elements primitius

Representació d'elements

Resum

Exercicis

Solucions

Construcció de cossos finits

Ara ens volem centrar a veure quins dels anells de la forma $\mathbb{Z}_3[x]/f(x)$ són cossos.

Exercici 17

1. Calculeu les taules de la suma i del producte a $\mathbb{Z}_2[x]/x^2 + x + 1$.
2. Calculeu les taules de la suma i del producte a $\mathbb{Z}_2[x]/x^2 + 1$.
3. Calculeu la taula del producte a $\mathbb{Z}_3[x]/x^2 + 1$.
4. Raoneu si $\mathbb{Z}_2[x]/x^2 + x + 1$, $\mathbb{Z}_2[x]/x^2 + 1$, o $\mathbb{Z}_3[x]/x^2 + 1$ són cossos.

Solució (p.114)

Construcció de cossos finits

Observem que si $f(x)$ és irreductible, aleshores és coprimer amb qualsevol polinomi que no sigui un múltiple seu i, per tant, qualsevol classe diferent de zero (la classe del zero correspon als múltiples de $f(x)$) és invertible. Per això podem afirmar el següent:

Si m és un primer i si $f(x)$ és irreductible a $\mathbb{Z}_m[x]$, aleshores $\mathbb{Z}_m[x]/f(x)$ és un cos.

Per contra, si m no és primer, els divisors de m no seran invertibles a $\mathbb{Z}_m[x]$ i, si m és primer, però $f(x)$ no és irreductible, els seus divisors no seran invertibles a $\mathbb{Z}_m[x]/f(x)$.

Construcció de cossos finits

Teorema 2

$\mathbb{Z}_m[x]/f(x)$ és un cos si i només si m és primer i $f(x)$ és irreductible a $\mathbb{Z}_m[x]$.

Si $\mathbb{Z}_p[x]/f(x)$ és cos l'anomenem \mathbb{F}_{p^n} , on $n = \text{grau}(f(x))$.

Exercici 18

Utilitzeu l'Exercici 11 per donar un polinomi que generi \mathbb{F}_{27} .

Solució (p.117)

Aritmètica polinomial

Polinomis a \mathbb{Z}_m

Divisió de polinomis

Algoritme d'Euclides i identitat de Bézout

Arrels de polinomis

Polinomis irreductibles

Factorització de polinomis

Congruències de polinomis i anells quocient $\mathbb{Z}_p/\mathbf{f}(x)$

Congruències de polinomis

Anells quocient $\mathbb{Z}_p/\mathbf{f}(x)$

Aritmètica dels anells quocient $\mathbb{Z}_p/\mathbf{f}(x)$

Cossos finits

Elements invertibles

Construcció de cossos finits

Ordre i elements primitius

Representació d'elements

Resum

Exercicis

Solucions

Ordre i elements primitius

Teorema 3

Per a qualsevol $\beta \in \mathbb{F}_{p^n}^*$, es té $\beta^{p^n-1} = 1$.

Exercici 19

Demostreu el teorema anterior. Podeu emprar els mateixos arguments que en la demostració del teorema d'Euler.

Ordre

L'**ordre** de $\beta \in \mathbb{F}_{p^n} \setminus \{0\}$ és el mínim exponent $i \neq 0$ tal que $\beta^i = 1$. El denotem per **ord** $_{\mathbb{F}_{p^n}}(a)$

Pel teorema anterior, si \mathbb{F}_{p^n} és un cos finit, tot element no nul de \mathbb{F}_{p^n} tindrà un ordre.

Ordre i elements primitius

Exercici 20

Demostreu que si $\beta^k = 1$ per un enter positiu k , aleshores l'ordre de β divideix k . Vegeu el resultat anàleg per l'ordre dels elements de \mathbb{Z}_m .

Com a conseqüència del resultat de l'exercici i del teorema 3 tenim el resultat següent.

L'ordre d'un element no nul de \mathbb{F}_{p^n} sempre divideix $p^n - 1$.

Exercici 21

Demostreu que, a $\mathbb{Z}_p[x]/f(x)$, si la classe $[x]_f$ és diferent de zero, aleshores té ordre més gran o igual que el grau de $f(x)$.

Solució (p.118)

Ordre i elements primitius

Elements primitius

Diem que $\beta \in \mathbb{F}_{p^n}$ és un **element primitiu** si el seu ordre és $p^n - 1$.

Si β és primitiu, aleshores

$$\mathbb{F}_{p^n} = \{0, 1, \beta, \dots, \beta^{p^n-2}\}.$$

Polinomis primitius

Diem que $f(x)$ és **primitiu** si la classe $[x]_f$ és un element primitiu de $\mathbb{Z}_p[x]/f(x)$.

Ordre i elements primitius

Exemple

Considerem, per exemple, el cos $\mathbb{F}_{16} = \mathbb{Z}_2[x]/x^4 + x^3 + 1$. Anomenem α a la classe $[x]_f$ on $f(x) = x^4 + x^3 + 1$. En particular, tindrem $f(\alpha) = 0$. Per tant, $\alpha^4 = -\alpha^3 - 1 = \alpha^3 + 1$. La resta de potències de α seran:

$$\begin{aligned}\alpha^0 &= 1 \\ \alpha^1 &= \alpha \\ \alpha^2 &= \alpha^2 \\ \alpha^3 &= \alpha^3 \\ \alpha^4 &= \alpha^3 + 1 \\ \alpha^5 &= \alpha\alpha^4 = \alpha(\alpha^3 + 1) = \alpha^4 + \alpha = \alpha^3 + \alpha + 1 \\ \alpha^6 &= \alpha\alpha^5 = \alpha(\alpha^3 + \alpha + 1) = \alpha^4 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1 \\ \alpha^7 &= \alpha\alpha^6 = \alpha(\alpha^3 + \alpha^2 + \alpha + 1) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + 1 + \alpha^3 + \alpha^2 + \alpha \\ &= 2\alpha^3 + \alpha^2 + \alpha + 1 = \alpha^2 + \alpha + 1 \\ \alpha^8 &= \alpha^3 + \alpha^2 + \alpha \\ \alpha^9 &= \alpha^2 + 1 \\ \alpha^{10} &= \alpha^3 + \alpha \\ \alpha^{11} &= \alpha^3 + \alpha^2 + 1 \\ \alpha^{12} &= \alpha + 1 \\ \alpha^{13} &= \alpha^2 + \alpha \\ \alpha^{14} &= \alpha^3 + \alpha^2 \\ \alpha^{15} &= 1\end{aligned}$$

Això ens permet veure que α és primitiu i $f(x)$ també.

Aritmètica polinomial

Polinomis a \mathbb{Z}_m

Divisió de polinomis

Algoritme d'Euclides i identitat de Bézout

Arrels de polinomis

Polinomis irreductibles

Factorització de polinomis

Congruències de polinomis i anells quocient $\mathbb{Z}_p/f(x)$

Congruències de polinomis

Anells quocient $\mathbb{Z}_p/f(x)$

Aritmètica dels anells quocient $\mathbb{Z}_p/f(x)$

Cossos finits

Elements invertibles

Construcció de cossos finits

Ordre i elements primitius

Representació d'elements

Resum

Exercicis

Solucions

Representació d'elements

Suposem que tenim un cos finit $\mathbb{Z}_p/(f(x))$ i que $d = \text{grau}(f(x))$.

Anomenem α a la classe de congruència mòdul $f(x)$ de l'element x .

En particular tindrem que $f(\alpha) = 0$.

Qualsevol element de $\mathbb{Z}_p/(f(x))$ es podrà expressar com un polinomi en α de grau més petit que d .

És el que anomenem **notació polinomial**.

D'altra banda, suposem que β és un element primitiu. Qualsevol element no nul es podrà expressar també com una potència de β amb un exponent més petit que $p^d - 1$.

És el que anomenem **notació exponencial** o **notació potencial**.

Finalment, podem representar els elements de $\mathbb{Z}_p/(f(x))$ per un vector de d coordenades (a_0, \dots, a_{d-1}) on a_i és el coeficient de grau i de la notació polinomial.

És el que anomenem **notació vectorial**.

Representació d'elements

Exemple

En l'exemple anterior,

$$\alpha^{11} \text{ (notació exponencial)} = 1 + \alpha^2 + \alpha^3 \text{ (notació polinomial)} = (1, 0, 1, 1) \text{ (notació vectorial)}.$$

La notació polinomial i la notació vectorial ens aniran molt bé per fer sumes i restes, mentre que la notació exponencial ens anirà molt bé per poder fer multiplicacions i divisions. Per això ens serà convenient poder fer servir totes les notacions a la vegada i per això emprarem les **taules d'equivalència** entre les diferents notacions.

Representació d'elements

Continuant l'exemple anterior,

pot.	pol.	vect.
α^0	1	(1000)
α^1	α	(0100)
α^2	α^2	(0010)
α^3	α^3	(0001)
α^4	$\alpha^3 + 1$	(1001)
α^5	$\alpha^3 + \alpha + 1$	(1101)
α^6	$\alpha^3 + \alpha^2 + \alpha + 1$	(1111)
α^7	$\alpha^2 + \alpha + 1$	(1110)
α^8	$\alpha^3 + \alpha^2 + \alpha$	(0111)
α^9	$\alpha^2 + 1$	(1010)
α^{10}	$\alpha^3 + \alpha$	(0101)
α^{11}	$\alpha^3 + \alpha^2 + 1$	(1011)
α^{12}	$\alpha + 1$	(1100)
α^{13}	$\alpha^2 + \alpha$	(0110)
α^{14}	$\alpha^3 + \alpha^2$	(0011)

Aritmètica polinomial

Polinomis a \mathbb{Z}_m

Divisió de polinomis

Algoritme d'Euclides i identitat de Bézout

Arrels de polinomis

Polinomis irreductibles

Factorització de polinomis

Congruències de polinomis i anells quocient $\mathbb{Z}_p/f(x)$

Congruències de polinomis

Anells quocient $\mathbb{Z}_p/f(x)$

Aritmètica dels anells quocient $\mathbb{Z}_p/f(x)$

Cossos finits

Elements invertibles

Construcció de cossos finits

Ordre i elements primitius



Representació d'elements

Resum

Exercicis

Solucions

Resum

\mathbb{Z}_m	$\mathbb{Z}_p[x]/f(x)$ (amb p primer)
<p>Divisió euclidiana a \mathbb{Z}:</p> <p>Donats $a, b \in \mathbb{Z}$ existeixen $q, r \in \mathbb{Z}$ tals que $a = bq + r$ amb $0 \leq r < b$.</p> <p>Fer congruències mòdul m és quedar-nos amb el residu de dividir per m \Rightarrow obtenim enters $< m$.</p>	<p>Divisió euclidiana a $\mathbb{Z}_p[x]$:</p> <p>Donats $a(x), b(x) \in \mathbb{Z}_p[x]$ existeixen $q(x), r(x) \in \mathbb{Z}_p[x]$ tals que $a(x) = b(x)q(x) + r(x)$ amb $0 \leq \text{grau}(r(x)) < \text{grau}(b(x))$.</p> <p>Fer congruències mòdul $f(x)$ és quedar-nos amb el residu de dividir per $f(x)$ \Rightarrow obtenim polinomis de grau $< \text{grau}(f(x))$.</p>
<p>$\mathbb{Z}_m = \{0, 1, \dots, m-1\}$ amb les operacions reduïdes mòdul m.</p> <p>\mathbb{Z}_m té m elements.</p>	<p>$\mathbb{Z}_p[x]/f(x) = \{a_0 + a_1x + \dots + a_{n-1}x^{n-1} \text{ amb } a_0, \dots, a_{n-1} \in \mathbb{Z}_p\}$ amb les operacions reduïdes mòdul p i mòdul $f(x)$, on $n = \text{grau } f(x)$.</p> <p>$\mathbb{Z}_p[x]/f(x)$ té p^n elements.</p> <p>Diem que la classe de x és un generador de $\mathbb{Z}_p[x]/f(x)$.</p>
<p>$a \in \mathbb{Z}_m$ és invertible si i només si $\text{mcd}(a, m) = 1$.</p> <p>L'invers es troba per la identitat de Bézout: $\lambda a + \mu m = 1 \Rightarrow \lambda a = 1 \Rightarrow a^{-1} = \lambda$.</p> <p>Anomenem \mathbb{Z}_m^* als invertibles de \mathbb{Z}_m.</p>	<p>$a(x) \in \mathbb{Z}_p[x]/f(x)$ és invertible si i només si $\text{mcd}(a(x), f(x))$ és constant.</p> <p>L'invers es troba per la identitat de Bézout: $\lambda(x)a(x) + \mu(x)f(x) = 1 \Rightarrow \lambda(x)a(x) = 1 \Rightarrow (a(x))^{-1} = \lambda(x)$.</p> <p>Anomenem $(\mathbb{Z}_p[x]/f(x))^*$ als invertibles de $\mathbb{Z}_p[x]/f(x)$.</p>
<p>Funció d'Euler: $\phi(m) = \#\{a : 1 \leq a < m, \text{mcd}(a, m) = 1\}$</p> <ul style="list-style-type: none"> $\phi(p) = p - 1$ si p és primer, $\phi(p^k) = p^k - p^{k-1}$ si p és primer, $\phi(ab) = \phi(a)\phi(b)$ si $\text{mcd}(a, b) = 1$. <p>Teorema d'Euler: $a^{\phi(m)} \equiv 1 \pmod m$ si $\text{mcd}(a, m) = 1$.</p>	
<p>\mathbb{Z}_m és cos si i només si m és primer.</p> <p>Si p és primer \mathbb{Z}_p també l'anomenem \mathbb{F}_p.</p>	<p>$\mathbb{Z}_p[x]/f(x)$ és cos si i només si $f(x)$ és irreductible.</p> <p>Si $\mathbb{Z}_p[x]/f(x)$ és cos l'anomenem \mathbb{F}_{p^n}.</p>
<p>L'ordre de $a \in \mathbb{Z}_m$ és el mínim exponent $i \neq 0$ tal que $a^i \equiv 1 \pmod m$.</p> <p>L'ordre sempre és un divisor de $\phi(m)$.</p> <p>Diem que $a \in \mathbb{Z}_m$ és primitiu si el seu ordre és $\phi(m)$.</p>	<p>L'ordre de $\beta \in \mathbb{F}_{p^n}$ és el mínim exponent $i \neq 0$ tal que $\beta^i = 1$.</p> <p>L'ordre sempre és un divisor de $p^n - 1$.</p> <p>Diem que $\beta \in \mathbb{F}_{p^n}$ és primitiu si el seu ordre és $p^n - 1$.</p>
	<p>Si β és primitiu, aleshores $\mathbb{F}_{p^n}^* = \{0, 1, \beta, \dots, \beta^{p^n-2}\}$.</p> <p>Diem que $f(x)$ és primitiu si la classe de x és un element primitiu de $\mathbb{Z}_p[x]/f(x)$.</p>

Sage permet construir cossos finits amb la comanda `FiniteField`

```
F64.<alpha>=FiniteField(64)
```

```
F64
```

`alpha` serà la classe de x com a congruència mòdul el polinomi generador. Així podem escriure, per exemple,

```
alpha^100
```

```
alpha^63
```

Per veure quin polinomi ha utilitzat sage per la construcció del cos:

```
charpoly(alpha)
```

Comprovem que la potència α^6 és la que correspon pel polinomi generador:

```
alpha^6
```

També podem forçar nosaltres que sage utilitzi un determinat polinomi amb de la manera següent:

```
F64.<alpha>=FiniteField(64,modulus=x^6+x^5+x^2+x+1)
```

Suposem que treballem en un cos finit F de p^m elements. Podem calcular qui són la p i la m així:

```
F=FiniteField(125)
p=F.characteristic()
print(p)
```

```
m=F.degree()
print(m)
```

Els vectors de m coordenades a \mathbb{Z}_p els podem escriure així:

```
V=VectorSpace(FiniteField(p),m)
```

Si v és un element de V , aleshores $F(v)$ és l'element de F que té forma vectorial igual a v . Observeu què passa quan executeu les comandes següents:

```
v=V.random_element()  
print(v)  
print(F(v))
```

Una manera de trobar la forma vectorial d'un element amb sage pot ser aquesta:

```
def formavect(F,beta):  
    llista=[v for v in  
        VectorSpace(FiniteField(F.characteristic()),F.degree())  
        if F(v)==beta]  
    return llista[0]
```

Fem unes comprovacions:

```
print(v,F(v),formavect(F,F(v)))  
F.<a>=FiniteField(125)  
print(a^101,formavect(F,a^101),F(formavect(F,a^101)))
```

Aritmètica polinomial

Congruències de polinomis i anells quocient $\mathbb{Z}_p/f(x)$

Cossos finits

Exercicis

Solucions

Exercici 22

1. Per quins polinomis $f(x)$ de $\mathbb{Z}_2[x]$ el quocient $\mathbb{Z}_2[x]/f(x)$ és un cos de 4 elements?
2. Doneu-ne un element primitiu i la taula d'equivalències potencial-vectorial-polinomial.
3. Doneu també una taula per a la suma i una taula per al producte.

Solució (p.119)

Exercici 23

Considerem $\mathbb{Z}_3[x]/x^2 + x + 2$

1. Demostreu que és un cos.
2. Quants elements té?
3. És $\alpha = [x]$ un element primitiu? Per què?
4. Doneu-ne una taula d'equivalències amb les notacions potencial, polinomial i vectorial.
5. Calculeu $\alpha^2 \left(\frac{\alpha^{20} - \alpha^5 + \alpha}{\alpha^3 - \alpha} \right)$.

Solució (p.122)

Exercici 24

Considerem els següents polinomis de $\mathbb{Z}_3[x]$.

- ▶ $f(x) = x^3 + x^2 + 2$,
- ▶ $g(x) = x^3 + 2x + 1$,
- ▶ $h(x) = x^3 + 2x^2 + 2$.

Sabem que

- ▶ $x^{11} \bmod f(x) = x + 1$,
- ▶ $x^{11} \bmod g(x) = x^2 + x + 2$,
- ▶ $x^{11} \bmod h(x) = 2x^2 + x + 1$.

1. Quins d'aquests polinomis són irreductibles?
2. Quins dels polinomis irreductibles són primitius?
3. Per quins polinomis, en fer quocient a $\mathbb{Z}_3[x]$, s'obté un cos? De quants elements?
4. Per quins dels polinomis anteriors que, en fer quocient, ens donen un cos, podem expressar qualsevol element del cos com a potència de la classe de x en el quocient?

Solució (p.126)

Exercici 25

Considerem $\mathbb{Z}_3[x]/x^2 + 1$

- (a) Demostreu que és un cos.
- (b) Quants elements té?
- (c) Anomenem α l'element del cos que correspon a la classe de x mòdul $x^2 + 1$. Quin és l'ordre de α ?
- (d) És $\alpha = [x]$ un element primitiu? Per què?
- (e) Trobeu un element primitiu β .
- (f) Escriviu α com una potència de β .
- (g) Doneu una taula d'equivalències amb les notacions potencial amb potències de β , polinomial amb polinomis en α i vectorial.
- (h) Calculeu $\beta^{15} \left(\frac{\beta^2 - \beta^3}{\beta^6 + \beta} \right)$.

Solució (p.128)

Exercici 26

Considerem el cos finit $\mathbb{F}_8 = \mathbb{Z}_2[x]/x^3 + x + 1$. Anomenem α a la classe de x .

1. Doneu la taula d'equivalències de les notacions exponencial i vectorial.
2. Doneu els oposats i els inversos dels elements de \mathbb{F}_8 .
3. Doneu la taula de les sumes i la taula de les restes de \mathbb{F}_8 .
4. Doneu la taula de les multiplicacions i la taula de les divisions de \mathbb{F}_8 .
5. Calculeu
$$\frac{x^5 + (\alpha + 1)x^4 + (\alpha^2 + \alpha + 1)x^3 + \alpha^2 x^2 + \alpha x + \alpha^2 + 1}{x^2 + \alpha^2 x + \alpha}.$$

Solució (p.131)

Exercici 27

Considerem el cos finit $\mathbb{F}_9 = \mathbb{Z}_3[x]/x^2 + 2x + 2$. Anomenem α a la classe de x .

1. Doneu la taula d'equivalències de les notacions exponencial i vectorial.
2. Doneu els oposats i els inversos dels elements de \mathbb{F}_9 .
3. Doneu la taula de les sumes i la taula de les restes de \mathbb{F}_9 .
4. Doneu la taula de les multiplicacions i la taula de les divisions de \mathbb{F}_9 .
5. Calculeu $\frac{x^8 - 1}{x^4 + \alpha^6 x^3 + x^2 + \alpha^3 x + \alpha^2}$.

Solució (p.134)

Exercici 28

- (a) Justifiqueu si són irreductibles els següents polinomis a $\mathbb{Z}_2[x]$:
- i. $x^4 + 1$
 - ii. $x^4 + x + 1$
 - iii. $x^4 + x^2 + 1$
 - iv. $x^4 + x^3 + x^2 + x + 1$
- (b) Escriviu cadascun dels polinomis de l'apartat (a) com a producte de polinomis irreductibles.
- (c) Doneu el màxim comú divisor de $x^4 + 1$ i $x^4 + x^2 + 1$.
- (d) Podeu expressar el màxim comú divisor de $x^4 + 1$ i $x^4 + x^2 + 1$ com a combinació lineal dels mateixos polinomis? Doneu-ne els coeficients i feu la comprovació.
- (e) Quines de les següents estructures són un cos i, en cas de ser-ho, quants elements tenen?
- i. $\mathbb{Z}_2[x]/x^4 + 1$
 - ii. $\mathbb{Z}_2[x]/x^4 + x + 1$
 - iii. $\mathbb{Z}_2[x]/x^4 + x^2 + 1$
 - iv. $\mathbb{Z}_2[x]/x^4 + x^3 + x^2 + x + 1$
- (f) En quins dels casos en què tenim un cos, si anomenem α a la classe de x , tenim que α és un element primitiu?
- (g) Doneu una taula exponencial-polinòmica-vectorial per un cas en què α sigui primitiu. Els apartats que segueixen els referirem al mateix cas (la mateixa α i la mateixa taula).
- (h) Quins són els ordres possibles dels elements del cos?
- (i) Per a cadascun dels ordres possibles, doneu un element del cos amb aquell ordre.

Solució (p.137)

Aritmètica polinomial

Congruències de polinomis i anells quocient $\mathbb{Z}_p/f(x)$

Cossos finits

Exercicis

Solucions

Solució de l'Exercici 2

[Torna a l'exercici \(p.18\)](#)

Solució de l'Exercici 3

Si avaluem el polinomi $x^5 + 2x^3 + 3x^2 + 1$ a $x = 3$ ens dona $243 + 2 \cdot 27 + 3 \cdot 9 + 1 = 243 + 54 + 27 + 1 = 325$.

Com que $325 \equiv 3 \pmod{7}$, deduïm que 3 no és una arrel de $x^5 + 2x^3 + 3x^2 + 1$ a $\mathbb{Z}_7[x]$.

Com que $325 \equiv 0 \pmod{5}$, deduïm que 3 és una arrel de $x^5 + 2x^3 + 3x^2 + 1$ a $\mathbb{Z}_5[x]$.

Com que $325 \equiv 1 \pmod{3}$, deduïm que 3 no és una arrel de $x^5 + 2x^3 + 3x^2 + 1$ a $\mathbb{Z}_3[x]$.

Com que $325 \equiv 1 \pmod{2}$, deduïm que 3 no és una arrel de $x^5 + 2x^3 + 3x^2 + 1$ a $\mathbb{Z}_2[x]$.

[Torna a l'exercici \(p.28\)](#)

Solució de l'Exercici 4

Sabem que un polinomi $f(x) \in \mathbb{Z}_2[x]$ és divisible per x si i només si 0 és una arrel. I 0 és una arrel si i només si $f(0) = 0$. Com que $f(0)$ és exactament el terme constant, deduïm que $f(x)$ és divisible per x si i només si el seu terme constant és 0.

Sabem que un polinomi $f(x) \in \mathbb{Z}_2[x]$ és divisible per $x + 1$ si i només si 1 és una arrel. I 1 és una arrel si i només si $f(1) = 0$. Com que $f(1)$ és exactament el nombre de termes de $f(x)$, deduïm que $f(x)$ és divisible per $x + 1$ si i només si el seu nombre de termes és parell.

[Torna a l'exercici \(p.28\)](#)

Solució de l'Exercici 5

1. 2 és invertible si p és senar perquè en aquest cas $\text{mcd}(2, p) = 1$.
2. L'element $p + 1$ és parell i l'invers de 2 serà l'enter $\frac{p+1}{2}$ ja que $2 \cdot \frac{p+1}{2} = p + 1 = 1$ a \mathbb{Z}_p .
- 3.

a	a^2
0	0
1	1
2	4
3	2
4	2
5	4
6	1

Solució de l'Exercici 5

4.

$$\begin{aligned}\sqrt{0}^{\mathbb{Z}_7} &= \{0\} \\ \sqrt{1}^{\mathbb{Z}_7} &= \{1, 6\} \\ \sqrt{2}^{\mathbb{Z}_7} &= \{3, 4\} \\ \sqrt{3}^{\mathbb{Z}_7} &= \emptyset = \{\} \\ \sqrt{4}^{\mathbb{Z}_7} &= \{2, 5\}\end{aligned}$$

5. Si substituïm x per 4 a $x^2 + 3x + 2 \in \mathbb{Z}_5[x]$ ens dona
 $4^2 + 3 \cdot 4 + 2 = 16 + 12 + 2 = 30 = 0$.

Si substituïm x per 3 a $x^2 + 3x + 2 \in \mathbb{Z}_5[x]$ ens dona
 $3^2 + 3 \cdot 3 + 2 = 9 + 9 + 2 = 20 = 0$.

6. ▶ Per $x^2 + 5x + 1$ tenim $b = 5, c = 1$ i les arrels seran $(2 + y)4$ mod 7 on y agafa tots els valors de $\sqrt{0}^{\mathbb{Z}_7} = \{0\}$, és a dir, hi ha una única arrel en aquest cas, que és 1.

Solució de l'Exercici 5

- ▶ Per $x^2 + 6$ tenim $b = 0, c = 6$ i les arrels seran $(x)4 \bmod 7$ on x agafa tots els valors de $\sqrt{4}^{\mathbb{Z}_7} = \{2, 5\}$, és a dir, les arrels en aquest cas són 1 i 6.
- ▶ Per $x^2 + 5x + 4$ tenim $b = 5, c = 4$ i les arrels seran $(2 + x)4 \bmod 7$ on x agafa tots els valors de $\sqrt{25 - 16}^{\mathbb{Z}_7} = \sqrt{2}^{\mathbb{Z}_7} = \{3, 4\}$, és a dir, les arrels en aquest cas són 6 i 3.

- 7.
- ▶ Si substituïm x per 1 a $x^2 + 5x + 1 \in \mathbb{Z}_5[x]$ ens dona $1 + 5 + 1 = 0$.
 - ▶ Si substituïm x per 1 i $6 = -1$ a $x^2 + 6 \in \mathbb{Z}_5[x]$ ens dona $1 + 6 = 0$.
 - ▶ Si substituïm x per 3 a $x^2 + 5x + 4 \in \mathbb{Z}_5[x]$ ens dona $3^2 + 5 \cdot 3 + 4 = 2 + 1 + 4 = 0$. Si substituïm x per 6 a $x^2 + 5x + 4 \in \mathbb{Z}_5[x]$ ens dona $6^2 + 5 \cdot 6 + 4 = 1 + 2 + 4 = 0$.

Torna a l'exercici (p.29)

Solució de l'Exercici 6

Suposem que $\text{grau}(f(x)) = n$. Vegem per inducció que, si a_1, \dots, a_s són arrels diferents de $f(x)$, aleshores $f(x) = (x - a_1) \cdots (x - a_s)q(x)$ per algun polinomi $q(x)$ de grau $n - s$, amb el que $s \leq n$.

Suposem $s = 1$. Si $x - a_1$ divideix $f(x)$, aleshores $f(x) = (x - a_1)q(x)$ per algun polinomi $q(x)$. Com que $\text{grau}(f(x)) = \text{grau}(x - a_1) + \text{grau}(q(x))$, tenim que $\text{grau}(q(x)) = n - 1$.

Suposem que el resultat és cert per $s - 1$ i demostrem-lo per s . Suposem que a_1, \dots, a_s són arrels diferents de $f(x)$. Per la hipòtesi d'inducció, $f(x) = (x - a_1) \cdots (x - a_{s-1})q(x)$ per algun polinomi $q(x)$ de grau $n - s + 1$.

Com que $x - a_s$ divideix $f(x) = (x - a_1) \cdots (x - a_{s-1})q(x)$, aleshores $f(a_s) = (a_s - a_1) \cdots (a_s - a_{s-1})q(a_s)$ ha de ser zero. Com que $a_s - a_1 \neq 0, \dots, a_s - a_{s-1} \neq 0$ i a \mathbb{Z}_p no hi ha divisors de zero, $q(a_s) = 0$. Per tant, $x - a_s$ divideix $q(x)$ i $q(x) = (x - a_s)\tilde{q}(x)$ per algun polinomi $\tilde{q}(x)$ de grau $n - s$.

Deduïm que $f(x) = (x - a_1) \cdots (x - a_{s-1})q(x) = (x - a_1) \cdots (x - a_s)\tilde{q}(x)$ per algun polinomi $\tilde{q}(x)$ de grau $n - s$.

Torna a l'exercici (p.33)

Solució de l'Exercici 7

Suposem que un polinomi $f(x)$ té grau 2 o 3 i que es pot descompondre en el producte següent:

$$f(x) = g(x)h(x),$$

amb $g(x)$ i $h(x)$ no constants. Les úniques opcions per als graus de $g(x)$ i $h(x)$ són:

Si grau(f) = 2		Si grau(f) = 3	
grau(g)	grau(h)	grau(g)	grau(h)
1	1	2	1
		1	2

En qualsevol cas, algun dels factors ha de ser de grau 1 i, per tant, de la forma $x - a$. En aquest cas a serà una arrel.

[Torna a l'exercici \(p.38\)](#)

Solució de l'Exercici 8

Analitzem per graus.

Grau 0: 1 és l'únic polinomi de grau 0 i és irreductible.

Grau 1: x i $x + 1$ són els únics polinomis de grau 1 i són irreductibles.

A partir de grau 2, observem que, pel lema 1,

- ▶ un polinomi és divisible per x si i només si no té terme constant,
- ▶ un polinomi és divisible per $x + 1$ si i només si té un nombre parell de coeficients.

Ara, per l'Exercici 7, pels casos de grau 2 i grau 3, aquestes condicions seran suficients per determinar els irreductibles. Així podem continuar:

Grau 2: $x^2 + x + 1$.

Grau 3: $x^3 + x^2 + 1$, $x^3 + x + 1$.

Solució de l'Exercici 8

Per grau 4, suposem que $f(x)$ té grau 4 i es pot descompondre com

$$f(x) = g(x)h(x),$$

amb $g(x)$ i $h(x)$ no constants. Els graus de $g(x)$ i $h(x)$ poden ser:

grau(g)	grau(h)
3	1
2	2
1	3

En els casos primer i tercer tindríem una arrel, situació que podem descartar imposant que hi hagi terme constant i un nombre senar de termes no nuls.

El segon cas només es podria donar si algun dels factors té arrels (descartables amb les dues condicions anteriors) o bé si $g(x)$ i $h(x)$ són irreductibles de grau 2, és a dir, $g(x) = x^2 + x + 1$ i $h(x) = x^2 + x + 1$. En aquest cas, $f(x)$ seria $x^4 + x^2 + 1$. Així, podem concloure:

Grau 4: $x^4 + x^3 + 1$, $x^4 + x + 1$, $x^4 + x^3 + x^2 + x + 1$. [Torna a l'exercici \(p.39\)](#)

Solució de l'Exercici 9

1. Fem la divisió de polinomis

$$\begin{array}{r} x^5 \qquad \qquad \qquad + x^2 + 1 \\ -(x^5 + x^4 + x^3 \qquad \qquad) \\ \hline x^4 + x^3 + x^2 + 1 \\ -(x^4 + x^3 + x^2 \qquad \qquad) \\ \hline 1 \end{array} \quad \left| \frac{x^2 + x + 1}{x^3 + x^2} \right.$$

Obtenim $q = x^3 + x^2$, $r = 1$. Podem comprovar que, en efecte, $(x^2 + x + 1)(x^3 + x^2) + 1 = x^5 + x^4 + x^4 + x^3 + x^3 + x^2 + 1 = x^5 + x^2 + 1$.

2. El polinomi g és irreductible perquè té grau 2 i no té arrels. Com que el polinomi f té grau 5, per veure que és irreductible hem de veure que no té factors irreductibles de grau 1 (ho sabem perquè no té arrels) ni factors irreductibles de grau 2. Això darrer ho sabem perquè l'únic polinomi irreductible de grau 2 és $x^2 + x + 1 = g$ i, del primer apartat, deduïm que g no divideix f .

Torna a l'exercici (p.39)

Solució de l'Exercici 10

1. Hi ha 9 polinomis mònicos de grau 2 a $\mathbb{Z}_3[x]$, ja que són tots els polinomis de la forma $x^2 + ax + b$ amb a i b variant cadascun en els tres valors de \mathbb{Z}_3 .
2. El polinomi $x^2 + ax + b$, per ser irreductible, com que té grau 2, no ha de tenir arrels. Perquè 0 no sigui arrel, cal que $0^2 + 0a + b \neq 0$. Això implica $b = 1$ o $b = 2$. Perquè 1 no sigui arrel, cal que $1 + a + b \neq 0$. Perquè 2 no sigui arrel, cal que $4 + 2a + b \neq 0$. Això ens dona tres opcions:
 - ▶ $b = 1, a = 0$
 - ▶ $b = 2, a = 1$
 - ▶ $b = 2, a = 2$

que corresponen als tres polinomis

- ▶ $x^2 + 1$
- ▶ $x^2 + x + 2$
- ▶ $x^2 + 2x + 2$

Torna a l'exercici (p.40)

Solució de l'Exercici 11

1. $x^3 + x^2 + 2 \in P,$

o bé

$$2x^{12} + x^8 + x^7 + 2x^6 + 2x^4 + 1 \in P.$$

2. 2.1 La suma dels coeficients de p és $p(1)$. Si $p(1)$ és un múltiple de 3 aleshores s'anul·la a \mathbb{Z}_3 i 1 és una arrel de p . Per tant, p no és irreductible.

2.2 Tenim que $2^2 = 4 = 1$ a \mathbb{Z}_3 . Per tant, $2^r = \begin{cases} 1 & \text{si } r \text{ és parell} \\ 2 & \text{si } r \text{ és senar} \end{cases}$

Tenim que $p(2)$ és la suma de coeficients més 1 i, per tant, $p(2)$ no s'anul·la a \mathbb{Z}_3 si i només si la suma de coeficients és congruent amb 2 mòdul 3.

3. El coeficient constant, com que és $p(0)$, no ha de ser nul.

Torna a l'exercici (p.41)

Solució de l'Exercici 12

Observem que el polinomi $2x^4 + 4x^2 + 3x + 1$ té arrels 1 i 2. Per tant, és divisible per $(x + 4)(x + 3) = x^2 + 2x + 2$.

Dividim $2x^4 + 4x^2 + 3x + 1$ entre $x^2 + 2x + 2$.

$$\begin{array}{r} 2x^4 + 4x^2 + 3x + 1 \\ -(2x^4 + 4x^3 + 4x^2) \\ \hline x^3 + 3x + 1 \\ -(x^3 + 2x^2 + 2x) \\ \hline 3x^2 + x + 1 \\ -(3x^2 + x + 1) \\ \hline 0 \end{array} \quad \begin{array}{r} x^2 + 2x + 2 \\ 2x^2 + x + 3 \end{array}$$

Ens dona $2x^2 + x + 3 = 2(x^2 + 3x + 4)$.

Com que $x^2 + 3x + 4$ té grau 2 i no té arrels, sabem que és irreductible.

Per tant, la factorització completa serà

$$2x^4 + 4x^2 + 3x + 1 = 2(x^2 + 3x + 4)(x + 3)(x + 4).$$

Torna a l'exercici (p.46)

Solució de l'Exercici 14

$$\mathbb{Z}_2[x]/x^3 + x + 1 = \\ \{[0], [1], [x], [x+1], [x^2], [x^2+1], [x^2+x], [x^2+x+1]\}.$$

[Torna a l'exercici \(p.58\)](#)

Solució de l'Exercici 15

1. $\mathbb{Z}_2[x]/x^3 + x + 1$ tindrà $2^3 = 8$ elements.
2. $\mathbb{Z}_3[x]/x^3 + x + 1$ tindrà $3^3 = 27$ elements.

Torna a l'exercici (p.58)

Solució de l'Exercici 16

1.

$$\begin{array}{r} x^2 + 2x + 2 \\ -(x^2 + 2x \quad) \\ \hline 2 \end{array} \quad \begin{array}{l} 2x + 1 \\ \hline 2x \end{array}$$

1	0	1	
0	1	x	
		$2x$	$x + 2$
$x^2 + 2x + 2$	$2x + 1$	2	0

Deduïm que $(x^2 + 2x + 2) + x(2x + 1) = 2$.

2. $2x + 1$ és invertible perquè és coprimer amb $x^2 + 2x + 2$. De la igualtat $(x^2 + 2x + 2) + x(2x + 1) = 2$ deduïm que $2(x^2 + 2x + 2) + 2x(2x + 1) = 1$. En conseqüència, l'invers de $(2x + 1)$ és $2x$.

Solució de l'Exercici 16

3. Observem que $x + 2 = 2(2x + 1)$. Com que $(2x + 1)(2x) = 1$, també $(2(2x + 1))(2(2x)) = 1$, és a dir, $(x + 2)x = 1$. Per tant, l'invers de $x + 2$ és x .
4.
 - ▶ $(2x+1)(2x) = 4x^2+2x = x^2+2x = x^2+2x-(x^2+2x+2) = -2 = 1 \pmod{x^2+2x+2}$.
 - ▶ $(x+2)(x) = x^2+2x = x^2+2x-(x^2+2x+2) = -2 = 1 \pmod{x^2+2x+2}$.

[Torna a l'exercici \(p.67\)](#)

Solució de l'Exercici 17

1. $A \mathbb{Z}_2[x]/x^2 + x + 1$:

+	[0]	[1]	[x]	[x + 1]
[0]	[0]	[1]	[x]	[x + 1]
[1]	[1]	[0]	[x + 1]	[x]
[x]	[x]	[x + 1]	[0]	[1]
[x + 1]	[x + 1]	[x]	[1]	[0]

×	[0]	[1]	[x]	[x + 1]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[x]	[x + 1]
[x]	[0]	[x]	[x + 1]	[1]
[x + 1]	[0]	[x + 1]	[1]	[x]

2. $A \mathbb{Z}_2[x]/x^2 + 1$:

+	[0]	[1]	[x]	[x + 1]
[0]	[0]	[1]	[x]	[x + 1]
[1]	[1]	[0]	[x + 1]	[x]
[x]	[x]	[x + 1]	[0]	[1]
[x + 1]	[x + 1]	[x]	[1]	[0]

×	[0]	[1]	[x]	[x + 1]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[x]	[x + 1]
[x]	[0]	[x]	[1]	[x + 1]
[x + 1]	[0]	[x + 1]	[x + 1]	[0]

Solució de l'Exercici 17

3. A $\mathbb{Z}_3[x]/x^2 + 1$:

\times	[0]	[1]	[2]	[x]	[x + 1]	[x + 2]	[2x]	[2x + 1]	[2x + 2]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[x]	[x + 1]	[x + 2]	[2x]	[2x + 1]	[2x + 2]
[2]	[0]	[2]	[1]	[2x]	[2x + 2]	[2x + 1]	[x]	[x + 2]	[x + 1]
[x]	[0]	[x]	[2x]	[2]	[x + 2]	[2x + 2]	[1]	[x + 1]	[2x + 1]
[x + 1]	[0]	[x + 1]	[2x + 2]	[x + 2]	[2x]	[1]	[2x + 1]	[2]	[x]
[x + 2]	[0]	[x + 2]	[2x + 1]	[2x + 2]	[1]	[x]	[x + 1]	[2x]	[2]
[2x]	[0]	[2x]	[x]	[1]	[2x + 1]	[x + 1]	[2]	[2x + 2]	[x + 2]
[2x + 1]	[0]	[2x + 1]	[x + 2]	[x + 1]	[2]	[2x]	[2x + 2]	[x]	[1]
[2x + 2]	[0]	[2x + 2]	[x + 1]	[2x + 1]	[x]	[2]	[x + 2]	[1]	[2x]

Solució de l'Exercici 17

4. Podem observar que, en el primer cas i en el tercer cas, en la taula del producte hi ha el valor $[1]$ en totes les files i en totes les columnes, excepte en les que corresponen a $[0]$. Això significa que qualsevol valor no nul de l'anell en té un altre de manera que el producte dels dos és $[1]$. Per tant, qualsevol valor no nul de l'anell té invers i això fa que l'anell sigui un cos. En el segon cas, el valor $[x + 1]$ no té invers perquè no hi ha cap valor que multiplicat per ell doni $[1]$. Per això el segon cas no es tracta d'un cos.

[Torna a l'exercici \(p.69\)](#)

Solució de l'Exercici 18

El polinomi buscat ha de ser irreductible i de grau 3.

Podem agafar $x^3 + 2x^2 + 1$ o bé $x^3 + x^2 + 2$.

[Torna a l'exercici \(p.71\)](#)

Solució de l'Exercici 21

Si l'ordre de la classe $[x]_f$ és k , aleshores tenim $x^k \equiv 1 \pmod{f(x)}$ i, per tant, $x^k - 1$ és un múltiple de $f(x)$.

Això implica que k ha de ser més gran o igual que el grau de $f(x)$.

Torna a l'exercici (p.74)

Solució de l'Exercici 22

1. Perquè $\mathbb{Z}_2[x]/f(x)$ sigui un cos de 4 elements, cal que $f(x)$ sigui irreductible i que el grau de $f(x)$ sigui 2. Els polinomis de grau 2 són

- ▶ x^2
- ▶ $x^2 + 1$
- ▶ $x^2 + x$
- ▶ $x^2 + x + 1$

Cap dels tres primers polinomis és irreductible a $\mathbb{Z}_2[x]$.

En efecte, $x^2 = x \cdot x$, $x^2 + 1 = (x + 1) \cdot (x + 1)$ i $x^2 + x = x(x + 1)$.

El quart és irreductible, ja que és de grau 2 i no té arrels ($0^2 + 0 + 1 \neq 0$ i $1^2 + 1 + 1 \neq 0$).

Agafem, doncs, $x^2 + x + 1$.

Comprovem que la classe de x és un element primitiu.

Anomenem $\alpha = [x]$.

Tenim $\alpha^2 = \alpha^2 - (\alpha^2 + \alpha + 1) = -\alpha - 1 = \alpha + 1 \neq 1$ i, per tant, és un element primitiu.

Solució de l'Exercici 22

La taula d'equivalències potencial-vectorial-polinomial és la següent:

<i>pot.</i>	<i>vec.</i>	<i>pol.</i>
0	(0,0)	0
α^0	(1,0)	1
α	(0,1)	α
α^2	(1,1)	$1 + \alpha$

Les taules de la suma i del producte són

+	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

\times	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

Solució de l'Exercici 22

Hem utilitzat, entre d'altres,

$$\alpha^2 + 1 = (\alpha + 1) + 1 = \alpha + 2 = \alpha$$

$$\alpha^2 + \alpha = (\alpha + 1) + \alpha = 2\alpha + 1 = 1$$

$$\alpha \cdot \alpha^2 = \alpha(\alpha + 1) = \alpha^2 + \alpha = (\alpha + 1) + \alpha = 2\alpha + 1 = 1$$

$$\alpha^2 \cdot \alpha^2 = (\alpha + 1)(\alpha + 1) = \alpha^2 + \alpha + \alpha + 1 = \alpha^2 + 2\alpha + 1 =$$

$$\alpha^2 + 1 = (\alpha + 1) + 1 = \alpha + 2 = \alpha$$

[Torna a l'exercici \(p.88\)](#)

Solució de l'Exercici 23

1. Veiem que 3 és primer i després cal veure si $x^2 + x + 2$ és irreductible i ho és perquè té grau 2 i no té arrels.

En efecte,

$$f(0) = 2 \neq 0$$

$$f(1) = 1 \neq 0$$

$$f(2) = 2 \neq 0$$

2. $3^2 = 9$.

3. Els únics ordres possibles dels elements de $\mathbb{Z}_3[x]/x^2 + x + 2$ són els divisors de $9 - 1 = 8$, és a dir, $\{1, 2, 4, 8\}$.

Però α^1 i α^2 són $\neq 1$ i $\alpha^4 = (\alpha^2)^2 = (2\alpha + 1)^2 = 4\alpha^2 + 4\alpha + 1 = \alpha^2 + \alpha + 1 = 2\alpha + 1 + \alpha + 1 = 2 \neq 1$.

Per tant, l'ordre de α no és 1, 2 ni 4 i ha de ser 8.

Solució de l'Exercici 23

4. Utilitzarem que $\alpha^2 = 2\alpha + 1$. Així,

$$\alpha^3 = \alpha\alpha^2 = \alpha(2\alpha + 1) = 2\alpha^2 + \alpha = 2(2\alpha + 1) + \alpha = 2\alpha + 2$$

$$\alpha^4 = \alpha\alpha^3 = \alpha(2\alpha + 2) = 2\alpha^2 + 2\alpha = 2(2\alpha + 1) + 2\alpha = 2$$

$$\alpha^5 = \alpha\alpha^4 = \alpha(2) = 2\alpha$$

$$\alpha^6 = \alpha\alpha^5 = \alpha(2\alpha) = 2\alpha^2 = 2(2\alpha + 1) = \alpha + 2$$

$$\alpha^7 = \alpha\alpha^6 = \alpha(\alpha + 2) = \alpha^2 + 2\alpha = (2\alpha + 1) + 2\alpha = \alpha + 1$$

$$\alpha^8 = \alpha\alpha^7 = \alpha(\alpha + 1) = \alpha^2 + \alpha = (2\alpha + 1) + \alpha = 1$$

Solució de l'Exercici 23

I obtenim la taula

<i>pot.</i>	<i>pol.</i>	<i>vect.</i>
0	0	(0, 0)
α	α	(0, 1)
α^2	$2\alpha + 1$	(1, 2)
α^3	$2\alpha + 2$	(2, 2)
α^4	2	(2, 0)
α^5	2α	(0, 2)
α^6	$\alpha + 2$	(2, 1)
α^7	$\alpha + 1$	(1, 1)
α^8	1	(1, 0)

Solució de l'Exercici 23

5.

$$\begin{aligned}\alpha^2 \left(\frac{\alpha^{20} - \alpha^5 + \alpha}{\alpha^3 - \alpha} \right) &= \alpha^2 \left(\frac{\alpha^4 - \alpha^5 + \alpha}{\alpha^3 - \alpha} \right) \\ &= \alpha^2 \left(\frac{2 - 2\alpha + \alpha}{2\alpha + 2 - \alpha} \right) \\ &= \alpha^2 \left(\frac{2 + 2\alpha}{\alpha + 2} \right) \\ &= \alpha^2 \left(\frac{\alpha^3}{\alpha^6} \right) \\ &= \frac{\alpha^5}{\alpha^6} \\ &= \frac{\alpha^{13}}{\alpha^6} \\ &= \alpha^7.\end{aligned}$$

[Torna a l'exercici \(p.89\)](#)

Solució de l'Exercici 24

1. Com que són polinomis de grau 3, n'hi ha prou de veure si tenen arrels.

- ▶ $f(x) = x^3 + x^2 + 2$ no té arrels, ja que $f(0) = 2 \neq 0$, $f(1) = 1 \neq 0$ i $f(2) = 2 \neq 0$. Per tant, és irreductible.
- ▶ $g(x) = x^3 + 2x + 1$ no té arrels, ja que $g(0) = 1 \neq 0$, $g(1) = 1 \neq 0$ i $g(2) = 1 \neq 0$. Per tant, és irreductible.
- ▶ $h(x) = x^3 + 2x^2 + 2$ és reductible, ja que $h(0) = 2 \neq 0$, $h(1) = 2 \neq 0$, però $h(2) = 0$. Per tant, $h(x)$ és divisible per $x - 2$.

2. Perquè un polinomi $a(x) \in \mathbb{Z}_p[x]$ sigui primitiu, cal que sigui irreductible i que la classe de x dins de $\mathbb{Z}_p/(a(x))$ sigui un element primitiu, és a dir, tingui ordre $p^{\text{grau}(a)} - 1$.

En el nostre cas, caldrà que l'ordre de la classe de x sigui 26.

Si el grau de $a(x)$ és 3, els ordres de tots els elements de $\mathbb{Z}_3/(a(x))$ seran divisors de 26. Per tant, només podran ser 1, 2, 13 o 26.

En els casos de f i g , la classe de x no tindrà ordre 1, ni 2, ja que

$$\begin{array}{ll} x \not\equiv 1 \pmod{f} & (\text{perquè } x - 1 \text{ no pot ser un múltiple de } x^3 + \dots) \\ x^2 \not\equiv 1 \pmod{f} & (\text{perquè } x^2 - 1 \text{ no pot ser un múltiple de } x^3 + \dots) \\ x \not\equiv 1 \pmod{g} & (\text{perquè } x - 1 \text{ no pot ser un múltiple de } x^3 + \dots) \\ x^2 \not\equiv 1 \pmod{g} & (\text{perquè } x^2 - 1 \text{ no pot ser un múltiple de } x^3 + \dots). \end{array}$$

Solució de l'Exercici 24

Per tant, l'ordre només pot ser 13 o 26. Per això mirarem si $x^{13} \equiv 1 \pmod f$ o $x^{13} \equiv 1 \pmod g$.

$$\begin{aligned}x^{13} &\equiv x^2 x^{11} \pmod f \\&\equiv x^2 (x+1) \pmod f \\&\equiv x^3 + x^2 \pmod f \\&\equiv f+1 \pmod f \\&\equiv 1 \pmod f\end{aligned}\qquad\begin{aligned}x^{13} &\equiv x^2 x^{11} \pmod g \\&\equiv x^2 (x^2 + x + 2) \pmod g \\&\equiv x(x^3 + x^2 + 2x) \pmod g \\&\equiv x(g(x) + 2 + x^2) \pmod g \\&\equiv x^3 + 2x \pmod g \\&\equiv g(x) + 2 \pmod g \\&\equiv 2 \pmod g \\&\neq 1 \pmod g\end{aligned}$$

Observem que, pel cas de $f(x)$, la classe de x té ordre 13 i, per tant, $f(x)$ no és primitiu. En canvi, pel cas de $g(x)$, la classe de x no té ordre 13 i, per tant, ha de tenir ordre 26. Deduïm que $g(x)$ és primitiu.

3. $f(x)$ i $g(x)$. El cos tindrà $3^3 = 27$ elements.
4. $g(x)$.

Torna a l'exercici (p.90)

Solució de l'Exercici 25

- (a) És un cos perquè, d'una banda, 3 és primer i, d'altra banda, $x^2 + 1$ té grau 2 i no té arrels i, per tant, és irreductible a $\mathbb{Z}_3[x]$.
- (b) $3^2 = 9$.
- (c) $\alpha^1 \neq 1$, $\alpha^2 = 2 \neq 1$, $\alpha^3 = 2\alpha \neq 1$, $\alpha^4 = (\alpha^2)^2 = 2^2 = 1$. Per tant, l'ordre de α és 4.
- (d) No ho és perquè per ser primitiu hauria de tenir ordre $9 - 1 = 8$.
- (e) Els únics ordres possibles són els divisors de 8 i, per tant, β és primitiu si i només si $\beta^4 \neq 1$. Agafem $\beta = \alpha + 1$ i veiem que és un element primitiu. En efecte, si $\beta = \alpha + 1$, aleshores $\beta^2 = (\alpha + 1)^2 = \alpha^2 + 2\alpha + 1$.

Solució de l'Exercici 25

Ara $\beta^4 = (\beta^2)^2$ serà

$$\begin{aligned}(\alpha^2 + 2\alpha + 1)^2 &= \alpha^2(\alpha^2 + 2\alpha + 1) + 2\alpha(\alpha^2 + 2\alpha + 1) + (\alpha^2 + 2\alpha + 1) \\&= (\alpha^4 + 2\alpha^3 + \alpha^2) + (2\alpha^3 + 4\alpha^2 + 2\alpha) + (\alpha^2 + 2\alpha + 1) \\&= \alpha^4 + 4\alpha^3 + 6\alpha^2 + 4\alpha + 1 \\&= \alpha^4 + \alpha^3 + \alpha + 1 \\&= (1) + (2\alpha) + \alpha + 1 \\&= 3\alpha + 2 \\&= 2 \neq 1\end{aligned}$$

Haguéssim pogut agafar $\beta = \alpha + 2$, $\beta = 2\alpha + 1$, $\beta = 2\alpha + 2$ i també ens haurien donat elements primitius.

- (f) Ho podem fer a partir de la taula de l'apartat següent i obtenim $\alpha = \beta^6$. Si en lloc d'agafar $\beta = \alpha + 1$ haguéssim agafat $\beta = 2\alpha + 2$, seria el mateix. Si haguéssim agafat $\beta = \alpha + 2$ o bé $\beta = 2\alpha + 1$, aleshores tindríem $\alpha = \beta^2$.
- (g) Depenent de quina β haguem agafat, tindrem alguna de les següents taules:

Solució de l'Exercici 25

pot.	pol.	vect.
0	0	(0,0)
β	$\alpha + 1$	(1,1)
β^2	2α	(0,2)
β^3	$2\alpha + 1$	(1,2)
β^4	2	(2,0)
β^5	$2\alpha + 2$	(2,2)
β^6	α	(0,1)
β^7	$\alpha + 2$	(2,1)
β^8	1	(1,0)

pot.	pol.	vect.
0	0	(0,0)
β	$\alpha + 2$	(2,1)
β^2	α	(0,1)
β^3	$2\alpha + 2$	(2,2)
β^4	2	(2,0)
β^5	$2\alpha + 1$	(1,2)
β^6	2α	(0,2)
β^7	$\alpha + 1$	(1,1)
β^8	1	(1,0)

pot.	pol.	vect.
0	0	(0,0)
β	$2\alpha + 1$	(1,2)
β^2	α	(0,1)
β^3	$\alpha + 1$	(1,1)
β^4	2	(2,0)
β^5	$\alpha + 2$	(2,1)
β^6	2α	(0,2)
β^7	$2\alpha + 2$	(2,2)
β^8	1	(1,0)

pot.	pol.	vect.
0	0	(0,0)
β	$2\alpha + 2$	(2,2)
β^2	2α	(0,2)
β^3	$\alpha + 2$	(2,1)
β^4	2	(2,0)
β^5	$\alpha + 1$	(1,1)
β^6	α	(0,1)
β^7	$2\alpha + 1$	(1,2)
β^8	1	(1,0)

(h) En tots els casos dona 1. Vegem-ho en el cas $\beta = \alpha + 1$:

$$\beta^{15} \left(\frac{\beta^2 - \beta^3}{\beta^6 + \beta} \right) = \beta^{-1} \left(\frac{\beta^2 - \beta^3}{\beta^6 + \beta} \right) = \frac{\beta - \beta^2}{\beta^6 + \beta} = \frac{1 - \beta}{\beta^5 + 1} = \frac{2\alpha}{2\alpha} = 1.$$

Torna a l'exercici (p.91)

Solució de l'Exercici 26

1.

pot.	vec.
0	000
α^0	100
α^1	010
α^2	001
α^3	110
α^4	011
α^5	111
α^6	101

2.

a	$-a$
0	0
1	1
α	α
α^2	α^2
α^3	α^3
α^4	α^4
α^5	α^5
α^6	α^6

a	a^{-1}
1	1
α	α^6
α^2	α^5
α^3	α^4
α^4	α^3
α^5	α^2
α^6	α

3.

+	1	α	α^2	α^3	α^4	α^5	α^6
1	0	α^3	α^6	α	α^5	α^4	α^2
α	α^3	0	α^4	1	α^2	α^6	α^5
α^2	α^6	α^4	0	α^5	α	α^3	1
α^3	α	1	α^5	0	α^6	α^2	α^4
α^4	α^5	α^2	α	α^6	0	1	α^3
α^5	α^4	α^6	α^3	α^2	1	0	α
α^6	α^2	α^5	1	α^4	α^3	α	0

-	1	α	α^2	α^3	α^4	α^5	α^6
1	0	α^3	α^6	α	α^5	α^4	α^2
α	α^3	0	α^4	1	α^2	α^6	α^5
α^2	α^6	α^4	0	α^5	α	α^3	1
α^3	α	1	α^5	0	α^6	α^2	α^4
α^4	α^5	α^2	α	α^6	0	1	α^3
α^5	α^4	α^6	α^3	α^2	1	0	α
α^6	α^2	α^5	1	α^4	α^3	α	0

Solució de l'Exercici 26

4.

\cdot	1	α	α^2	α^3	α^4	α^5	α^6
1	1	α	α^2	α^3	α^4	α^5	α^6
α	α	α^2	α^3	α^4	α^5	α^6	1
α^2	α^2	α^3	α^4	α^5	α^6	1	α
α^3	α^3	α^4	α^5	α^6	1	α	α^2
α^4	α^4	α^5	α^6	1	α	α^2	α^3
α^5	α^5	α^6	1	α	α^2	α^3	α^4
α^6	α^6	1	α	α^2	α^3	α^4	α^5

/	1	α	α^2	α^3	α^4	α^5	α^6
1	1	α^6	α^5	α^4	α^3	α^2	α
α	α	1	α^6	α^5	α^4	α^3	α^2
α^2	α^2	α	1	α^6	α^5	α^4	α^3
α^3	α^3	α^2	α	1	α^6	α^5	α^4
α^4	α^4	α^3	α^2	α	1	α^6	α^5
α^5	α^5	α^4	α^3	α^2	α	1	α^6
α^6	α^6	α^5	α^4	α^3	α^2	α	1

Solució de l'Exercici 26

5. Per la taula d'equivalències observem que

$$x^5 + (\alpha + 1)x^4 + (\alpha^2 + \alpha + 1)x^3 + \alpha^2 x^2 + \alpha x + \alpha^2 + 1 = x^5 + \alpha^3 x^4 + \alpha^5 x^3 + \alpha^2 x^2 + \alpha x + \alpha^6.$$

Fem la divisió:

$$\begin{array}{r} x^5 + \alpha^3 x^4 + \alpha^5 x^3 + \alpha^2 x^2 + \alpha x + \alpha^6 \\ -(x^5 + \alpha^2 x^4 + \alpha x^3) \\ \hline \alpha^5 x^4 + \alpha^6 x^3 + \alpha^2 x^2 + \alpha x + \alpha^6 \\ -(\alpha^5 x^4 + x^3 + \alpha^6 x^2) \\ \hline \alpha^2 x^3 + x^2 + \alpha x + \alpha^6 \\ -(\alpha^2 x^3 + \alpha^4 x^2 + \alpha^3 x) \\ \hline \alpha^5 x^2 + x + \alpha^6 \\ -(\alpha^5 x^2 + x + \alpha^6) \\ \hline 0 \end{array} \quad \left| \begin{array}{l} x^2 + \alpha^2 x + \alpha \\ x^3 + \alpha^5 x^2 + \alpha^2 x + \alpha^5 \end{array} \right.$$

$$\text{Per tant, } \frac{x^5 + (\alpha + 1)x^4 + (\alpha^2 + \alpha + 1)x^3 + \alpha^2 x^2 + \alpha x + \alpha^2 + 1}{x^2 + \alpha^2 x + \alpha} = x^3 + \alpha^5 x^2 + \alpha^2 x + \alpha^5.$$

Torna a l'exercici (p.92)

Solució de l'Exercici 27

1.

pot.	vec.
0	00
α^0	10
α^1	01
α^2	11
α^3	12
α^4	20
α^5	02
α^6	22
α^7	21

2.

a	$-a$
0	0
1	α^4
α	α^5
α^2	α^6
α^3	α^7
α^4	1
α^5	α
α^6	α^2
α^7	α^3

a	a^{-1}
1	1
α	α^7
α^2	α^6
α^3	α^5
α^4	α^4
α^5	α^3
α^6	α^2
α^7	α

3.

+	1	α	α^2	α^3	α^4	α^5	α^6	α^7
1	α^4	α^2	α^7	α^6	0	α^3	α^5	α
α	α^2	α^5	α^3	1	α^7	0	α^4	α^6
α^2	α^7	α^3	α^6	α^4	α	1	0	α^5
α^3	α^6	1	α^4	α^7	α^5	α^2	α	0
α^4	0	α^7	α	α^5	1	α^6	α^3	α^2
α^5	α^3	0	1	α^2	α^6	α	α^7	α^4
α^6	α^5	α^4	0	α	α^3	α^7	α^2	1
α^7	α	α^6	α^5	0	α^2	α^4	1	α^3

-	1	α	α^2	α^3	α^4	α^5	α^6	α^7
1	0	α^3	α^5	α	α^4	α^2	α^7	α^6
α	α^7	0	α^4	α^6	α^2	α^5	α^3	1
α^2	α	1	0	α^5	α^7	α^3	α^6	α^4
α^3	α^5	α^2	α	0	α^6	1	α^4	α^7
α^4	1	α^6	α^3	α^2	0	α^7	α	α^5
α^5	α^6	α	α^7	α^4	α^3	0	1	α^2
α^6	α^3	α^7	α^2	1	α^5	α^4	0	α
α^7	α^2	α^4	1	α^3	α	α^6	α^5	0

Solució de l'Exercici 27

4.

·	1	α	α^2	α^3	α^4	α^5	α^6	α^7
1	1	α	α^2	α^3	α^4	α^5	α^6	α^7
α	α	α^2	α^3	α^4	α^5	α^6	α^7	1
α^2	α^2	α^3	α^4	α^5	α^6	α^7	1	α
α^3	α^3	α^4	α^5	α^6	α^7	1	α	α^2
α^4	α^4	α^5	α^6	α^7	1	α	α^2	α^3
α^5	α^5	α^6	α^7	1	α	α^2	α^3	α^4
α^6	α^6	α^7	1	α	α^2	α^3	α^4	α^5
α^7	α^7	1	α	α^2	α^3	α^4	α^5	α^6

/	1	α	α^2	α^3	α^4	α^5	α^6	α^7
1	1	α^7	α^6	α^5	α^4	α^3	α^2	α
α	α	1	α^7	α^6	α^5	α^4	α^3	α^2
α^2	α^2	α	1	α^7	α^6	α^5	α^4	α^3
α^3	α^3	α^2	α	1	α^7	α^6	α^5	α^4
α^4	α^4	α^3	α^2	α	1	α^7	α^6	α^5
α^5	α^5	α^4	α^3	α^2	α	1	α^7	α^6
α^6	α^6	α^5	α^4	α^3	α^2	α	1	α^7
α^7	α^7	α^6	α^5	α^4	α^3	α^2	α	1

5.

$$\begin{array}{r}
 x^8 \\
 -(x^8 + \alpha^6 x^7 + x^6 + \alpha^3 x^5 + \alpha^2 x^4 + \alpha^4) \\
 \hline
 \alpha^2 x^7 + \alpha^4 x^6 + \alpha^7 x^5 + \alpha^6 x^4 + \alpha^4 \\
 -(\alpha^2 x^7 + x^6 + \alpha^2 x^5 + \alpha^5 x^4 + \alpha^4 x^3) \\
 \hline
 x^6 + x^5 + \alpha^4 x^4 + x^3 + \alpha^4 \\
 -(x^6 + \alpha^6 x^5 + x^4 + \alpha^3 x^3 + \alpha^2 x^2) \\
 \hline
 \alpha^7 x^5 + x^4 + \alpha x^3 + \alpha^6 x^2 + \alpha^4 \\
 -(\alpha^7 x^5 + \alpha^5 x^4 + \alpha^7 x^3 + \alpha^2 x^2 + \alpha x) \\
 \hline
 \alpha^2 x^4 + x^3 + \alpha^2 x^2 + \alpha^5 x + \alpha^4 \\
 -(\alpha^2 x^4 + x^3 + \alpha^2 x^2 + \alpha^5 x + \alpha^4) \\
 \hline
 0
 \end{array}
 \quad \left| \frac{x^4 + \alpha^6 x^3 + x^2 + \alpha^3 x + \alpha^2}{x^4 + \alpha^2 x^3 + x^2 + \alpha^7 x + \alpha^2} \right.$$

Per tant, $\frac{x^8 - 1}{x^4 + \alpha^6 x^3 + x^2 + \alpha^3 x + \alpha^2} = x^4 + \alpha^2 x^3 + x^2 + \alpha^7 x + \alpha^2.$

Solució de l'Exercici 27

[Torna a l'exercici \(p.93\)](#)

Solució de l'Exercici 28

- (a)
- El primer polinomi s'anul·la en 1 i, per tant, és reductible.
 - El segon polinomi no té arrels. Per ser reductible hauria de ser el quadrat de l'únic polinomi reductible de grau 2, és a dir, hauria de ser $(x^2 + x + 1)^2 = x^4 + x^2 + 1$, però veiem que no ho és. Per tant, és irreductible.
 - El tercer polinomi acabem de veure que és $(x^2 + x + 1)^2 = x^4 + x^2 + 1$, per això és reductible.
 - El quart polinomi és irreductible pel mateix argument que el segon.
- (b) $x^4 + 1 = (x^2 + 1)^2 = (x + 1)^4$,
 $x^4 + x + 1 = x^4 + x + 1$,
 $x^4 + x^2 + 1 = (x^2 + x + 1)^2$,
 $x^4 + x^3 + x^2 + x + 1 = x^4 + x^3 + x^2 + x + 1$.
- (c) 1, perquè no tenen factors irreductibles no constants en comú.
- (d) Utilitzem l'algoritme d'Euclides.

1	0	1	x^2
0	1	-1	$x^2 + 1$
		1	x^2
$x^4 + x^2 + 1$	$x^4 + 1$	x^2	1

Obtenim que $(x^2)(x^4 + x^2 + 1) + (x^2 + 1)(x^4 + 1) = 1$.

Comprovem el resultat: $(x^2)(x^4 + x^2 + 1) + (x^2 + 1)(x^4 + 1) = (x^6 + x^4 + x^2) + (x^6 + x^2) + (x^4 + 1) = 1$.

- (e) La segona i la quarta. Tenen $2^4 = 16$ elements.
- (f) Sabem que els únics ordres possibles de α són els divisors de 15, és a dir, 1, 3, 5, 15. Perquè α sigui primitiu cal que el seu ordre sigui màxim, és a dir, 15.
- En el segon cas, α té ordre 15, ja que 1, 3 són més petits que el grau del polinomi generador i $\alpha^5 = \alpha \alpha^4 = \alpha(\alpha + 1) = \alpha^2 + \alpha \neq 1$. Per tant, α és primitiu.
- En el quart cas, $\alpha^5 = \alpha(\alpha^3 + \alpha^2 + \alpha + 1) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1 + \alpha^3 + \alpha^2 + \alpha = 1$. Per tant, α té ordre $5 < 15$ i no és primitiu.

Solució de l'Exercici 28

(g)

exp.	pol.	vect.
α^0	1	1000
α^1	α	0100
α^2	α^2	0010
α^3	α^3	0001
α^4	$\alpha + 1$	0011
α^5	$\alpha^2 + \alpha$	0110
α^6	$\alpha^3 + \alpha^2$	0011
α^7	$\alpha^3 + \alpha + 1$	1101
α^8	$\alpha^2 + 1$	1010
α^9	$\alpha^3 + \alpha$	0101
α^{10}	$\alpha^2 + \alpha + 1$	1110
α^{11}	$\alpha^3 + \alpha^2 + \alpha$	0111
α^{12}	$\alpha^3 + \alpha^2 + \alpha + 1$	1111
α^{13}	$\alpha^3 + \alpha^2 + 1$	1011
α^{14}	$\alpha^3 + 1$	1001

(h) Tots els divisors de $16 - 1 = 15$, que són 1, 3, 5, 15.

(i) 1 té ordre 1, $\alpha^5 = \alpha^2 + \alpha$ té ordre 3, α^3 té ordre 5 i α té ordre 15.

Torna a l'exercici (p.94)