Aritmètica modular

Maria Bras-Amorós, Oriol Farràs Ventura

24 d'octubre de 2023

Congruències

Congruències

Definició

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

$$a = r \mod m.$$

Lema 1

Donats dos enters a, b i $m > 0$, és equivalent:

- Els residus de dividir a i b entre m coincideixen.
- $a - b$ és un múltiple de m.

Congruències

Lema 1

Donats dos enters a, b i $m > 0$, és equivalent:

- Els residus de dividir a i b entre m coincideixen.
- $a - b$ és un múltiple de m.

Exemple

Exemple amb $m = 7$
Si dos nombres tenen el mateix residu quan els divideixo entre 7*,*
(Exemple: $52 = 7 \times 7 + 3$, $73 = 7 \times 10 + 3$*)*
aleshores la seva diferència és un múltiple de 7*.*
(Exemple: $52 - 73 = -21$ *és un múltiple de* 7*)*

Congruències

Lema 1

Donats dos enters a, b i $m > 0$, és equivalent:

- Els residus de dividir a i b entre m coincideixen.
- $a - b$ és un múltiple de m.

Exemple

Al revés també és cert.
Si la diferència entre dos nombres és un múltiple de 7*,*
(Exemple: $149 - 100 = 49$*)*
aleshores els dos nombres tenen el mateix residu quan els divideixo entre 7*.*
(Exemple: $149 = 7 \times 21 + 2$*,* $100 = 7 \times 14 + 2$*)*

Congruències

Lema 1

Donats dos enters a, b i $m > 0$, és equivalent:

- Els residus de dividir a i b entre m coincideixen.
- $a - b$ és un múltiple de m.

Demostració

(sketch)

$a = q_a m + r$ *i* $b = q_b m + r$ *implica que* $a - b = (q_a - q_b)m$.

$a - b$ *és un múltiple de* m, $a = q_a m + r_a$ *i* $b = q_b m + r_b$, *implica* $(q_a - q_b)m + (r_a - r_b)$ *és un múltiple de* m *i, per tant,* $r_a - r_b$ *és un múltiple de* m. □

Congruències

Congruència

Dos enters a i b són **congruents mòdul** un enter m si es compleixen les condicions equivalents del lema 1. Escrivim indistintament $a \equiv b \mod m$ o bé $a \equiv b(m)$.

En el cas anterior, diríem

$52 \equiv 73(7)$ o $52 \equiv 73 \mod 7$

i

$149 \equiv 100(7)$ o $149 \equiv 100 \mod 7$

Congruències

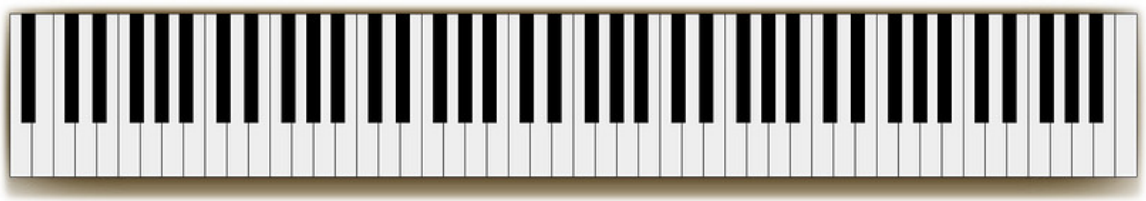
Exemple

Les congruències mòdul 7 les utilitzem en el calendari. Dos dies del mateix mes cauen en el mateix dia de la setmana si són congruents mòdul 7.

Congruències

Exemple

També fem congruències mòdul 7 *en la interpretació de les notes musicals. Dues notes separades per* 7, 14, 21, *etc. salts de nota són la mateixa llevat d'un canvi d'octava.*



Congruències

Exemple

Estem molt familiaritzats amb les congruències mòdul 2*. Els nombres només poden ser o bé congruents amb* 0 *o bé congruents amb* 1 *mòdul* 2*. En el primer cas es tracta dels nombres parells, mentre que en el segon cas es tracta dels senars.*

Exercici 1

Demostreu que si $a \equiv b \mod m$ i d divideix m, aleshores $a \equiv b \mod d$. Solució (p.90)

Exemple

Vegem un exemple del resultat de l'exercici:

$$8726 \equiv 26 \mod 100$$

Aleshores també tindrem

$$98726 \equiv 26 \mod 50, \qquad 98726 \equiv 26 \mod 10, \ldots$$

El contrari no és cert. Per exemple,

$$1 \equiv 51 \mod 50$$

però, en canvi,

$$1 \not\equiv 51 \mod 100$$

Congruències

Lema 2

La relació de congruència és una **relació d'equivalència**. És a dir, satisfà les propietats següents:

- **reflexiva** ($a \equiv a \mod m$ per tot a i tot m enters),
- **simètrica** ($a \equiv b \mod m$ si i només si $b \equiv a \mod m$),
- **transitiva** (si $a \equiv b \mod m$ i $b \equiv c \mod m$, aleshores $a \equiv c \mod m$).

Diem que a i a' són de la mateixa **classe d'equivalència** mòdul m si $a \equiv a' \mod m$.

Operacions amb congruències

Lema 3: La suma i el producte de classes queden ben definits

Si $a_1 \equiv a_2 \mod m$ i $b_1 \equiv b_2 \mod m$, aleshores

$$a_1 + b_1 \equiv a_2 + b_2 \mod m,$$

$$a_1 \cdot b_1 \equiv a_2 \cdot b_2 \mod m.$$

Per exemple, tenim que

$$\begin{aligned} 5 &\equiv 12 \mod 7 \\ 11 &\equiv -3 \mod 7 \end{aligned}$$

El que ens diu el lema és que, aleshores,

$$\begin{aligned} 5 + 11 &\equiv 12 - 3 \mod 7 \\ 5 \cdot 11 &\equiv 12 \cdot (-3) \mod 7 \end{aligned}$$

Operacions amb congruències

Les classes d'equivalència ens permetran fer els càlculs de manera més fàcil. Per exemple, si vull calcular la reducció mòdul 3 de

$$754 + 389 \quad , \quad 754 \cdot 389 \quad \text{o} \quad 754^{1000}$$

puc reduir primer els operands:

$$\begin{aligned} 754 &= 1 \mod 3 \\ 389 &= 2 \mod 3, \end{aligned}$$

i les operacions em queden reduïdes a

$$1 + 2 \equiv 0 \mod 3 \quad , \quad 1 \cdot 2 \equiv 2 \mod 3 \quad \text{i} \quad 1^{1000} \equiv 1 \mod 3$$

Operacions amb congruències

Una altra conseqüència del lema 3, és que si $a \equiv b \mod m$, aleshores $ka \equiv kb \mod m$.

Però el recíproc no és cert.

La simplificació no queda ben definida.

És a dir, pot ser que $ka \equiv kb \mod m$, però, en canvi, $a \not\equiv b \mod m$.

Per exemple, $2 \cdot 1 \equiv 2 \cdot 3 \mod 4$, però, en canvi, $1 \not\equiv 3 \mod 4$.

Operacions amb congruències

Lema 4

Si $\text{mcd}(k, m) = 1$, aleshores podem simplificar:

$$ka \equiv kb \mod m \iff a \equiv b \mod m.$$

Demostració

Suposem que $\text{mcd}(k, m) = 1$.

$$\begin{aligned} ka \equiv kb \mod m &\iff m \mid k(a-b) \\ &\iff m \mid a-b \\ &\iff a \equiv b \mod m \end{aligned}$$

□

Operacions amb congruències

Lema 5

En general, agafant $k' = \frac{k}{\text{mcd}(k,m)}$ i $m' = \frac{m}{\text{mcd}(k,m)}$, podem simplificar:

$$ka \equiv kb \mod m \iff k'a \equiv k'b \mod m'.$$

Demostració

$$\begin{aligned} ka \equiv kb \mod m &\iff m \mid k(a-b) \\ &\iff \frac{m}{\text{mcd}(k,m)} \mid \frac{k}{\text{mcd}(k,m)}(a-b) \\ &\iff k'a \equiv k'b \mod m'. \end{aligned}$$

□

Resolució de congruències

Donats enters a, b, m, amb $m > 0$, volem saber per quins valors de x, mòdul m, es compleix que

$$ax \equiv b \mod m.$$

Per exemple, suposem que volem resoldre les congruències lineals següents:

1. $35x \equiv 20(60)$.
2. $32x \equiv 58(60)$.
3. $47x \equiv 17(60)$.
4. $39x \equiv 18(60)$.
5. $51x \equiv 26(60)$.
6. $8x \equiv 8(60)$.

Resolució de congruències. Existeixen solucions?

Es pot demostrar, utilitzant la identitat de Bézout, que existiran solucions si i només si $\mathrm{mcd}(a, m)$ divideix b.

Vegem si tenen solució les congruències anteriors:

1. $35x \equiv 20(60)$ té solució perquè $\mathrm{mcd}(35, 60) = 5$ divideix 20.
2. $32x \equiv 58(60)$ no té solució perquè $\mathrm{mcd}(32, 60) = 4$ no divideix 58.
3. $47x \equiv 17(60)$ té solució perquè $\mathrm{mcd}(47, 60) = 1$ divideix 17.
4. $39x \equiv 18(60)$ té solució perquè $\mathrm{mcd}(39, 60) = 3$ divideix 18.
5. $51x \equiv 26(60)$ no té solució perquè $\mathrm{mcd}(51, 60) = 3$ no divideix 26.
6. $8x \equiv 8(60)$ té solució perquè $\mathrm{mcd}(8, 60) = 4$ divideix 8.

Resolució de congruències. Podem simplificar?

Si $\text{mcd}(a, m)$ divideix b, aleshores podem dividir tots els paràmetres entre $\text{mcd}(a, m)$.

Vegem com queden simplificades les congruències anteriors, de la forma $a'x \equiv b' \mod m'$, amb $\text{mcd}(a', m') = 1$:

1. $35x \equiv 20(60)$ queda simplificada com $7x \equiv 4(12)$.
2. $32x \equiv 58(60)$ no té solució.
3. $47x \equiv 17(60)$ no es pot simplificar més.
4. $39x \equiv 18(60)$ queda simplificada com $13x \equiv 6(20)$.
5. $51x \equiv 26(60)$ no té solució.
6. $8x \equiv 8(60)$ queda simplificada com $2x \equiv 2(15)$.

Resolució de congruències. Com trobem *una* solució?

Com que ara $\mathrm{mcd}(m', a') = 1$, per la identitat de Bézout existiran λ i μ tals que $\mu a' = 1 - \lambda m' \equiv 1 \mod m'$.

Busquem, doncs, aquest paràmetre μ de la identitat de Bézout.

Un cop tenim el paràmetre μ tal que

$$\mu a' \equiv 1 \mod m',$$

deduïm que

$$(b'\mu)a' \equiv b' \mod m'$$

i, per tant,

$$x \equiv b'\mu$$

és una primera solució.

Resolució de congruències. Com trobem *una* solució?

1. $35x \equiv 20(60)$ queda simplificada com

$$7x \equiv 4(12)$$

i per això resolem primer $7x' \equiv 1(12)$:

λ	1	0	1	-1	3	
μ	0	1	-1	2	-5	
quocients			1	1	2	
residus	12	7	5	2	1	0

Deduïm que $(12)\cdot(3)+(7)\cdot(-5)=1$ i, per tant,

$$7\cdot 7 \equiv 1 \mod 12.$$

Multiplicant-ho tot per 4, es complirà

$$\begin{aligned} 7(7\cdot 4) &\equiv 1\cdot 4 \mod 12 \\ 7\cdot 28 &\equiv 4 \mod 12 \\ 7\cdot 4 &\equiv 4 \mod 12. \end{aligned}$$

Per tant,

$$x \equiv 4(12)$$

és *una* solució.

Resolució de congruències. Com trobem *una* solució?

2. $32x \equiv 58(60)$ no té solució.

Resolució de congruències. Com trobem *una* solució?

3. $47x \equiv 17(60)$ no es pot simplificar més. Resolem primer $47x' \equiv 1(60)$:

λ	1	0	1	-3	4	-7	11	-18	
μ	0	1	-1	4	-5	9	-14	23	
quocients			1	3	1	1	1	1	
residus	60	47	13	8	5	3	2	1	0

Deduïm que $(60)\cdot(-18)+(47)\cdot(23)=1$ i, per tant,

$$47\cdot 23 \equiv 1 \mod 60.$$

Multiplicant-ho tot per 17, es complirà

$$\begin{aligned} 47(23\cdot 17) &\equiv 1\cdot 17 \mod 60 \\ 47\cdot 391 &\equiv 17 \mod 60 \\ 47\cdot 31 &\equiv 17 \mod 60. \end{aligned}$$

Per tant,

$$x \equiv 31(60)$$

és *una* solució.

Resolució de congruències. Com trobem *una* solució?

4. $39x \equiv 18(60)$ queda simplificada com

$$13x \equiv 6(20)$$

i per això resolem primer $13x' \equiv 1(20)$:

λ	1	0	1	-1	2	
μ	0	1	-1	2	-3	
quocients			1	1	1	
residus	20	13	7	6	1	0

Deduïm que $(20)\cdot(2)+(13)\cdot(-3)=1$ i, per tant,

$$13\cdot 17 \equiv 1 \mod 20.$$

Multiplicant-ho tot per 6, es complirà

$$\begin{aligned} 13(17\cdot 6) &\equiv 1\cdot 6 \mod 20 \\ 13\cdot 102 &\equiv 6 \mod 20 \\ 13\cdot 2 &\equiv 6 \mod 20. \end{aligned}$$

Per tant,

$$x \equiv 2(20)$$

és *una* solució.

Resolució de congruències. Com trobem *una* solució?

5. $51x \equiv 26(60)$ no té solució.

Resolució de congruències. Com trobem *una* solució?

6. $8x \equiv 8(60)$ queda simplificada com

$$2x \equiv 2(15)$$

i per això resolem primer $2x' \equiv 1(15)$:

λ	1	0	1	
μ	0	1	-7	
quocients			7	
residus	15	2	1	0

Deduïm que $(15)\cdot(1)+(2)\cdot(-7)=1$ i, per tant,

$$2\cdot 8 \equiv 1 \mod 15.$$

Multiplicant-ho tot per 2, es complirà

$$\begin{aligned} 2(8\cdot 2) &\equiv 1\cdot 2 \mod 15 \\ 2\cdot 16 &\equiv 2 \mod 15 \\ 2\cdot 1 &\equiv 2 \mod 15. \end{aligned}$$

Per tant,

$$x \equiv 1(15)$$

és *una* solució.

Resolució de congruències. I *totes* les solucions?

Si $a'x_0 \equiv b'(m')$, aleshores també

$$a'(x_0 + m') \equiv b'(m'),$$

$$a'(x_0 + 2m') \equiv b'(m'),$$

$$a'(x_0 + 3m') \equiv b'(m'),$$

$$\vdots$$

Totes les solucions mòdul m seran

$$x_0, x_0 + m', x_0 + 2m', x_0 + 3m', \ldots, x_0 + (m - m').$$

En total n'hi haurà

$$m/m' = \mathrm{mcd}(a, m).$$

Resolució de congruències. I *totes* les solucions?

1. $35x \equiv 20(60)$ tenia solució $x \equiv 4(12)$. Totes les seves solucions mòdul 60 seran $x = 4, 16, 28, 40, 52(60)$. Observem que n'hi ha $5 = \text{mcd}(35, 60)$.
2. $32x \equiv 58(60)$ no té solució.
3. $47x \equiv 17(60)$ només té una solució, ja que $\text{mcd}(47, 60) = 1$. La solució és $x \equiv 31(60)$.
4. $39x \equiv 18(60)$ tenia solució $x \equiv 2(20)$. Totes les seves solucions mòdul 60 seran $x = 2, 22, 42(60)$. Observem que n'hi ha $3 = \text{mcd}(39, 60)$.
5. $51x \equiv 26(60)$ no té solució.
6. $8x \equiv 8(60)$ tenia solució $x \equiv 1(15)$. Totes les seves solucions mòdul 60 seran $x = 1, 16, 31, 46(60)$. Observem que n'hi ha $4 = \text{mcd}(8, 60)$.

Sumari

Lema 6

Considerem la congruència $ax \equiv b \mod m$.

1. Té solució si i només si $\mathrm{mcd}(a, m) \mid b$.
2. L'enter x és solució de $ax \equiv b \mod m$ si i només si ho és de

$$\frac{a}{\mathrm{mcd}(a,m)} x \equiv \frac{b}{\mathrm{mcd}(a,m)} \mod \frac{m}{\mathrm{mcd}(a,m)}.$$

3. Si existeix una solució x_0, aleshores n'existeixen $\mathrm{mcd}(a, m)$ i el conjunt de solucions és donat per

$$x \equiv x_0 + k \frac{m}{\mathrm{mcd}(a,m)} \mod m,$$

amb $k = 0, 1, \ldots, \mathrm{mcd}(a, m) - 1$.

Procediment per resoldre $ax \equiv b \mod m$

- Si $\mcd(a,m) \nmid b$, aleshores no hi ha solució.
- Si $\mcd(a,m) \mid b$
  - Si $\mcd(a,m) = 1$
    - Calculem els coeficients λ i μ de la identitat de Bézout

      $$\lambda m + \mu a = 1.$$

    - La solució és única i és $x \equiv \mu b \mod m$.
  - Si $\mcd(a,m) \neq 1$
    - Busquem la solució x_0 de la congruència

      $$\frac{a}{\mcd(a,m)} x \equiv \frac{b}{\mcd(a,m)} \mod \frac{m}{\mcd(a,m)}$$

      que compleix $\mcd\left(\frac{a}{\mcd(a,m)}, \frac{m}{\mcd(a,m)}\right) = 1$.
    - El conjunt de solucions serà

      $$x \equiv x_0 + k \frac{m}{\mcd(a,m)} \mod m,$$

      amb $k = 0, \ldots, \mcd(a,m) - 1$.

Podem resoldre congruències amb la funció `solve_mod`

```
print("solve_mod(35*x==20,60)=",solve_mod(35*x==20,60))
print("solve_mod(32*x==58,60)=",solve_mod(32*x==58,60))
print("solve_mod(47*x==17,60)=",solve_mod(47*x==17,60))
print("solve_mod(39*x==18,60)=",solve_mod(39*x==18,60))
print("solve_mod(51*x==26,60)=",solve_mod(51*x==26,60))
print("solve_mod(8*x==8,60)=",solve_mod(8*x==8,60))
```

Anells $\mathbb{Z}_m$

Pel lema 2 sabem que la relació de congruència és una relació d'equivalència.

Per això, podem dividir $\mathbb{Z}$ en m classes d'equivalència donades per la relació de congruència mòdul m.

Definim $\mathbb{Z}_m$ com el conjunt de les m classes d'equivalència.

Així,

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\},$$

on $[r]_m$ representa la classe de tots els enters que dividits entre m tenen residu r.

Per extensió, escriurem $[a]_m = [r]_m$ si $a = qm + r$ amb $0 \leq r < m$.

Anells $\mathbb{Z}_m$

Exemple

En el cas de $\mathbb{Z}_2$, la classe de $[0]_2$ és la classe dels nombres parells, i $[1]_2$ la dels nombres imparells.

Exemple

En el cas de $\mathbb{Z}_3$, dividim el conjunt d'enters d'acord amb el residu de la divisió per 3:

$$\begin{array}{ccccccccccc} & & & & \mathbb{Z} & & & & & & \\ \ldots & -2 & -1 & 0 & 1 & 2 & 3 & 4 & \ldots & \to & \begin{array}{c|c|c} [0]_3 & [1]_3 & [2]_3 \\ \vdots & \vdots & \vdots \\ -3 & -2 & -1 \\ 0 & 1 & 2 \\ 3 & 4 & 5 \\ \vdots & \vdots & \vdots \end{array} \end{array}$$

Per tant,

$$[0]_3 = \{\ldots, -3, 0, 3, 6, \ldots\} = \{3k : k \in \mathbb{Z}\}$$
$$[1]_3 = \{\ldots, -2, 1, 4, 7, \ldots\} = \{3k+1 : k \in \mathbb{Z}\}$$
$$[2]_3 = \{\ldots, -1, 2, 5, 8, \ldots\} = \{3k+2 : k \in \mathbb{Z}\}$$

Classes d'equivalència

Podem veure que, en general,

$$[r]_m = \{mk + r : k \in \mathbb{Z}\}$$

El conjunt format per les classes d'equivalència d'una relació d'equivalència s'anomena **conjunt quocient**. Més endavant veurem altres conjunts quocients.

Aritmètica modular

Pel lema 3 sabem que dins de $\mathbb{Z}_m$ hi ha les dues operacions internes ben definides:

$$[r_1]_m + [r_2]_m = [r_1 + r_2]_m,$$

$$[r_1]_m \cdot [r_2]_m = [r_1 \cdot r_2]_m.$$

Ara analitzem les propietats de $(\mathbb{Z}_m, +, \cdot)$:

- L'operació suma a $\mathbb{Z}_m$ és associativa i commutativa perquè ho és a $\mathbb{Z}$.
- El neutre per a la suma és $[0]_m$ i l'invers per a la suma està ben definit com

  $$-[a]_m = [-a]_m.$$

  La resta està ben definida, aleshores, com la suma de l'invers.
- L'operació producte a $\mathbb{Z}_m$ és associativa i commutativa perquè ho és a $\mathbb{Z}$ i satisfà la propietat distributiva amb la suma.
- El neutre pel producte és $[1]_m$.

Aritmètica modular

Per tot l'anterior, podem afirmar el següent:

$(\mathbb{Z}_m, +, \cdot)$ és un anell commutatiu amb unitat.

En aquest curs només considerarem la suma i el producte a $\mathbb{Z}_m$ que acabem de definir. Per tant, per simplificar la notació, quan parlem de $\mathbb{Z}_m$ ens referim a l'anell $(\mathbb{Z}_m, +, \cdot)$.

En general, $\mathbb{Z}_m$ no és un cos perquè pot haver-hi elements que no tinguin invers. Per exemple, a $\mathbb{Z}_4$,

$$[2]_4 \cdot [0]_4 = [0]_4,$$

$$[2]_4 \cdot [1]_4 = [2]_4,$$

$$[2]_4 \cdot [2]_4 = [0]_4,$$

$$[2]_4 \cdot [3]_4 = [2]_4.$$

Per tant, no existeix cap classe $[a]_4$ tal que $[2]_4 \cdot [a]_4 = [1]_4$.

Podem definir $\mathbb{Z}_m$ amb la funció `Integers(m)`

```
print("Integers(27)=",Integers(27))

Z27=Integers(27)

print("Z27(50)=",Z27(50))

print("Z27(20+23)=",Z27(20+23))
print("Z27(20)+Z27(23)=",Z27(20)+Z27(23))

print("Z27(30*2)=",Z27(30*2))
print("Z27(30)*Z27(2)=",Z27(30)*Z27(2))
```

Aprofitem per veure la diferència entre conjunt i llista. La podeu veure amb les següents comandes?

```
Z27=Integers(27)
print("[Z27(a) for a in [1..100]]=",
          [Z27(a) for a in [1..100]])
print("{Z27(a) for a in [1..100]}=",
          {Z27(a) for a in [1..100]})
```

Aritmètica modular

Per simplificar la notació, sovint escriurem a en comptes de $[a]_m$.

Exercici 2

Comproveu que a $\mathbb{Z}_2$ es compleix:

- $-a = a$ per tot a,
- $(a+b)^2 = a^2 + b^2$.
- Demostreu per inducció que a $\mathbb{Z}_2$ es compleix $(a_1 + a_2 + \cdots + a_n)^2 = a_1^2 + a_2^2 + \cdots + a_n^2$, per tot n.

Solució (p.91)

Exercici 3

Comproveu que a $\mathbb{Z}_p$, amb p primer, es compleix que

$$(a_1 + a_2 + \cdots + a_n)^p = a_1^p + a_2^p + \cdots + a_n^p,$$

per tot n.

Taules d'operacions

Coneixem les taules de la suma i el producte binaris:

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

Taules d'operacions

Podem construir les mateixes taules per a qualsevol mòdul.

Vegem, per exemple, les taules de la suma i el producte mòdul 6:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Taules d'operacions

. . . i les taules de la suma i el producte mòdul 7:

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

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Taules d'operacions

Podem fer algunes observacions en aquestes taules:

- Les taules són simètriques. Això és a causa de la commutativitat de les operacions.
- A la taula de la suma, la fila corresponent al 0 és una còpia de la primera fila. Això ens indica que el 0 és el neutre per a la suma.
- A la taula del producte, la fila corresponent a l'1 és una còpia de la primera fila. Això ens indica que l'1 és el neutre pel producte.

Invertibles i divisors de zero

Sigui $(A, +, \cdot)$ un anell amb neutre 0 respecte de $+$.

Si per un element a n'existeix un altre (que anomenem a^{-1}) tal que $a \cdot a^{-1} = 1$, aleshores diem que a^{-1} és l'**invers** de a.

Per exemple, a $\mathbb{Z}_5$, l'invers de 2 és $2^{-1} = 3$, perquè a $\mathbb{Z}_5$, $2 \cdot 3 = 6 = 1$.

Compte: si $a \in \mathbb{Z}$, l'element a^{-1} dins de $\mathbb{Z}_m$ no el podem confondre amb el racional $\frac{1}{a}$.

Invertibles i divisors de zero

Els elements de A que tenen invers es diuen **invertibles**.

Un element $a \in A$, $a \neq 0$ és un **divisor de zero** si existeix $b \in A$, $b \neq 0$ tal que $a \cdot b = b \cdot a = 0$.

Invertibles i divisors de zero I

Lema 7

Considerem l'anell $\mathbb{Z}_m$ i un element $a \in \mathbb{Z}_m$, $a \neq 0$. Aleshores

1. a és invertible si i només si $\text{mcd}(a, m) = 1$.
2. a és un divisor de zero si i només si $\text{mcd}(a, m) \neq 1$.

Per tant, tot $a \in \mathbb{Z}_m$ és invertible o bé és divisor de zero.

Observem que hem comès un abús de notació al lema, ja que mcd només està definit per parelles d'enters. Però vam veure que si $a_1, a_2 \in [a]_m$, aleshores $\text{mcd}(a_1, m) = \text{mcd}(a_2, m)$ i, per tant, $\text{mcd}(a, m)$ està ben definit.

Invertibles i divisors de zero II

Demostració

Pel lema 6, $ax = b \mod m$ *té solució si i només si* $\mcd(a, m)$ *divideix b i, en el cas de tenir-ne, el nombre de solucions diferents mòdul m és* $\mcd(a, m)$.

1. *L'element a és invertible si i només si* $ax = 1 \mod m$ *té solució, que és equivalent al fet que* $\mcd(a, m)$ *divideixi* 1 *pel lema 6. Com que l'únic divisor positiu de* 1 *és ell mateix, a serà invertible si i només si* $\mcd(a, m) = 1$.
2. *L'element a és divisor de zero si i només* $ax = 0 \mod m$ *té més d'una solució, que és equivalent a* $\mcd(a, m) > 1$ *pel lema 6.*

□

Invertibles

Identitat de Bézout i l'invers d'un element

Si a és invertible a $\mathbb{Z}_m$, aleshores $\text{mcd}(m, a) = 1$.
Per la identitat de Bézout sabem que existiran λ i μ tals que

$$\lambda m + \mu a = 1.$$

Això significa que $\mu a = 1 - \lambda m$ i, per tant,

$$\mu a \equiv 1 \mod m$$

Deduïm, doncs, que $a^{-1} = \mu$.

Invertibles

Teorema 1

$\mathbb{Z}_m$ és un cos si i només si m és primer.

Anomenem $\mathbb{Z}_m^*$ al conjunt d'elements invertibles de $\mathbb{Z}_m$.

Exercici 4

Calculeu $\mathbb{Z}_m^*$ per $1 < m \leq 12$. Solució (p.92)

Funció d'Euler

Ara definim una funció $\phi : \mathbb{N} \to \mathbb{N}$ que s'anomena **funció d'Euler**.

Nota (p.125)

Definim, equivalentment,

$$\begin{aligned} \phi(m) &= \#\{a : 0 \leq a < m \text{ i } \operatorname{mcd}(a, m) = 1\} \\ &= \#\mathbb{Z}_m^* \end{aligned}$$

Propietats

Lema 8

- Si p és primer, aleshores $\phi(p) = p - 1$.
- Si $\mcd(a, b) = 1$, aleshores $\phi(ab) = \phi(a)\phi(b)$.
- Si p és primer, aleshores $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$.

El primer punt es pot veure directament de la definició de ϕ. L'últim punt es pot comprovar veient que exactament 1 de cada p enters entre 0 i $p^k - 1$ és no coprimer amb p^k.

Funció d'Euler

Exercici 5

Calculeu

- $\phi(18)$,
- $\phi(27)$,
- $\phi(35)$.

Solució (p.93)

Exercici 6

Comproveu que si la descomposició d'un enter n en producte de primers és $n = p_1^{n_1} \cdot \cdots \cdot p_k^{n_k}$, aleshores

$$\phi(n) = p_1^{n_1-1}(p_1-1) \cdot p_2^{n_2-1}(p_2-1) \cdot \cdots \cdot p_k^{n_k-1}(p_k-1)$$

Solució (p.95)

Podem trobar els invertibles utilitzant el gcd

```
[a for a in Integers(27) if gcd(a,27) == 1]
```

Quants n'hi ha?

```
print("len([a for a in Integers(27) if gcd(a,27)==1])=",
      len([a for a in Integers(27) if gcd(a,27) == 1]))
print("euler_phi(27)=",euler_phi(27))
```

També podem trobar l'invers de cadascun dels invertibles

```
[[a,a^(-1)] for a in Integers(27) if gcd(a,27)==1]
```

O bé

```
[[a,inverse_mod(a,27)] for a in [0..26] if gcd(a,27)==1]
```

Comprovem que $\mathbb{Z}_{27}$ no és un cos

```
is_field(Integers(27))
```

Teorema de Fermat i teorema d'Euler

Teorema 2: Teorema de Fermat Nota (p.125)

Si p és primer i $\text{mcd}(a, p) = 1$, aleshores

$$a^{p-1} \equiv 1 \mod p.$$

Teorema 3: Teorema d'Euler

Si $\text{mcd}(a, m) = 1$, aleshores

$$a^{\phi(m)} \equiv 1 \mod m.$$

Podeu veure una demostració del teorema d'Euler a l'apèndix (p.115) de la secció.

Teorema de Fermat i teorema d'Euler

Exercici 7

Comproveu que el teorema de Fermat és un cas particular del teorema d'Euler.

Els teoremes anteriors són útils per trobar elements inversos.

En efecte, si a és no nul a $\mathbb{Z}_p$, aleshores

$$a^{-1} = a^{p-2} \mod p,$$

i si a és invertible a $\mathbb{Z}_m$, aleshores

$$a^{-1} \equiv a^{\phi(m)-1} \mod m.$$

Teorema de Fermat i teorema d'Euler

Exercici 8

1. És $\mathbb{Z}_{27}$ un cos? Per què?
2. Quants elements de $\mathbb{Z}_{27}$ són invertibles?
3. Justifiqueu per què té invers el 8 a $\mathbb{Z}_{27}$.
4. Trobeu l'invers de 8 a $\mathbb{Z}_{27}$ utilitzant la identitat de Bézout.
5. Trobeu l'invers de 8 a $\mathbb{Z}_{27}$ utilitzant el teorema d'Euler.
6. Comproveu que l'element trobat és, en efecte, l'invers.

Solució (p.96)

Ordre i elements primitius

Ordre

L'**ordre** d'un element no nul $a \in \mathbb{Z}_m$ és el mínim exponent $i \neq 0$ tal que $a^i = 1$. El denotem per $\mathbf{ord_m(a)}$.

Lema 9

L'ordre de l'element a de $\mathbb{Z}_m$ existeix si i només si $\text{mcd}(a, m) = 1$.

Demostració

Si existeix l'ordre de l'element a aleshores existeix l'invers de a, ja que és $a^{\text{ord}_m(a)-1}$. *Pel lema 7 es dedueix que* $\text{mcd}(a, m) = 1$.

□

Ordre i elements primitius

Ordre

L'**ordre** d'un element no nul $a \in \mathbb{Z}_m$ és el mínim exponent $i \neq 0$ tal que $a^i = 1$. El denotem per $\mathbf{ord}_m(a)$.

Lema 9

L'ordre de l'element a de $\mathbb{Z}_m$ existeix si i només si $\text{mcd}(a, m) = 1$.

Demostració

Si $\text{mcd}(a, m) = 1$*, pel teorema d'Euler existeix un exponent positiu tal que a elevat a l'exponent dona* 1*. Per tant, hi haurà un exponent positiu* mínim *tal que a elevat a l'exponent dona* 1*.* □

Ordre i elements primitius

Exercici 9

Comproveu si a $\mathbb{Z}_{18}$ les classes de 3 i 7 tenen ordre, fent servir la definició i fent servir la condició anterior.

Solució (p.98)

Exercici 10

Demostreu que si $a \in \mathbb{Z}_m^*$ i a^{-1} és l'invers de a a $\mathbb{Z}_m$, aleshores $\text{ord}_m(a^{-1}) = \text{ord}_m(a)$. Solució (p.99)

Ordre i elements primitius

Lema 10

Si $a^k = 1$ a $\mathbb{Z}_m$ per un enter positiu k, aleshores l'ordre de a divideix k.

Demostració

Suposem que la divisió euclidiana de k per $\mathrm{ord}_m(a)$ *té quocient q i residu r, aleshores* $a^k = (a^{\mathrm{ord}_m(a)})^q a^r$. *Però com que* $a^k = 1$ *i* $a^{\mathrm{ord}_m(a)} = 1$, *aleshores* $a^r = 1$. *Això, tenint en compte que* $0 \leq r < \mathrm{ord}_m(a)$, *només és possible si* $r = 0$, *és a dir, si* $\mathrm{ord}_m(a) \mid k$. □

Ordre i elements primitius

En conseqüència, tenim el resultat següent:

L'ordre de qualsevol element divideix $\phi(m)$.

Exercici 11

Calculeu l'ordre de tots els elements de $\mathbb{Z}_7$ i comproveu que tots els ordres divideixen $\phi(7)$.

Solució (p.100)

Ordre i elements primitius

Elements primitius

Un element de $\mathbb{Z}_m$ és **primitiu** si el seu ordre és $\phi(m)$.

No ha d'existir necessàriament un element primitiu. Per exemple, a $\mathbb{Z}_8$ no hi ha elements primitius.

Exercici 12

Comproveu que $\mathbb{Z}_8$ no té elements primitius.

Solució (p.101)

Si existeix un element primitiu, β, aleshores les seves potències cobreixen tot $\mathbb{Z}_m^*$.

$$\mathbb{Z}_m^* = \{1 = \beta^0, \beta, \beta^2, \ldots, \beta^{\phi(m)-1}\}.$$

Ordre i elements primitius

Lema 11

Suposem que β és un element primitiu de $\mathbb{Z}_m$. L'element β^j amb $1 \leq j < \phi(m)$ també és primitiu si i només si $\text{mcd}(j, \phi(m)) = 1$.

Demostració

Tindrem que $(\beta^j)^k = \beta^{kj}$ *és igual a* 1 *si i només si* $\text{ord}_m(\beta) \mid kj$, *és a dir, si i només si* $\phi(m) \mid kj$.

Llavors, β^j *serà primitiu si i només si* $\phi(m)$ *no divideix cap dels valors* kj *amb* k *entre* 1 *i* $\phi(m) - 1$.

Si $\text{mcd}(j, \phi(m)) \neq 1$, *aleshores* $\phi(m)$ *divideix* $\frac{\phi(m)}{\text{mcd}(j,\phi(m))} j$ *que, pel que acabem de veure, suposa que* β^j *no és primitiu.*

Si $\text{mcd}(j, \phi(m)) = 1$, *aleshores* $\phi(m)$ *només pot dividir* kj *si* $\phi(m)$ *divideix* k, *cosa que no és possible si* $k \leq \phi(m) - 1$. *Per tant, en aquest cas* β^j *és primitiu.* □

Ordre i elements primitius

Com a conseqüència tenim el següent:

Si hi ha un element primitiu, aleshores n'hi ha exactament $\phi(\phi(m))$.

Exercici 13

(a) Comproveu que $\mathbb{Z}_{18}$ té elements primitius. Solució (p.102)

(b) Quants i quins són els elements primitius de $\mathbb{Z}_{18}$? Solució (p.103)

Podem calcular l'ordre d'un element amb `multiplicative_order`:

```
Z27=Integers(27)
multiplicative_order(Z27(8))
```

Mirant la llista de tots els ordres, veiem que tots divdeixen $\phi(27)$:

```
[multiplicative_order(a) for a in Z27 if gcd(27,a)==1]
```

Construïm nosaltres mateixes una funció booleana per a veure si un element és primitiu:

```
def is_primitive(a,m):
  ep=euler_phi(m)
  return(multiplicative_order((Integers(m))(a))==ep)
```

Comprovem que a $\mathbb{Z}_{23}$ el 2 no és primitiu però el 7 sí que ho és

```
print("is_primitive(2,23)=",is_primitive(2,23))
print("is_primitive(7,23)=",is_primitive(7,23))
```

Exponenciació

Lema 12

- Si $a = mq + r$ amb $0 \leq r < m$ i $\text{mcd}(a, m) = 1$, aleshores $a^N \equiv r^N \mod m$ per tot $N > 0$.
- Si $N = \phi(m)q + r$ amb $0 \leq r < \phi(m)$, aleshores $a^N = a^r \mod m$.

Demostració

- *Podem provar-ho per inducció. Per $N = 0$ es compleix. Suposem que es compleix $a^i \equiv r^i \mod m$ per tot $i < N$. Aleshores $a^N \equiv a \cdot a^{N-1} \equiv a \cdot r^{N-1} \equiv (mq + r)r^{N-1} \equiv r^N \mod m$.*
- $a^N \equiv a^{\phi(m)q}a^r \equiv (a^{\phi(m)})^q a^r \equiv a^r \mod m$.

□

Exercicis

Exercici 14

(a) Calculeu l'invers de 16 a $\mathbb{Z}_{29}$ Solució (p.104)

(b) Calculeu l'invers de 258 a $\mathbb{Z}_{2791}$. Solució (p.105)

Exercicis

Exercici 15

(a) Expresseu tots els elements no nuls de $\mathbb{Z}_{19}$ com a potències de 2. Solució (p.106)

(b) És possible expressar tots els elements no nuls de $\mathbb{Z}_{23}$ com a potències de 2? Solució (p.107)

(c) Busqueu un element β de $\mathbb{Z}_{23}$ tal que tot element no nul de $\mathbb{Z}_{23}$ es pugui escriure com a potència de β. Solució (p.107)

Exercicis

Exercici 16

Sigui l'anell $\mathbb{Z}_{18}$

1. És un cos?
2. Quants elements invertibles té i quins són?
3. Quants divisors de zero té?
4. Busqueu un element primitiu.
5. Quants elements primitius té?

Solució (p.108)

Exercicis

Exercici 17

Sigui l'anell $\mathbb{Z}_{27}$

1. És un cos?
2. Quants elements invertibles té i quins són?
3. Quants divisors de zero té?
4. Busqueu un element primitiu.
5. Busqueu un element diferent de $0, 1$ que no sigui primitiu. Quin ordre té?

Solució (p.109)

Exercicis

Exercici 18

Comproveu que si β és un element primitiu de $\mathbb{Z}_m$ i si k és un enter positiu que divideix $\phi(m)$, aleshores

- $\text{ord}_m(\beta^{\frac{\phi(m)}{k}}) = k$,
- $\text{ord}_m(\beta^k) = \frac{\phi(m)}{k}$.

Solució (p.110)

Exercicis

Exercici 19

Calculeu el residu de dividir

- 4187^{3515} entre 3,
- 4187^{3515} entre 5.

Solució (p.111)

Exercici 20

Trobeu les classes a $\mathbb{Z}_{100}$ de

- 6^{41},
- 7^{41},
- 15^{41}.

Solució (p.112)

Exercicis

Exercici 21

- Quin és el darrer dígit de 7^{378}?
- Quines són les dues darreres xifres de 2793^{2792}?

Solució (p.113)

Solució de l'Exercici 1

$a \equiv b \mod m$ és equivalent al fet que $a - b$ és un múltiple de m.

Si $a - b$ és un múltiple de m, aleshores també ho és de d.

Si $a - b$ és un múltiple de d, aleshores $a \equiv b \mod d$.

Torna a l'exercici (p.12)

Solució de l'Exercici 2

- Podem comprovar que $[0]_2 + [0]_2 = [0]_2$ i que $[1]_2 + [1]_2 = [0]_2$. Per tant, l'oposat de qualsevol $a \in \mathbb{Z}_2$ és a.
- Observem que $1^2 = 1$ i $0^2 = 0$. Aleshores $(a+b)^2 = a^2 + 2ab + b^2 \equiv a^2 + b^2 \equiv a + b \mod 2$.
- Sabem que és cert per $n = 2$. Suposem que és cert fins a $n-1$, aleshores $(a_1 + a_2 + \cdots + a_{n-1} + a_n)^2 = ((a_1 + a_2 + \cdots + a_{n-1}) + a_n)^2 = (a_1 + a_2 + \cdots + a_{n-1})^2 + a_n^2 = a_1^2 + a_2^2 + \cdots + a_{n-1}^2 + a_n^2$.

Torna a l'exercici (p.46)

Solució de l'Exercici 4

- $\mathbb{Z}_2^* = \{1\}$
- $\mathbb{Z}_3^* = \{1, 2\}$
- $\mathbb{Z}_4^* = \{1, 3\}$
- $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$
- $\mathbb{Z}_6^* = \{1, 5\}$
- $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$
- $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$
- $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$
- $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$
- $\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
- $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$

Torna a l'exercici (p.57)

Solució de l'Exercici 5

- $$\begin{aligned}\phi(18) &= \phi(2\cdot 9)\\ &= \phi(2)\phi(9) \text{ (propietat 2)}\end{aligned}$$

$\phi(2) = 1$ (propietat 1)
$\phi(9) = \phi(3^2) = 3^2 - 3^1 = 9 - 3 = 6$ (propietat 3)

$$\begin{aligned}&= 1\cdot 6\\ &= 6\end{aligned}$$

Solució de l'Exercici 5

- $$\begin{aligned}\phi(27) &= \phi(3^3)\\ &= 3^3 - 3^2 \text{ (propietat 3)}\\ &= 27 - 9\\ &= 18\end{aligned}$$

- $$\begin{aligned}\phi(35) &= \phi(5\cdot 7)\\ &= \phi(5)\phi(7) \text{ (propietat 2)}\\ &= 4\cdot 6 \text{ (propietat 1)}\\ &= 24\end{aligned}$$

Torna a l'exercici (p.61)

Solució de l'Exercici 6

En general

$$\begin{aligned}
\phi(n) &= \phi(p_1^{n_1} \cdot p_2^{n_2} \cdot \cdots \cdot p_k^{n_k}) \\
&= \phi(p_1^{n_1}) \cdot \phi(p_2^{n_2}) \cdot \cdots \cdot \phi(p_k^{n_k}) \text{ (propietat 2)} \\
&= (p_1^{n_1-1}(p_1-1)) \cdot (p_2^{n_2-1}(p_2-1)) \cdot \cdots \cdot (p_k^{n_k-1}(p_k-1)) \text{ (propietat 3)}
\end{aligned}$$

Torna a l'exercici (p.61)

Solució de l'Exercici 8

1. No, perquè 27 no és primer.
2. $\phi(27) = 27 - 9 = 18$.
3. Perquè $\text{mcd}(8, 27) = 1$.
4. Utilitzem l'algoritme d'Euclides per trobar els coeficients de la identitat de Bézout:

1	0	1	-2	3
0	1	-3	7	-10
		3	2	1
27	8	3	2	1

Deduïm que $3 \cdot 27 + (-10) \cdot 8 = 1$. Reduint mòdul 27 obtenim $(-10) \cdot 8 = 17 \cdot 8 = 1$ i, per tant, l'invers de 8 mòdul 27 és 17.

Solució de l'Exercici 8

5. Pel teorema d'Euler tenim que $8^{18} = 1 \mod 27$, d'on deduïm que a $\mathbb{Z}_{27}$ l'invers de 8 és 8^{17}. Podem calcular aquesta potència de moltes maneres diferents. En posem una de possible: com que podem reduir els exponents per múltiples de $\phi(27) = 18$, tenim $8^{17} = 2^{3\cdot 17} = 2^{17+17+17} = 2^{17}2^{17}2^{17}$ (perquè $2^{17} = 2^{-1}$, a causa del fet que $2 \cdot 2^{17} = 1$)
$= 2^{17}2^{-1}2^{-1} = 2^{17-1-1} = 2^{15} = 2^5 \cdot 2^5 \cdot 2^5 = 32 \cdot 32 \cdot 32$ (perquè $32 \equiv 5 \mod 27$)
$= 5 \cdot 5 \cdot 5 = 125 = 4 \cdot 27 + 17 = 17.$
6. Es tracta de comprovar que $8 \cdot 17 = 1$ a $\mathbb{Z}_{27}$ i, com en l'apartat anterior, hi ha moltes maneres de fer-ho. En proposem una: $8 \cdot 17 = 136 = 27 \cdot 5 + 1 = 1$.

Torna a l'exercici (p.67)

Solució de l'Exercici 9

Observem,

$$\begin{aligned} 3^1 &= 3 \\ 3^2 &= 9 \\ 3^3 &= 3 \cdot 3^2 = 3 \cdot 9 = 27 = 18 + 9 = 9 \\ 3^4 &= 3 \cdot 3^3 = 3 \cdot 9 = 27 = 18 + 9 = 9 \\ &\vdots \end{aligned}$$

$$\begin{aligned} 7^1 &= 7 \\ 7^2 &= 49 = 18 \cdot 2 + 13 = 13 \\ 7^3 &= 7 \cdot 7^2 = 7 \cdot 13 = 91 = 18 \cdot 5 + 1 = 1 \\ &\vdots \end{aligned}$$

Per tant, no hi ha cap exponent $i > 0$ tal que $3^i = 1$.
Però sí que $7^i = 1$ per $i = 3$.
Per la definició, 7 té ordre però 3 no en té.

Podem comprovar-ho ara amb la condició del mcd. En efecte, $\text{mcd}(3, 18) = 3 \neq 1$, mentre que $\text{mcd}(7, 18) = 1$.

Torna a l'exercici (p.71)

Solució de l'Exercici 10

D'una banda, $(a^{-1})^{\mathrm{ord}_m(a)} = 1$ perquè
$(a^{-1})^{\mathrm{ord}_m(a)} = (a^{-1})^{\mathrm{ord}_m(a)} a^{\mathrm{ord}_m(a)} = (a^{-1}a)^{\mathrm{ord}_m(a)} = 1^{\mathrm{ord}_m(a)} = 1.$
D'altra banda, si $(a^{-1})^k = 1$, aleshores $a^k = a^k(a^{-1})^k = (aa^{-1})^k = 1$
i, per tant, $k \geq \mathrm{ord}_m(a)$.

Torna a l'exercici (p.71)

Solució de l'Exercici 11

Calculem els ordres de tots els elements de $\mathbb{Z}_7$.

$1^1 = 1$

$\mathrm{ord}_7(1) = 1$

$2^1 = 2$
$2^2 = 4$
$2^3 = 1$

$\mathrm{ord}_7(2) = 3$

$3^1 = 3$
$3^2 = 2$
$3^3 = 6$
$3^4 = 4$
$3^5 = 5$
$3^6 = 1$

$\mathrm{ord}_7(3) = 6$

$4^1 = 4$
$4^2 = 2$
$4^3 = 1$

$\mathrm{ord}_7(4) = 3$

$5^1 = 5$
$5^2 = 4$
$5^3 = 6$
$5^4 = 2$
$5^5 = 3$
$5^6 = 1$

$\mathrm{ord}_7(5) = 6$

$6^1 = 6$
$6^2 = 1$

$\mathrm{ord}_7(6) = 2$

Ara podem observar que tots els ordres són divisors de $\phi(7) = 6$.

Torna a l'exercici (p.73)

Solució de l'Exercici 12

Perquè a sigui un element primitiu de $\mathbb{Z}_8$ ha de tenir ordre. Per tenir ordre ha de ser coprimer amb 8 i, per tant, ha de ser senar. Analitzem les potències de tots els senars:

$1^1 = 1$	$3^1 = 3$	$5^1 = 5$	$7^1 = 7$
	$3^2 = 9 = 1$	$5^2 = 25 = 1$	$7^2 = 49 = 1$
$\mathrm{ord}_8(1) = 1$	$\mathrm{ord}_8(3) = 2$	$\mathrm{ord}_8(5) = 2$	$\mathrm{ord}_8(7) = 2$

A més, per ser primitiu, el seu ordre ha de ser $\phi(8) = 8 - 4 = 4$.

Observem que no n'hi ha cap que tingui ordre 4. Per tant, $\mathbb{Z}_8$ no té elements primitius.

Torna a l'exercici (p.74)

Solució de l'Exercici 13(a)

1. Perquè a sigui un element primitiu de $\mathbb{Z}_{18}$ ha de tenir ordre. Per tenir ordre ha de ser coprimer amb 18 i, per tant, ha de ser senar i no múltiple de 3.
   D'altra banda, els ordres possibles a $\mathbb{Z}_{18}$ seran tots els divisors de $\phi(18) = \phi(9)\phi(2) = 9 - 3 = 6$, és a dir, $1, 2, 3$ o 6.
   Si trobem un element que no tingui ordre $1, 2$, ni 3, aleshores per força tindrà ordre 6 i per força serà primitiu.
   Provem amb $a = 5$. Observem les seves primeres potències:
   $$\begin{aligned} 5^1 &= 5 \\ 5^2 &= 25 = 7 \\ 5^3 &= -1 \end{aligned}$$
   Veiem que l'ordre de 5 no és 1, ni 2, ni 3, aleshores per força es tracta d'un element primitiu.

Solució de l'Exercici 13(b)

2. Ara podem afirmar que, com que existeix un element primitiu, el nombre d'elements primitius serà $\phi(\phi(18)) = \phi(6) = 2$.
   L'altre element primitiu serà 5^j per alguna j entre 2 i 5 amb $\text{mcd}(j, \phi(18)) = 1$ i això només és possible per $j = 5$.
   Així doncs, l'altre element primitiu serà $5^5 = 5^2 \cdot 5^3 = -7 = 11$.

Torna a l'exercici (p.76)

Solució de l'Exercici 14(a)

Fem la taula d'Euclides per a 29 i 16.

1	0	1	-1	5	
0	1	-1	2	-9	
		1	1	4	3
29	16	13	3	1	0

Deduïm que

$$5 \cdot 29 + (-9) \cdot 16 = 1$$

i, per tant, $(-9) \cdot 16 \equiv 20 \cdot 16 \equiv 1(29)$.

En conseqüència, l'invers de 16 a $\mathbb{Z}_{29}$ és 20.

Torna a l'exercici (p.82)

Solució de l'Exercici 14(b)

Fem la taula d'Euclides per a 2791 i 258.

1	0	1	-1	5	-11	
0	1	-10	11	-54	119	
		10	1	4	2	23
2791	2587	211	47	23	1	0

Deduïm que

$$(-11)\cdot 2791 + 119\cdot 258 = 1$$

i, per tant, $119\cdot 258 \equiv 1(2791)$.

En conseqüència, l'invers de 258 a $\mathbb{Z}_{2791}$ és 119.

Torna a l'exercici (p.82)

Solució de l'Exercici 15(a)

(a)

2^0	=	1	1	=	2^0
2^1	=	2	2	=	2^1
2^2	=	4	3	=	2^{13}
2^3	=	8	4	=	2^2
2^4	=	16	5	=	2^{16}
2^5	=	13	6	=	2^{14}
2^6	=	7	7	=	2^6
2^7	=	14	8	=	2^3
2^8	=	9	9	=	2^8
2^9	=	18	10	=	2^{17}
2^{10}	=	17	11	=	2^{12}
2^{11}	=	15	12	=	2^{15}
2^{12}	=	11	13	=	2^5
2^{13}	=	3	14	=	2^7
2^{14}	=	6	15	=	2^{11}
2^{15}	=	12	16	=	2^4
2^{16}	=	5	17	=	2^{10}
2^{17}	=	10	18	=	2^9

Solució de l'Exercici 15(b,c)

(b) No és possible. En efecte, a $\mathbb{Z}_{23}$,

$$
\begin{aligned}
2^0 &= 1\\
2^1 &= 2\\
2^2 &= 4\\
2^3 &= 8\\
2^4 &= 16\\
2^5 &= 9\\
2^6 &= 18\\
2^7 &= 13\\
2^8 &= 3\\
2^9 &= 6\\
2^{10} &= 12\\
2^{11} &= 1\\
2^{12} &= 2\\
&\vdots
\end{aligned}
$$

(c) Per exemple, 7. Podeu comprovar-ho vosaltres mateixos.

Torna a l'exercici (p.83)

Solució de l'Exercici 16

1. No és un cos.
2. 6 invertibles, que són $1, 5, 7, 11, 13$ i 17.
3. 11.
4. Per exemple, el 5.
5. 2.

Torna a l'exercici (p.84)

Solució de l'Exercici 17

1. No és un cos.
2. $\phi(27) = 3^3 - 3^2 = 18$ invertibles, que són $\{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26\}$.
3. 8.
4. Per exemple, el 2.
5. 4, que té ordre 9.

Torna a l'exercici (p.85)

Solució de l'Exercici 18

Els dos resultats són equivalents. Demostrarem el primer, i el segon és anàleg.

Diguem $\gamma = \beta^{\frac{\phi(m)}{k}}$. Per demostrar que l'ordre de γ és k cal fer dues comprovacions:

- Cal veure que $\gamma^k = 1$,
- Cal veure que $\gamma^r \neq 1$ per tot exponent r amb $0 < r < k$.

Vegem el primer punt: $\gamma^k = (\beta^{\frac{\phi(m)}{k}})^k = \beta^{\phi(m)} = 1$.

Per al segon punt, suposem que r és un enter amb $0 < r < k$. Ara, $\gamma^r = (\beta^{\frac{\phi(m)}{k}})^r = \beta^{\frac{r\phi(m)}{k}}$. Com que $\frac{r\phi(m)}{k}$ és un enter (perquè k divideix $\phi(m)$) i és més petit que $\phi(m)$ (perquè $\frac{r}{k} < 1$), aleshores (com que β és primitiu) $\beta^{\frac{r\phi(m)}{k}} \neq 1$. Per tant, $\gamma^r \neq 1$.

Torna a l'exercici (p.86)

Solució de l'Exercici 19

- $4187 \equiv 2(3)$, per tant, $4187^{3515} \equiv 2^{3515}(3)$.
  Ara, com que $2^2 = 1$, deduïm que $2^{3515} \equiv 2(3)$.
- $4187 \equiv 2(5)$, per tant, $4187^{3515} \equiv 2^{3515}(5)$.
  Ara, com que $\mathrm{mcd}(2,5) = 1$ i, per tant, $2^{\phi(5)} = 2^4 = 1$, deduïm que $2^{3515} \equiv 2^3(5)$.
  Per tant, $4187^{3515} \equiv 3(5)$.

Torna a l'exercici (p.87)

Solució de l'Exercici 20

Calculem primer $\phi(100) = \phi(25)\phi(4) = 20 \cdot 2 = 40$.

Utilitzarem el teorema d'Euler. És a dir, que si $\text{mcd}(a, m) = 1$, aleshores $a^{\phi(m)} \equiv 1(m)$.

- Es pot resoldre de moltes maneres. Per exemple, $6^{41} = 2^{41}3^{41} = 2^{41}3 = (2^{10})^4 \cdot 2 \cdot 3 = (24)^4 \cdot 2 \cdot 3 = (76)^2 \cdot 2 \cdot 3 = (-24)^2 \cdot 2 \cdot 3 = 76 \cdot 2 \cdot 3 = 76 \cdot 6 = 456 = 56(100)$.
- $7^{41} = 7$.
- $15^{41} = 3 \cdot 5^{41}$.
  Aquí observem que $5^a \equiv 25(100)$ per tota $a > 1$. Deduïm que $15^{41} = 3 \cdot 25 = 75$.

Torna a l'exercici (p.87)

Solució de l'Exercici 21

Observem que ens estan demanant una quantitat mòdul 10 i una altra quantitat mòdul 100.

D'altra banda, observem primer que $\phi(10) = 4$, mentre que $\phi(100) = 40$, com hem vist abans.

- $7^{378}(10) \equiv 7^2(10) \equiv 9(10)$.
- $2793^{2792}(100) \equiv 93^{392}(100) \equiv 93^{32}(100) \equiv (-7)^{32}(100) \equiv 7^{32}(100)$.
  Arribats a aquest punt podem observar que
  $7^4 = 2401 \equiv 1(100)$.
  Deduïm que $7^{32} \equiv 1(100)$.
  Per tant, $2793^{2792} \equiv 1(100)$.

Torna a l'exercici (p.88)

Apèndix 1: Demostració del teorema d'Euler (p.65)

Demostració

Suposem que $\mathbb{Z}_m^* = \{u_1, \ldots, u_{\phi(m)}\}$.
Anomenem $U = u_1 \cdot u_2 \cdot \cdots \cdot u_{\phi(m)}$.
Observem que $U \in \mathbb{Z}_m^*$ *i que el seu invers és*

$$U^{-1} = u_{\phi(m)}^{-1} \cdot u_{\phi(m)-1}^{-1} \cdot \cdots \cdot u_1^{-1}.$$

Ara considerem $a \in \mathbb{Z}_m^*$.
Observem que els elements $au_1, \ldots, au_{\phi(m)}$ *pertanyen tots a* $\mathbb{Z}_m^*$, *per tenir inversos, respectivament,* $u_1^{-1}a^{-1}, \ldots, u_{\phi(m)}^{-1}a^{-1}$.
D'altra banda tots ells són diferents, ja que si $au_i = au_j$, *aleshores multiplicant per* a^{-1} *a les dues bandes de la igualtat veiem que* u_i *hauria de ser igual a* u_j. *Per això,* $\mathbb{Z}_m^* = \{au_1, \ldots, au_{\phi(m)}\}$.

Així doncs, U també el podrem escriure com

$au_1 \cdot au_2 \cdot \cdots \cdot au_{\phi(m)} = a^{\phi(m)}U$, *obtenint que* $U = a^{\phi(m)}U$. *Ara, multiplicant per* U^{-1} *a les dues bandes de la igualtat obtenim que* $a^{\phi(m)} = 1$ *a* $\mathbb{Z}_m$. □

Apèndix 2: Operacions i estructures algebraiques

Una **operació binària** en un conjunt A és una correspondència del producte cartesià $A \times A = \{(a, b) : a \in A \text{ i } b \in A\}$ en A.

Per exemple, la suma en els naturals la podem entendre com l'aplicació

$$\begin{array}{rccc} + : & (\mathbb{N}, \mathbb{N}) & \to & \mathbb{N} \\ & (a, b) & \mapsto & a + b \end{array}$$

Una operació binària $*$ en un conjunt A pot tenir les següents propietats:

- **Propietat associativa** si $a * (b * c) = (a * b) * c$ per tot $a, b, c \in A$.
- **Existència d'element neutre** si existeix un element de A, que anomenem e_n, tal que $a * e_n = e_n * a = a$ per tot $a \in A$.
- **Existència d'element invers** si per tot element $a \in A$ existeix un element de A, que anomenem e_a, tal que $a * e_a = e_a * e = e_n$.
- **Propietat commutativa** si $a * b = b * a$ per tot $a, b \in A$.

Torna a les propietats aritmètiques de $\mathbb{Z}_m$ (p.42)

Apèndix 2: Operacions i estructures algebraiques

Un **grup** és un conjunt A amb una operació associativa amb element neutre i invers. El grup és un **grup commutatiu** si l'operació és commutativa.

Exemples:

- Els enters $\mathbb{Z}$ amb la suma habitual són un grup (commutatiu).
- Els naturals $\mathbb{N}$ amb la suma no són un grup perquè no tots els elements tenen element invers.
- Els enters amb el producte habitual tampoc són grup perquè no sempre existeix l'element invers.

Apèndix 2: Operacions i estructures algebraiques

- Considerem el conjunt $\{a, e, i\}$ amb l'operació $*$ donada per la taula

$*$	a	e	i
a	e	i	a
e	i	a	e
i	a	e	i

Observem que l'operació és commutativa per ser la taula simètrica i que té com a element neutre l'element i. L'invers de a per $*$ és e i l'invers de e per $*$ és a. L'invers de i és ell mateix. També es pot comprovar que l'operació és associativa. Per tant el conjunt $\{a, e, i\}$ amb l'operació $*$ és un grup commutatiu.

Apèndix 2: Operacions i estructures algebraiques

- Considerem el conjunt $\{a, e, i, o\}$ amb l'operació $+$ donada per la taula

$+$	a	e	i	o
a	o	i	e	a
e	i	o	a	e
i	e	a	o	i
o	a	e	i	o

Observem que l'operació és commutativa per ser la taula simètrica i que té com a element neutre l'element o. Tots els elements es tenen a ells mateixos com al seu propi invers. També es pot comprovar que l'operació és associativa. Per tant, el conjunt $\{a, e, i, o\}$ amb l'operació $+$ és un grup commutatiu.

Apèndix 2: Operacions i estructures algebraiques

Una segona operació $**$ en el conjunt A pot tenir la següent propietat respecte de la primera operació $*$.

- **Propietat distributiva** si $a**(b*c) = (a**b)*(a**c)$ per tot $a, b, c \in A$.

Un **anell** és un conjunt A amb dues operacions $\oplus$ i $\otimes$ tal que $\oplus$ li confereix estructura de grup commutatiu i tal que $\otimes$ és associativa i satisfà la proietat distributiva respecte de $\oplus$. Podeu comprovar, com a exercici, que l'element neutre de $\oplus$ multiplicat per qualsevol element de l'anell dona altra vegada el neutre respecte de $\oplus$.

Torna a l'anell $\mathbb{Z}_m$ (p.43).

L'anell és **unitari** i **commutatiu** si $\otimes$ té element neutre i satisfà la propietat commutativa, respectivament.

Apèndix 2: Operacions i estructures algebraiques

Un **cos** és un anell unitari i commutatiu on $\otimes$ satisfà que tot element diferent del neutre de $\oplus$ té invers. En aquest cas l'invers d'un element respecte de $\oplus$ s'anomena el seu **element oposat**, i es deixa el nom d'**element invers** per a l'invers respecte de $\otimes$.

Torna al cos $\mathbb{Z}_p$ (p.57)

Exemples:

- Els enters $\mathbb{Z}$, amb la suma i el producte habituals, són un anell. Però no són un cos perquè no tots els elements tenen element invers.
- Els racionals $\mathbb{Q}$ i els reals $\mathbb{R}$ sí que són cossos.

Apèndix 2: Operacions i estructures algebraiques

- El conjunt $\{a, e, i, o\}$ dels exemples anteriors és un cos respecte de l'operació $\oplus = +$ descrita a la segona taula, amb neutre o, i respecte de l'operació $\otimes = *$ descrita a la primera ampliant-la amb el neutre de $+$, que multiplicat per qualsevol element dona o. És a dir

$*$	a	e	i	o
a	e	i	a	o
e	i	a	e	o
i	a	e	i	o
o	o	o	o	o

Només queda comprovar que l'operació $*$ és distributiva respecte de $+$, que ho deixem com a exercici.

Notes històriques

Leonhard Euler (1707-1783) ha estat un dels matemàtics més importants i prolífics. L'estudi de les propietats de la funció d'Euler ha permès descobrir moltes propietats dels nombres enters.

Torna a la funció d'Euler (p.59)

Teorema 62: Aquest teorema sovint és anomenat teorema "petit" de Fermat. Pierre de Fermat (1601-1665) va contribuir molt a l'aritmètica i és especialment famós per un teorema que va enunciar (sense demostració) que deia que $x^n + y^n = z^n$ no té solució entera per $n > 2$. Aquest teorema (el "gran") no va ser demostrat fins el 1995 per Andrew Wiles. Torna al teorema (p.65)