Introducció a l'aritmètica

Maria Bras-Amorós, Oriol Farràs Ventura

29 de setembre de 2023

Divisió d'enters

Teorema 1: Divisió d'enters

Donats dos enters qualssevol a i b, existeixen dos altres enters únics q i r tals que $a = bq + r$ amb $0 \leq r < |b|$.

Exemple

$a = 5$, $b = 2 \rightarrow q = 2$, $r = 1$

$a = -7$, $b = 3 \rightarrow q = -3$, $r = 2$

Dividend, divisor, quocient, residu

L'enter a i b són, respectivament, el **dividend** i el **divisor** de la divisió. L'enter q és el **quocient**. L'enter r és el **residu**.

Divisió d'enters

Exercici 1: Curiositat

Trobeu el quocient i el residu per a les següents parelles de valors de dividends i divisors.

- 9 i 1
- 98 i 12
- 987 i 123
- 9876 i 1234
- 98765 i 12345
- 987654 i 123456
- 9876543 i 1234567
- 98765432 i 12345678
- 987654321 i 123456789

Divisors

Múltiples i divisors

Si en la divisió entera de a entre b el residu és 0, aleshores diem que

- a és un **múltiple** de b,
- b és un **divisor** d'a,
- b **divideix** a.

Escrivim $\boldsymbol{b \mid a}$ i denotem el quocient per $\frac{\boldsymbol{a}}{\boldsymbol{b}}$.

Si b és un divisor de a, com que tindrem $a = b \cdot q$, aleshores $q := \frac{a}{b}$ també és un divisor de a.

Divisors

Exercici 2

Comproveu que 12345679 és un divisor de 111111111. Deduïu que 12345679 és un divisor de 222222222, 333333333, 444444444, etc.

El cas del 0 i de l'1

El 0 és múltiple de qualsevol enter i l'1 és un divisor de qualsevol enter.

Divisors de 12

Mirem els residus de dividir 12 entre els enters positius més petits o iguals que ell.

enter	q	r
1	12	0
2	6	0
3	4	0
4	3	0
5	2	2
6	2	0
7	1	5
8	1	4
9	1	3
10	1	2
11	1	1
12	1	0

Observem que el residu és zero només per als enters $1, 2, 3, 4, 6, 12$. Aquest és el conjunt dels divisors positius de 12.

Divisors de 16

Repetim l'experiment amb l'enter 16.

enter	q	r
⋮	⋮	⋮
10	1	6
11	1	5
12	1	4
13	1	3
14	1	2
15	1	1
16	1	0

El conjunt de divisors positius de 16 és, doncs, $\{1, 2, 4, 8, 16\}$.

Propietats I

Exercici 3

Comproveu que si $a \mid b$ i $b \mid c$, aleshores $a \mid c$. Solució (p.64)

Exercici 4

Comproveu que si $a \mid b$ i existeix d tal que $d \mid a$ i $d \mid b$, aleshores $\frac{a}{d} \mid \frac{b}{d}$. Solució (p.65)

Propietats II

Exercici 5

Demostreu que si $a \mid b$ i $a \mid c$, aleshores

- $a \mid -b$
- $a \mid b + c$
- $a \mid b - c$

Solució (p.66)

Exercici 6

Demostreu que si $a = bq + r$ amb $0 \leq r < |b|$ i d és un divisor comú de a i b, aleshores també és un divisor de r.

Solució (p.67)

(Més endavant veurem l'aplicació d'aquest resultat al càlcul del mcd.)

Propietats III

Exercici 7

Demostreu que si $d > 1$, aleshores d no és divisor de $qd + 1$ per cap enter q. Solució (p.68)

Aparellem divisors

El conjunt de divisors positius d'un enter positiu els podem agrupar per parelles de manera que el producte de cada parella ens dona l'enter.

$$\begin{aligned} 1 \cdot 12 &= 12 \\ 2 \cdot 6 &= 12 \\ 3 \cdot 4 &= 12 \end{aligned}$$

Aparellem divisors

Si el nombre de divisors positius és senar, aleshores l'enter intermedi es multiplica per ell mateix. Per tant, en aquest cas l'enter és un quadrat.

$$\begin{aligned} 1 \cdot 16 &= 16 \\ 2 \cdot 8 &= 16 \\ 4 \cdot 4 &= 16 \end{aligned}$$

Criteris de divisibilitat

A l'escola tots hem après aquests criteris:

Criteri de divisibilitat del 2

Un nombre és divisible per 2 si acaba en $0, 2, 4, 6$ o 8.

Criteri de divisibilitat del 3

Un nombre és divisible per 3 si la suma de les seves xifres és divisible entre 3.

Criteris de divisibilitat

Criteri de divisibilitat del 4

Un nombre és divisible per 4 si les seves dues últimes xifres són un múltiple de 4.

Criteri de divisibilitat del 5

Un nombre és divisible per 5 si acaba en 0 o 5.

Criteris de divisibilitat

Criteri de divisibilitat del 6

Un nombre és divisible per 6 si ho és per 2 i per 3.

Criteri de divisibilitat del 7

??? No se'n coneix cap.

⋮

Criteri de divisibilitat del 10

Un nombre és divisible per 10 si acaba en 0.

Criteris de divisibilitat

Exercici 8

Intenteu demostrar per inducció els criteris de divisibilitat del 2, el 5 i el 10. Intenteu demostrar el criteri del 4.

Observem que tots aquests criteris són específics per a valors molt concrets i molt petits. En general no hi ha criteris de divisibilitat per a nombres grans.

Màxim comú divisor

Màxim comú divisor

El **màxim comú divisor** de dos enters és el màxim dels divisors que tenen en comú.

Coprimers

Diem que dos enters són primers entre ells o **coprimers** si el seu màxim comú divisor és 1.

Propietats del mcd

Observem que per a tot enter a es compleix que $\mcd(0,a) = a$, $\mcd(1,a) = 1$, exactament al revés que les taules de multiplicar del 0 i l'1.

Exercici 9

Demostreu que si $a = bq + r$ amb $0 \leq r < |b|$, aleshores $\mcd(a,b) = \mcd(b,r)$.

Solució (p.69)

Mínim comú múltiple

Mínim comú múltiple

El **mínim comú múltiple** de dos enters és el mínim dels múltiples no nuls que tenen en comú. Denotem el mínim comú múltiple de a, b per $\mathrm{mcm}(a, b)$.

Exercici 10

1. Demostreu que si M és múltiple de a i múltiple de b, aleshores M també és múltiple de $\mathrm{mcm}(a, b)$.
2. Demostreu que, per a qualsevol parella d'enters a, b,

$$\mathrm{mcm}(a, b) \cdot \mathrm{mcd}(a, b) = ab.$$

Mètode de càlcul del mcd seguint la definició

Una primera manera de trobar el màxim comú divisor, aplicant la definició, és buscant la llista de divisors positius dels dos enters, trobant la seva intersecció i seleccionant el més gran de tots els divisors de la intersecció.

Per exemple, per trobar $\mathrm{mcd}(12,16)$ calculem les llistes de divisors positius de 12 i 16:

- Divisors positius de 12: $\{1,2,3,4,6,12\}$
- Divisors positius de 16: $\{1,2,4,8,16\}$
- Intersecció dels dos conjunts: $\{1,2,4\}$
- Màxim de la intersecció: 4
- Per tant, $\mathrm{mcd}(12,16) = 4$.

Aquest mètode ens obliga a calcular la llista de tots els divisors dels dos nombres, la qual cosa pot ser molt costosa, especialment per a nombres grans.

Mètode de càlcul del mcd que havíem après a l'escola

Recordem el mètode que fèiem servir a l'escola. Es basa en l'existència i la unicitat de la descomposició de tot enter en producte de primers, que veurem en la secció següent.

Suposem que volem calcular $\mathrm{mcd}(5600, 1764)$.

Descomponem els enters en producte de primers.

5600	2
2800	2
1400	2
700	2
350	2
175	5
35	5
7	7
1	

$5600 = 2^5 \cdot 5^2 \cdot 7$

1764	2
882	2
441	3
147	3
49	7
7	7
1	

$1764 = 2^2 \cdot 3^2 \cdot 7^2$

Deduïm que $\mathrm{mcd}(5600, 1764) = 2^2 \cdot 7 = 28$.

Buf! I això que hem fet servir regles de divisibilitat, que només coneixem per alguns enters petits.

Alternativa d'Euclides

Utilitzarem el resultat de l'Exercici 9.

Dividim 5600 entre 1764. Ens queda quocient $q = 3$, residu $r = 5600 - 5292 = 308$. Tenim

$$\mathrm{mcd}(5600, 1764) = \mathrm{mcd}(1764, 308).$$

Alternativa d'Euclides

Utilitzarem el resultat de l'Exercici 9.

Dividim 5600 entre 1764. Ens queda quocient $q = 3$, residu $r = 5600 - 5292 = 308$. Tenim

$$\mathrm{mcd}(5600, 1764) = \mathrm{mcd}(1764, 308).$$

Més fàcil, no? Doncs ho repetim.

Alternativa d'Euclides

Utilitzarem el resultat de l'Exercici 9.

Dividim 5600 entre 1764. Ens queda quocient $q = 3$, residu $r = 5600 - 5292 = 308$. Tenim

$$\mathrm{mcd}(5600, 1764) = \mathrm{mcd}(1764, 308).$$

Més fàcil, no? Doncs ho repetim.

Dividim 1764 entre 308. Ens queda quocient $q = 5$ i residu $r = 1764 - 1540 = 224$. Per tant,

$$\mathrm{mcd}(5600, 1764) = \mathrm{mcd}(1764, 308) = \mathrm{mcd}(308, 224).$$

Alternativa d'Euclides

Dividim 308 entre 224. Ens queda quocient $q = 1$, residu $r = 84$.
Per tant,

$$\mathrm{mcd}(5600, 1764) = \mathrm{mcd}(308, 224) = \mathrm{mcd}(224, 84).$$

Alternativa d'Euclides

Dividim 308 entre 224. Ens queda quocient $q = 1$, residu $r = 84$. Per tant,

$$\mathrm{mcd}(5600, 1764) = \mathrm{mcd}(308, 224) = \mathrm{mcd}(224, 84).$$

Dividim 224 entre 84. Ens queda quocient $q = 2$, residu $r = 224 - 168 = 56$. Per tant,

$$\mathrm{mcd}(5600, 1764) = \mathrm{mcd}(224, 84) = \mathrm{mcd}(84, 56).$$

Alternativa d'Euclides

Dividim 308 entre 224. Ens queda quocient $q = 1$, residu $r = 84$. Per tant,

$$\mathrm{mcd}(5600, 1764) = \mathrm{mcd}(308, 224) = \mathrm{mcd}(224, 84).$$

Dividim 224 entre 84. Ens queda quocient $q = 2$, residu $r = 224 - 168 = 56$. Per tant,

$$\mathrm{mcd}(5600, 1764) = \mathrm{mcd}(224, 84) = \mathrm{mcd}(84, 56).$$

Dividim 84 entre 56. Ens queda quocient $q = 1$, residu $r = 84 - 56 = 28$. Per tant,

$$\mathrm{mcd}(5600, 1764) = \mathrm{mcd}(84, 56) = \mathrm{mcd}(56, 28).$$

Alternativa d'Euclides

Dividim 308 entre 224. Ens queda quocient $q = 1$, residu $r = 84$. Per tant,

$$\mathrm{mcd}(5600, 1764) = \mathrm{mcd}(308, 224) = \mathrm{mcd}(224, 84).$$

Dividim 224 entre 84. Ens queda quocient $q = 2$, residu $r = 224 - 168 = 56$. Per tant,

$$\mathrm{mcd}(5600, 1764) = \mathrm{mcd}(224, 84) = \mathrm{mcd}(84, 56).$$

Dividim 84 entre 56. Ens queda quocient $q = 1$, residu $r = 84 - 56 = 28$. Per tant,

$$\mathrm{mcd}(5600, 1764) = \mathrm{mcd}(84, 56) = \mathrm{mcd}(56, 28).$$

Dividim 56 entre 28. Ens queda quocient $q = 2$, residu $r = 0$. Per tant,

$$\mathrm{mcd}(5600, 1764) = \mathrm{mcd}(56, 28) = \mathrm{mcd}(28, 0) = 28.$$

Alternativa d'Euclides

De tot aquest procediment hem deduït que

$$\mathrm{mcd}(5600, 1764) = 28.$$

Ho podem resumir en aquesta taula:

quocients			3	5	1	2	1	2
residus	5600	1764	308	224	84	56	28	0

El màxim comú divisor és el darrer residu abans del 0.

Algoritme d'Euclides

Suposem que volem calcular $\mathrm{mcd}(a, b)$:

Algoritme

Input: a, b
Anomenem $r_{-2} = a$, $r_{-1} = b$.
Sigui $i = -1$.
Mentres $r_i \neq 0$,

- incrementem i en un,
- definim q_i, r_i com el quocient i el residu de la divisió de r_{i-2} entre r_{i-1}.

Output: r_{i-1}.

Nota (p.82)

El quocient i el residu de la divisió de 5600 entre 1764 són, respectivament,

```
5600 // 1764
5600 % 1764
```

Podem buscar el gcd de 5600 i 1764 per divisions successives

```
rr=5600
r=1764
while r>0:
  rrr=rr
  rr=r
  r=rrr%rr
  print (r)
print("El gcd es",rr)
```

Identitat de Bézout

Utilitzant la notació de l'algoritme d'Euclides podem posar la taula d'aquesta forma:

i	-2	-1	0	1	2	3	4	5
q_i			3	5	1	2	1	2
r_i	5600	1764	308	224	84	56	28	0

A cada pas tenim

$$r_i = r_{i-2} - q_i r_{i-1}.$$

Identitat de Bézout

Si ara definim $\lambda_{-2} = 1$, $\mu_{-2} = 0$, es compleix

$$r_{-2} = \lambda_{-2} \cdot 5600 + \mu_{-2} \cdot 1764$$

Identitat de Bézout

Si ara definim $\lambda_{-2} = 1$, $\mu_{-2} = 0$, es compleix

$$r_{-2} = \lambda_{-2} \cdot 5600 + \mu_{-2} \cdot 1764$$

i si definim $\lambda_{-1} = 0$, $\mu_{-1} = 1$, es compleix

$$r_{-1} = \lambda_{-1} \cdot 5600 + \mu_{-1} \cdot 1764.$$

Identitat de Bézout

Si ara definim $\lambda_{-2} = 1$, $\mu_{-2} = 0$, es compleix

$$r_{-2} = \lambda_{-2} \cdot 5600 + \mu_{-2} \cdot 1764$$

i si definim $\lambda_{-1} = 0$, $\mu_{-1} = 1$, es compleix

$$r_{-1} = \lambda_{-1} \cdot 5600 + \mu_{-1} \cdot 1764.$$

Suposem que fins al pas $k = i - 1$ es compleix que

$$r_k = \lambda_k \cdot 5600 + \mu_k \cdot 1764.$$

Identitat de Bézout

Podem continuar definint recursivament a cada pas

$$\lambda_i = \lambda_{i-2} - q_i \lambda_{i-1},$$

$$\mu_i = \mu_{i-2} - q_i \mu_{i-1}.$$

Això ens permet escriure

$$\begin{aligned} r_i &= r_{i-2} - q_i r_{i-1} \\ &= (\lambda_{i-2} \cdot 5600 + \mu_{i-2} \cdot 1764) - q_i(\lambda_{i-1} \cdot 5600 + \mu_{i-1} \cdot 1764) \\ &= (\lambda_{i-2} - q_i \lambda_{i-1}) \cdot 5600 + (\mu_{i-2} - q_i \mu_{i-1}) \cdot 1764 \\ &= \lambda_i \cdot 5600 + \mu_i \cdot 1764 \end{aligned}$$

Aquest procediment ens permet obtenir l'anomenada **identitat de Bézout**.

Identitat de Bézout

Teorema 2: Identitat de Bézout

Donats dos enters a i b, definim $r_{-2} = a, r_{-1} = b$ i, per $i \geq 0$, definim recursivament r_i i q_i com el residu i el quocient de dividir r_{i-2} entre r_{i-1}. A més a més, definim $\lambda_{-2} = 1$, $\mu_{-2} = 0$, $\lambda_{-1} = 0$, $\mu_{-1} = 1$ i, per $i \geq 0$ definim

$$\lambda_i = \lambda_{i-2} - q_i\lambda_{i-1} \qquad \mu_i = \mu_{i-2} - q_i\mu_{i-1}$$

Aleshores,

- Existeix $k \geq 0$ tal que $r_{k+1} = 0$.
- Es compleix $\mathrm{mcd}(a, b) = r_k$.
- Per tot $i \geq 0$ es compleix $\lambda_i a + \mu_i a = r_i$.

En particular, si definim $\lambda = \lambda_k$ i $\mu = \mu_k$, aleshores es compleix l'anomenada **Identitat de Bézout**,

$$\lambda a + \mu b = \mathrm{mcd}(a, b).$$

Identitat de Bézout

Els coeficients λ i μ de la identitat de Bézout es poden trobar per la manera que acabem de descriure.

Vegem-ho en la següent taula on, per cada i a partir de $i = 0$, calculem $\lambda_i = \lambda_{i-2} - q_i\lambda_{i-1}$ i $\mu_i = \mu_{i-2} - q_i\mu_{i-1}$.

i	-2	-1	0	1	2	3	4	5
λ_i	1	0	1	-5	6	-17	23	
μ_i	0	1	-3	16	-19	54	-73	
q_i			3	5	1	2	1	2
r_i	5600	1764	308	224	84	56	28	0

Comprovem que
$23 \cdot 5600 - 73 \cdot 1764 = 128800 - 128772 = 28 = \mathrm{mcd}(5600, 1764)$.

Identitat de Bézout

Exercici 11

Calculeu el màxim comú divisor de les següents parelles d'enters i expresseu-lo com a combinació lineal dels dos enters.

- 365 i 70 Solució (p.70)
- 2671 i 156 Solució (p.76)

Els coeficients de la identitat de Bézout els podríem trobar anàlogament.

```
rr=5600
r=1764
ll=1
mm=0
l=0
m=1
```

```
while r>0:
  rrr=rr
  lll=ll
  mmm=mm
  rr=r
  ll=l
  mm=m
  r=rrr%rr
  q=rrr//rr
  l=lll-q*ll
  m=mmm-q*mm
  print (l,m,r)
```

Per tant, la identitat de Bézout es

```
print (rr,"=",ll,"*5600","+",mm,"*1764")
```

Sage té una funció per aquest càlcul:

```
xgcd(5600,1764)
```

Identitat de Bézout

Exercici 12

Sabem que donats dos enters a, b *coprimers*, n'existeixen dos més, λ i μ tals que $\lambda a + \mu b = 1$. Demostreu el recíproc, és a dir, si donats dos enters a i b, n'existeixen dos més, λ i μ tals que $\lambda a + \mu b = 1$, aleshores a i b són coprimers.

Solució (p.77)

Exercici 13

Sabem que donats dos enters a, b *qualssevol*, si d és el $\text{mcd}(a, b)$, aleshores existeixen dos enters més, λ i μ tals que $\lambda a + \mu b = d$. Demostreu amb un contraexemple que no sempre és cert que si existeixen dos enters λ i μ tals que $\lambda a + \mu b = d$, aleshores $d = \text{mcd}(a, b)$.

Solució (p.78)

Identitat de Bézout

Exercici 14

Demostreu que donats dos enters a i b *qualssevol*, els enters $\frac{a}{\text{mcd}(a,b)}$ i $\frac{b}{\text{mcd}(a,b)}$ són coprimers.

Solució (p.79)

Nombres primers

Nombres primers

Diem que un nombre positiu és **primer** si els seus divisors són exactament quatre i són ± 1 i $\pm p$.

S'exclou d'aquesta definició el nombre 1.
Aplicant la definició de nombres primers, veiem que qualsevol enter es pot descompondre en producte de nombres primers.

Nombres primers

Del treball que hem fet amb el 12, deduïm que

$$12 = 2 \cdot 6.$$

Això és una descomposició, però no ho és en primers perquè el 6 no és primer. Per resoldre-ho descomponem també el 6 i apliquem la propietat associativa:

$$12 = 2 \cdot 6 = 2 \cdot (2 \cdot 3) = 2 \cdot 2 \cdot 3.$$

Teorema fonamental de l'aritmètica

Exercici 15

1. Utilitzeu la identitat de Bézout per demostrar que si $a \mid bc$ i $\mathrm{mcd}(a, b) = 1$, aleshores $a \mid c$.
2. Demostreu que si p és primer i $p \mid ab$ aleshores $p \mid a$ o bé $p \mid b$.
3. Demostreu que si p és primer i $p \mid a_1 \cdot a_2 \cdot \cdots \cdot a_t$, aleshores existeix algun i entre 1 i t tal que $p \mid a_i$.

Solució (p.80)

Teorema fonamental de l'aritmètica

Teorema 3: Teorema fonamental de l'aritmètica

Qualsevol enter descompon en productes de primers i aquesta descomposició és única.

La construcció anterior justifica que existeix la descomposició. La unicitat és una conseqüència del darrer apartat de l'Exercici 15.

Exercici 16

Demostreu el Teorema Fonamental de l'Aritmètica.

Inifinitud dels nombres primers

Teorema 4

Hi ha infinits nombres primers. Nota (p.82)

Demostració

Procedim per reducció a l'absurd.

Suposem que $p_1 < \cdots < p_n$ *són tots els primers.*

Aleshores $p_1 \cdot \cdots \cdot p_n + 1$ *també és primer (perquè no hi ha cap primer que el divideixi, per l'Exercici 7).*

Però, en canvi, és més gran que p_n*.*

Això és una contradicció. □

Sage té una booleà per determinar si un enter és primer:

```
print("is_prime(72)=",is_prime(72))
print("is_prime(17)=",is_prime(17))
```

i una funció per factoritzar en primers:

```
print("factor(72)=",factor(72))
print("factor(17)=",factor(17))
```

Amb el constructor de llistes `[expressio(x) for x in domini(x) if condicional(x)]` podem escriure els primers primers

```
print([i for i in [1..100] if is_prime(i)])
```

Solució de l'Exercici 3

Si $a \mid b$, aleshores existeix q pel qual $b = aq$.
Si $b \mid c$, aleshores existeix q' pel qual $c = bq'$.
Per tant, $c = bq' = (aq)q' = a(qq')$.

Torna a l'exercici (p.11)

Solució de l'Exercici 4

Si $a \mid b$, aleshores existeix q pel qual $b = aq$.
Si, a més a més, $d \mid a$ i $d \mid b$, aleshores existeixen $q_a = \frac{a}{d}$ i $q_b = \frac{b}{d}$ pels quals $a = dq_a$ i $b = dq_b$.
Aleshores $dq_b = dq_a q$ que, per la propietat de l'invers de $\mathbb{Z}$, implica que $q_b = q_a q$ i, per tant,

$$\frac{a}{d} \mid \frac{b}{d}.$$

Torna a l'exercici (p.11)

Solució de l'Exercici 5

- Si $a \mid b$, aleshores existeix un enter q pel qual $b = qa$. En aquest cas, $-b = -qa = (-q)a$, i, per tant, $a \mid -b$.
- Si $a \mid b$ i $a \mid c$, aleshores existeixen enters q_0 i q_1 pels quals $b = q_0 a$ i $c = q_1 a$. Per tant, $b + c = (q_0 + q_1)a$ i $b - c = (q_0 - q_1)a$, el que implica que $a \mid b + c$ i $a \mid b - c$.

Torna a l'exercici (p.12)

Solució de l'Exercici 6

Podem fer servir el fet que $r = a - bq$. Com que a i bq són divisibles per d, r també ho és (per l'exercici anterior).

Torna a l'exercici (p.12)

Solució de l'Exercici 7

Podem demostrar-ho per reducció a l'absurd. Suposem que un enter $d > 1$ és divisor de $qd + 1$. Aleshores existeix q' pel qual $q'd = qd + 1$. Per l'exercici anterior, d és divisor de 1. Per tant, d és 1 o -1, fet que contradiu $d > 1$.

Torna a l'exercici (p.13)

Solució de l'Exercici 9

És suficient veure que un enter divideix a i b si i només si divideix b i r.

- Si $d \mid a$ i $d \mid b$, aleshores $d \mid r$ per l'Exercici 6.
- Si $d \mid b$ i $d \mid r$, aleshores existeixen b' i r' pels quals $b = db'$ $r = dr'$. Per tant, $a = bq + r = db'q + dr' = d(b'q + r')$.

Torna a l'exercici (p.24)

Solució de l'Exercici 11

i	-2	-1	0	1	2	3
λ_i	1	0				
μ_i	0	1				
q_i						
r_i	365	70				

Pas base

$r_{-2} = 365$ $\lambda_{-2} = 1$ $\mu_{-2} = 0$

$r_{-1} = 70$ $\lambda_{-1} = 0$ $\mu_{-1} = 1$

Torna a l'exercici (p.47)

Solució de l'Exercici 11

i	-2	-1	0	1	2	3
λ_i	1	0	1			
μ_i	0	1	-5			
q_i			5			
r_i	365	70	15			

Pas 0

$$365 = 70 \times 5 + 15$$

$$r_0 = 15,\ q_0 = 5$$

$$\lambda_0 = \lambda_{-2} - q_0\lambda_{-1} = 1 - 5(0) = 1$$

$$\mu_0 = \mu_{-2} - q_0\mu_{-1} = 0 - 5(1) = -5$$

Torna a l'exercici (p.47)

Solució de l'Exercici 11

i	-2	-1	0	1	2	3
λ_i	1	0	1	-4		
μ_i	0	1	-5	21		
q_i			5	4		
r_i	365	70	15	10		

Pas 1

$$70 = 15 \times 4 + 10$$

$$r_1 = 10,\ q_1 = 4$$

$$\lambda_1 = \lambda_{-1} - q_1 \lambda_0 = 0 - 4(1) = -4$$

$$\mu_1 = \mu_{-1} - q_1 \mu_0 = 1 - 4(-5) = 21$$

Torna a l'exercici (p.47)

Solució de l'Exercici 11

i	-2	-1	0	1	2	3
λ_i	1	0	1	-4	5	
μ_i	0	1	-5	21	-26	
q_i			5	4	1	
r_i	365	70	15	10	5	

Pas 2

$$15 = 10 \times 1 + 5$$

$$r_2 = 5,\ q_2 = 1$$

$$\lambda_2 = \lambda_0 - q_2\lambda_1 = 1 - 1(-4) = 5$$

$$\mu_2 = \mu_0 - q_2\mu_1 = -5 - 1(21) = -26$$

Torna a l'exercici (p.47)

Solució de l'Exercici 11

i	-2	-1	0	1	2	3
λ_i	1	0	1	-4	5	
μ_i	0	1	-5	21	-26	
q_i			5	4	1	2
r_i	365	70	15	10	5	0

Pas 3

$$10 = 5 \times 2 + 0$$

Torna a l'exercici (p.47)

Solució de l'Exercici 11

i	-2	-1	0	1	2	3
λ_i	1	0	1	-4	5	
μ_i	0	1	-5	21	-26	
q_i			5	4	1	2
r_i	365	70	15	10	5	0

Identitat de Bézout buscada

$$5 \times 365 + (-26) \times 70 = \mathrm{mcd}(365, 70)$$

En efecte,

$$5 \times 365 + (-26) \times 70 = 1825 - 1820 = 5$$

Torna a l'exercici (p.47)

Solució de l'Exercici 40

i	-2	-1	0	1	2	3	4
λ_i	1	0	1	-8	33	-41	
μ_i	0	1	-17	137	-565	702	
q_i			17	8	4	1	3
r_i	2671	156	19	4	3	1	0

Identitat de Bézout buscada:

$$(-41) \times 2671 + (702) \times 156 = \text{mcd}(2671, 156) = 1$$

En efecte,

$$(-41) \times 2671 + (702) \times 156 = -109511 + 109512 = 1$$

Torna a l'exercici (p.47)

Solució de l'Exercici 12

Suposem que existeixen dos enters λ i μ tals que

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

Si $\mathrm{mcd}(a, b) \neq 1$, aleshores ha d'existir un divisor $d > 1$ comú de a i de b. Aleshores existeixen enters q_a i q_b tals que $a = dq_a$ i $b = dq_b$ i, per tant, $\lambda dq_a + \mu dq_b = 1$. Deduïm que

$$d(\lambda q_a + \mu q_b) = 1.$$

Com que tant d com $\lambda q_a + \mu q_b$ són enters, la igualtat anterior només serà possible si $d = 1$. Per tant, a i b han de ser coprimers.

Torna a l'exercici (p.51)

Solució de l'Exercici 13

Per exemple, $5, 7$ són coprimers i $6 \cdot 5 + (-4) \cdot 7 = 2 \neq \text{mcd}(5, 7)$.

Torna a l'exercici (p.51)

Solució de l'Exercici 14

Per la identitat de Bézout sabem que existeixen enters λ i μ tals que

$$\lambda a + \mu b = \text{mcd}(a, b).$$

Per tant, tenim que els mateixos enters λ i μ compleixen

$$\lambda \frac{a}{\text{mcd}(a, b)} + \mu \frac{b}{\text{mcd}(a, b)} = 1.$$

Ara, per l'Exercici 12 deduïm que $\frac{a}{\text{mcd}(a,b)}$ i $\frac{b}{\text{mcd}(a,b)}$ són coprimers.

Torna a l'exercici (p.52)

Solució de l'Exercici 15

1. Per la identitat de Bézout sabem que existeixen λ i μ tals que $\lambda a + \mu b = 1$. Multipliquem la igualtat per c i obtenim $\lambda ac + \mu bc = c$. Com que $a \mid bc$, deduïm que $a \mid c$.
2. Si $p \nmid a$, aleshores $\mathrm{mcd}(a, p) = 1$ i, pel punt anterior, deduïm que $p \mid b$.
3. Es pot demostrar per inducció sobre t utilitzant els passos anteriors.

Torna a l'exercici (p.58)

Notes històriques

- Aquest algoritme per calcular el mcd s'atribueix a Euclides (300 aC aprox.). Euclides va desenvolupar una gran tasca a l'Alexandria Ptolomeica estudiant i recopilant els resultats matemàtics que es coneixien en aquell moment. Tot aquest saber es va exposar magistralment en un tractat compost de tretze volums conegut com els Elements d'Euclides.
Torna (p.37)
- Teorema 4: Aquest resultat i aquesta demostració també apareixen als Elements d'Euclides. De fet, també és conegut com el teorema d'Euclides. Torna (p.61)