Euler versus Euclides i Fermat

Una aproximació a la reflexió matemàtica

Josep Pla i Carrera

Facultat de Matemàtiques
Universitat de Barcelona

Exposat a Barcelona,
el dia 10 de novembre de 2007

ABEAM

**Icona en memòria de Leonhard Euler,
en el tricentenari del seu naixement**

Índex

Euler versus Euclides i Fermat

Els políedres regulars i la fórmula d'EULER

PART PRIMERA

ELS POLÍEDRES REGULARS I LA FÓRMULA D'EULER

Els constituents de l'univers

Al·legoria sobre els sòlids platònics

il·lustració de MARIA ISABEL BINIMELIS per a la conferència

Els sòlids platònics

(Barcelona, 1996)

de l'amiga, la doctora PILAR BAYER.

Els constituents de l'univers

Recordem que PLATÓ [Atenes, 427 aC–Atenes, 347 aC], al *Menó*, estableix la classificació dels cinc elements de la Naturalesa, en base als cinc sòlids platònics. Són:

El tetràedre és el foc, perquè és el més lleuger.

L'hexàedre o cub és la terra per la seva estabilitat i rigidesa.

L'octàedre era l'aire perquè és livià.

L'icosàedre és l'aigua —rodó—, perquè simbolitzés la fluïdesa.

El dodecàedre —el cinquè— és l'element del Cosmos, l'Univers, la quinta essència, perquè és l'element dels déus.

PLATÓ

Retrat de PLATÓ a l'obra de RAFFAELLO SANZIO [1483–1520], l'*Escola d'Atenes*.

L'original, datat entre 1508 i 1511, és a les *Estances de Rafael* a la ciutat del Vaticà.

La cara és un retrat de MIQUEL ÀNGEL BUONARROTI.

PLATÓ

Atenes, ∼427 aC
Atenes, ∼347 aC

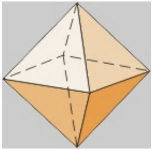
Els constituents de l'univers

Sòlids platònics o Políedres regulars

tetràedre

foc

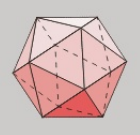
c	v	a
4	4	6



octàedre

aire

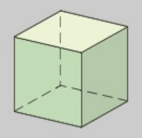
c	v	a
8	6	12



icosàedre

aigua

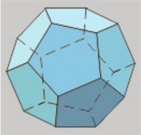
c	v	a
20	12	30



hexàedre

terra

c	v	a
6	8	12



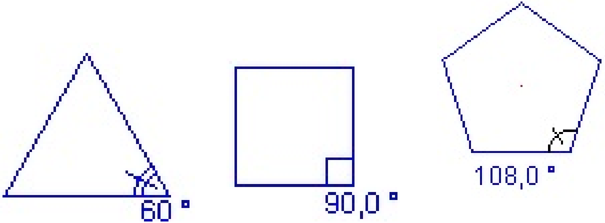
dodecàedre

quinta essència

c	v	a
12	20	30

Els constituents de l'univers

Els políedres regulars possibles



De políedres regulars solament n'hi poden haver cinc —els cinc anteriors— atès el valor dels angles dels polígons regulars que els formen.

Pregunta:

Per què no pot haver-n'hi amb polígons regulars de sis o més costats?

Resposta:

Només cal pensar què passa quan els volem construir amb cartolina, un exercici molt instructiu que tots haguríem de fer, almenys, un cop.

Els constituents de l'univers

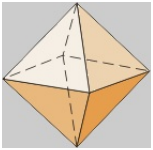
El 26 de novembre de 1750, LEONHARD EULER [1707–1783] llegeix a l'Acadèmia de Berlín el text "Elementa doctrinæ solidorum" (**E230**), publicat l'any 1758, a *Novi Commentarii academiæ scientiarum Petropolitanæ* **4**, 109–140, on estableix la fórmula d'Euler del sòlids platònics:

$$\mathbf{c} + \mathbf{v} - \mathbf{a} = \mathbf{2}$$

tetràedre

foc

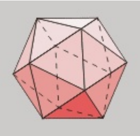
c	v	a
4	4	6



octàedre

aire

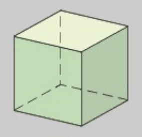
c	v	a
8	6	12



icosàedre

aigua

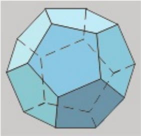
c	v	a
20	12	30



hexàedre

terra

c	v	a
6	8	12



dodecàedre

quinta essència

c	v	a
12	20	30

LEONHARD EULER

LEONHARD EULER

Basilea,
15 d'abril de 1707
Sant Petersburg,
18 de setembre de 1783

La fórmula d'Euler: dues preguntes interessants

Observació:

En el cas dels cinc polídres regulars, constatar la validesa de la fórmula d'Euler —$\mathbf{c} + \mathbf{v} - \mathbf{a} = \mathbf{2}$— és un exercici ben trivial.

Tanmateix podem fer-nos dues preguntes:

La pregunta primera és la pregunta feta a l'inrevés:

Pregunta primera:

Si acceptem que els polídres regulars han de satisfer la fórmula d'Euler, podem demostrar que **només n'hi poden haver cinc**?

La fórmula d'Euler: dues preguntes interessants

Resposta:

De fet, la resposta és un exercici diofantí elemental.

Imaginem què succeeix en cada un dels $\mathbf{v}$ vèrtexs possibles.

Per fer-ho, suposem que hi concorren $\mathbf{n} \geq \mathbf{3}$ polígons de tipus $\mathbf{t}$, on $\mathbf{t} \geq \mathbf{3}$ indica el número d'arestes del polígon regular.

Ara, amb una mica de reflexió, posem les cares i les arestes en funció de $\mathbf{v}$, $\mathbf{n}$ i $\mathbf{t}$. Obtenim: $\mathbf{c} = \frac{\mathbf{v}\times\mathbf{n}}{\mathbf{t}}$ i $\mathbf{a} = \frac{\mathbf{v}\times\mathbf{n}}{\mathbf{2}}$.

En resulta l'equació: $\mathbf{2} \times \mathbf{v} \times \mathbf{n} + \mathbf{2} \times \mathbf{v} \times \mathbf{t} - \mathbf{v} \times \mathbf{n} \times \mathbf{t} = \mathbf{4} \times \mathbf{t}$.

D'on:

$$\frac{\mathbf{1}}{\mathbf{t}} + \frac{\mathbf{1}}{\mathbf{n}} = \frac{\mathbf{1}}{\mathbf{2}} + \frac{\mathbf{1}}{\mathbf{a}}.$$

Ara fem el tipus $\mathbf{t} = \mathbf{3}$, $\mathbf{4}$, $\mathbf{5}$, $\mathbf{6}$, etc. I, per a cada valor de $\mathbf{t}$, resolem, amb solucions positives, l'equació indeterminada que en resulta.

La fórmula d'Euler: dues preguntes interessants

La pregunta segona és:

Pregunta segona:

Si acceptem el concepte de políedre en general, entès com un sòlid de l'espai tancat per cares poligonals, no necessàriament regulars, podem afirmar que també satisfà la fórmula d'Euler?

Tenim dues maneres de respondre la pregunta:

Respostes possibles:

1. **Demostrar**-ne la validesa general.
2. **Proporcionar un exemple** d'un possible políedre regular **en el qual la fórmula d'Euler falli** d'allò més estrepitosament.

La fórmula d'Euler: dues preguntes interessants

Una primera demostració —apartentment prou senzilla— és la que realitzà LOUIS-AUGUSTIN CAUCHY [1789–1857], l'any 1813.

Es basa en dos fets bàsics:

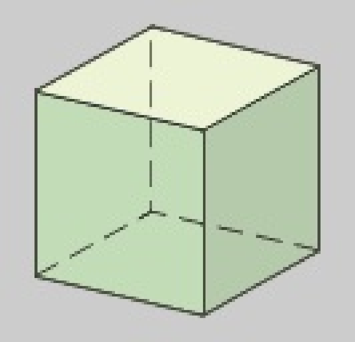
1. El políedre és aplanable.
2. El políedre, un cop aplanat, és triangulable.

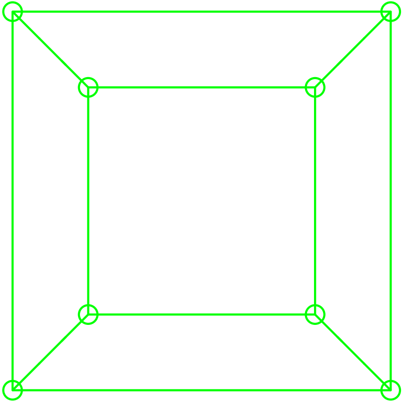
LOUIS-AUGUSTIN CAUCHY

LOUIS-AUGUSTIN CAUCHY

París,
21 d'agost de 1789
París,
23 de maig de 1857

La fórmula d'Euler: dues preguntes interessants

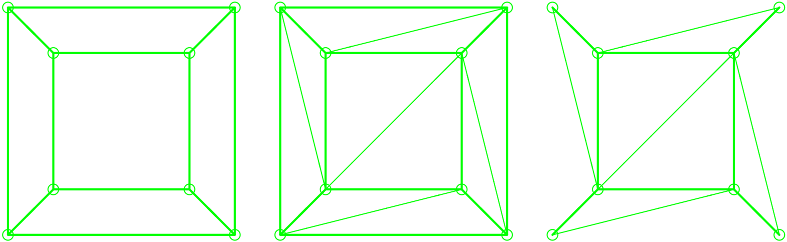




Hem suprimit una cara. Per tant, $\mathbf{c}^* = \mathbf{c} - \mathbf{1}$.

Hem aplanat la figura, tot deformant-la adequadament de manera que les arestes es mantinguin juntes. En la nova figura: $\mathbf{c}^* + \mathbf{v} - \mathbf{a} = \mathbf{1}$.

La fórmula d'Euler: dues preguntes interessants

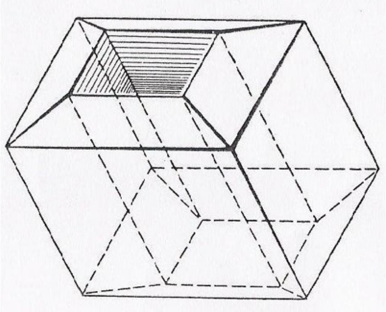


Problema.

Refeu aquest còmput per a cada un dels altres políedres regulars.

La fórmula d'Euler: dues preguntes interessants

Ara bé la definició de políedre general és prou clara i definitòria. Què hi entra i què no hi entra? Hi entra, per exemple, el sòlid següent?



D'una banda, respon a la definició anterior. És un sòlid tancat per polígons.

Però, si li comptem les cares, les arestes i els vèrtexs, tenim: $\mathbf{c} = \mathbf{16}$, $\mathbf{a} = \mathbf{32}$, $\mathbf{v} = \mathbf{16}$. És clar, doncs, que $\mathbf{c} + \mathbf{v} - \mathbf{a} = \mathbf{16} + \mathbf{16} - \mathbf{32} = \mathbf{0}$.

No satisfà la fórmula d'Euler.

Una de dos:

(1) O no és un políedre; (2) Un políedre no té perquè complir-la.

La fórmula d'Euler: la resposta

El sòlid anterior, o bé no és aplanable o bé no és triangulable perquè no compleix la demostració de Cauchy, que es basa en aquests dos fets fonamentals.

Amb aquesta anàlisi hem obert la capsa dels trons. No hi ha políedres i prou. Els políedres —de fet, els sòlids de l'espai de tres dimensions— **tenen assignat un valor**, que actualment es coneix amb el nom de característica d'Euler-Poincaré del sòlid en qüestió.

El nom compost es deu a les aportacions del matemàtic francès del segle XIX HENRI POINCARÉ [1854–1912] el qual en donà la clau, tot iniciant l'estudi —i els invariants— de la topologia algèbrica.

Si voleu una anàlisi detallada i completa d'aquesta evolució conceptual, podeu consultar la tesi doctoral —ara ja té uns quants anys— d'IMRE LAKATOS [1922-9174], *Pruebas y refutaciones*. Traducció castellana de CARLOS SOLÍS. Alianza Editorial. Madrid, 1978.

JULES HENRI POINCARÉ

JULES HENRI POINCARÉ

Nancy (Lorraine),
29 d'abril de 1854

París,
17 de juliol de 1912

IMRE LAKATOS

IMRE LAKATOS

Hongria,
9 de novembre de 1922
Londres,
2 de febrer de 1974

Qüestions aritmètiques euclidianes

Part segona

Qüestions aritmètiques euclidianes

Un teorema i un mètode

A VII 30 i 31 dels *Elements*, EUCLIDES estableix:

Teorema.

Tot nombre és primer o divisible per un nombre primer.

La demostració és d'una gran elegància i es basa en el fet que, **per definició**: Tot nombre N o és primer o és compost.

Demostració.

1. Si N és primer, ja hem acabat.
2. Si N és compost, $N = N_1 \times N_2$, on $N_i < N$, $i = 1, 2$, i aleshores
    1. Si N_1 és primer, ja hem acabat.
    2. Si N_1 és compost, $N_1 = N_{11} \times N_{12}$, on $N_{1j} < N_1$, $j = 1, 2$, aleshores
        1. Si N_{11} és primer, ja hem acabat.
        2. Si N_{11} és compost, $N_{11} = N_{111} \times N_{112}$, , on $N_{11k} < N_{11}$, $k = 1, 2$, etc.

Un teorema i un mètode

S'obté una successió decreixent de nombres naturals

$$N > N_1 > N_{11} > N_{111} > \cdots > N_{11\cdots 1} > \cdots$$

S'ha d'aturar i, per tant, s'ha d'arribar, amb un nombre finit de passos, a un cert nombre $N_{11\cdots 1}$, **necessàriament primer**. ∎

EUCLIDES D'ALEXANDRIA

De la mateixa obra de RAFFAELLO.

EUCLIDES D'ALEXANDRIA

?, ∼325 aC
Alexandria (Egipte), ∼265 aC

Un teorema i un mètode

La demostració d'EUCLIDES amaga un mètode matemàtic que serà represès i posat de relleu amb tot el seu potencial per PIERRE DE FERMAT.

A la carta d'agost de 1659, adreçada a PIERRE DE CARCAVI perquè la faci arribar a CHRISTIAAN HUYGENS, l'anomena el mètode del descens infinit. I diu: *M'ha servit per resoldre un grapat de problemes*:

1. *Cap nombre de la forma* $3n-1$ *no és de la forma* p^2+3q^2.
2. *No hi ha cap triangle pitagòric aritmètic d'àrea igual a un quadrat*.
3. *No hi ha cap solució entera per a l'equació* $x^3+y^3=z^3$.
4. *Tots els nombres de la forma* $2^{2^k}+1$ *són primers*.
5. *L'equació* $y^2-Nx^2=1$, *on* N *no és un quadrat perfecte, té infinites solucions enteres*.
6. ***Tot nombre primer** de la forma* $4k+1$ *és la suma de **dos** quadrats*.
7. ***Tot nombre natural*** N *és la suma de **quatre o menys** quadrats*.

PIERRE DE FERMAT

PIERRE DE FERMAT

Beaumont-de-Lomagnes,
17 d'agost de 1601
Castres,
12 de gener de 1665

El mètode del descens infinit en FERMAT i EULER

Per copsar la diferència entre FERMAT i EULER en la manera d'usar el mètode del descens infinit, l'usarem per veure que $\sqrt{2}$ **és irracional**.

Inici de la demostració.

Observem que $1 = (\sqrt{2}+1) \times (\sqrt{2}-1)$. D'on: $\sqrt{2}+1 = \frac{1}{\sqrt{2}-1}$.

Suposem que $\sqrt{2}$ és racional. En resulta, atès que $1 < \sqrt{2} = \frac{p}{q} < 2$:

1. $\sqrt{2} = \dfrac{1}{\sqrt{2}-1} - 1 = \dfrac{1}{\frac{p}{q}-1} - 1 = \dfrac{q}{p-q} - 1 = \dfrac{2q-p}{p-q} = \dfrac{p_1}{q_1}$.
2. $p_1 > 0$ i $q_1 > 0$.
3. $q_1 < q$.

El mètode del descens infinit en FERMAT i EULER

El raonament de FERMAT

Si existeix una fracció $\frac{p}{q} = \sqrt{2}$, n'existeix una altra $\frac{p_1}{q_1} = \sqrt{2}$, amb $q > q_1 > 0$.

Amb la fracció $\frac{p_1}{q_1} = \sqrt{2}$ construïm la fracció $\frac{p_2}{q_2} = \sqrt{2}$, amb $q > q_1 > q_2 > 0$.

I després una altra i així iteradament. Així **obtenim la successió decreixent il·limitada**:

$$q > q_1 > q_2 > \cdots > p_k > \cdots 0.$$

Impossible!!!

El raonament d'EULER

Si existeix una fracció $\frac{p}{q} = \sqrt{2}$, n'existeix una $\frac{p_0}{q_0}$ que **té denominador mínim** entre tots les fraccions $\frac{p}{q} = \sqrt{2}$.

Amb aquesta fracció $\frac{p_0}{q_0}$, de denominador mínim, en podem fabricar $\frac{p_1}{q_1} = \sqrt{2}$, amb $q_1 < q_0$.

Impossible!!!

Una conjectura doble

Conjectura euclidiana (?)

Amb els nombres primers 2, 3, 5, 7, 11, 13, 17, etc., fem els euclidians:

$$\begin{aligned} 2+1 &= 3, \\ 2\times 3+1 &= 7, \\ 2\times 3\times 5+1 &= 31, \\ 2\times 3\times 5\times 7+1 &= 211, \\ 2\times 3\times 5\times 7\times 11+1 &= 2\,311. \end{aligned}$$

Tots són primers. **Podríem creure**:

Si agafem els k primers nombres primers $2, 3, 5, \ldots, p_k$, i calculem

$$P_k := 2\times 3\times \cdots \times p_k + 1,$$

*P_k **sempre** és primer.*

Conjectura fermatiana

Les conjectures eren corrents al segle XVII. Per exemple, FERMAT s'adonà —**exercici**— que un nombre de la forma 2^n+1 solament pot ser primer quan l'exponent n és de la forma $n = 2^k$. Calculà els nombres $F_k = 2^{2^k}+1$:

$$\begin{aligned} F_0 &:= 2^{2^0}+1 = 3, \\ F_1 &:= 2^{2^1}+1 = 5, \\ F_2 &:= 2^{2^2}+1 = 17, \\ F_3 &:= 2^{2^3}+1 = 257, \\ F_4 &:= 2^{2^4}+1 = 65\,537. \end{aligned}$$

I afirmà: F_k ***sempre** és primer*.

Un exercici simple

Exrecici

Podríem usar el garbell d'Eratòstenes per determinar els nombres primers més petits, per exemple, que 100, o que 200, o que 1000.

Ara podríem agafar **totes** les col·leccions finites possibles, d'un, dos, tres, etc., nombres primers **i**, amb elles, **construir** el nombre d'Euclides corresponent, i veure quins són primers i quins són compostos.

Podríem fer una anàlisi de la distribució i, si s'escau, intentar de fer una conjectura.

Atenció! Cal que en les col·leccions que agafem **no** hi hagi un cert nombre primer fix, perquè altrament el resultat és evident.

Una conjectura doble

El fet d'analitzar uns quants casos **no** és garantia suficient per poder afirmar —sense escletxa d'error— la validesa de l'afirmació. Pot ser que, si continuem, **allò que hem afirmat esdevingui fals**.

Conjectura euclidiana

Considerem, per exemple, $P_5 =$

$= 2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 =$
$= 30\,031.$

És compost:

De fet, $P_5 = 30\,031 = 59 \times 509$.

Conjectura fermetiana

L'any 1732, publicat l'any 1738, LEONARD EULER demostrà que la conjectura de Fermat **és falsa**.

El nombre de Fermat $F_6 := 2^{2^6} + 1$ **és compost**:

$$2^{2^6} + 1 = 4\,294\,967\,297 = 641 \times 6\,700\,417.$$

Pregunta:

La conjectura torna a donar-se més endevant?

Una conjectura doble

La calculadora WIRIS —o qualsevol altra— pot ser força útil per mirar de respondre la pregunta anterior.

Això no obstant, dediqueu-vos a la conjectura euclidiana, amb més intensitat que no pas a l'altra. La raó és que, de la conjectura de Fermat, ara com ara **no** sabem si n'hi ha cap altre nombre primer diferent dels cinc que va trobar FERMAT. Podríem dir que avui la conjectura va al revés:

Conjectura:

Els únics primers de Fermat són: F_0, F_1, F_2, F_3 i F_4.

Pel que fa a la conjectura d'EUCLIDES us faig la pregunta següent:

Pregunta:

Hi ha d'altres nombres P_k, amb $k \neq 1, 2, 3, 4, 5$, que siguin primers? N'hi ha infinits?

Una demostració impecable

EUCLIDES, però, obvia la conjectura numèrica que hem fet abans, i fa una demostració **impecable**, basant-se en el teorema anterior.

Demostració.

Suposa que, de nombres primers, n'hi ha una col·lecció finita: p_1, p_2, ..., p_n. El nombre d'Euclides E_n: $E_n = (p_1 \times p_2 \times \cdots \times p_n) + 1$.

Com hem dit abans, poden donar-se **dos** casos:

1. El nombre E_n és primer, evidentment més gran que cada un dels de la col·lecció finita p_1, p_2, ...,p_n.
2. El nombre E_n és compost. Aleshores admet un divisor primer q, que no pot ser cap dels anteriors.

N'hi ha, doncs, un que **no pertany** a la col·lecció p_1, p_2,...,p_n.

Teorema d'Euclides (*Elements* IX 20)

Una col·lecció finita de nombres primers mai no els conté tots.

Un exercici simple

Exrecici

Podríem usar el garbell d'Eratòstenes per determinar els nombres primers més petits, per exemple, que 100, o que 200, o que 1000.

Ara podríem agafar **totes** les col·leccions finites possibles, d'un, dos, tres, etc., nombres primers **i**, amb elles, **construir** el nombre d'Euclides corresponent, i veure quins són primers i quins són compostos.

Podríem fer una anàlisi de la distribució i, si s'escau, intentar de fer una conjectura.

Atenció! Cal que en les col·leccions que agafem **no** hi hagi un cert nombre primer fix, perquè altrament el resultat és evident.

ARISTÒTIL, EL FILÒSOF

De l'*Escola d'Atenes*.

ARISTÒTIL

Estagira (Grècia), ∼384 aC
Chalcis (Grècia), ∼322 aC

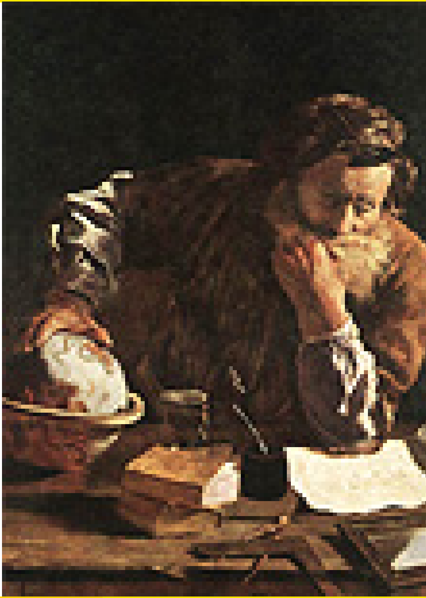
L'infinit en acte **no és possible**. **Només ho és**, de possible, l'infinit en potència.

Com hem vist, això obliga a EUCLIDES a fer una demostració en la qual **no** intervé la totalitat dels nombres primers.

ARQUIMEDES DE SIRACUSA

Pintura de DOMENICO FETTI [1589 –1623], pintor italià, època barroca, realitzada a Màntua l'any 1620.

Comprat per GIOVANNI VENTURA ROSSI per a la col·lecció d'AUGUST III DE SAXÒNIA, és al museu d'art *Alte Meister* de Dresde (Alemanya).



ARQUIMEDES

Siracusa (Sicília), ∼287 aC
Siracusa (Sicília), ∼212 aC

Està constrenyit per la mateixa limitació.

Una limitació invencible

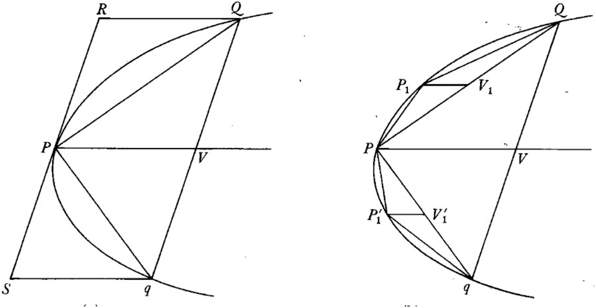
ARQUIMEDES calcula l'àrea S d'un segment de paràbola PQq.

Per aconseguir el valor total $\frac{4}{3}T$ li cal:

(1) El romanent $\frac{1}{3} \times \frac{1}{4^n} T$ de la suma finita $T + \frac{1}{4}T + \cdots \frac{1}{4^n} T$.

Obté: $T + \frac{1}{4}T + \frac{1}{4^2}T + \cdots \frac{1}{4^n}T + \frac{1}{3}\frac{1}{4^n}T = \frac{4}{3}T$.

(2) Un procés de demostració força delicat i complex.



Els nombres perfectes parells

Una curiositat és la següent:

Curiositat

Donat un nombre natural N en determinem tots els divisors, primers o no. Després en calculem la suma

$$\sigma^*(N) = \sum_{d|N, d\neq N} d, \text{ o bé } \sigma(N) = \sum_{d|N} d = \sigma^*(N) + N.$$

Poden donar-se **tres resultats**: $\sigma^*(N)\ [\sigma(N)] \begin{cases} < N\ [< 2N], \\ = N\ [= 2N], \\ > N\ [> 2N]. \end{cases}$

Els grecs excloïen, com a part —i els divisors eren parts—, el propi nombre N. **El tot mai no pot ser una part**. És una de les nocions comunes dels *Elements*.

Els nombres perfectes parells

EUCLIDES tanca les definicions del llibre setè —el primer dels tres llibres aritmètics— amb la definició 22:

Definició 22 [*Elements* VII definició 22].

Un nombre [natural] P és perfecte quan és igual a la suma de les seves parts alíquotes.

El darrer —el llibre IX— amb la proposició:

Teorema 36 [*Elements* IX proposició 36].

Tot nombre que té com a divisors $1, 2, \ldots, 2^{k-1}$ i la suma $p := 1 + 2 + \cdots + 2^{k-1} = \left(2^k - 1\right)$ és un nombre primer, aleshores el darrer de tots per la suma és perfecte.

Els nombres perfectes parells

EUCLIDES, com és habitual en ell, no en dóna cap exemple. Tampoc no fa cap esment als nombres deficients [$\sigma^*(N) < N$], ni als nombres abundants [$\sigma^*(N) < N$].

Per això cal esperar l'*Artmètica* de NICÒMAC DE GERASA.

Conjectures de NICÒMAC DE GERASA

A banda de parlar dels nombres deficients i abundants i establir-ne algunes propietats, ofereix quatre nombres perfectes. Són:

$$6, \quad 28, \quad 496, \quad 8\,128.$$

A més fa tres conjectures:

1. N'hi ha un per a cada ordre decimal.
2. Acaben en 6 o 8,
3. i ho fan de forma alternada.

NICÒMAC DE GERASA

NICÒMAC DE GERASA

Gerasa (avui Jordània), $\sim$60
?, $\sim$120

Els nombres perfectes parells

Exercici de classificació

Podem fer una classificació dels nombres més petits que 100, que 200 o que 1 000 en deficients, perfectes i abundants.

Anàlisi dels nombres perfectes més petits que 100

Entre els nombres més petits que 100 solament trobem dos nombres perfectes [parells] i cap [de senar].

nombre	divisors	sumes parcials	suma
6	$1, 2$	$1 + 2 = 3$ (p)	$2 \times 6 = 12$
	$1 \times 3, 2 \times 3$	$3 + 6 = 9$	$= 3 + 9$
28	$1, 2, 4$	$1 + 2 + 4 = 7$ (p)	$2 \times 28 = 56$
	$1 \times 7, 2 \times 7, 4 \times 7$	$7 + 14 + 28 = 49$	$= 7 + 49$

Els nombres perfectes parells

Anàlisi del comportament dels divisors de $N = 2^{k-1}p$

Ara és fàcil adonar-se que, si $N = 2^{k-1}p$, amb p primer, els únics divisors de N són:

$$\begin{gathered} 1,\, 2, \ldots, 2^{k-1}, \\ 1 \times p,\, 2 \times p, \ldots, 2^{k-1} \times p \end{gathered}$$

I les sumes parcials són:

$$\begin{aligned} s_1 &:= 1 + 2 + \cdots + 2^{k-1} = 2^k - 1, \\ s_2 &:= 1 \times p + 2 \times p + \cdots + 2^{k-1} \times p = \left(2^k - 1\right) \times p. \end{aligned}$$

La suma total és:

$$\sigma = s_1 + s_2 = \left(2^k - 1\right) + \left(2^k - 1\right) \times p = \left(2^k - 1\right)(1 + p).$$

Volem que $\sigma = \left(2^k - 1\right)(1 + p) = 2N = 2^k p$. Però, si el nombre primer p és $p = 2^k - 1$, el resultat **és evident**.

Els nombres de Mersenne: conjectura

Tot rau, doncs, a estudiar els nombres de la forma $M_k = 2^k - 1$ i a veure quan són primers i quan, no.

Conjectura de Mersenne

L'any 1644, MARIN MERSENNE, al *Cogitata Physico-Mathemtica*, afirmà, sense prova ni justificació de cap mena:

El únics nombres $n \leq 257$ per als quals $2^n - 1$ és primer són:

$n = 2, 3, 5, 7, 13, 17, 19, 31, (61), \cancel{67}, (89), (107), 127,$ *i* $\cancel{257}$.

Dues observacions menors

1. Els dos últims tenen 39, i 78 dígits.
2. La correcció i completació de la llista de Mersenne s'aconseguí, amb computadores, l'any 1952.

Aquesta és la raó per la qual s'anomenen nombres de Mersenne.

MARIN MARSENNE

MARIN MERSENNE

Oize, 8 de setembre 1588
París, 1 de setembre de 1648

Primeres contribucions d'EULER

LEONHARD EULER féu, com és característic en ell, aportacions menors de caire generalitzador, i aportacions força més rellevants.

Ara n'esmentarem ara algunes:

Aportacions d'EULER

1. Introdueix, usant la descomposició en factors primers de N: $N = 2^{\alpha_0} 3^{\alpha_1} \cdots p_k^{\alpha_k}$, on els k és natural, i els α_i poden ser nuls:
    1. La funció $n(N)$ que compta els divisors de N.
    2. La funció $\sigma(N)$ que proporciona la suma. dels divisors de N.
2. Aquestes dues funcions són multiplicatives.

Definició de funció multiplicativa

Una funció f, definida en el conjunt $\mathbb{N}$ és multiplicativa si, i només si, $f(M \times N) = f(M) \times f(N)$, per a tot parell M, N que $mcd(M, N) = 1$.

Primeres contribucions d'EULER

Exercicis

1. A partir d'exemples concrets de factorització, com ara per exemple les de 6, 7, 10, 12, 28, 81, 144, etc., —i procedint amb una mica de mètode— determinar les expressions analítiques d'ambdues funcions.
2. Provar que són efectivament multiplicatives.
3. Usar ambdues funcions, amb els nombres més petits que 100, que 200, que 1 000, etc., per veure si hi ha alguna correlació entre el caràcter deficient, perfecte, i abundant dels nombres i el nombre de divisors que tenen.
4. Hi ha infinits nombres deficients. Per què?

Observació

Ara com ara no sabem si n'hi ha infinits de perfectes, o d'abundants. En ambdós casos, la conjectura, és que **sí**.

Contribucions d'EULER

Contribucions d'Euler

L'any 1747, a l'article De Nvmeris amicabilibvs, EULER proporciona dos resultats novells sobre els nombres perfectes. Són:

1. Val el recíproc del teorema d'Euclides sobre els nombres perfectes parells.

Teorema 1

Si P és un nombre perfecte parell, aleshores P és necessàriament de la forma $P := 2^{n-1}(2^n - 1)$, on $2^n - 1$ és primer.

2. Estableix la forma que conté els nombres perfectes senars:

Teorema 2

Si Q és un nombre perfecte senar, aleshores necessàriament Q és de la forma $Q := (4m+1)^{4\lambda+1}RR$, on $4m+1$ és un nombre primer i R un nombre senar.

Una carta molt notable de FERMAT

Carta de FERMAT

En una carta de juny de 1640, adreçada a MERSENNE, PIERRE DE FERMAT comença amb una taula.

Aquesta tècnica, que era molt usual a l'època —i que, per desgràcia hem oblidat,— consistia a treballar per indici.

La carta de PIERRE DE FERMAT diu textualment:

> *6. Un resultat que m'estimo moltíssim és l'abreujament que he trobat per als nombres perfectes, al qual estic disposat a mantenir-m'hi vinculat, si el senyor Frenicle no em fa partícip del seu mètode.*

n	2	3	4	5	6	7	8	9	10	11	12	13
M_n	3	7	15	31	63	127	255	511	1 023	2 047	4 095	81 091
E_n	2	6	14	30	62	126	254	510	1 022	2 046	4 094	81 090

on $M_n = 2^n - 1$ i $E_n = 2^n - 2 = 2\left(2^{n-1} - 1\right)$.

Una carta molt notable de FERMAT

Carta de FERMAT

Els nombres com ara M_n, amb $n = 2, 3, 4$, etc., s'els anomenen el radicals dels nombres perfectes, atès que, sempre que són primers, els produeixen.

Heusací tres proposicions que he trobat, damunt de les quals penso construir quelcom d'important.

1. *Quan l'exponent d'un radical és compost, el radical també ho és.*
2. *Quan l'exponent és un nombre primer, afirmo que el seu radical menys una unitat és mesurat pel doble de l'exponent.*
3. *Quan l'exponent és un nombre primer, afirmo que el seu radical només pot ser mesurat pels nombres primers que són una unitat més grans que un múltiple del doble del exponent o que el doble de l'exponent.*

Són tres proposicions molt boniques que he trobat i he demostrat, però amb esforç.

Síntesi de la carta de Fermat

$$M_n = 2^n - 1 \quad \text{és} \quad \begin{cases} \text{compost}, & \text{si } n \text{ és compost}. \\ \text{indeterminat}, & \text{si } n \text{ és primer (!!!!)}. \end{cases}$$

Si n és primer i $M_n = 2^n - 1$ és compost, els **únics** divisors primers que admet M_n són els de la forma $2\lambda n + 1$ (!!!!).

Si n és primer, $M_n = 2^{n-1} - 1$ és compost, i admet el **divisor primer n** (!!!!). (Cas particular del teorema petit, que enucia en una carta a Mersenne d'octubre del mateix any.)

Síntesi de la carta de FERMAT

Aportacions de FERMAT i EULER

Durant molt de temps hom creia que, si n era primer, $M_n = 2^n - 1$ també, malgrat que això falla quan $n = 11$. No sabem si NICÒMAC DE GERASA ja ho sabia. A Occident ho aclarí HUDALRICUS REGIUS l'any 1536, malgrat que $2^{11} - 1 = 2\,047 = 23 \times 89$ és molt petit i, per tant, fàcil de factoritzar.

FERMAT usà el seu criteri per veure que $2^{23} - 1$ i $2^{37} - 1$ són compostos, en contra de l'afirmació feta per PEITRO ANTONI CATALDI l'any 1 603.

L'any 1732, EULER usant el criteri de FERMAT i una taula amb els nombres primers inferiors a $46\,339$ provà que $2^{31} - 1$ és efectivament primer. No pogué però amb M_{67}, M_{127} i M_{257}.

L'any 1731, EULER donà una demostració del teorema petit de Fermat que ja havia establert entre 1676 i 680, GOTTFRIED WILHELM LEIBNIZ, però que quedà entre els seus manuscrits i no fou trobada fins ben entrat el segle XX.

La primera demostració, d'EULER, del teorema petit

Ítems de la primera demostració d'EULER del teorema petit de FERMAT

La demostració rau en dues observacions ben elementals:

1. $$2^p = (1+1)^p = 1 + \binom{p}{1} + \binom{p}{2} + \cdots + \binom{p}{p-1} + 1.$$

2. Una propietat del triangle aritmètic o triangle de Pascal, que exposarem sense comentari i la deixarem com a darrer **exercici**.

Aquesta demostració permet una demostració vàlida per a tot nombre natural a, primer amb p, atès que

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-1} a + 1.$$

Una propietat del triangle aritmètic o de Pascal

Exercici

Observeu i aviam què veieu.

$$\begin{array}{ccccccccccccccccc}
&&&&&&&&1&&&&&&&&\\
&&&&&&&1&&1&&&&&&&\\
&&&&&&1&&2&&1&&&&&&\\
&&&&&1&&3&&3&&1&&&&&\\
&&&&1&&4&&6&&4&&1&&&&\\
&&&1&&5&&10&&10&&5&&1&&&\\
&&1&&6&&15&&20&&15&&6&&1&&\\
&1&&7&&21&&35&&35&&21&&7&&1&\\
1&&8&&28&&56&&70&&56&&28&&8&&1\\
\vdots&&\vdots&&\vdots&&\vdots&&\vdots&&\vdots&&\vdots&&\vdots&&\vdots
\end{array}$$

Per què cal imposar que l'exponent p de 2^p o, en general, de $(a+1)^p$ sigui primer? **Què canvia, si p no és primer?**