1. Divisió entera

ELS NOMBRES NATURALS

El conjunt dels nombres naturals s'introdueix per mitjà de dues propietats:

- Es tracta d'una família amb un primer element.
- Per cadascun dels seus elements n'existeix un altre que és el seu *següent*.

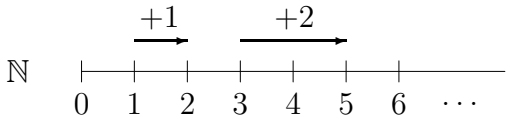
Els elements d'aquesta família són els nombres naturals. Anomenem *zero* al primer element (per alguns autors, u); el següent de *zero* és l'u; el següent de l'u és el *dos*, etc.

Pel conjunt dels nombres naturals fem servir el símbol $\mathbb{N}$. El conjunt $\mathbb{N}$ en forma extensiva és

$$\mathbb{N} = \{\, 0,\, 1,\, 2,\, 3,\, 4,\, 5,\, \ldots \,\}$$

En el conjunt dels nombres naturals es defineixen dues operacions: *suma* i *producte*. Aquestes operacions assignen a cada parella de nombres un tercer nombre que és el resultat de la suma o del producte de la parella.

$$\begin{array}{ccc} \mathbb{N}\times\mathbb{N} & \xrightarrow{+} & \mathbb{N} \\ (\,a,\,b\,) & \longmapsto & a+b \end{array} \qquad \begin{array}{ccc} \mathbb{N}\times\mathbb{N} & \xrightarrow{\cdot} & \mathbb{N} \\ (\,a,\,b\,) & \longmapsto & a\cdot b \end{array}$$



Ambdues operacions són definides com les coneixem habitualment. Per exemple, sumar 1 a qualsevol nombre dóna com a resultat el següent d'aquest nombre; sumar 2 dóna com a resultat el següent del següent d'aquest nombre, i així successivament.

Propietats de les operacions amb nombres naturals

Les operacions suma i producte de nombres naturals tenen unes propietats que es citen a continuació. Qualsevol altre operació que es pugui definir i tingui aquestes mateixes propietats s'assimilarà a les operacions amb nombres naturals. Tot i això, la falta d'alguna de les propietats marcarà una important diferència amb la suma o amb el producte en $\mathbb{N}$.

(i) Commutativa de la suma S'obté el mateix resultat sumant un primer nombre a un segon que aquest segon al primer.

$$a + b = b + a \qquad \text{per a tots els nombres } a,\ b \text{ de } \mathbb{N}$$

(ii) Associativa de la suma Per sumar tres nombres és indiferent sumar el tercer al resultat de la suma del primer amb el segon, que sumar el primer al resultat de la suma del segon amb el tercer.

$$(a + b) + c = a + (b + c) \qquad \forall\, a, b, c \in \mathbb{N}$$

(iii) Element neutre de la suma Existeix un únic nombre que sumat a qualsevol altre nombre dóna com a resultat el mateix nombre: es tracta del nombre 0. El nombre 0 és l'element neutre de la suma en $\mathbb{N}$.

$$\exists!\, 0 \in \mathbb{N} \,/\, \forall\, a \in \mathbb{N} \quad a + 0 = a$$

Les tres propietats següents són iguals a les tres anteriors però ara pel producte en $\mathbb{N}$.

(iv) Commutativa del producte

$$a{\cdot}b = b{\cdot}a \qquad \forall\, a, b \in \mathbb{N}$$

(v) Associativa del producte

$$(a{\cdot}b){\cdot}c = a{\cdot}(b{\cdot}c) \qquad \forall\, a, b, c \in \mathbb{N}$$

(vi) Element neutre del producte

$$\exists!\, 1 \in \mathbb{N} \,/\, \forall\, a \in \mathbb{N} \quad a{\cdot}1 = a$$

L'última propietat relaciona les dues operacions en $\mathbb{N}$.

(vii) Distributiva del producte respecte a la suma

$$a{\cdot}(b + c) = a{\cdot}b + a{\cdot}c \qquad \forall\, a, b, c \in \mathbb{N}$$

Aquesta propietat, d'esquerra a dreta, permet eliminar el parèntesi, mentre que de dreta a esquerra es coneix com a *treure factor comú*.

EL PROBLEMA DE LA RESTA

L'expressió $b - a$ es coneix com la resta dels nombres b i a. El primer dels nombres rep el nom de *minuend* mentre que el segon és el *subtrahend*. El problema de la resta $b - a$ consisteix en determinar el nombre x que sumat al subtrahend dóna com a resultat el minuend.

$$8 - 5 = 3 \quad \text{ja que} \quad 5 + 3 = 8.$$

Efectuar la resta $b - a$ en $\mathbb{N}$ equival a resoldre en $\mathbb{N}$ l'equació:

$$\boxed{a + x = b}$$

La suma en $\mathbb{N}$ dóna com a resultat nombres que són següents al nombre a, de manera que l'equació anterior només tindrà una solució en $\mathbb{N}$ si el nombre b és un d'aquests nombres, és a dir, $b \geq a$.

Només quan el minuend és major que el subtrahend és possible la resta en $\mathbb{N}$. Ens interessaria treballar amb un conjunt de nombres on sempre es pogués restar, o el que és el mateix, on l'equació $a + x = b$ tingués sempre solució.

El nou conjunt de nombres hauria de complir aquests requisits:

- Que els seus elements s'obtinguin a partir dels nombres naturals i que aquests quedin inclosos al nou conjunt numèric.
- Que es mantinguin les operacions de suma i producte definides en $\mathbb{N}$ i que s'ampliïn als nous elements, conservant totes les seves propietats.
- Que la resta sigui sempre possible, és a dir, que l'equació $a + x = b$ sempre tingui solució al nou conjunt.

El conjunt numèric que es construeix complint totes aquestes condicions és el dels nombres *enters*.

ELS NOMBRES ENTERS

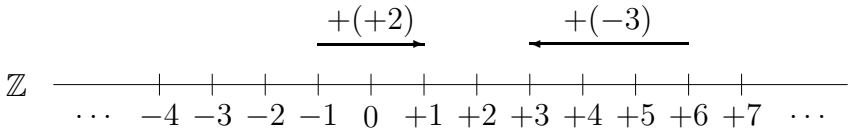
El conjunt dels nombres enters es designa amb el símbol $\mathbb{Z}$. En aquest conjunt, a més del número 0, trobem dos tipus de nombres:

$$\begin{array}{lll} \text{enters positius:} & +n & \text{amb } n \in \mathbb{N}^* = \mathbb{N} \setminus \{0\} \\ \text{enters negatius:} & -n & \text{amb } n \in \mathbb{N}^* = \mathbb{N} \setminus \{0\} \end{array}$$

Denotem el conjunt dels nombres enters positius amb $\mathbb{Z}^+$ i el dels negatius amb $\mathbb{Z}^-$. Aleshores,

$$\mathbb{Z} = \mathbb{Z}^+ \cup \mathbb{Z}^- \cup \{0\}.$$

Són definides en $\mathbb{Z}$ les operacions suma i producte. Sumar a un nombre un enter positiu suposa avançar en sentit de 0 a 1 (cap a la dreta), mentre que sumar un enter negatiu suposa avançar en sentit contrari.



Una resta com $3 - 6$ te solució en $\mathbb{Z}$, ja que el nombre que cal sumar a 6 per obtenir 3 és el nombre enter -3. Totes les propietats que compleixen la suma i el producte de nombres naturals les compleixen la suma i el producte en $\mathbb{Z}$. A més, la suma en $\mathbb{Z}$ compleix una nova propietat:

(viii) Element oposat de la suma Per cada nombre enter es pot trobar un altre nombre enter (el seu oposat) de manera que al sumar-los s'obté el neutre de la suma. L'oposat d'un nombre $a \in \mathbb{Z}$ es simbolitza $-a$.

$$\forall\, a \in \mathbb{Z} \quad \exists (-a) \in \mathbb{Z} \,/\, a + (-a) = 0.$$

Aquesta propietat és la que permet escriure la solució de l'equació $a + x = b$ en $\mathbb{Z}$. Sumant a ambdós costats l'oposat d'a:

$$(-a) + a + x = (-a) + b\ ; \quad 0 + x = b + (-a)\ ; \quad \boxed{x = b + (-a)}$$

Una vegada resolta en $\mathbb{Z}$ l'equació anterior, ens plantegem per la possible solució en $\mathbb{Z}$ d'una equació del tipus

$$\boxed{a\,x = b \quad \text{amb } a, b \in \mathbb{Z}}$$

És el cas d'equacions com $3\,x = 6$ ó $4\,x = 7$. La primera té coma solució el nombre $x = 2$, mentre que la segona no té solució en $\mathbb{Z}$. Hem arribat al problema de la *divisibilitat*.

Divisibilitat en $\mathbb{Z}$ Donats dos nombres enters, $a \in \mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$, $b \in \mathbb{Z}$, diem que a *divideix* a b (o b és *múltiple* d'a) si i només si existeix un nombre enter $q \in \mathbb{Z}$ tal que $b = a\,q$.

$$a \in \mathbb{Z}^*,\ b \in \mathbb{Z}, \quad a|b \ \Leftrightarrow\ \exists\, q \in \mathbb{Z} \,/\, b = a\,q$$

Per exemple, 3 divideix a 15, o 15 és múltiple de 3, $3|15$, perquè $15 = 3{\cdot}5$. També $2|-24$, perquè $-24 = 2{\cdot}(-12)$. Tot i això, $4 \not| 7$.

LA DIVISIÓ ENTERA

Hem vist que no tot nombre enter és divisor de qualsevol altre nombre enter. En aquest context introduïm el concepte de *divisió entera*.

Per a qualssevol dos nombres $a \in \mathbb{Z}^*$, $b \in \mathbb{Z}$, existeixen dos únics nombres q, $r \in \mathbb{Z}$ tals que

$$\boxed{b = a\,q + r \quad \text{amb } 0 \leq r < |a|}$$

Els nombres b, a, q, r reben, respectivament, els noms de *Dividend*, *divisor*, *quocient* i *resta* o *residu*. La fórmula anterior és la coneguda expressió

$$\boxed{\text{Dividend} = \text{divisor} \cdot \text{quocient} + \text{residu}}$$

on el residu és un nombre positiu menor que el valor absolut del divisor.

Exemple Divisió entera de 17 entre 5 usant l'algorisme habitual de divisió d'enters positius:

$$\begin{array}{rl} 17 & \underline{|\,5} \\ \underline{2} & 3 \end{array}$$

És a dir, $17 = 5{\cdot}3 + 2 \quad \text{amb } 0 \leq 2 < |5|$.

Divisió entera de -17 entre 5:

$$-17 = 5{\cdot}(-4) + 3 \quad \text{amb } 0 \leq 3 < |5|.$$

Divisió entera de 17 entre -5:

$$17 = (-5){\cdot}(-3) + 2 \quad \text{amb } 0 \leq 2 < |-5|.$$

Divisió entera de -17 entre -5:

$$-17 = (-5){\cdot}4 + 3 \quad \text{amb } 0 \leq 3 < |-5|.$$

▶ L'exemple anterior mostra que el cas en el qual el divisor és un enter negatiu es redueix fàcilment a una divisió entera amb divisor enter positiu. Ens ocuparem principalment d'aquest supòsit.

▶ Donats el dividend $b \in \mathbb{Z}$ i el divisor $a \in \mathbb{N}^*$, provarem que existeixen els nombres q, $r \in \mathbb{Z}$ de manera que $b = a\,q + r$, amb $0 \leq r < a$, i que són únics.

Suposem que $a\,q$ és el major múltiple d'a que és menor o igual que b, això és:

$$\left.\begin{array}{rcl} a\,q & \leq & b \\ & & b \;<\; a\,(q+1) \end{array}\right\}$$

Només cal agafar com a residu $r = b - a\,q$ de manera que, segons la primera desigualtat, $r \geq 0$. Restant $a\,q$ a la segona desigualtat:

$$r = b - a\,q < a\,(q+1) - a\,q = a,$$

i el residu r és estrictament menor que el divisor a.

Suposem que existissin nombres enters q_1, r_1 y q_2, r_2 ($q_1 \neq q_2$, $r_1 \neq r_2$) tals que

$$\left.\begin{array}{lll} b = a\,q_1 + r_1 & \text{amb} & 0 \leq r_1 < a \\ b = a\,q_2 + r_2 & \text{amb} & 0 \leq r_2 < a \end{array}\right\}.$$

Restant ambdues igualtats:

$$0 = a\,(q_1 - q_2) + r_1 - r_2.$$

Al ser $r_1 \neq r_2$, si $r_1 > r_2$:

$$a\,(q_1 - q_2) = r_1 - r_2,$$

és a dir, el nombre a divideix a $r_1 - r_2$, però $0 \leq r_1 < a$ i $0 \leq r_2 < a$, d'on $r_1 - r_2 < a$.

Aleshores, $r_1 - r_2 < a$ i $a \mid (r_1 - r_2)$ fa que necessàriament $r_1 - r_2 = 0$; $r_1 = r_2$ i també $q_1 = q_2$, la qual cosa prova la unicitat del quocient i del residu en la divisió entera.

▶ Fent servir l'algorisme de la divisió entera es poden provar nombroses propietats dels nombres enters com les que s'enuncien a continuació:

Propietat El quadrat de qualsevol nombre imparell es pot escriure de la forma $8\,k + 1$ amb $k \in \mathbb{N}$.

Els nombres imparells (positius) són 1, 3, 5, 7, ... i els seus respectius quadrats són $1^2 = 1$, $3^2 = 9$, $5^2 = 25$, $7^2 = 49$, ... Tots aquests nombres donen com a residu 1 al dividir-los per 8, tal y com estableix l'enunciat que es vol provar.

Per a demostrar la propietat fem servir el fet que tot nombre imparell dóna residu 1 al dividir-lo per 2, de manera que qualsevol d'aquests nombres es pot escriure de la forma:

$$n = 2\,q + 1 \quad \text{per a un determinat } q \in \mathbb{Z}.$$

Aleshores,

$$n^2 = (2\,q + 1)^2 = 4\,q^2 + 4\,q + 1 = 4\,(q^2 + q) + 1.$$

En una primera lectura hem obtingut que tot nombre imparell dóna residu 1 al dividir-lo entre 4, ja que és un múltiple de 4 més 1. Però, a més,

$$q^2 + q = q\,(q + 1) = 2\,k,$$

ja que el producte de dos nombres consecutius és parell per ser el producte d'un parell por un imparell. Substituint a l'expressió de n^2,

$$n^2 = 8\,k + 1,$$

essent k el quocient i 1 el residu de la divisió entera de $n^2 > 0$ entre 8.

L'enunciat que acabem de provar afirma que el quadrat d'un nombre imparell és múltiple de 8 més 1. El recíproc, però, no és cert. Per exemple, $33 = 8{\cdot}4 + 1$, però no és el quadrat de cap nombre enter, ni parell ni imparell.

Propietat Si a és un nombre enter tal que $2 \not| a$ i $3 \not| a$, llavors $24|(a^2 - 1)$.

Visualitzarem el resultat amb els primers nombres enters positius que no són divisibles ni per 2 ni per 3.

$$\begin{array}{ll} a = 1,\ a^2 - 1 = 0 = 24{\cdot}0; & a = 5,\ a^2 - 1 = 24 = 24{\cdot}1; \\ a = 7,\ a^2 - 1 = 48 = 24{\cdot}2; & a = 11,\ a^2 - 1 = 120 = 24{\cdot}5; \quad \ldots \end{array}$$

Per a demostrar la propietat usem l'algorisme de la divisió entera prenent com a divisor el nombre 6. Qualsevol nombre $a \in \mathbb{Z}$ al ser dividit per 6 ofereix sis possibles residus: 0, 1, 2, 3, 4 ó 5.

$$\begin{array}{llll} a = 6q & a = 2{\cdot}3{\cdot}q & \Rightarrow & a \text{ és múltiple de 2 i de 3} \\ a = 6q + 1 & & & \\ a = 6q + 2 & a = 2(3q + 1) & \Rightarrow & a \text{ és múltiple de 2} \\ a = 6q + 3 & a = 3(2q + 1) & \Rightarrow & a \text{ és múltiple de 3} \\ a = 6q + 4 & a = 2(3q + 2) & \Rightarrow & a \text{ és múltiple de 2} \\ a = 6q + 5 & & & \end{array}$$

En conseqüència, els enters a que no són divisibles ni per 2 ni per 3 són aquells que el residu de la seva divisió entera per 6 és 1 ó 5. Per aquests nombres calculem $a^2 - 1$. En el primer cas:

$$a^2 - 1 = (6q + 1)^2 - 1 = 36q^2 + 12q = 12q(3q + 1)$$

Aquest nombre és múltiple de 12. Per afirmar que és múltiple de 24 només caldria garantir que $q(3q+1)$ és parell; això és així ja que si q és parell el producte és parell, mentre que si q és imparell $3q$ també és imparell i $3q+1$ és parell. En el segon cas:

$$a^2-1=(6q+5)^2-1=36q^2+60q+24=12[3q^2+5q+2]=12[q(3q+5)+2]$$

Com en el cas anterior, a^2-1 és múltiple de 12. Per assegurar que és múltiple de 24, $q(3q+5)+2$ hauria de ser múltiple de 2, o el que és el mateix, $q(3q+5)$ hauria de ser parell. Si q és parell el producte és parell, en canvi si q és imparell $3q$ també ho és i $3q+5$ és parell. Això conclou la prova de la propietat.

MÀXIM COMÚ DIVISOR

Considerem qualsevol parella de nombres enters $a,\, b \in \mathbb{Z}^*$. El nombre enter $d \neq 0$ és divisor comú de a i de b si $d|a$ i $d|b$.

Si a més a més és $d>0$ i tot divisor comú de a i de b divideix a d, aleshores, d és el màxim comú divisor de a i de b. Ho denotem

$$d = mcd(a,b).$$

Exemple Determinació del màxim comú divisor de 12 i 16.

$$\text{Divisors de } 12 = \{\pm1,\, \pm2,\, \pm3,\, \pm4,\, \pm6,\, \pm12\}$$

$$\text{Divisors de } 16 = \{\pm1,\, \pm2,\, \pm4, \pm8,\, \pm16\}$$

$$\text{Divisors comuns de 12 i de } 16 = \{\pm1,\, \pm2,\, \pm4\}$$

El nombre enter positiu 4 forma part del conjunt dels divisors comuns de 12 i 16. Tots els demés divisors comuns divideixen a 4, llavors

$$4 = mcd(12,\, 16).$$

Teorema (Identitat de Bezout)
Donats dos nombres qualssevol $a,\, b \in \mathbb{Z}^*$, el seu màxim comú divisor d és un nombre únic que compleix la propietat de ser l'enter positiu més petit que pot expressar-se com a combinació lineal entera d'ambdós nombres:

$$\boxed{d = a\,x + b\,y} \quad \text{per a determinats } x,\, y \in \mathbb{Z}.$$

► La identitat de Bezout és un important resultat del que es deriven nombroses propietats, algunes de les quals apareixeran al llarg dels diferents temes. Tot i això, la demostració de la identitat no és imprescindible per comprendre les seves aplicacions, pel que pot ser omesa en una primera lectura.

Demostració de la identitat de Bezout. Considerem el subconjunt de $\mathbb{Z}$ format per totes les combinacions lineals enteres positives dels nombres a i b:

$$M = \{\, a\,x + b\,y > 0 \;/\; x,\, y \in \mathbb{Z}\}$$

Es compleix $M \neq \emptyset$, ja que $|a| = (\pm 1)\cdot a + 0\cdot b > 0$. El *Principi de la bona ordenació* estableix que tot subconjunt d'enters positius no buit té un primer element. Anomenem d al primer element de M:

$$d = a\,x_1 + b\,y_1$$

Provarem que $d|a$. En cas contrari existiran enters q i r tals que $a = d\,q + r$ amb $0 < r < d$. Llavors:

$$r = a - d\,q = a - (a\,x_1 + b\,y_1)\,q = a\,(1 - x_1 q) + b\,(-y_1\,q)$$

D'aquí, $r \in M$ essent $r > 0$ i $r < d$. Així d no és, com suposàvem, el primer element de M. Contradicció (!). Queda provat que $d|a$ i, anàlogament, $d|b$.

Fins aquí esta demostrat que aquell primer element de M és divisor comú de a i de b. Falta provar que és el màxim. Suposem d' un altre divisor comú de a i de b: $a = d'\,p_1$, $b = d'\,p_2$. En aquest cas,

$$d = a\,x_1 + b\,y_1 = d'\,p_1\,x_1 + d'\,p_2\,y_1 = d'\,(p_1\,x_1 + p_2\,y_1),$$

d'on, $d'|d$ i $d = mcd(a, b)$

Finalment, el màxim comú divisor d és únic. Si n'existissin dos, d_1 i d_2, es compliria: $d_1|d_2$ i $d_2|d_1$. Prenent valors absoluts, $|d_1| \leq |d_2|$ i $|d_2| \leq |d_1|$, la qual cosa implica $|d_1| = |d_2|$. Com que, per definició, el màxim comú divisor és positiu, es conclou $d_1 = d_2$.

Exemple En cada cas, el màxim comú divisor es pot expressar com la combinació lineal que es detalla. A més, cap altre enter positiu menor pot escriure's d'aquesta forma.

$$\begin{aligned} mcd(21,\,12) = 3 \quad &\Rightarrow \quad 3 = 21\cdot(-1) + 12\cdot 2 \\ mcd(400,\,144) = 16 \quad &\Rightarrow \quad 16 = 400\cdot 4 + 144\cdot(-11) \\ mcd(64,\,25) = 1 \quad &\Rightarrow \quad 1 = 64\cdot 9 + 25\cdot(-23) \end{aligned}$$

► Primeres conseqüències de la identitat de Bezout

1. Dos enters a, b amb $mcd(a,b) = 1$ es diu que són *primers entre si*.

$$\boxed{a,\, b \in \mathbb{Z}^* \,/\, mcd(a,b) = 1 \;\Leftrightarrow\; \exists\, x,\, y \in \mathbb{Z} \,/\, a\,x + b\,y = 1}$$

2. Teorema d'Euclides A la divisió entera, el màxim comú divisor del dividend i del divisor coincideix amb el màxim comú divisor del divisor i del residu.

$$\boxed{\text{Si}\;\; b = a\,q + r \;\; \text{amb} \;\; 0 \leq r < |a|, \;\; \text{aleshores} \;\; mcd(b,a) = mcd(a,r)}$$

La conseqüència 1 és el cas particular de la identitat de Bezout en el que $mcd(a,b) = 1$. Per comprovar la conseqüència 2 únicament cal considerar la cadena d'igualtats

$$mcd(b,a) = mcd(\, a\,q + r,\; a\,) = mcd(a,r).$$

L'ALGORISME D'EUCLIDES

L'aplicació reiterada d'aquesta última propietat permet calcular el màxim comú divisor de dos nombres enters que, per comoditat, suposarem positius.

En un primer estadi, prenem el major d'aquests nombres com a dividend i el menor com a divisor. El seu *mcd* és el mateix que el del divisor i el del residu, que és un nombre menor que el divisor. En un segon estadi considerem aquests dos nombres com a nous dividend i divisor, respectivament, i repetim el procés.

El mètode finalitza quan el dividend és múltiple del divisor, moment en que el residu de la divisió entera és 0, essent el *mcd*, per tant, l'últim residu abans d'obtenir residu 0. Aquest procediment comporta un nombre finit de passos, ja que cada vegada el residu és un nombre estrictament menor que el divisor.

En l'algorisme d'Euclides, dividend i divisor es disposen igual que a l'algorisme de la divisió entera, així com el residu de la divisió, que es col·loca a sota del dividend. La diferència consisteix en que el quocient es col·loca a sobre del divisor. Així aquest divisor queda disposat per ser el següent dividend i el residu passa a ocupar la posició del següent divisor. La taula adjunta mostra

el procediment per a calcular $mcd(400, 144)$.

quocients:		2	1	3	2
	400	144	112	32	16
residus:	112	32	**16**	0	

El nombre marcat en negreta és l'últim residu abans d'obtenir residu 0, de manera que $mcd(400, 144) = 16$. La taula anterior permet calcular el *mcd* de dos nombres usant repetidament el teorema d'Euclides:

$$mcd(400, 144) = mcd(144, 112) = mcd(112, 32) = mcd(32, 16) = 16,$$

ja que 32 és múltiple de 16. Aquesta última és una divisió *exacta* (residu 0).

► L'algorisme d'Euclides permet obtenir el màxim comú divisor de dos nombres sense necessitat de descomposar-los.

► L'algorisme d'Euclides ofereix un mètode per a escriure el màxim comú divisor com a combinació entera d'ambdós nombres (identitat de Bezout).

Comprovem aquesta última afirmació sobre l'exemple anterior. Escrivim les tres divisions enteres que apareixen, des de la primera entre 400 i 144 fins aquella en que apareix el seu *mcd* 16, aïllant de cadascuna el seu residu.

$$\left.\begin{array}{rcl} 400 &=& 144\cdot 2 + 112 \\ 144 &=& 112\cdot 1 + 32 \\ 112 &=& 32\cdot 3 + 16 \end{array}\right\} \quad \Longrightarrow \quad \left.\begin{array}{rcl} 112 &=& 400 + 144\cdot(-2) \\ 32 &=& 144 + 112\cdot(-1) \\ 16 &=& 112 + 32\cdot(-3) \end{array}\right\}$$

A l'última igualtat de la dreta, el nombre $16 = mcd(400, 144)$ esta escrit com a combinació lineal entera de 112 i de 32. Si es substitueix el residu anterior, 32, s'obté el número 16 com combinació de 144 i 112:

$$16 = 112 + 32\cdot(-3) = 112 + [144 + 112\cdot(-1)].(-3) = 144\cdot(-3) + 112\cdot 4.$$

Ara només cal substituir el residu anterior, 112, per tal de poder expressar el nombre 16 com a combinació lineal entera de 400 i de 144. El procés acaba aquí, ja que 112 és el primer residu obtingut.

$$16 = 144\cdot(-3) + 112\cdot 4 = 144\cdot(-3) + [400 + 144\cdot(-2)]\cdot 4 = 400\cdot 4 + 144\cdot(-11).$$

$$\boxed{16 = 400\cdot 4 + 144\cdot(-11)}$$

Exemple Obtenció del màxim comú divisor de 64 i de 25 i expressió com a combinació lineal entera d'ambdós nombres.

	2	1	1	3	1	2
64	25	14	11	3	2	1
14	11	3	2	**1**	0	

Per l'algorisme d'Euclides, $mcd(64, 25) = 1$. A continuació escrivim les cinc divisions enteres que s'han fet fins a obtenir el mcd aïllant els seus respectius residus:

$$\left.\begin{array}{rcl} 64 &=& 25\cdot 2 + 14 \\ 25 &=& 14\cdot 1 + 11 \\ 14 &=& 11\cdot 1 + 3 \\ 11 &=& 3\cdot 3 + 2 \\ 3 &=& 2\cdot 1 + 1 \end{array}\right\} \quad \Longrightarrow \quad \left.\begin{array}{rcl} 14 &=& 64 + 25\cdot(-2) \\ 11 &=& 25 + 14\cdot(-1) \\ 3 &=& 14 + 11\cdot(-1) \\ 2 &=& 11 + 3\cdot(-3) \\ 1 &=& 3 + 2\cdot(-1) \end{array}\right\}$$

A l'última igualtat de la dreta es substitueix el residu anterior, 2, i successivament els residus restants en ordre invers a com s'han obtingut, fins a acabar al residu 14.

$$1 = 3 + 2\cdot(-1) = 3 + [11 + 3\cdot(-3)]\cdot(-1) = 11\cdot(-1) + 3\cdot 4;$$
$$1 = 11\cdot(-1) + 3\cdot 4 = 11\cdot(-1) + [14 + 11\cdot(-1)]\cdot 4 = 14\cdot 4 + 11\cdot(-5);$$
$$1 = 14\cdot 4 + 11\cdot(-5) = 14\cdot 4 + [25 + 14\cdot(-1)]\cdot(-5) = 25\cdot(-5) + 14\cdot 9;$$
$$1 = 25\cdot(-5) + 14\cdot 9 = 25\cdot(-5) + [64 + 25\cdot(-2)]\cdot 9 = 64\cdot 9 + 25\cdot(-23).$$

$$\boxed{1 = 64\cdot 9 + 25\cdot(-23)}$$

Exercicis

1. Calcular $mcd(21, 12)$ i expressar-lo com a combinació lineal entera d'ambdós nombres.

2. Igual que l'exercici anterior per als nombres 1476 i 900.