2. Nombres primers

ELS NOMBRES PRIMERS

Diem que un nombre enter p és *primer* si $p > 1$ i els únics enters positius que divideixen a p són 1 i p.

Els primers nombres primers són: 2, 3, 5, 7, 11, 13, 17, 19.

El nombre enter 1 no és primer. Qualsevol enter positiu $n > 1$ no primer pot escriure's com a $n = n_1 \cdot n_2$, on n_1, n_2 són alguns dels seus divisors diferents a la unitat. Així podem escriure

$$4 = 2 \cdot 2,\ 6 = 2 \cdot 3,\ \ldots\ 90 = 2 \cdot 45 = 3 \cdot 30 = 5 \cdot 18 = 10 \cdot 9,\ \ldots$$

La descomposició d'un nombre no primer com a producte d'altres no és única. No obstant, observem que el nombre primer 2 divideix 90 i, en tots els casos, 2 divideix algun dels factors en els quals es descompon el nombre 90. Aquest és un fet general que es recull en la següent propietat.

Lema d'Euclides
Suposem $a, b, c \in \mathbb{Z}$. Si a i c són primers entre sí i $c|a\,b$ aleshores $c|b$.

La prova d'aquesta propietat està basada en la identitat de Bezout. Si a i c són primers entre sí el seu màxim comú divisor és 1. Aleshores existeixen dos nombres $x, y \in \mathbb{Z}$ tals que $a\,x + c\,y = 1$.

Multiplicant ambdós membres per b s'obté $b\,a\,x + b\,c\,y = b$.

Per hipòtesi $c|a\,b$ llavors $c|b\,a\,x$. També $c|b\,c\,y$, d'on $c|(b\,a\,x + b\,c\,y)$, és a dir, $c|b$.

La conseqüència més directa del Lema d'Euclides és una condició alternativa a la definició de nombre primer.

► Són equivalents:

(1) p és primer
(2) $\forall\, a, b \in \mathbb{Z},$ si $p|a\,b$ aleshores $p|a$ o $p|b$.

Aquesta condició alternativa ens indica que els nombres primers són els elements de $\mathbb{Z}$ que podem considerar com a més elementals. Els nombres no primers no compleixen aquesta condició. Observem diferents casos.

$$5 \text{ és primer: } 5|8\cdot 10 \Rightarrow 5|10 \qquad 2 \text{ és primer: } 2|8\cdot 10 \Rightarrow 2|8,\ 2|10$$

$$6|4\cdot 9 \text{ però } 6\not|\,4,\ 6\not|\,9 \Rightarrow 6 \text{ no és primer}$$

$$10|16\cdot 25 \text{ però } 10\not|\,16,\ 10\not|\,25 \Rightarrow 10 \text{ no és primer}$$

Per tal de provar (1) $\Rightarrow$ (2) suposem que p és un primer tal que $p|a\,b$. Si $mcd(p,a)=1$, de manera anàloga al Lema d'Euclides, $p|b$. Si p no és primer amb a, considerem $d=mcd(p,a)$ que complirà $d>1$, $d|p$ i $d|a$. Com que p és primer necessàriament $d=p$, per tant $p|a$.

La demostració (2) $\Rightarrow$ (1) la farem pel contrarrecíproc. Provarem,$\neg(1) \Rightarrow \neg(2)$. Suposem que p no és primer. En aquest cas existeixen dos nombres enters a i b tals que $1<a,b<p$ complint $p=a\,b$. Així doncs, $p|a\,b$ però ni $p\not|\,a$ ni $p\not|\,b$.

Obtenció de nombres primers: el Sedàs d'Erastòstenes

El sedàs d'Eratòstenes (s. III a.C.) permet determinar els primers nombres primers fins al nombre que es determini. En l'exemple fins al 100.

El procediment consisteix a assenyalar el primer nombre primer, 2, i a eliminar tots els seus múltiples. El següent nombre primer és el primer nombre no eliminat, 3. S'assenyala aquest i s'eliminen tots els seus múltiples. El següent primer torna a ser el primer nombre no eliminat, 5. Es repeteixen els passos anteriors fins a completar la taula.

1	$\boxed{2}$	$\boxed{3}$	$\not4$	$\boxed{5}$	$\not6$	$\boxed{7}$	$\not8$	$\not9$	$\not{10}$
$\boxed{11}$	$\not{12}$	$\boxed{13}$	$\not{14}$	$\not{15}$	$\not{16}$	$\boxed{17}$	$\not{18}$	$\boxed{19}$	$\not{20}$
$\not{21}$	$\not{22}$	$\boxed{23}$	$\not{24}$	$\not{25}$	$\not{26}$	$\not{27}$	$\not{28}$	$\boxed{29}$	$\not{30}$
$\boxed{31}$	$\not{32}$	$\not{33}$	$\not{34}$	$\not{35}$	$\not{36}$	$\boxed{37}$	$\not{38}$	$\not{39}$	$\not{40}$
$\boxed{41}$	$\not{42}$	$\boxed{43}$	$\not{44}$	$\not{45}$	$\not{46}$	$\boxed{47}$	$\not{48}$	$\not{49}$	$\not{50}$
$\not{51}$	$\not{52}$	$\boxed{53}$	$\not{54}$	$\not{55}$	$\not{56}$	$\not{57}$	$\not{58}$	$\boxed{59}$	$\not{60}$
$\boxed{61}$	$\not{62}$	$\not{63}$	$\not{64}$	$\not{65}$	$\not{66}$	$\boxed{67}$	$\not{68}$	$\not{69}$	$\not{70}$
$\boxed{71}$	$\not{72}$	$\boxed{73}$	$\not{74}$	$\not{75}$	$\not{76}$	$\not{77}$	$\not{78}$	$\boxed{79}$	$\not{80}$
$\not{81}$	$\not{82}$	$\boxed{83}$	$\not{84}$	$\not{85}$	$\not{86}$	$\not{87}$	$\not{88}$	$\boxed{89}$	$\not{90}$
$\not{91}$	$\not{92}$	$\not{93}$	$\not{94}$	$\not{95}$	$\not{96}$	$\boxed{97}$	$\not{98}$	$\not{99}$	$\not{100}$

El procediment del sedàs d'Erastòstenes consisteix a eliminar tots els múltiples dels primers obtinguts. Podríem pensar si aquest mètode arribaria a eliminar tots els nombres a partir d'un determinat i a partir d'aquest ja no hi hauria més nombres primers. El següent resultat mostra que el que succeeix és essencialment el contrari.

Propietat La quantitat de nombres primers és infinita.

La demostració es realitza per reducció a l'absurd, la qual cosa significa, que es suposa el contrari del que es vol provar fins que s'arriba a una contradicció.

Suposem que la quantitat de nombres primers fos finita i que aquests primers fossin els nombres p_1, p_2,... p_k. Considerem llavors el nombre

$$m = p_1\, p_2 \cdots p_k + 1.$$

La resta de la divisió de m entre tots els nombres primers p_1, p_2,... p_k és 1. Cap primer divideix m, per tant m és un nombre primer. Contradicció!

Observació La propietat anterior ens permet obtenir nombres primers.

A partir dels primers $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$ obtenim:

$$\begin{aligned} m_1 &= p_1\, p_2\, p_3 + 1 = 31 \qquad \text{primer} \\ m_2 &= p_1\, p_2\, p_3\, p_4 + 1 = 211 \quad \text{primer} \end{aligned}$$

Però no tots els primers s'obtenen d'aquesta manera.

La següent propietat estableix un mínim de comprovacions necessàries per a determinar si un enter és un nombre primer.

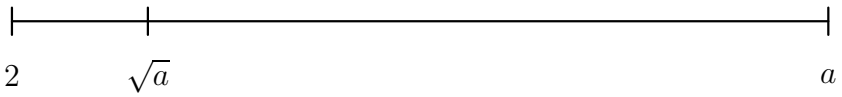
Propietat Suposem que a és un nombre enter ($a > 1$). Si cap nombre primer p amb $p \leq \sqrt{a}$ divideix a, llavors a és un nombre primer.

Si a fos un nombre compost podria escriure's en la forma $a = n_1\, n_2$. Com a $a = \sqrt{a}\sqrt{a}$, si $n_1 \geq \sqrt{a}$ llavors $n_2 \leq \sqrt{a}$. Sempre entre els divisors de a algun és menor o igual que $\sqrt{a}$. Suposem que és $n_1 \leq \sqrt{a}$. Si n_1 és primer ja és un dels que comprovaríem. Si n_1 no és primer serà compost i amb aquest repetim el procés les vegades que sigui necessari fins que un divisor sigui primer. Aquest és, a més a més, menor que $\sqrt{a}$.

En conseqüència, si un nombre a és compost té algun divisor primer menor o igual que $\sqrt{a}$. Si cap primer $p \leq \sqrt{a}$ divideix a vol dir que aquest és un nombre primer.

Exemple Determinar si el nombre 83 és o no primer.

Com que $\sqrt{83} = 9, 11\ldots$, hem de considerar els nombres primers menors 2, 3, 5 y 7. Com que 83 no és divisible per cap d'ells, resulta que és un nombre primer.



El sedàs d'Erastòstenes que hem obtingut conté els nombres primers menors que 100. Utilitzant la propietat anterior tenim els primers necessaris per a comprovar si qualsevol nombre menor que 10.000 és o no primer.

EL TEOREMA FONAMENTAL DE L'ARITMÈTICA

Aquest resultat essencial sobre els nombres enters va ser establert per Euclides i es troba al llibre IX dels seus *Elements*: tot nombre enter pot factoritzar-se en forma única com a producte de nombres primers.

Teorema Suposem que $n > 1$ és un nombre enter. Aleshores, existeixen nombres primers p_1, p_2, ..., p_r tals que

$$n = p_1\, p_2 \cdots p_r \quad \text{on} \quad p_1 \leq p_2 \leq \cdots \leq p_r. \tag{1}$$

Aquesta factorització és única en el sentit que si existissin altres nombres primers q_1, q_2, ..., q_s tals que $n = q_1\, q_2 \cdots q_s$, llavors $r = s$ i $q_i = p_i$ per a $i = 1, 2, \ldots, r$.

Demostració. En primer lloc provarem que sempre existeix una factorització com a (1). Per reducció a l'absurd, suposarem que existeix un enter $m > 1$ que no pot expressar-se en la forma (1).

Definim el conjunt $S = \{m \in \mathbb{Z},\, m > 1 \,/\, m$ no és expressable com a $(1)\}$.

El conjunt S suposem que és no buit. En ser tots els seus elements positius, pel principi de la bona ordenació, S té un primer element; suposem que és m_0.

El nombre m_0 no és primer ja que si ho fos podríem escriure $m_0 = m_0$ i no pertanyeria a S. Llavors m_0 és compost i pot expressar-se com a $m_0 = u\, v$ amb $1 < u,\, v < m_0$ i $u,\, v \in \mathbb{Z}$. Com que u i v són menors que m_0 no

pertanyen a S i poden factoritzar-se en la forma (1), per tant el seu producte $m_0 = u\,v$ té una expressió en factors com a (1). Contradicció!

Per tal de provar la unicitat de la factorització, suposarem que n'hi hagués dues:

$$n = p_1\,p_2\,\cdots\,p_r = q_1\,q_2\,\cdots\,q_s.$$

Si $r \neq s$ podem suposar que $r < s$. Llavors ha d'existir un primer element j, $1 \leq j \leq r$, tal que $p_j \neq q_j$. En cas contrari

$$p_1\,p_2\,\cdots\,p_r = p_1\,p_2\,\cdots\,p_r\,q_{r+1}\,\cdots q_s,$$

d'on s'obté l'absurd $1 = q_{r+1}\,\cdots q_s$. Així podem suposar que j és el primer element tal que $p_j \neq q_j$. Llavors

$$p_j\,p_{j+1}\,\cdots\,p_r = q_j\,q_{j+1}\,\cdots\,q_s,$$

Ara suposem que $p_j < q_j$. Per la igualtat anterior $p_j | q_j\,q_{j+1}\,\cdots\,q_s$ i, en ser p_j primer, $p_j | q_h$ per algun $h \in \{j, j+1, \ldots, s\}$ (generalització de la condició de primer). En ser q_h primer necessàriament $p_j = q_h$. Però $q_j \leq q_h$, la qual cosa contradiu que $p_j < q_j$.

El cas $p_j > q_j$ es raona de forma anàloga. S'ha arribat a contradicció. Per tant $r = s$.

Finalment, si $r = s$ i existís algun $p_i \neq q_i$, un raonament similar portaria novament a contradicció.

L'expressió habitual de la factorització d'un nombre enter positiu conté agrupats els factors primers repetits.

Conseqüència Per a cada nombre enter $n > 1$ existeixen uns nombres primers únics p_1, p_2, …, p_t de manera que

$$\boxed{n = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t} \quad \text{amb} \quad p_1 < p_2 < \cdots < p_t}$$

on $m_i \in \mathbb{N}^*$, $1 \leq i \leq t$, són les multiplicitats respectives de cada primer.

Exemple Descomposició factorial dels nombres 400 i 144.

400	2
200	2
100	2
50	2
25	5
5	5
1	

$400 = 2^4\,5^2$

144	2
72	2
36	2
18	2
9	3
3	3
1	

$144 = 2^4\,3^2$

► El teorema fonamental de l'Aritmètica permet provar altres propietats relatives a la disposició dels nombres primers com la que s'enuncia a continuació.

Propietat Existeixen infinits nombres primers de la forma $4n+3$ amb $n \in \mathbb{N}$.

Suposem que només existís un nombre finit de primers de la forma $4n+3$ amb $n \in \mathbb{N}$. Siguin aquests q_1, q_2,... q_t. Considerem el nombre

$$s = 4\,q_1\,q_2 \cdots q_t - 1 = 4\,(q_1\,q_2 \cdots q_t - 1) + 3.$$

El nombre s pertany a la família considerada sent $q_i < s$ per a tot i des de 1 fins a t. Si s és primer ja hem arribat a contradicció. Si s és compost pot factoritzar-se en la forma

$$s = p_1\,p_2\,\cdots\,p_r.$$

El nombre s és imparell i, en conseqüència, tots els seus factors p_i, $1 \leq i \leq r$ són imparells.

Segons l'algoritme de la divisió entera (divisor 4), tot imparell s'escriu en la forma $4\,k+1$ ó $4\,k+3$.

El producte de nombres de la forma $4\,k+1$ és un altre nombre de la mateixa forma. Com que s és de la forma $4\,k+3$, algun dels p_i ha de ser d'aquesta forma.

Suposem que per a cert j $(1 \leq j \leq r)$ es té $p_j = 4\,k' + 3$.

El nombre primer p_j no pot ser cap dels primers q_i ja que aquests divideixen $s+1$ mentre que els p_i divideixen s i dos enters consecutius sempre són primers entre sí.

Hem trobat un nombre primer $p_j = 4\,k' + 3$ diferent dels q_i que havíem suposat que eren els únics primers d'aquesta forma. Contradicció!

Observació La propietat anterior afirma que infinits primers són de la forma $4n+3$ amb $n \in \mathbb{N}$, però no diu que tot nombre d'aquesta forma sigui primer. Només cal pensar $n = 3$ i observar que $4{\cdot}3 + 3 = 15$ no és primer.

MÍNIM COMÚ MÚLTIPLE

Donats dos nombres qualssevol a, $b \in \mathbb{Z}^*$ definim el seu mínim comú múltiple com el menor dels múltiples positius comuns d'ambdós nombres.

Ho denotem

$$D = mcm(a, b).$$

Exemple Determinació del mínim comú múltiple de 24 i 32.

$$\dot{24} = \{\ldots, -24,\ 0,\ 24,\ 48,\ 72,\ \mathbf{96},\ 120,\ 144,\ 168,\ \mathbf{192},\ 216,\ 240,\ \ldots\}$$
$$\dot{32} = \{\ldots, -32,\ 0,\ 32,\ 64,\ \mathbf{96},\ 128,\ 160,\ \mathbf{192},\ 224,\ \ldots\}$$

$$\text{Múltiples positius comuns de 24 i 32} = \{\,96,\ 192,\ \ldots\}$$

En conseqüència, $96 = mcm(24,\ 32)$.

► A partir de la factorització dels nombres enters es pot determinar el seu màxim comú divisor i el seu mínim comú múltiple. Ens ocupem del cas en el qual ambdós nombres són positius. En els demés casos les factoritzacions només difereixen en un $\pm$.

Propietat Suposem dos nombres enters $a,\ b > 1$ la factorització dels quals s'expressa amb els mateixos nombres primers:

$$a = p_1^{\alpha_1}\, p_2^{\alpha_2}\, \cdots p_t^{\alpha_t}, \qquad b = p_1^{\beta_1}\, p_2^{\beta_2}\, \cdots p_t^{\beta_t},$$

on alguna de les α_i o β_i pot ser zero. Llavors:

(i) $mcd(a,\ b) = p_1^{\min\{\alpha_1,\,\beta_1\}}\, p_2^{\min\{\alpha_2,\,\beta_2\}}\, \cdots\, p_t^{\min\{\alpha_t,\,\beta_t\}}$;

(ii) $mcm(a,\ b) = p_1^{\max\{\alpha_1,\,\beta_1\}}\, p_2^{\max\{\alpha_2,\,\beta_2\}}\, \cdots\, p_t^{\max\{\alpha_t,\,\beta_t\}}$;

(iii) com a conseqüència de (i) i (ii): $\boxed{mcd(a,\ b)\, mcm(a,\ b) = a\, b}$

És evident que l'expressió en (i) ofereix un divisor comú d'ambdós nombres. Suposem que existís un altre divisor comú d'a i de b. Necessàriament seria

$$c = p_1^{\gamma_1}\, p_2^{\gamma_2}\, \cdots p_t^{\gamma_t},$$

on cada $\gamma_i \leq \alpha_i$ i cada $\gamma_i \leq \beta_i$. Llavors $\gamma_i \leq \min\{\alpha_i,\ \beta_i\}$ per a $1 \leq i \leq t$ de manera que c divideix al nombre de l'expressió en (i) que resulta ser, per tant, el $mcd(a,\ b)$.

De manera similar es justifica que l'expressió en (ii) és el $mcm(a,\ b)$.

Exemple Determinació de $mcd(400,\ 144)$ i $mcm(400,\ 144)$.

Ja havíem obtingut les factoritzacions d'ambdós nombres. Ara les completem amb els mateixos primers segons l'enunciat de la propietat anterior:

$$400 = 2^4\, 3^0\, 5^2, \qquad 144 = 2^4\, 3^2\, 5^0.$$

Aleshores,

$$mcd(400,\,144) = 2^4\,3^0\,5^0 = 16, \qquad mcm(400,\,144) = 2^4\,3^2\,5^2 = 3600.$$

Els nombres primers estan repetits en ambdues factoritzacions. En formar el *mcd* i el *mcm* es reparteix cadascun dels primers en un o altre nombre. És així que es compleix la igualtat

$$mcd(400,\,144)\,mcm(400,\,144) = 16\cdot 3600 = 57600 = 400\cdot 144.$$

► La fórmula $mcd(a,\,b)\,mcm(a,\,b) = a\,b$ permet determinar el *mcm* o el *mcd* si es coneix l'altre. En particular,

$$\boxed{mcm(a,\,b) = \frac{a\,b}{mcd(a,\,b)}}$$

Suposem que sabem que $mcd(1476,\,900) = 36$ sense tenir les factoritzacions, llavors

$$mcm(1476,\,900) = \frac{1476\cdot 900}{mcd(1476,\,900)} = \frac{1476\cdot 900}{36} = 41\cdot 900 = 36900.$$

► L'obtenció del *mcd* i del *mcm* es pot estendre a tres o més nombres. De la mateixa manera que en la propietat anterior, si escrivim les factoritzacions amb els mateixos nombres primers,

$$a = p_1^{\alpha_1}\,p_2^{\alpha_2}\,\cdots p_t^{\alpha_t}, \quad b = p_1^{\beta_1}\,p_2^{\beta_2}\,\cdots p_t^{\beta_t}, \quad c = p_1^{\gamma_1}\,p_2^{\gamma_2}\,\cdots p_t^{\gamma_t},$$

llavors:

$$\begin{aligned} mcd(a,\,b,\,c) &= p_1^{\min\{\alpha_1,\beta_1,\gamma_1\}}\,p_2^{\min\{\alpha_2,\beta_2,\gamma_2\}}\,\cdots\,p_t^{\min\{\alpha_t,\beta_t,\gamma_t\}} \\ mcm(a,\,b,\,c) &= p_1^{\max\{\alpha_1,\beta_1,\gamma_1\}}\,p_2^{\max\{\alpha_2,\beta_2,\gamma_2\}}\,\cdots\,p_t^{\max\{\alpha_t,\beta_t,\gamma_t\}} \end{aligned}$$

Per exemple, si escrivim els nombres $72 = 2^3\,3^2$, $66 = 2\cdot 3\cdot 11$ i $48 = 2^4\,3$ mitjançant factoritzacions amb els mateixos nombres primers

$$72 = 2^3\,3^2\,11^0, \quad 66 = 2^1\,3^1\,11^1, \quad 48 = 2^4\,3^1\,11^0,$$

obtenim

$$mcd(72,\,66\,48) = 2^1\,3^1\,11^0 = 6, \quad mcm(72,\,66\,48) = 2^4\,3^2\,11^1 = 1584.$$

Ara no es compleix la relació que el producte del *mcd* pel *mcm* sigui igual al producte dels nombres. Aquesta expressió és vàlida exclusivament per a dos nombres.

OBTENCIÓ DELS DIVISORS D'UN ENTER

A partir de la factorització com a producte de primers podem obtenir tots els divisors de qualsevol nombre enter.

Desenvoluparem el mètode sobre un exemple concret. Suposem el nombre

$$720 = 2^4\, 3^2\, 5.$$

Per a construir la taula dels seus divisors enters positius triem un nombre primer que tingui la multiplicitat més alta. En aquest cas, 2.

La primera fila de la taula es construeix amb les potències d'aquest primer des de 0 fins a la seva multiplicitat.

	2^0	2^1	2^2	2^3	2^4
	1	2	4	8	16
3	3	6	12	24	48
3^2	9	18	36	72	144
5	5	10	20	40	80
	15	30	60	120	240
	45	90	180	360	720

La primera fila conté tots els divisors potències del primer 2. Per a obtenir les següents files es considera el següent primer i es multiplica la primera fila per las potències d'aquest, amb exponents que van des de 1 fins a la seva multiplicitat, 2.

Ja hem obtingut les combinacions de les potències de 2 i de 3. Ara es repeteix el procés amb el següent primer, 5. Les files calculades es multipliquen per les potències de 5. L'exponent varia des de 1 fins a la seva multiplicitat que és també 1.

Si hi hagués més primers en la factorització, totes les files calculades es multiplicarien per les seves respectives potències, des de 1 fins a la seva multiplicitat.

Propietat Si el nombre enter $n > 1$ s'expressa com a $n = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$ amb $p_1 < p_2 < \cdots < p_t$ primers, llavors el nombre de divisors enters positius de n és

$$(m_1 + 1)(m_2 + 1) \cdots (m_t + 1)$$

La demostració d'aquesta propietat és constructiva i s'obté de la mateixa manera que s'ha determinat el nombre de divisors positius en un cas particular.

▶ El nombre de divisors enters d'un nombre és el doble de la quantitat establerta en la propietat.

▶ A la taula els divisors no apareixen, en general, en ordre creixent. No obstant, la taula facilita agrupar-los en parelles de manera que el seu producte sigui igual al nombre que es considera.

Exemple Determinació dels divisors enters del nombre 2700.

En primer lloc factoritzem el nombre: $2700 = 2^2\,3^3\,5^2$.

Construïm la taula de divisors positius escollint com a primer primer 3.

	3^0	3^1	3^2	3^3
	1	3	9	27
2	2	6	18	54
2^2	4	12	36	108
5	5	15	45	135
	10	30	90	270
	20	60	180	540
5^2	25	75	225	675
	50	150	450	1350
	100	300	900	2700

El nombre de divisors enters de 2700 és $2\,(2+1)(3+1)(2+1) = 72$.

A partir de la taula es pot descomposar el nombre 2700:

$$2700 = 1 \cdot 2700 = 3 \cdot 900 = 9 \cdot 300 = 27 \cdot 100 = 2 \cdot 1350 = \ldots$$

Exercicis

1. Determinar els 48 divisors enters del nombre 600.
2. Obtenir els divisors positius del nombre 440 i escriure les seves possibles descomposicions com a producte de dos enters positius.