MAT^2
MATerials MATemàtics
Volum 2023, treball no. 3, 85 pp. ISSN: 1887-1097
Publicació electrònica de divulgació del Departament de Matemàtiques
de la Universitat Autònoma de Barcelona
www.mat.uab.cat/web/matmat

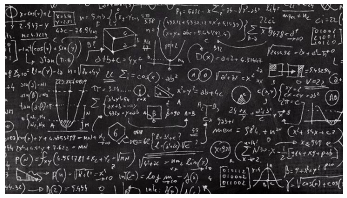
Mètodes de demostració

Armengol Gasull

Els objectius de les matemàtiques són la modelització i comprensió quantitativa i/o qualitativa del món per un costat, i el seu desenvolupament intern per un altra. En aquest treball ens centrarem en aquesta segona vessant.

Quan ens enfrontem a un problema matemàtic i volem avançar en la seva comprensió, arribem a un dels punts clau de les matemàtiques: Com saber si un resultat és cert? Per assegurar-ho el que cal és fer-ne una demostració.





En aquest treball trobarem il·lustrats, mitjançant una llarga sèrie d'exemples, diferents mètodes de demostració. Tot i que tots estan basats en la concatenació de raonaments lògics, els classificarem en diferents aproximacions centrant-nos en la part preponderant de la deducció. Els mètodes més usats es poden catalogar com:

- Raonaments;
- Inducció;
- Càlculs.

Dedicarem una secció a cadascun d'ells. A la Secció 4, que titulem "Altres Mètodes", inclourem exemples de proves basades en mètodes de demostració que no acaben d'encaixar en cap de les tres categories principals. Així farem demostracions que utilitzen el principi de les caselles, el mètode del descens infinit de Fermat, proves combinatòries, proves per invariància o paritat, proves geomètriques i proves sense paraules.

És materialment impossible ser exhaustius i ens deixem al tinter altres mètodes com per exemple les *proves assistides per ordinador*. El treball [35] sobre l'anomenat *problema dels quatre colors*, referent a la impossibilitat d'acolorir un mapa de països amb només quatre colors seguint certes regles naturals, mostra un cas paradigmàtic.

Per a veure altres classificacions de mètodes es poden consultar, per exemple, els índexs dels llibres [4, 17, 19, 24, 45, 46].

Com a cloenda incloem una secció amb un recull de *demostracions falses*, també anomenades *fal·làcies matemàtiques*.

Cada secció d'aquest treball es pot llegir de manera quasi totalment independent de les altres. Al final del text hi ha un índex més detallat del contingut d'aquest article.

Voldríem incidir en que la classificació de les demostracions no és gens fàcil ja que de vegades els mètodes es barregen com veurem en alguns casos. Així, per exemple, les demostracions sobre la irracionalitat del número e o la del càlcul d'una integral definida racional, que es presenten, respectivament, com a proves per reducció a l'absurd (Secció 1.4.7) i per inducció (Secció 2.8) podrien haver estat incloses sense problema com a proves basades en càlculs (Secció 3).

La motivació en escriure aquest treball ha estat proporcionar un recull d'exemples útils i interessants per tal d'entendre i consolidar el que significa fer una demostració en matemàtiques. Està dirigit tant a alumnes de Batxillerat i de primers cursos de Facultats de Ciències i Enginyeries, com als seus professors. La major part dels resultats es presentaran en forma de proposicions.

Unes recopilacions molt més ambicioses i de les que hem extret uns quants exemples es poden trobar als llibres [17, 46]. Els llibres [3, 7, 15, 26, 38, 42], els llibres dedicats a les Olimpíades Matemàtiques [4, 8, 19, 24, 25, 43, 45], el treball [36], o la plana web [6] també contenen molts exemples útils. Finalment comentar que també es poden consultar els llibres ja clàssics [1, 28, 29, 30] o el treball [20] i les seves referències. En aquestes darreres recopilacions els resultats s'han triat més amb un criteri de bellesa en les proves que no pas com il·lustració de diferents mètodes de demostració.

1 Raonaments

De manera esquemàtica podem considerar els tipus de raonaments següents:

- **Raonament directe:** En aquestes demostracions hi ha cadenes de deduccions, de manera que de cada afirmació A_i en deduïm una altra, A_{i+1}. Esquemàticament les podem representar dins d'una llista com:

$$A_1 \Longrightarrow A_2 \Longrightarrow A_3 \Longrightarrow \cdots \Longrightarrow A_n.$$

A lògica, s'anomena *modus ponens*, o també *modus ponendo ponens*, expressió en llatí que significa *el mode que en afirmar, afirma.*

- **Equivalència:** En aquest cas hi ha dues afirmacions que s'impliquen mútuament. Esquemàticament

$$A_1 \iff A_2.$$

- **Contra-recíproc:** En lloc de demostrar directament el que ens interessa demostrem una afirmació equivalent. Es basa en dir que cada cop que succeeix A_1 també ha de passar A_2 és el mateix que dir que si no passa A_2 mai podrà passar A_1. Més formalment,

$$(A_1 \implies A_2) \iff (\overline{A_2} \implies \overline{A_1}),$$

on denotem per $\overline{A}$ la negació de l'afirmació A. A lògica, s'anomena *modus tollens*, o també *modus tollendo tollens*, expressió en llatí que significa *el mode que en negar, nega.*

- **Reducció a l'absurd:** Suposem que el contrari del que volem demostrar és cert i a partir d'aquesta suposició acabem arribant a un resultat absurd. Com a conclusió sabem que el que volíem demostrar ha de ser cert. El seu esquema seria

$$(\overline{A} \implies \text{resultat fals o absurd}) \implies A.$$

No s'ha de confondre amb l'anterior. La principal diferència és que l'argumentació es basa fortament en usar $\overline{A}$ per arribar a un resultat fals i no pas en probar que certs resultats impliquen A i que això és contradictori amb que $\overline{A}$ ocorri.

Aquests raonaments transcendeixen les matemàtiques. De fet són la base de la lògica humana. Per aclarir-ho donem un exemple de cadascun d'ells en un context no matemàtic. Per fer les nostres deduccions ens basarem en el fet següent, del qual coneixem la seva veracitat: un objecte uniforme i massís sura a l'aigua només si té densitat menor o igual que la de l'aigua. En particular, si té densitat més alta s'enfonsa.

Exemple de raonament directe: Sabem que les pedres tenen densitat més gran que la de l'aigua. Per tant un raonament directe dirà que si posem una pedra a l'aigua aquesta s'enfonsarà.

Exemple d'equivalència: És equivalent tenir la densitat més gran que l'aigua que enfonsar-se a l'aigua.

Exemple de contra-recíproc: Posem una ploma a l'aigua i no s'enfonsa. D'aquí es dedueix que la ploma té densitat més petita que la de l'aigua.

Exemple de reducció a l'absurd: És ben conegut que la densitat del or és més gran que la de l'aigua. Vull veure si un cert anell (el qual de fet és

de plàstic recobert amb or) és d'or. Suposo que és d'or i per tant sé que si el poso a l'aigua s'enfonsarà. El poso al aigua i no s'enfonsa. Per tant tinc una contradicció amb el que hauria de passar. El motiu és que he començat suposant una cosa que ha portat a una conclusió falsa.

1.1 Raonament directe

En aquesta secció agruparem unes quantes demostracions basades principalment en cadenes de deduccions.

1.1.1 Una fracció irreductible

Es compleix per a tot $k \in \mathbb{N}$ que *la fracció* $\dfrac{15\,k+4}{10\,k+3}$ *és irreductible.*

Provarem que si $\ell \in \mathbb{N}$ és un divisor comú del numerador i el denominador aleshores $\ell = 1$. Per aquest ℓ existeixen $n, m \in \mathbb{N}$ tals que

$$15\,k+4 = n\,\ell \quad \text{i} \quad 10\,k+3 = m\,\ell.$$

Per tant, tenint en compte que $3 \times 3 - 2 \times 4 = 1$, es compleix

$$(3\,m-2\,n)\,\ell = 3\,m\,\ell - 2\,n\,\ell = 3\,(10\,k+3) - 2\,(15\,k+4) = 1.$$

L'expressió de l'esquerra es divisible per ℓ. Per tant la de la dreta, que és 1, també, i com a conseqüència ℓ divideix a 1. Així $\ell = 1$ tal com volíem demostrar.

1.1.2 La mediant de dues fraccions

La fracció $(a+c)/(b+d)$ s'anomena *la mediant* de a/b i c/d.

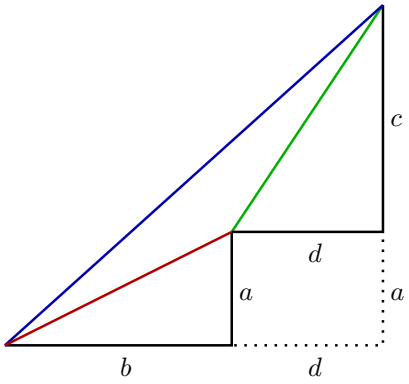


Figura 1: La mediant de dues fraccions

Proposició 1.1. *Siguin $a, b, c, d > 0$ tals que $a/b < c/d$. Aleshores*

$$\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}.$$

Prova. La demostració és una consequència de les dues cadenes d'igualtats següents:

$$\frac{a+c}{b+d} - \frac{a}{b} = \frac{b\,c - a\,d}{b\,(b+d)} = \frac{d}{b+d}\left(\frac{c}{d} - \frac{a}{b}\right) > 0,$$
$$\frac{c}{d} - \frac{a+c}{b+d} = \frac{b\,c - a\,d}{d\,(b+d)} = \frac{b}{b+d}\left(\frac{c}{d} - \frac{a}{b}\right) > 0.$$

□

De fet la Figura 1 també ens proporciona una prova gràfica de la desigualtat ja que el pendent $(a+c)/(b+d)$ de la recta recta superior està entre les de les rectes amb pendents a/b i c/d si es posa el mateix origen a totes tres.

1.1.3 Valors que mai són quadrats perfectes

Proposició 1.2. *Considerem el polinomi $P(n) = n^2 + 7n + 14$. Aleshores, per a cap valor natural $n \in \mathbb{N}$, el número $P(n)$ és un quadrat perfecte.*

Prova. Observem en primer lloc que per a tot $n \in \mathbb{N}$,

$$n^2 + 6n + 9 < n^2 + 7n + 14 < n^2 + 8n + 16,$$

degut a que $n > 0$. Per tant, $(n+3)^2 < P(n) < (n+4)^2$. Com que $n+3 > 0$, prenent arrels quadrades, obtenim que $n + 3 < \sqrt{P(n)} < n + 4$. Com que $\sqrt{P(n)}$ està entre dos enters consecutius, $\sqrt{P(n)}$ no pot ser enter i, equivalentment, $P(n)$ no pot ser mai un quadrat perfecte. □

La Secció 1.2.3 mostra un refinament d'aquest resultat.

1.1.4 Una propietat dels números primers

Si agafem el primer 173, l'elevem al quadrat i el dividim per 24, obtenim quocient 1, és a dir $173^2 = 29929 = 1247 \times 24 + 1$. Per a altres primers com 104729 o 373587883:

$$104729^2 = 10968163441 = 457006810 \times 24 + 1,$$
$$373587883^2 = 139567906324421689 = 5815329430184237 \times 24 + 1.$$

No és una casualitat que la resta sempre sigui 1.

Proposició 1.3. *Per a qualsevol número primer $p \geq 5$, la resta de la divisió de p^2 entre 24 és 1.*

Prova. Hem de demostrar que $p^2 - 1 = (p+1)(p-1)$ és múltiple de 24. Observem els dos fets següents:

- $p+1$ i $p-1$ són ambdós parells consecutius. A més, un d'ells és múltiple de 4 i l'altre és múltiple de 2.
- Si considerem la terna $p-1, p, p+1$, on $p \geq 5$ és primer, segur que o bé $p-1$ o bé $p+1$ és múltiple de 3 (p no té divisors).

Per tant, per a primers $p \geq 5$,

$$p^2 - 1 = (p-1)(p+1) = 2 \times 4 \times 3 \times k = 24 \times k,$$

per a algun $k \in \mathbb{N}$, tal i com volíem demostrar. □

Observi's que usant el contra-recíproc del que hem demostrat s'obté un criteri de no primalitat, ja que el que hem provat és equivalent a: *si per $n \geq 5$ la resta de dividir n^2 entre 24 no és 1, aleshores n no és primer.*

1.1.5 Un gran forat sense números primers

Euclides ja va demostrar que hi ha infinits números primers. Una idea de quants n'hi ha la dóna el resultat de Hadamard i de la Vallée-Poussin, provat al 1896, que diu que, si $\pi(n)$ denota el nombre de números primers menors o iguals que n,

$$\lim_{n\to\infty} \frac{\pi(n)\ln(n)}{n} = 1,$$

és a dir que per a n gran, $\pi(n) \approx \frac{n}{\ln(n)}$. Per altra banda, demostrarem a continuació que *per a tot $m \in \mathbb{N}$ hi ha m números consecutius tals que cap d'ells és primer.* Per a fer-ho podem prendre els m números consecutius:

$$(m+1)!+2,\ (m+1)!+3,\ \ldots,\ (m+1)!+m,\ (m+1)!+m+1.$$

Aleshores, per a cada $k \in \{2, \ldots, m+1\}$, $(m+1)!+k$ és divisible per k, ja que $(m+1)!$ conté el factor k. Per tant, cap dels m números anteriors és primer, tal i com volíem provar.

1.1.6 Polinomis amb valors primers

El polinomi $Q(n) = n^2+n+41$, donat per Euler al 1772, és força curiós ja que proporciona valors primers per a $n = 0, 1, 2, \ldots, 38, 39$. Així, per exemple, $Q(0) = 41$, $Q(39) = 1601$, però $Q(40) = 40^2 + 40 + 41 = 40 \times 41 + 41 = 41^2$ ja no és primer. Goldbach, l'any 1752 va demostrar el resultat següent:

Proposició 1.4. *No hi ha cap polinomi amb coeficients enters P tal que el número $P(n)$ és primer per a tot $n \in \mathbb{N}$.*

Prova. Prenem $m = P(0)$. Aleshores, clarament, si $m \neq 0$, $P(m)$ no és primer ja que, si s'escriu $P(x) = a_k\, x^k + a_{k-1}\, x^{k-1} + \cdots + a_2\, x^2 + a_1\, x + a_0$, amb $a_j \in \mathbb{Z}$, es compleix que

$$P(m) = a_k\, m^k + a_{k-1}\, m^{k-1} + \cdots + a_2\, m^2 + a_1\, m + m$$

és divisible per m ja que tots els seus sumands ho són. Si $P(0) = m = 0$ aleshores $P(n)$ és divisible per n per a tot $n \neq 0$. □

1.1.7 Una expressió que mai és un número primer

Proposició 1.5. *Per a $n \geq 2$ natural, el número $n^4 + 4^n$ mai és primer.*

Prova. Per a n parell el resultat és trivial ja que $n^4 + 4^n$ sempre és parell. Per a demostrar-ho quan $n = 2k + 1, k \geq 1$, és senar usarem la igualtat següent, deguda a la matemàtica francesa Sophie Germain (1776–1831),

$$\begin{aligned} a^4 + 4\,b^4 &= a^4 + 4\,a^2\,b^2 + 4\,b^4 - 4\,a^2\,b^2 = \left(a^2 + 2\,b^2\right)^2 - (2\,a\,b)^2 \\ &= (a^2 + 2\,b^2 + 2\,a\,b)(a^2 + 2\,b^2 - 2\,a\,b). \end{aligned}$$

Per tant és té

$$\begin{aligned} n^4 + 4^n &= n^4 + 4 \cdot 4^{2k} = (2\,k+1)^4 + 4\left(2^k\right)^4 \\ &= \left((2\,k+1)^2 + 2\left(2^k\right)^2 + 2\,(2\,k+1)\,2^k\right) \\ &\qquad \times \left((2\,k+1)^2 + 2\left(2^k\right)^2 - 2\,(2\,k+1)\,2^k\right), \end{aligned}$$

fet que implica que $n^4 + 4^n$ no és primer, tal i com volíem veure. □

1.1.8 Condició de creixement

Recordem que una funció $f : \mathcal{I} \longrightarrow \mathbb{R}$, on $\mathcal{I} \subset \mathbb{R}$ és un interval obert, es diu que és creixent a $\mathcal{I}$ si per a qualssevol $x, y \in \mathcal{I}$ tals que $x < y$, es compleix $f(x) < f(y)$.

Proposició 1.6. *Sigui $f : \mathcal{J} \longrightarrow \mathbb{R}$ una funció derivable al punt $a \in \mathcal{J}$ i creixent en un entorn $\mathcal{I}_a$ de a. Aleshores $f'(a) \geq 0$.*

Prova. Com que f és derivable a a, es compleix

$$f'(a) = \lim_{h \to 0} \frac{f(a+h) - f(a)}{h}.$$

En particular, per a calcular $f'(a)$ podem agafar $h > 0$ i prou petit per tal que $a + h \in \mathcal{I}_a$. Per tant tenim que $(f(a+h) - f(a))/h > 0$ i passant al límit obtenim que $f'(a) = \lim_{h \to 0^+} (f(a+h) - f(a))/h \geq 0$ tal i com volíem demostrar. □

Observi's que l'implicació contrària no és certa. Hi ha funcions derivables, amb derivada 0 a un punt però que no són creixents. Per exemple $f(x) = -x^3$ és decreixent, derivable a $x = 0$ i $f'(0) = 0$.

1.1.9 Condició necessària per la convergència d'una sèrie

Donada una sèrie $\sum_{n=1}^{\infty} a_n$, (suma infinita de números reals) es diu que és convergent si considerem les seves sumes parcials $S_m = \sum_{n=1}^{m} a_n$ i es compleix que $\lim_{m\to\infty} S_m = S \in \mathbb{R}$ existeix i és finit. Aleshores s'escriu $\sum_{n=1}^{\infty} a_n = S$.

Un exemple senzill de sèrie convergent és

$$\sum_{n=1}^{\infty} \frac{1}{n(n+1)} = 1,$$

ja que

$$a_n = \frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1}$$

i per tant

$$\begin{aligned} S_m &= a_1 + a_2 + \cdots + a_{m-1} + a_m \\ &= \left(\frac{1}{1} - \frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{3}\right) + \cdots + \left(\frac{1}{m-1} - \frac{1}{m}\right) + \left(\frac{1}{m} - \frac{1}{m+1}\right) \\ &= \left(\frac{1}{1} - \cancel{\frac{1}{2}}\right) + \left(\cancel{\frac{1}{2}} - \cancel{\frac{1}{3}}\right) + \cdots + \left(\cancel{\frac{1}{m-1}} - \cancel{\frac{1}{m}}\right) + \left(\cancel{\frac{1}{m}} - \frac{1}{m+1}\right) \\ &= 1 - \frac{1}{m+1}. \end{aligned}$$

D'aquí, doncs, $S = \lim_{m\to\infty} S_m = 1$. Les sumes infinites en les que hi ha aquest tipus de cancel·lacions s'anomenen *sèries telescòpiques*.

Un exemple de sèrie no convergent el dóna l'anomenada sèrie harmònica $\sum_{n=1}^{\infty} \frac{1}{n}$. Una prova, de voltants del 1350, es basa en la idea següent

$$\begin{aligned} 1 + \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right) & \\ + \left(\frac{1}{9} + \frac{1}{10} + \frac{1}{11} + \frac{1}{12} + \frac{1}{13} + \frac{1}{14} + \frac{1}{15} + \frac{1}{16}\right) + \frac{1}{17} \cdots & \\ > 1 + \frac{1}{2} + \frac{2}{4} + \frac{4}{8} + \frac{8}{16} + \frac{1}{17} + \cdots & \\ = 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{17} + \cdots, & \end{aligned}$$

i s'atribueix al filòsof francès Nicole Oresme (1323–1382). Amb una mica més de feina s'obté que per $k \geq 1$, $S_{2^k} \geq 1 + k/2$. Per tant $\lim_{m\to\infty} S_m = \infty$ i la sèrie és divergent.

Demostrem a continuació que $\lim_{n\to\infty} a_n = 0$ és una condició necessària per a la convergència de $\sum_{n=1}^{\infty} a_n$. Observi's que la sèrie harmònica permet veure que aquesta condició no és suficient.

Proposició 1.7. *Si* $\sum_{n=1}^{\infty} a_n$ *és convergent, aleshores* $\lim_{n\to\infty} a_n = 0$.

Prova. Sabem que per a tot $n \in \mathbb{N}$, $S_n - S_{n-1} = a_n$. Prenent límits en aquesta igualtat, com que $\lim_{m\to\infty} S_m = S$, arribem a que $S - S = \lim_{n\to\infty} a_n$. Per tant, $\lim_{n\to\infty} a_n = 0$, tal i com volíem veure. □

El que hem vist en aquesta secció també es pot escriure de manera més esquemàtica com:

$$\sum_{n=1}^{\infty} a_n < \infty \Longrightarrow \lim_{n\to\infty} a_n = 0 \quad \text{i} \quad \lim_{n\to\infty} a_n = 0 \quad \not\Longrightarrow \sum_{n=1}^{\infty} a_n < \infty.$$

1.2 Equivalències

Inclourem en aquesta secció afirmacions que es pot demostrar que són equivalents.

1.2.1 Equació de segon grau

Considerem l'equació $a\,x^2 + b\,x + c = 0$, amb $a \neq 0$ i volem determinar explícitament els valors de x que la compleixen. Tenim la cadena d'equivalències següent

$$\begin{aligned} a\,x^2 + b\,x + c = 0 &\Longleftrightarrow x^2 + \frac{b}{a}x + \frac{c}{a} = 0 \quad (a \neq 0) \\ &\Longleftrightarrow \left(x + \frac{b}{2\,a}\right)^2 - \frac{b^2}{4\,a^2} + \frac{c}{a} = 0 \\ &\Longleftrightarrow \left(x + \frac{b}{2\,a}\right)^2 = \frac{b^2 - 4\,a\,c}{4\,a^2} \\ &\Longleftrightarrow x + \frac{b}{2\,a} = \pm\frac{\sqrt{b^2 - 4\,a\,c}}{2\,a} \\ &\Longleftrightarrow x = \frac{-b \pm \sqrt{b^2 - 4\,a\,c}}{2\,a}, \end{aligned}$$

que dóna la coneguda fórmula per resoldre aquestes equacions.

1.2.2 Un número més el seu invers

Donat qualsevol $x > 0$ demostrarem que $x + 1/x \geq 2$, desigualtat que a primera vista no és evident. Tenim

$$x + \frac{1}{x} \geq 2 \iff \frac{x^2+1}{x} \geq 2 \iff x^2 + 1 \geq 2\,x \quad (x > 0)$$
$$\iff x^2 - 2\,x + 1 \geq 0 \iff (x-1)^2 \geq 0.$$

Com que la darrera desigualtat és trivialment certa, totes les altres, que són equivalents, també ho són. De fet la prova mostra també que la desigualtat és estricta per a qualsevol $x \neq 1$.

1.2.3 Valors que mai són quadrats perfectes, continuació

Aquí refinarem els resultats de la Secció 1.1.3.

Proposició 1.8. *Considerem el polinomi $P(n) = n^2 + 7n + 14$. Aleshores per a $n \in \mathbb{Z}$ el número $P(n)$ és un quadrat perfecte si, i només si, n és -2 o -5.*

Prova. A la Secció 1.1.3 ja hem demostrat que per a $n \in \mathbb{N}$, $P(n)$ mai és un quadrat perfecte. Ara bé, com que

$$P\Big(-m - \frac{7}{2}\Big) = P\Big(m - \frac{7}{2}\Big) = m^2 + \frac{7}{2}$$

i ja sabem que mai és un quadrat perfecte per a $m = (2\,k+1)/2$ i $k \geq 4$, el mateix passa per a $m = -(2\,k+1)/2$ i $k \geq 4$. En resum, mai és un quadrat perfecte per a $n \in \mathbb{Z}$ i, o bé $n \geq 1$, o bé $n \leq -8$. Per a $n \in \{-7, -6, \ldots, -1, 0\}$, mirant cas per cas obtenim que els únics quadrats perfectes són $P(-2) = P(-5) = 2^2$, tal i com volíem demostrar. □

1.2.4 Criteris de divisibilitat

Proposició 1.9. *(i) Un número natural és divisible per 3 si, i només si, la suma de les seves xifres és divisible per 3.*

(ii) Un número natural és divisible per 9 si, i només si, la suma de les seves xifres és divisible per 9.

(iii) Un número natural és divisible per 11 si, i només si, la suma de les seves xifres situades a llocs parells menys la suma de les seves xifres situades a llocs senars és divisible per 11.

Prova. Un número n és divisible per k si, i només si, n objectes es poden agrupar en grups de k elements (de fet, exactament en n/k grups). Si denotem per $n_\ell, n_{\ell-1}, \ldots, n_1, n_0$, amb tots els $n_i \in \mathbb{N}, 0 \leq n_i \leq 9$, les $\ell + 1$ xifres ordenades d'un número natural n tenim que

$$n = n_\ell \times 10^\ell + n_{\ell-1} \times 10^{\ell-1} + \cdots + n_2 \times 10^2 + n_1 \times 10^1 + n_0 \times 10^0.$$

Així, per saber si hi ha divisibilitat, un camí natural és veure primer el que passa quan ens centrem en números de la forma 10^j, $j = 0, 1, \ldots, \ell$.

Les afirmacions següents no són difícils de demostrar:

(I) Si agrupem 10^j objectes en grups de 3, sempre sobra un element. Més matemàticament, $10^j - 1$ sempre és divisible entre 3. Aquesta darrera afirmació és conseqüència de les igualtats

$$10 = 3 \times 3 + 1,\ 10^2 = 3 \times 33 + 1, \ldots, 10^6 = 3 \times 333\,333 + 1, \ldots$$

(II) De manera similar, si agrupem 10^j objectes en grups de 9, sempre sobra un element, ja que

$$10 = 9 + 1,\ 10^2 = 9 \times 11 + 1, \ldots, 10^6 = 9 \times 111\,111 + 1, \ldots$$

(III) Finalment, si agrupem 10^{2j} en grups d'11, sempre sobra un element, ja que

$$10^0 = 11 \times 0 + 1,\ 10^2 = 11 \times 9 + 1,\ 10^4 = 11 \times 909 + 1,$$
$$10^6 = 11 \times 90909 + 1,\ 10^8 = 11 \times 9090909 + 1, \ldots,$$

mentre que si agrupem 10^{2j+1} en grups de 11, sempre en falta un per tenir tots els grups plens, ja que

$$10^1 = 11 - 1,\ 10^3 = 11 \times 91 - 1,\ 10^5 = 11 \times 9091 - 1,$$
$$10^7 = 11 \times 909091 - 1,\ 10^9 = 11 \times 90909091 - 1, \ldots$$

Anem a demostrar (i). Si agrupem tots els n objectes en grups de 3, usant (I) obtenim que queden tots repartits excepte, en principi, $N = \sum_{j=0}^{\ell} n_j$ elements, ja que de cada bloc format per 10^j objectes en queda un sense agrupar, i hi ha precisament N blocs. Aleshores n serà divisible entre 3 si, i només si, N ho és, tal i com volíem demostrar.

La prova de (ii) es fa exactament igual, usant (II) en lloc de (I).

Per a demostrar (iii) la idea és semblant, però amb petites modificacions. Definim

$$N_p = \sum_{j=0,\,\text{parell}}^{\ell} n_j, \quad N_s = \sum_{j=0,\,\text{senar}}^{\ell} n_j.$$

Raonant de forma anàloga que als punts anteriors, per una banda, tots els objectes que corresponen a potències 10^{2j} queden agrupats en blocs d'11, excepte en principi N_p objectes, mentre que per altra banda falten N_s objectes entre els que provenen dels blocs 10^{2j+1}. Si $N_p \geq N_s$ està clar que n és divisible entre 11 si, i només si, $N_p - N_s$ també ho és, ja que $N_p - N_s$ són precisament els objectes que quedarien per agrupar en blocs d'11. Si $N_p < N_s$

vol dir que faltarien agrupar $N_s - N_p$ objectes per a que tots fossin grups d'11, però aquesta quantitat és divisible entre 11 si, i només si, aquesta resta ho és, de nou tal i com volíem demostrar. □

Així, per exemple, si agafem $n = 57\,753\,267$ i escrivim $p \div q$ per dir que p divideix a q tenim:

- $3 \div 57\,753\,267 \iff 3 \div 42 \iff 3 \div 6$. Per tant 3 divideix a n.
- $9 \div 57\,753\,267 \iff 9 \div 42 \iff 9 \div 6$. Per tant 9 no divideix a n.
- $11 \div 57\,753\,267 \iff 11 \div (21 - 21) = 0$. Per tant 11 divideix a n.

Una prova conceptualment similar a la que hem fet, però més elegant matemàticament consisteix a escriure les igualtats entre números enters mòdul k. En poques paraules això vol dir que s'identifica cada número n amb la resta $0 \leq m < n$, després de dividir entre k, i normalment s'escriu $\overline{n} = \overline{m}$, si no hi ha confusió amb la k, o també $n \equiv m \mod k$. Aquesta operació es comporta perfectament amb la suma, la resta, el producte i la divisió ja que $\overline{p+q} = \overline{p} + \overline{q}$ i $\overline{p \times q} = \overline{p} \times \overline{q}$. Així, per exemple, la prova del punt (i) consisteix a usar $k = 3$, i el que hem explicat a la prova es pot escriure com

$$\begin{aligned}\overline{n} &= \overline{n_\ell} \times \overline{10^l} + \overline{n_{\ell-1}} \times \overline{10^{\ell-1}} + \cdots + \overline{n_2} \times \overline{10^2} + \overline{n_1} \times \overline{10} + \overline{n_0} \times \overline{10^0} \\ &= \overline{n_\ell} + \overline{n_{\ell-1}} + \cdots + \overline{n_2} + \overline{n_1} + \overline{n_0} = \overline{n_\ell + n_{\ell-1} + \cdots + n_1 + n_0}.\end{aligned}$$

El conjunt $\mathbb{Z}$ de tots els números enters quan es consideren mòdul k, se sol denotar com $\mathbb{Z}/k\mathbb{Z}$, i en aquest conjunt que té k elements $\{\overline{0}, \overline{1}, \ldots, \overline{k-1}\}$ hi ha definides la suma i el producte que hem introduït a dalt. Més matemàticament diríem que tant $\mathbb{Z}$ com $\mathbb{Z}/k\mathbb{Z}$ tenen estructura d'*anell*.

De vegades un resultat d'equivalència, com per exemple (i) de la Proposició 1.9 s'enuncia dient: una *condició necessària i suficient* per a que un número natural sigui divisible per 3 és que la suma de les seves xifres sigui també divisible per 3.

1.2.5 Sobre el Teorema de Pitàgores

Anem a demostrar dues equivalències, suposant ja conegut el Teorema de Pitàgores.

La primera és:

Proposició 1.10. *Un triangle amb costats a, b i c amb $a \leq b \leq c$ és rectangle si, i només si, $a^2 + b^2 = c^2$.*

Prova. La demostració consisteix a provar els dos fets següents:

(i) Quan el triangle és rectangle, amb catets a i b, i hipotenusa c, es compleix $a^2 + b^2 = c^2$.

(ii) Si $a^2 + b^2 = c^2$ aleshores el triangle és rectangle.

El punt (i) és precisament el Teorema de Pitàgores que suposem conegut. La Figura 2 il·lustra una de les seves múltiples proves. De fet, està basada en una prova sense paraules, vegeu també la Secció 4.6.5.

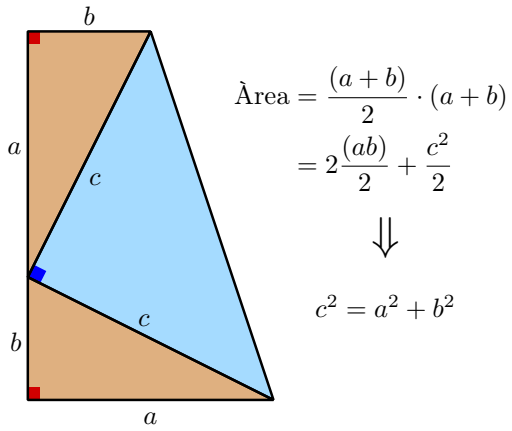


Figura 2: Una prova del Teorema de Pitàgores

Per a demostrar (ii) a continuació veurem quants triangles amb costats a, b i c es poden construir. Per això prenem un segment de longitud c i extrems als punts $p_i = (x_i, y_i), i = 1, 2$, que seran dos dels vèrtexs del triangle. El tercer vèrtex és a $q = (x, y)$ i ha d'estar a distància a de p_1 i a distància b de p_2. És a dir (x, y) ha de ser solució del sistema

$$\begin{cases} (x - x_1)^2 + (y - y_1)^2 = a^2, \\ (x - x_2)^2 + (y - y_2)^2 = b^2. \end{cases}$$

Geomètricament, les solucions són els talls de dues circumferències. Restant les equacions, obtenim el sistema equivalent

$$\begin{cases} (x - x_1)^2 + (y - y_1)^2 = a^2, \\ 2(x_2 - x_1)x + 2(y_2 - y_1)y = a^2 - b^2 + x_2^2 - x_1^2 + y_2^2 - y_1^2. \end{cases}$$

Com que $x_1 = x_2$ i $y_1 = y_2$ no es poden donar simultàniament, aïllant x o y de la segona equació i substituint el seu valor a la primera obtenim que el sistema té com a molt dues solucions. Com que les que corresponen als dos triangles rectangles amb costats a, b i c en els que el punt q és a una o l'altra banda de la recta que passa per p_1 i p_2 són solucions, arribem a la conclusió de que aquestes són les úniques solucions del problema. Per tant, el triangle és rectangle tal i com volíem demostrar. □

La segona equivalència és:

Proposició 1.11. *El Teorema de Pitàgores és equivalent a que, per a tot* $x \in \mathbb{R}$, $\sin^2(x) + \cos^2(x) = 1$.

Prova. En primer lloc demostrarem que el Teorema de Pitàgores implica la relació trigonomètrica. Per la definició de sinus i cosinus, $\sin(0) = 0$, $\cos(0) = 1$, $\sin(\pi/2) = 1$ i $\cos(\pi/2) = 0$. A més, per a $x = \theta \in (0, \pi/2)$ podem construir un triangle rectangle amb catets $\sin(x)$ i $\cos(x)$, amb hipotenusa 1, vegeu la Figura 3. Aleshores $\sin^2(x) + \cos^2(x) = 1$. Per a demostrar-la per a tot $x \in \mathbb{R}$, es poden fer servir les propietats del sinus i el cosinus. Per exemple, per a $x \in [\pi, 3\pi/2]$ es compleix degut a que $\sin(x + \pi) = -\sin(x)$ i $\cos(x + \pi) = -\cos(x)$. Per a cobrir tot $[0, 2\pi]$ podem usar altres relacions. Finalment, per ser funcions 2π periòdiques, la relació és certa per a tot número real.

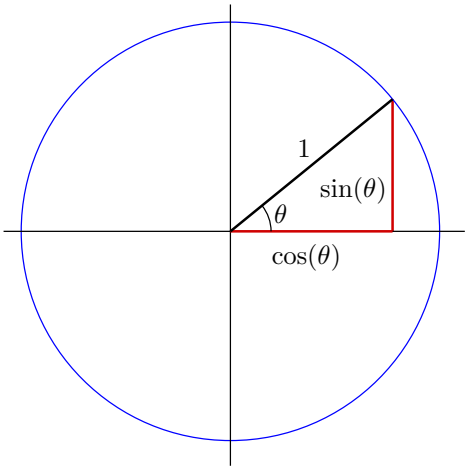


Figura 3: Definició de $\sin(\theta)$ i $\cos(\theta)$

Per a demostrar el Teorema de Pitàgores a partir de la relació, agafem un triangle rectangle qualsevol, amb catets a i b, i hipotenusa c. De nou, per la definició de sinus i cosinus, $\sin(x) = a/c$ i $\cos(x) = b/c$. Aleshores

$$1 = \sin^2(x) + \cos^2(x) = \left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = \frac{a^2 + b^2}{c^2}.$$

Per tant $a^2 + b^2 = c^2$, tal i com volíem veure. □

1.2.6 Una equació diferencial simple

És ben conegut que si $g(x) = \mathrm{e}^{k\,x}$ aleshores la seva derivada és $g'(x) = k\,\mathrm{e}^{k\,x} = k\,g(x)$. Volem demostrar que l'afirmació recíproca també es satisfà.

Per això usarem que si una funció derivable h té derivada idènticament zero en un interval $\mathcal{I}$, aleshores és una funció constant en aquest interval. Aquesta darrera afirmació és conseqüència del *Teorema de valor mitjà,* que diu que si $h : [a,b] \to \mathbb{R}$ és una funció contínua en un interval tancat $[a,b]$, i derivable en l'interval obert (a,b), aleshores existeix $c \in (a,b)$ tal que $h(b)-h(a) = h'(c)\,(b-a)$. En efecte, pel Teorema de valor mitjà, si $h'\big|_{\mathcal{I}} = 0$, per a tot $a, b \in \mathcal{I}$ es compleix $h(a) - h(b) = h'(c)\,(b-a) = 0\,(b-a) = 0$.

Proposició 1.12. *Sigui $f : \mathbb{R} \longrightarrow \mathbb{R}$ una funció derivable. Aleshores es té $f'(x) = k\,f(x)$ si, i només si, $f(x) = c\,\mathrm{e}^{k\,x}$, per a una certa constant $c \in \mathbb{R}$.*

Prova. Com acabem d'observar, si f és de la forma esmentada compleix $f'(x) = k\,f(x)$. Anem a demostrar la implicació contraria. Sigui f una funció complint $f'(x) = k\,f(x)$. Considerem $h(x) = f(x)\,\mathrm{e}^{-k\,x}$. Aleshores

$$h'(x) = f'(x)\,\mathrm{e}^{-k\,x} - k\,f(x)\mathrm{e}^{-k\,x} = (f'(x) - k\,f(x))\,\mathrm{e}^{-k\,x} = 0.$$

D'on obtenim que $h(x) \equiv c$, per a una certa constant $c \in \mathbb{R}$, ja que, com hem vist abans de la proposició, les úniques funcions amb derivada idènticament 0 són les funcions constants. Per tant $f(x) = c\,\mathrm{e}^{k\,x}$ tal i com volíem veure. □

1.2.7 Les matrius que commuten amb totes

Demostrarem el resultat següent per matrius 2×2 amb coeficients reals o complexos tot i que és cert per matrius $n \times n$, per a tot $n \in \mathbb{N}$. La idea que fem servir en la prova quan $n = 2$ també pot ser usada, adaptant-la adequadament, pel cas general.

Proposició 1.13. *Sigui A una matriu 2×2. Aleshores $AB = BA$ per a tota matriu B si, i només si, $A = a\,\mathrm{Id}$, on $\mathrm{Id} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.*

Prova. Quan $A = a\,\mathrm{Id}$ és clar que

$$A\,B = a\,\mathrm{Id}\;B = a\,B = B\,a = B\,a\,\mathrm{Id} = B\,A,$$

per a tota matriu B.

Anem a demostrar la implicació contraria.

Com que $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ commuta amb totes les matrius B, imposem que commuta amb certes matrius concretes. Així tenim que

$$\begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 0 & c \end{pmatrix}$$

i, per tant, $c = 0$ i $d = a$. Fent uns càlculs semblants però amb $B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ arribem a que $b = 0$ i per tant $A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = a\,\mathrm{Id}$, tal i com volíem provar. □

1.2.8 Involucions

Donat un conjunt qualsevol X, i una aplicació $f : X \longrightarrow X$, direm que f és una involució si $f(f(x)) = x$ per a tot $x \in X$. Equivalentment, escriurem $f \circ f = \mathrm{Id}$, on $\mathrm{Id} : X \longrightarrow X$, és l'aplicació identitat, és a dir $\mathrm{Id}(x) = x$, per a tot $x \in X$.

Un dels exemples més senzills d'involució és la funció $f(x) = 1/x$, definida a $X = (0, \infty)$.

Proposició 1.14. *Siguin $f, g : X \longrightarrow X$, dues involucions. Aleshores f i g commuten si, i només si, $f \circ g$ també és una involució.*

Prova. Com que f i g són involucions tenim que $f \circ f = \mathrm{Id}$ i també que $g \circ g = \mathrm{Id}$. D'aquestes dues igualtats es dedueix que tant f com g són bijectives i les seves respectives inverses són elles mateixes. En aquesta prova usarem repetidament aquest fet en la cadena d'equivalències següent:

$$\begin{aligned} f \circ g \text{ involució} &\iff f \circ g \circ f \circ g = \mathrm{Id} \iff f \circ f \circ g \circ f \circ g = f \circ \mathrm{Id} \\ &\iff g \circ f \circ g = f \iff g \circ f \circ g \circ g = f \circ g \\ &\iff g \circ f = f \circ g \iff f \text{ i } g \text{ commuten.} \end{aligned}$$

□

1.3 Contra-recíproc

Aquesta secció conté unes quantes demostracions basades en el mètode del contra-recíproc, el qual recordeu ens diu que $(A_1 \Longrightarrow A_2) \Longleftrightarrow (\overline{A_2} \Longrightarrow \overline{A_1})$.

1.3.1 Quan és parell n^2?

Anem a demostrar que *si $n \in \mathbb{N}$ és tal que n^2 és parell, aleshores n també és parell.* És molt més còmode demostrar el contra-recíproc, és a dir, *si $n \in \mathbb{N}$ és senar aleshores n^2 és senar.* Per això, escrivim $n = 2\,k + 1$, amb $k \in \mathbb{N}$. Aleshores $n^2 = 2\,(2\,k^2 + 2\,k) + 1$ és senar tal i com volíem veure.

1.3.2 La prova del 9

Aquesta prova era una eina molt utilitzada en l'època pre-calculadores ja que ens permet testar de manera ràpida possibles errors a les multiplicacions i divisions. Està basada en els càlculs amb números enters mòdul k, dels que ja n'hem parlat al final de la Secció 1.2.4, prenent $k = 9$. Més concretament en el fet següent: Donats $n, m \in \mathbb{N}$, si $\ell = m \times n$ aleshores $\overline{\ell} = \overline{m} \times \overline{n}$. La prova en sí és precisament el contra-recíproc de l'afirmació anterior:

Prova del 9: *Si $\overline{k} \neq \overline{m} \times \overline{n}$ aleshores $k \neq m \times n$.*

El que fa especialment fàcil d'usar aquesta prova és el fet que ja hem demostrat que quan $k = 9$, si

$$n = n_\ell \times 10^l + n_{\ell-1} \times 10^{\ell-1} + \cdots + n_2 \times 10^2 + n_1 \times 10 + n_0 \times 10^0,$$

aleshores $\overline{n} = \overline{n_\ell + n_{\ell-1} + \cdots + n_1 + n_0}$.

Veiem un exemple d'aplicació: $935762 \times 76943 \neq 72001335566$ ja que $\overline{935762} \times \overline{76943} = \overline{32} \times \overline{29} = \overline{5} \times \overline{11} = \overline{5} \times \overline{2} = \overline{1}$ mentre que $\overline{72001335566} = \overline{38} = \overline{11} = \overline{2}$. Observi's que el fet que fent la prova del 9 es compleixi que $\overline{k} = \overline{m} \times \overline{n}$ no garanteix que el resultat de l'operació que volem testar sigui correcte. Així, per exemple $\overline{935762} \times \overline{76943} = \overline{72009335566} = \overline{1}$ però $935762 \times 76943 = 72000335566$.

Sovint es parla de que $\overline{k} = \overline{m} \times \overline{n}$ és una *condició necessària* per tal que $k = m \times n$ però no és una *condició suficient*.

Clarament, a partir del fet que si $k = m \times n + p$ aleshores $\overline{k} = \overline{m} \times \overline{n} + \overline{p}$ s'obté una prova del 9 per la divisió de números enters tenint en compte també el residu.

1.3.3 Una desigualtat senzilla

Anem a provar que *si* $m, n \in \mathbb{Z}$ *i* $m + n \geq 2\,k - 1$, *per a un cert* $k \in \mathbb{Z}$, *aleshores o bé* $m \geq k$, *o bé* $n \geq k$. Potser és adequat comentar aquí que, en el llenguatge científic, quan es parla de que A *o* B *es compleixen* el que es vol dir és que *o bé es compleix* A, *o bé es compleix* B, *o bé es compleixen alhora* A *i* B. En llenguatge col·loquial aquesta tercera opció de vegades s'exclou.

El contra-recíproc del que volem demostrar ens diu que *si* $m, n, k \in \mathbb{Z}$ *són tals que* $m < k$ *i* $n < k$ *aleshores* $m + n < 2\,k - 1$. Aquest fet és quasi trivial, ja que com que m i n són enters sabem que $m \leq k - 1$ i $n \leq k - 1$ i per tant $m + n \leq 2\,k - 2 < 2\,k - 1$, tal i com volíem veure.

1.3.4 Irracionalitat de certs números

Demostrarem que, *per a tot* $k \in \mathbb{N}$, *si* $x > 0$ *és irracional aleshores* $\sqrt[k]{x}$ *també és irracional*. El seu contra-recíproc és molt més fàcil de provar. Aquest afirma: *per a tot* $k \in \mathbb{N}$ *i* $x > 0$, *si* $\sqrt[k]{x}$ *és racional aleshores* $x > 0$ *també és racional*. Per a demostrar-ho tenim que

$$\sqrt[k]{x} = \frac{p}{q} \in \mathbb{Q} \Longrightarrow x = \frac{p^k}{q^k} \in \mathbb{Q},$$

tal i com volíem veure.

1.3.5 Paritat de les ternes pitagòriques

Demostrarem que *si* m, n *i* $p \in \mathbb{Z}$ *i* $m^2 + n^2 = p^2$ *aleshores o bé* m *o bé* n *són números parells*. Anem a demostrar el contra-recíproc de l'afirmació amb

què hem començat aquesta secció. Aquest ens diu: *si $m, n \in \mathbb{Z}$ i ambdós són senars aleshores no hi ha cap $p \in \mathbb{Z}$ tal que* $m^2+n^2 = p^2$. Per a demostrar-la observem que per una banda, com que $m = 2\,k+1$ i $n = 2\,\ell+1$ amb $k, \ell \in \mathbb{Z}$, tenim que

$$m^2 + n^2 = (2\,k+1)^2 + (2\,\ell+1)^2 = 4(k^2+\ell^2+k+\ell)+2, \tag{1}$$

però per l'altra, per a tot $p \in \mathbb{Z}$ hi ha un $j \in \mathbb{Z}$ tal que es compleix una de les dues possibilitats següents:

$$p^2 = \begin{cases} 4j^2 & \text{quan} \quad p = 2j, \\ 4(j^2+j)+1 & \text{quan} \quad p = 2j+1. \end{cases} \tag{2}$$

Aleshores és impossible que existeixi $p \in \mathbb{Z}$ tal que $m^2 + n^2 = p^2$, ja que ambdues expressions tenen resta diferent quan les dividim entre 4, i per tant el resultat queda provat.

Observi's que l'escriptura de les igualtats mòdul $k = 4$, seguint les notacions introduïdes a la Secció 1.2.4, proporciona una prova més compacta: com que m i n són senars, usant (1) tenim que $\overline{m^2+n^2} = \overline{2}$. Per altra banda, usant (2) tenim que $\overline{p} \in \{\overline{0}, \overline{1}\}$. Per tant $\overline{m^2+n^2} \neq \overline{p^2}$ i per tant $m^2 + n^2 \neq p^2$, sigui quin sigui $p \in \mathbb{Z}$ tal com es volia provar.

De fet, Euclides ja va demostrar molt més. Totes les ternes pitagòriques primitives (és a dir, tals que m, n i p compleixen $m^2 + n^2 = p^2$ i no tenen cap divisor comú més gran que 1) venen donades per

$$m = u^2 - v^2, \quad n = 2\,u\,v, \quad q = u^2 + v^2, \tag{3}$$

amb u i v enters positius, $u > v$, coprimers i els dos no senars a la vegada (vegeu per exemple [20, 39]). Potser la més coneguda és $3^2 + 4^2 = 5^2$ i correspon a $u = 2$ i $v = 1$.

1.3.6 Darrera xifra dels números perfectes

Es diu que un número natural ℓ és perfecte si és igual a la suma de tots els seus divisors menors que ell mateix. El més petit és $6 = 1+2+3$. El primer en estudiar-los va ser Euclides, qui ja va demostrar que si $2^n - 1$ és primer, aleshores $\ell = 2^{n-1}(2^n - 1)$ és un número perfecte. Els números primers de la forma $2^n - 1$ s'anomenen primers de Mersenne, en honor al matemàtic francès Marin Mersenne (1588–1648).

De fet, tots els números perfectes coneguts són de la forma $2^{n-1}(2^n - 1)$. Els quatre primers ja els va donar Euclides i són 6, 28, 496 i 8128. Els tres següents eren coneguts al segle XII pel matemàtic egipci Ismail ibn Fallus i són: $33\,550\,336 = 2^{12}\big(2^{13}-1\big)$, $8\,589\,869\,056 = 2^{16}\big(2^{17}-1\big)$ i $137\,438\,691\,328 = 2^{18}\big(2^{19}-1\big)$. Al segle XVIII Euler va provar que tots els números perfectes parells eren de la forma $2^{n-1}(2^n - 1)$. Aquest resultat se

sol conèixer com el Teorema d'Euclides–Euler. Avui en dia es coneixen 51 números perfectes, tots són parells, i el més gran, trobat a finals del 2018, correspon a $n = 82\,589\,933$ i té més de 24×10^6 dígits.

La demostració de la proposició següent usa tant el mètode del contra-recíproc en un dels passos intermedis, com raonaments directes. En general, la majoria de demostracions barregen mètodes diferents.

Proposició 1.15. *Tots els números perfectes parells acaben en* 6 *o en* 8.

Prova. Ja sabem pel Teorema d'Euclides–Euler que tots els números perfectes parells són de la forma $2^{n-1}(2^n-1)$ amb 2^n-1 primer. Anem a demostrar en primer lloc que quan $2^n - 1$ és primer, n també és primer. Això és degut a que si n no és primer, $n = p\,q$ i aleshores

$$2^n - 1 = \big(2^p\big)^q - 1 = (2^p - 1)\big(\big(2^p\big)^{q-1} + \big(2^p\big)^{q-2} + \cdots + 2^p + 1\big),$$

ja que $x^q - 1 = (x-1)(x^{q-1} + x^{q-2} + \cdots + x + 1)$, i per tant $2^n - 1$ tampoc és primer. Observi's que en aquest punt l'argument usa el contra-recíproc. La condició no és suficient, com mostra l'exemple $2^{11} - 1 = 2047 = 23 \times 89$.

Considerem, doncs, n primer. Per a $n = 2$, $\ell = 2\,(2^2 - 1) = 6$ i el resultat és cert. Si $n > 2$, aleshores o bé $n = 4\,m + 1$, o bé $n = 4\,m + 3$ ja que tots els primers més gran que 2 són senars. Recordem que, donats $r, s \in \mathbb{N}$, $r \equiv s \pmod{10}$ si, i només si, acaben amb la mateixa xifra. Per tant, en el primer cas,

$$\begin{aligned} 2^{n-1}\big(2^n - 1\big) &= 2^{4m}\big(2^{4m+1} - 1\big) = 16^m(2 \times 16^m - 1) \\ &\equiv 6^m\big(2 \times 6^m - 1\big) \equiv 6\,(12 - 1) \equiv 6 \pmod{10}, \end{aligned}$$

ja que $6^m \equiv 6 \pmod{10}$. De manera similar, si $n = 4\,m + 3$,

$$\begin{aligned} 2^{n-1}\big(2^n - 1\big) &= 2^{4m+2}\big(2^{4m+3} - 1\big) = 4 \times 16^m\big(8 \times 16^m - 1\big) \\ &\equiv 4 \times 6\,(8 \times 6 - 1) \equiv 4\,(8 - 1) \equiv 8 \pmod{10}. \end{aligned}$$

Per tant, el resultat està demostrat. □

1.4 Reducció a l'absurd

Recollim a continuació uns quants exemples de demostracions per reducció a l'absurd.

1.4.1 Sobre el número racional positiu més petit

Anem a demostrar, usant reducció a l'absurd, que *no hi ha cap número racional positiu que sigui el més petit de tots*. Amb aquest objectiu en ment, i per tal d'arribar a una contradicció, suposem que sí que existeix. Anomenem-lo $0 < r \in \mathbb{Q}$. Aleshores clarament $0 < r/2 < r$, i $r/2 \in \mathbb{Q}$, per tant hem arribat a una contradicció amb el fet que r era el més petit.

Òbviament, el fet de que si r és racional implica que $r/2$ també ho és permet construir una successió de números racionals $r/2^n, n \in \mathbb{N}$, que tendeixen a zero. Usant aquesta successió també es demostra de manera directa i constructiva el resultat desitjat.

Proves similars serveixen per veure que no hi cap número real positiu que sigui el més petits de tots, ni cap número irracional amb les mateixes propietats. I ja posats, tampoc hi ha cap número algebraic, ni transcendent amb aquestes propietats. Recordem que un número $a \in \mathbb{R}$ es diu algebraic si hi ha un polinomi no trivial P, amb coeficients a $\mathbb{Z}$ i tal que $P(a) = 0$. Un número no algebraic es diu transcendent. El punt clau és que si $x > 0$ és real, racional, irracional, algebraic o transcendent, $x/2 > 0$ també ho és.

1.4.2 Hi ha infinits primers de la forma $4\,n - 1$

Com que hi ha infinits números primers ja sabem que o bé n'hi ha un nombre infinit de la forma $4\,n-1$, o bé n'hi ha un nombre infinit de la forma $4\,n+1$, o bé les dues opcions es donen.

Anem a veure que la primera opció, és a dir, *hi ha un nombre infinit de primers de la forma* $4\,n-1$, és certa. La prova és una adaptació de la prova d'Euclides de la infinitud dels números primers també basada en la reducció a l'absurd.

Suposem que no, per tal d'arribar a contradicció. Siguin p_1, p_2,...,p_k tots els primers de la forma $4\,n - 1$. Considerem

$$N = 4\,p_1\,p_2 \cdots p_k - 1.$$

Aleshores N no pot ser primer, ja que seria de la forma $4\,n - 1$ i no és a la llista de tots els primers d'aquesta forma. Clarament cap p_j divideix a N. A més, a la descomposició de N en factors primers n'hi ha com a mínim un de la forma $4\,n - 1$, ja que si tots fossin de la forma $4\,n + 1$, N també ho seria ja que $(4\,n + 1)(4\,m + 1) = 4\,(4\,n\,m + n + m) + 1$. Aquest primer seria de la forma $4\,n - 1$ i no és cap dels p_j, $j \leq k$, obtenint la contradicció desitjada.

De fet, Dirichlet al 1837 va demostrar que, variant $n \in \mathbb{N}$, qualsevol expressió $a\,n + b$ amb a i b enters coprimers dóna lloc a infinits números primers.

1.4.3 El número $\log_2 3$ és irracional

Suposem, per tal d'obtenir una contradicció que fos racional, és a dir que $\log_2 3 = p/q$, amb p i q números naturals. Aleshores,

$$3 = 2^{\log_2 3} = 2^{p/q} \Longrightarrow 3^q = 2^p.$$

Com que 3^q és senar i 2^q és parell ja hem obtingut la contradicció desitjada i per tant $\log_2 3$ és irracional.

1.4.4 El número $\sqrt{2}$ és irracional

Suposem, per tal d'arribar a una contradicció, que $\sqrt{2}$ és racional. Per tant $\sqrt{2} = p/q$, amb p i q números naturals, que a més podem suposar primers entre si. Aleshores $2 = p^2/q^2$ i com a conseqüència $p^2 = 2\,q^2$. En particular, p^2 és un número parell i per tant p també ho ha de ser (vegeu la Secció 1.3.1). Aleshores $p = 2\,k$, amb $k \in \mathbb{N}$, i substituint $4\,k^2 = p^2 = 2\,q^2$. D'aquesta darrera igualtat obtenim que $q^2 = 2\,k^2$, i per tant, argumentant com abans, q és també parell. En resum hem provat que tant p com q tenen el divisor 2, resultat que està en contradicció amb la tria de p i q primers entre si. Per tant $\sqrt{2}$ és irracional, tal i com ja es va demostrar a la Grècia clàssica. A la Secció 4.2.3 farem una segona prova basada en el mètode del descens infinit de Fermat.

1.4.5 Nombre d'arrels reals d'un polinomi

Una conseqüència del Teorema del valor mitjà, que ja hem recordat a la Secció 1.2.6, és que donats dos zeros a i b, amb $a < b$, d'una funció derivable $f : \mathbb{R} \longrightarrow \mathbb{R}$ hi ha com a mínim un valor c, amb $a < c < b$, tal que $f'(c) = 0$. La Figura 4 il·lustra aquest fet que és conegut com a Teorema de Rolle.

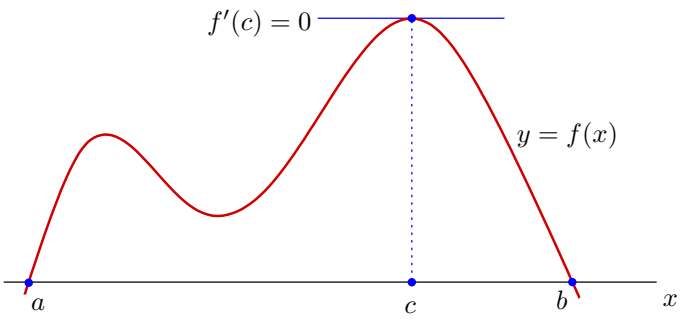


Figura 4: Teorema de Rolle

Demostrarem usant el Teorema de Rolle i per reducció a l'absurd el resultat següent.

Proposició 1.16. *Sigui $p \neq 0$ un polinomi amb tres monomis. Aleshores p té com a molt dues arrels positives i dues arrels negatives. A més, hi ha polinomis d'aquest tipus amb quatre arrels reals no nul·les.*

Prova. Dividint, si cal, per una potència de x, no és restrictiu suposar que

$$p(x) = u\,x^n + v\,x^m + w, \quad \text{amb} \quad u\,v\,w \neq 0 \quad \text{i} \quad n > m.$$

Per tal d'arribar a contradicció, suposem que p té tres arrels positives $0 < s_1 < s_2 < s_3$. Aleshores, pel Teorema de Rolle sabem que p' té com a mínim

dues arrels positives, t_1 i t_2 tals que $0 < s_1 < t_1 < s_2 < t_2 < s_3$. Ara bé, el polinomi $p'(x) = n\,u\,x^{n-1} + m\,v\,x^{m-1}$ té com a molt una arrel positiva, que existeix quan $-m\,v/(n\,u) > 0$ i és $t = (-m\,v/(n\,u))^{1/(n-m)}$, arribant a la contradicció desitjada.

El resultat per arrels negatives és conseqüència del resultat per arrels positives simplement considerant el polinomi $q(x) = p(-x)$.

Per a veure que el resultat és òptim és suficient considerar el polinomi $p(x) = (x^2-1)(x^2-4) = x^4 - 5\,x^2 + 4$, que té tres monomis i arrels reals $\pm 1, \pm 2$. □

De fet, de manera semblant es pot demostrar una extensió per a polinomis amb un nombre arbitrari de monomis, però veurem més endavant (Secció 2.7) que és molt més còmode demostrar-la usant el mètode d'inducció.

1.4.6 El conjunt $\mathbb{R}$ no és numerable

Recordem que un conjunt C es diu numerable si hi ha una aplicació bijectiva entre C i els números naturals $\mathbb{N}$.

Per a demostrar-ho, suposarem que sí que ho és, i arribarem a una contradicció. Serà útil pensar que el números reals es poden identificar amb les seves expressions decimals. Sigui $f : \mathbb{N} \to \mathbb{R}$ una aplicació bijectiva entre els dos conjunts. Aleshores tots el números reals es poden ordenar i serien:

$$f(1), f(2), f(3), \ldots, f(n), \ldots$$

Les imatges dels primers números reals podrien ser, per exemple, els de la Figura 5.

n	$f(n)$
1	0 . **4** 0 0 0 0 0 1 0 0 0 0 0 0 0 0 …
2	8 . 5 **0** 0 6 0 7 0 8 6 6 6 9 0 0 …
3	7 . 5 0 **5** 0 0 9 4 0 0 4 4 1 0 1 …
4	5 . 5 0 7 **0** 4 0 0 7 0 4 8 0 5 0 …
5	6 . 9 0 0 2 **6** 0 0 0 0 0 0 5 0 6 …
6	6 . 8 5 8 0 9 **5** 8 2 0 5 0 0 2 0 …
7	6 . 5 0 5 0 5 5 **5** 0 6 5 5 8 0 8 …
8	8 . 7 2 0 8 0 6 4 **0** 0 0 0 4 0 8 …
9	0 . 5 5 0 0 0 0 8 8 **8** 8 0 0 7 7 …
10	0 . 5 0 0 2 0 7 2 2 0 **7** 8 0 5 1 …
11	2 . 9 0 0 0 0 8 8 0 0 0 **0** 9 0 0 …
12	6 . 5 0 2 8 0 0 0 8 0 0 9 **6** 7 1 …
13	8 . 8 9 0 0 8 0 2 4 0 0 8 0 **5** 0 …
14	8 . 5 0 0 0 9 7 4 2 0 8 0 2 2 **6** …
⋮	⋮

Figura 5: Un intent de construcció d'una aplicació bijectiva entre $\mathbb{N}$ i $\mathbb{R}$, i unes xifres decimals marcades.

Ara considerem un número real y de manera que per a tot $k \in \mathbb{N}$:

La xifra decimal k-èssima de y és diferent de la de $f(k)$.

Per exemple, y podria començar com: $y = 0.6202977123333\ldots$ És clar que no hi ha cap $n \in \mathbb{N}$ tal que $f(n) = y$, ja que és diferent de tots els de la llista. Per tant hem arribat a una contradicció i $\mathbb{R}$ no és numerable.

La construcció d'aquest element y sense preimatge se sol designar com *procediment diagonal de Cantor* en honor del matemàtic alemany Georg Cantor (1845–1918) qui va ser el primer en usar aquesta construcció.

1.4.7 La irracionalitat de e

Reproduïm a continuació la prova de Fourier del fet que e *és un número irracional*. Si definim $S_n = \sum_{m=0}^{n} \frac{1}{m!}$, aleshores

$$\mathrm{e} = \lim_{n\to\infty} S_n = \sum_{m=0}^{\infty} \frac{1}{m!}.$$

Observem que per a tot $j \geq 1$,

$$\frac{n!}{(n+j)!} = \frac{1}{n+j} \times \frac{1}{n+j-1} \times \cdots \times \frac{1}{n+2} \times \frac{1}{n+1} \leq \frac{1}{(n+1)^j},$$

amb igualtat només per a $j = 1$. Per tant,

$$\begin{aligned} \mathrm{e} - S_n &= \sum_{m=n+1}^{\infty} \frac{1}{m!} = \frac{1}{n!} \sum_{m=n+1}^{\infty} \frac{n!}{m!} = \frac{1}{n!} \sum_{j=1}^{\infty} \frac{n!}{(n+j)!} \\ &< \frac{1}{n!} \sum_{j=1}^{\infty} \frac{1}{(n+1)^j} = \frac{1}{n!} \frac{\frac{1}{(n+1)}}{1 - \frac{1}{(n+1)}} = \frac{1}{n!n}, \end{aligned}$$

on a la penúltima igualtat hem sumat una sèrie geomètrica. Prenent $n = 2$, com que $S_2 = 5/2$, obtenim

$$2 < \mathrm{e} < S_2 + \frac{1}{4} = \frac{11}{4} < 3.$$

Suposem, per tal d'arribar a contradicció que e és racional, és a dir que $\mathrm{e} = p/q \in \mathbb{Q}$. Observem primer que $q \geq 2$ ja que $2 < \mathrm{e} < 3$ i per tant e no pot ser enter. Si prenem la desigualtat anterior per a $n = q$, s'obté

$$S_q < \mathrm{e} = \frac{p}{q} < S_q + \frac{1}{q!\,q}.$$

Multiplicant-la per $q!$ tenim que

$$q!\,S_q < q!\,\mathrm{e} = q!\frac{p}{q} = (q-1)!\,p < q!\,S_q + \frac{1}{q} < q!\,S_q + 1.$$

Com que $q!\,S_q$ és enter obtenim que $(q-1)!\,p$ és un enter situat entre dos enters consecutius, fet que ens dóna la contradicció buscada. Per tant e és irracional.

1.4.8 El tot i les seves parts

És molt clar que si un conjunt A és finit (amb n elements) aleshores no hi ha cap aplicació bijectiva entre ell i el conjunt dels seus subconjunts $\mathcal{P}(A)$, ja que aquest segon conjunt té $2^n > n$ elements. Vegeu per exemple la Secció 4.3.3 per a una prova de que $\mathcal{P}(A)$ té 2^n elements. Tal i com va demostrar Cantor, aquest resultat és cert per a qualsevol conjunt.

Proposició 1.17. *No hi ha cap aplicació bijectiva entre un conjunt A i el conjunt $\mathcal{P}(A)$.*

Prova. Suposem, per tal d'arribar a una contradicció, que A és un conjunt tal que entre A i $\mathcal{P}(A)$ hi ha una aplicació bijectiva f. Definim el subconjunt d'A següent,

$$B := \{x \in A \,:\, x \notin f(x)\} \in \mathcal{P}(A).$$

Aleshores, existeix un $y \in A$ tal que $f(y) = B$. Ara bé, si $y \in B$, per definició $y \notin f(y) = B$ i tenim una contradicció. Per altra banda, si $y \notin B$ tenim que $y \in f(y) = B$, de nou una contradicció. Per tant, un y tal que $f(y) = B$ no pot existir, i la proposició queda demostrada. □

2 Inducció

Encara que no amb el formalisme actual, les primeres proves d'inducció es remunten al segle X. El terme *inducció matemàtica* va ser introduït de manera rigorosa pel matemàtic britànic Augustus De Morgan l'any 1838, vegeu per exemple [13] o [17, Cap. 8] .

Figura 6: Inducció i figures de dòmino

Una demostració per inducció apareix quan tenim un nombre infinit d'afirmacions que volem demostrar: Afirmació(1), Afirmació(2), Afirmació(3), ..., Afirmació(n),... Si podem fer els dos passos següents, aleshores haurem vist que les afirmacions seran certes:

Pas 1. Demostrar que l'Afirmació(1) és certa. *Es a dir, tombar la primera peça del dòmino.*

Pas 2. Demostrar que, per a tot número natural m, si l'Afirmació(m) és certa, aleshores l'Afirmació($m+1$) també ho és. *És a dir, que si tombem el dòmino m-èssim, aleshores el dòmino $(m+1)$-èssim també cau, vegeu la Figura 6.*

Resumint el principi d'inducció diu que, si podem fer els passos 1 i 2, aleshores l'Afirmació(n) és certa per a tot $n \in \mathbb{N}$.

2.1 Suma dels primers enters positius

Anem a veure com a primer exemple que es compleix que

$$S_n = 1 + 2 + 3 + \cdots + (n-1) + n = \frac{n(n+1)}{2}. \tag{4}$$

Es diu que en Gauss amb només 7 o 8 anys va deduir-la quan el seu mestre els hi va posar a classe com a exercici per tenir-los entretinguts que calculessin $1 + 2 + 3 + \cdots + 100$. Més endavant veurem com es pensa que ho va fer en Gauss.

La fórmula és certa per a $n = 1$ ja que $S_1 = 1 = \frac{1\times 2}{2}$. Suposem ara que la fórmula és certa per a $n = m$ i veiem que també ho és per a $n = m + 1$:

$$\begin{aligned} S_{m+1} &= 1 + 2 + 3 + \cdots + m + (m+1) = S_m + (m+1) \\ &= \frac{m(m+1)}{2} + (m+1) = \frac{(m+1)(m+2)}{2}. \end{aligned}$$

Per tant, pel principi d'inducció, (4) és certa.

2.2 Fórmula de Nichomacus

Nicomachus de Gerasa va ser un matemàtic i filòsof grec que va viure al segle primer després de Crist. Se li atribueix una versió geomètrica de la fórmula per a la suma dels primers n cubs:

$$1^3 + 2^3 + \cdots + (n-1)^3 + n^3 = \big(1 + 2 + \cdots + (n-1) + n\big)^2. \tag{5}$$

Sembla ser que una de les primeres proves que va usar les idees principals de l'inducció va ser per a demostrar aquesta fórmula i és deguda al matemàtic persa al-Karaji (953–1029). Anem a demostrar-la, usant la terminologia moderna.

Per a $n = 1$ és certa ja que $1^3 = 1^2$. També ho és per a $n = 2$, donat que $1^3 + 2^3 = 9 = (1+2)^2$. Per acabar, demostrem-la quan $n = m + 1$ a partir

de saber-la per a $n = m$. Tenim

$$\begin{aligned}\big(1+2+\cdots+m+(m+1)\big)^2 &= (1+2+\cdots+m)^2+(m+1)^2\\ &\quad +2\big(1+2+\cdots+m\big)(m+1)\\ &= 1^3+2^3+\cdots+m^3+(m+1)^2\\ &\quad +2\frac{m(m+1)}{2}(m+1)\\ &= 1^3+2^3+\cdots+m^3+(m+1)^3,\end{aligned}$$

on a la penúltima igualtat hem usat (4). A la Secció 4.6.1 veurem una prova sense paraules de (5).

2.3 Una propietat de divisibilitat

Sovint hi ha més d'una manera de demostrar un resultat cert. Per exemple, en aquesta secció provarem usant inducció un resultat senzill de divisibilitat i a continuació donarem dues demostracions alternatives.

Provarem que *per a tot* $1 \le n \in \mathbb{N}$, $11^n - 6$ *és divisible entre 5*. Clarament aquest resultat és equivalent a l'afirmació següent: per a tot $1 \le n \in \mathbb{N}$, hi ha un $q \in \mathbb{N}$ tal que $11^n = 5\,q + 6$. Demostrem aquesta darrera afirmació per inducció. Per a $n = 1$ és certa ja que $11 = 5 + 6$. Suposem-la certa per a $n = m$, és a dir $11^m = 5\,\ell + 6$ per a un cert $\ell \in \mathbb{N}$, i la demostrarem per a $n = m + 1$,

$$\begin{aligned}11^{m+1} &= 11^m\,11 = (5\,\ell+6)\,11 = 55\,\ell+66\\ &= 55\,\ell+60+6 = 5\,(11\,\ell+12)+6,\end{aligned}$$

tal i com volíem veure.

Veiem a continuació dues proves directes alternatives de l'afirmació.

La primera prova consisteix a observar que 11^n és un número que acaba en 1. Aleshores clarament $11^n - 6$ acaba en 5 i és ben conegut que tots els números que acaben en 5 són divisibles entre 5.

La segona usa de nou els càlculs amb números enters mòdul k dels que ja hem parlar al final de la Secció 1.2.4, en aquesta ocasió amb $k = 5$. Tenim

$$\overline{11^n - 6} = \overline{11^n} - \overline{6} = \overline{11}^n - \overline{1} = \overline{1}^n - \overline{1} = \overline{1} - \overline{1} = \overline{0}.$$

Per tant la divisió de $11^n - 6$ entre 5 té resta 0, com volíem demostrar.

2.4 Els números de Fibonacci

Una de les seqüències de números naturals més famosa és la formada pels números de Fibonacci: $0, 1, 1,\ 2, 3, 5, 8, 13, 21, 34, 55, \ldots$ i ve definida per la recurrència

$$F_0 = 0,\ F_1 = 1 \quad \text{i} \quad F_{n+1} = F_n + F_{n-1} \text{ per a } n \ge 1.$$

Un segell italià recent dedicat a Fibonacci

A continuació, demostrarem per inducció algunes propietats i relacions entre els números de Fibonacci. Per això necessitarem les notacions següents:

$$\varphi = \frac{1+\sqrt{5}}{2} \approx 1.618, \quad \psi = -\frac{1}{\varphi} = 1-\varphi = \frac{1-\sqrt{5}}{2} \approx -0.618\,.$$

2.4.1 Fórmula de Binet

Demostrem en primer lloc, per inducció, que si $x \in \{\varphi, \psi\}$ aleshores

$$x^n = x\,F_n + F_{n-1}, \quad n \geq 1.$$

Clarament, la fórmula és certa per a $n = 1$. Ara bé, com que $x^2 - x - 1 = 0$, també és certa per a $n = 2$. Suposant-la certa per a $n = m$, tenim que

$$\begin{aligned} x^{m+1} &= x\big(x\,F_m + F_{m-1}\big) = x^2\,F_m + x\,F_{m-1} = (x+1)\,F_m + x\,F_{m-1} \\ &= x\,\big(F_m + F_{m-1}\big) + F_m = x\,F_{m+1} + F_m, \end{aligned}$$

és a dir, obtenim que és certa per a $n = m+1$, tal i com volíem veure. Per tant, per a tot $n \geq 1$, sabem que

$$\varphi^n = \varphi\,F_n + F_{n-1} \quad \text{i} \quad \psi^n = \psi\,F_n + F_{n-1}.$$

Restant ambdues equacions, arribem a $\varphi^n - \psi^n = (\varphi - \psi)\,F_n$, resultat equivalent a la fórmula de Binet,

$$F_n = \frac{\varphi^n - \psi^n}{\varphi - \psi} = \frac{\varphi^n - \psi^n}{\sqrt{5}}, \quad n \geq 1.$$

El matemàtic francès Jacques Philippe Marie Binet va donar aquesta fórmula l'any 1843, tot i que sembla que tant Daniel Bernoulli com de Moivre ja la coneixien al segle XVII.

2.4.2 Suma dels quadrats

Demostrarem

$$\sum_{i=1}^{n} {F_i}^2 = F_n\, F_{n+1}.$$

Per a $n = 1$ és cert ja que ${F_1}^2 = 1 = F_1\, F_2$. Suposem la fórmula certa per a $n = m$ i demostrem-la per a $n = m + 1$.

$$\begin{aligned}\sum_{i=1}^{m+1} {F_i}^2 &= \sum_{i=1}^{m} {F_i}^2 + (F_{m+1})^2 = F_m\, F_{m+1} + (F_{m+1})^2 \\ &= F_{m+1}\left(F_{m+1} + F_m\right) = F_{m+1}\, F_{m+2}.\end{aligned}$$

Per tant la fórmula queda demostrada.

2.4.3 Dues relacions més

Demostrarem que

$$F_{2n+1} = (F_{n+1})^2 + (F_n)^2 \quad \text{i} \quad F_{n+1}\, F_{n-1} - (F_n)^2 = (-1)^n.$$

Començarem provant per inducció que

$$M^n := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}. \tag{6}$$

Per a $n = 1$, és clarament cert. Per demostrar-ho per a $n = m + 1$, a partir del cas $n = m$ observem que

$$\begin{aligned}M^{m+1} &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^m = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} F_{m+1} & F_m \\ F_m & F_{m-1} \end{pmatrix} \\ &= \begin{pmatrix} F_{m+1} + F_m & F_m + F_{m-1} \\ F_{m+1} & F_m \end{pmatrix} = \begin{pmatrix} F_{m+2} & F_{m+1} \\ F_{m+1} & F_m \end{pmatrix},\end{aligned}$$

tal i com volíem demostrar. Per tant, com que $M^{2n} = M^n M^n$, tenim que

$$\begin{pmatrix} F_{2n+1} & F_{2n} \\ F_{2n} & F_{2n-1} \end{pmatrix} = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}\begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}.$$

Fent el producte de matrius i igualant l'element de la primera fila i la primera columna tenim que $F_{2n+1} = (F_{n+1})^2 + (F_n)^2$, tal i com volíem provar. Per demostrar la segona relació nomes cal prendre determinants a ambdós costats de (6) i usar que $\det(M^n) = (\det(M))^n = (-1)^n$. Aquesta segona igualtat s'anomena *identitat de Cassini.*

2.4.4 Fites per a F_n

Anem a demostrar que

$$\varphi^{n-2} \leq F_n < \varphi^n \quad \text{per a } n \geq 1. \tag{7}$$

Comencem demostrant la desigualtat inferior. Per a $n = 1$ és certa ja que $\varphi^{-1} < 1 = F_1$ i per a $n = 2$ també, donat que $\varphi^0 = 1 = F_2$. Veiem que és certa per a $n = m + 1$, a partir del resultat per a $n = m - 1$ i per a $n = m$. Observem aquí, que hem usat una petita variació de la inducció clàssica, ja que necessitem que sigui certa per als dos primers casos i usem els dos casos anteriors per demostrar el següent (*és com si necessitéssim tirar dos dòminos consecutius per fer caure el següent*). Usant un cop més que $\varphi^2 = \varphi + 1$,

$$\begin{aligned} F_{m+1} = F_m + F_{m-1} &\geq \varphi^{m-2} + \varphi^{m-3} = \varphi^{m-1}\left(\frac{1}{\varphi} + \frac{1}{\varphi^2}\right) \\ &= \varphi^{m-1}\frac{\varphi+1}{\varphi^2} = \varphi^{m-1}\frac{\varphi^2}{\varphi^2} = \varphi^{m-1}. \end{aligned}$$

Per tant, la desigualtat inferior és certa. La prova de l'altra desigualtat és similar i es compleix per a $n \geq 0$. En primer lloc, clarament $0 = F_0 < \varphi^0 = 1$ i $1 = F_1 < \varphi$. Ara bé, suposant-la certa per a $n = m$ i $n = m - 1$ tenim

$$\begin{aligned} F_{m+1} = F_m + F_{m-1} &< \varphi^m + \varphi^{m-1} = \varphi^{m+1}\left(\frac{1}{\varphi} + \frac{1}{\varphi^2}\right) \\ &= \varphi^{m+1}\frac{\varphi+1}{\varphi^2} = \varphi^{m+1}\frac{\varphi^2}{\varphi^2} = \varphi^{m+1}, \end{aligned}$$

tal i com volíem demostrar. Per tant (7) queda demostrat.

Com que $8/5 < \varphi < 5/3$, una conseqüència directa de (7) és que

$$\left(\frac{8}{5}\right)^{n-2} < F_n < \left(\frac{5}{3}\right)^n \quad \text{per a } n \geq 1.$$

2.5 Tres desigualtats

2.5.1 Factorial i una potència

Anem a demostrar que *per a tot natural $n \geq 4$, es compleix la desigualtat* $n! > 2^n$. Per a $n = 4$ és certa ja que $4! = 24 > 16 = 2^4$. Suposem-la certa per a $n = m \geq 4$ i demostrem-la per a $n = m + 1$,

$$(m+1)! = (m+1) \times m! > (m+1) \times 2^m > 2 \times 2^m = 2^{m+1},$$

ja que $m + 1 \geq 5 > 2$. De forma que el resultat queda demostrat.

2.5.2 Una desigualtat clàssica

Demostrarem per inducció que

$$(1+x)^n \geq 1+n\,x, \quad \text{sempre que } -1 \leq x \in \mathbb{R} \text{ i } 0 < n \in \mathbb{N}.$$

Per a $n = 1$ és cert ja que obtenim una igualtat. Demostrem-ho per a $n = m+1$ a partir del cas $n = m$ i usant que $1 + x \geq 0$. Es compleix

$$\begin{aligned}(1+x)^{m+1} &= (1+x)(1+x)^m \\ &\geq (1+x)(1+m\,x) \\ &= 1+(m+1)\,x+m\,x^2 \\ &\geq 1+(m+1)\,x,\end{aligned}$$

tal i com volíem veure. Per tant la desigualtat està provada.

2.5.3 Una desigualtat curiosa

Anem a demostrar per inducció que per a tot $n \in \mathbb{N}$ i per a tot $x \in \mathbb{R}$,

$$|\sin(n\,x)| \leq n\ |\sin(x)|\,. \tag{8}$$

Per a $n = 0$ o $n = 1$ la desigualtat és clarament certa, i de fet és una igualtat. Suposem que és certa per a $n = m$ i demostrem-la per a $n = m+1$.

$$\begin{aligned}|\sin((m+1)\,x)| &= |\sin(m\,x)\cos(x)+\cos(m\,x)\sin(x)| \\ &\leq |\sin(m\,x)|\ |\cos(x)|+|\cos(m\,x)|\ |\sin(x)| \\ &\leq |\sin(m\,x)|+|\sin(x)| \\ &\leq m\ |\sin(x)|+|\sin(x)| \\ &= (m+1)\ |\sin(x)|\,,\end{aligned}$$

tal i com volíem veure. Per tant (8) és certa.

La desigualtat és ben curiosa, ja que es compleix quan $n \in \mathbb{N}$, però ja no ho fa quan $n \in \mathbb{Q}$. Per exemple, per a $n = 1/2$, prenent $x = \pi$, tenim que $1 = |\sin(\pi/2)| = |\sin(n\,x)| > n\,|\sin(x)| = |\sin(\pi)|\,/2 = 0$. Per tant, no sembla fàcil trobar una prova analítica de (8) no basada en inducció.

2.6 Nombre de cordes

Considerem n punts sobre una circumferència. Sigui C_n el nombre de cordes que s'obtenen ajuntant tots els punts de dos en dos. Anem a demostrar que $C_n = n(n-1)/2$.

Utilitzarem inducció. Per a $n = 1$ és clar que $C_1 = 0$ (no hi ha cap corda). Si es vol, per a $n = 2$, $C_2 = 1 = 2 \times 1/2$ ja que només hi ha una corda, la que uneix els dos punts.

Suposem ara que per a $n = m$, $C_m = m(m-1)/2$ i calculem C_{m+1}. Observem que si agafem els $m+1$ i els dividim en dos grups, un que anomenem $\mathcal{A}$, amb m punts, i un altra amb un sol punt, p. Aleshores el nombre total de cordes està format per les que tenen com extrems dos punts del conjunt $\mathcal{A}$, és a dir C_m cordes, més les m cordes que comencen a p i acaben a cadascun dels punts de A. D'aquestes clarament n'hi ha m. Així,

$$C_{m+1} = C_m + m = \frac{m(m-1)}{2} + m = \frac{(m+1)m}{2},$$

tal i com volíem demostrar. Vegeu aquest argument il·lustrat a la Figura 7 per a $m = 5$.

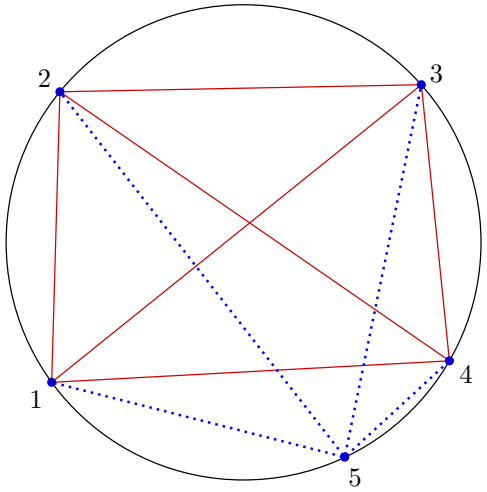


Figura 7: $C_5 = C_4 + 4 = 6 + 4 = 10$

El resultat anterior també admet una prova combinatòria, ja que hi ha tantes cordes com subconjunts de dos elements té un conjunt de n elements. Aquí identifiquem cada corda amb els seus dos punts extrems. És ben conegut que el nombre de subconjunts de k elements és $\binom{n}{k}$, vegeu la Secció 4.3. Així $C_n = \binom{n}{2} = n(n-1)/2$.

2.7 Nombre d'arrels reals d'un polinomi, segona part

La demostració següent barreja els mètodes d'inducció i reducció a l'absurd i estén els resultats de la Secció 1.4.5.

Proposició 2.1. *Sigui $p \neq 0$ un polinomi amb $n+1$ monomis, $0 \leq n \in \mathbb{N}$. Aleshores p té com a molt n arrels positives i n arrels negatives. A més, hi ha polinomis d'aquest tipus amb $2\,n$ arrels no nul·les, n positives i n negatives.*

Prova. Si $n = 0$ el resultat és clarament cert ja que els polinomis amb un monomi, $p(x) = a_1\, x^{k_1}$ no tenen cap arrel ni positiva ni negativa. Anem

a demostrar-ho quan $n = m + 1$, suposant el resultat cert per a $n = m$. Considerem un polinomi amb $n + 1 = m + 2$ monomis,

$$p(x) = a_1\, x^{k_1} + a_2\, x^{k_2} + \cdots + a_{m+1}\, x^{k_{m+1}} + a_{m+2}\, x^{k_{m+2}}, \tag{9}$$

amb $a_1 a_2 \cdots a_{m+1} a_{m+2} \neq 0$ i $k_1 > k_2 > \cdots > k_{m+1} > k_{m+2} \geq 0$. Si aquest polinomi tingués $n+1 = m+2$ arrels positives (o més), aleshores, considerem $q(x) = p(x)/x^{k_{m+2}}$, el qual tindrà el mateix número d'arrels positives que $p(x)$. Pel Teorema de Rolle, $q'(x)$ en tindria com a mínim $m+1$, fet que està en contradicció amb la hipòtesi d'inducció, la qual estem suposant certa, ja que $q'(x)$ té només $m + 1$ monomis. Per tant el resultat està provat pel que fa a quantitat d'arrels positives.

La prova de la resta de la proposició es segueix de manera similar a la part final de la prova de la Proposició 1.16. □

De fet, aquesta proposició és una versió simplificada de la famosa regla de Descartes per a polinomis de la forma (9). Aquesta regla assegura que la quantitat de solucions positives de $p(x) = 0$ (tenint en compte la seva multiplicitat) és $N = \sigma - 2\,\ell$, on σ és el nombre de canvis de signe de la llista ordenada $[a_1, a_2, \ldots, a_{m+1}, a_{m+1}]$ i $\ell \in \mathbb{N} \cup \{0\}$ és desconegut, vegeu [12].

2.8 Càlcul d'una integral definida

Anem a demostrar, usant inducció sobre n, que per a tot parell k, n d'enters no negatius

$$\int_0^1 x^k (1-x)^n \,\mathrm{d}x = \frac{k!\, n!}{(k+n+1)!}. \tag{10}$$

Per a $n = 0$ el resultat és cert ja que

$$\int_0^1 x^k (1-x)^0 \,\mathrm{d}x = \int_0^1 x^k \,\mathrm{d}x = \frac{1}{k+1} = \frac{k!\, 0!}{(k+0+1)!}.$$

Veiem que si és cert per a $n = m$ i qualsevol k, aleshores és cert per a $n = m + 1$ i k arbitrari. Usarem la fórmula d'integració per parts,

$$\int_a^b u(x)\, v'(x) \,\mathrm{d}x = u(x)\, v(x)\Big|_{x=a}^{x=b} - \int_a^b u'(x)\, v(x) \,\mathrm{d}x, \tag{11}$$

prenent $u(x) = (1-x)^{m+1}$ i $v(x) = x^{k+1}/(k+1)$,

$$\begin{aligned}\int_0^1 x^k (1-x)^{m+1} \,\mathrm{d}x &= \frac{1}{k+1} x^{k+1} (1-x)^{m+1}\Big|_{x=0}^{x=1} \\ &\quad + \frac{m+1}{k+1} \int_0^1 x^{k+1} (1-x)^m \,\mathrm{d}x \\ &= \frac{(m+1)}{(k+1)} \frac{(k+1)!\, m!}{(k+m+2)!} = \frac{k!\, (m+1)!}{(k+m+1+1)!},\end{aligned}$$

tal i com volíem demostrar.

De fet, la igualtat (10) es pot estendre a exponents reals positius, o fins i tot complexos amb part real positiva, introduint les funcions gamma i beta, denotades respectivament per Γ i B. Així, per a tot $z_1, z_2 \in \mathbb{C}$ amb part real positiva, es pot demostrar que

$$B(z_1, z_2) = \frac{\Gamma(z_1)\,\Gamma(z_2)}{\Gamma(z_1 + z_2)},$$

on

$$\Gamma(z) = \int_0^\infty t^{z-1}\,\mathrm{e}^{-t}\,\mathrm{d}t \quad \text{i} \quad B(z_1, z_2) = \int_0^1 t^{z_1-1}\,(1-t)^{z_2-1}\,\mathrm{d}t.$$

No farem la prova, que és una mica més tècnica i complicada que la de (10). Aquesta darrera igualtat implica (10), ja que no és difícil demostrar que per $n \in \mathbb{N}$, $\Gamma(n) = (n-1)!$

Acabem aquesta secció amb un exemple divertit.

2.9 El problema dels bitllets

Anem a demostrar que amb un número il·limitat de bitllets de només 5 i 7 euros com els de la Figura 8 es pot pagar de manera exacta qualsevol quantitat entera més gran o igual que 24.

Figura 8: Bitllets de 5 i 7 euros

En aquesta prova usarem la inducció d'una manera poc formal. Primer veiem que es poden pagar de manera exacta les quantitats: 24, 25, 26, 27 i 28;

$$\begin{aligned} 24 &= 2\times 5 + 2\times 7, & 25 &= 5\times 5 + 0\times 7,\\ 26 &= 1\times 5 + 3\times 7, & 27 &= 4\times 5 + 1\times 7,\\ 28 &= 0\times 5 + 4\times 7. \end{aligned}$$

A partir d'aquest resultats veiem que es poden pagar de manera exacta totes les quantitats més grans que 23 senzillament afegint prou bitllets de 5

euros. *És com si tinguéssim 5 files de dòminos que van caient.*

$$
\begin{aligned}
&24 \to 29 \to 34 \to 39 \to 44 \to 49 \to 54 \to 59 \to 64 \to 69 \to \cdots \\
&25 \to 30 \to 35 \to 40 \to 45 \to 50 \to 55 \to 60 \to 65 \to 70 \to \cdots \\
&26 \to 31 \to 36 \to 41 \to 46 \to 51 \to 56 \to 61 \to 66 \to 71 \to \cdots \\
&27 \to 32 \to 37 \to 42 \to 47 \to 52 \to 57 \to 62 \to 67 \to 72 \to \cdots \\
&28 \to 33 \to 38 \to 43 \to 48 \to 53 \to 58 \to 63 \to 68 \to 73 \to \cdots
\end{aligned}
$$

De fet, aquest és un problema clàssic que s'anomena en anglès "the coin problem", és a dir, *el problema de les monedes*, o també *el problema de Frobenius*. Si tenim una quantitat il·limitada de monedes amb només dos valors: p i q, naturals, aquest problema consisteix a veure a partir de quin valor minimal M, anomenat *número de Frobenius*, es poden pagar totes les quantitats de manera exacta. És conegut que si p i q són primers entre si, aquesta quantitat és $M = pq - p - q$, vegeu [41]. En el nostre cas $p = 5$, $q = 7$ i $M = 5 \times 7 - 5 - 7 = 23$. Quan hi ha més de dues monedes, no es coneix cap fórmula tancada per M, però sí que hi ha algoritmes per determinar el número de Frobenius per a valors donats de les monedes. També és interessant veure des d'aquest punt de vista per què molts sistemes de monedes tenen les de 2 i 5 unitats. Amb aquests valors es pot pagar de manera exacta qualsevol quantitat superior a $M = 10 - 2 - 5 = 3$.

Observi's que si p i q tenen algun factor en comú ja no hi ha cap valor M amb la propietat desitjada. Per exemple, si p i q són ambdós parells només es poden pagar quantitats parells.

Si pel pagament de qualsevol quantitat entera C admetem tornar canvi, llavors no hi ha cap restricció sobre C. Això es degut a la igualat de Bézout que assegura que donats qualssevol enters positius p i q, primers entre si, existeixen $n, m \in \mathbb{Z}$ tals que $n \times p + m \times q = 1$. A partir d'aquesta igualtat tenim que $\big(C \times n\big) \times p + \big(C \times m\big) \times q = C$. Per tant, per pagar 23, usant que $3 \times 5 - 2 \times 7 = 1$, obtenim que $69 \times 5 - 46 \times 7 = 23$, tot i que hi ha solucions més simples, com per exemple $6 \times 5 - 1 \times 7 = 23$.

3 Càlculs

L'habilitat en el càlcul sempre ha estat una de les vessants importants dins de les matemàtiques. De fet, el primer contacte d'un infant amb elles comença amb els càlculs que involucren números naturals, continua amb les fraccions, i de mica en mica es va complicant incloent altres elements com el raonament més abstracte o la geometria. En aquesta secció inclourem uns quant exemples de demostracions en las que la part essencial és saber calcular.

3.1 Prova de Gauss de que $1+2+\cdots+100=5050$.

Demostrem seguint la idea atribuïda a Gauss quan $n=100$, que es compleix (4). Per això escrivim

$$\begin{array}{rccccccccccc} S_n = & 1 & + & 2 & + & 3 & +\cdots+ & n-1 & + & n \\ +S_n = & n & + & n-1 & + & n-2 & +\cdots+ & 2 & + & 1 \\ \hline 2\,S_n = & (n+1) & + & (n+1) & + & (n+1) & +\cdots+ & (n+1) & + & (n+1) \end{array}$$

Per tant, com que el terme $n+1$ surt n vegades:

$$2\,S_n = n(n+1) \implies S_n = \frac{n(n+1)}{2}.$$

3.2 Una igualtat divertida

Demostrarem per a tot $n \in \mathbb{N}$ la igualtat entre números naturals que tenen totes les seves xifres repetides següent:

$$\underbrace{111\ldots1}_{2n\text{ cops}} = \underbrace{222\ldots2}_{n\text{ cops}} + \left(\underbrace{333\ldots3}_{n\text{ cops}}\right)^2.$$

Per a provar-la usem que

$$\begin{aligned} \underbrace{111\ldots1}_{2n\text{ cops}} - \underbrace{222\ldots2}_{n\text{ cops}} &= \underbrace{111\ldots1}_{n\text{ cops}}\underbrace{000\ldots0}_{n\text{ cops}} - \underbrace{111\ldots1}_{n\text{ cops}} = \underbrace{111\ldots1}_{n\text{ cops}} \times (10^n - 1) \\ &= \underbrace{111\ldots1}_{n\text{ cops}} \times \underbrace{999\ldots9}_{n\text{ cops}} = \underbrace{333\ldots3}_{n\text{ cops}} \times \underbrace{333\ldots3}_{n\text{ cops}}, \end{aligned}$$

tal i com volíem veure. Així $11 = 2 + 3^2$, $1111 = 22 + 33^2$, ...

3.3 Una equació curiosa

Anem a demostrar que l'únic número de tres xifres "abc" que coincideix amb $a! + b! + c!$ és 145. Aquesta condició s'escriu com

$$100\,a + 10\,b + c = a! + b! + c!, \tag{12}$$

amb $a \neq 0$ i $a, b, c \in \{0, 1, 2, \ldots, 8, 9\}$. Com que $7! > 1000$ ja sabem que $a, b, c \leq 6$. Però $6! = 720$, fet que implica que $a, b, c \leq 5$. A més, $5! + 5! + 5! = 360$, per tant $a \leq 3$.

Ara bé, si $a = 3$, $300 \leq 100a + 10b + c \leq 355$, però $a! + b! + c! \leq 3! + 5! + 5! = 246 < 300$. Per tant, $a \leq 2$.

Quan $a = 2$, $200 \leq 100\,a + 10\,b + c \leq 255$. En aquest cas $a! + b! + c!$ val 242 quan $(b, c) = (5, 5)$ i no es compleix (12). En qualsevol altre cas $a! + b! + c! \leq 2! + 4! + 5! = 146 < 200$. Així, $a = 2$ tampoc proporciona solucions de (12).

Per acabar, si $a = 1$ aleshores $100 \leq 100\,a + 10\,b + c \leq 155$. Per tal que es compleixi (12) s'ha de tenir $100 \leq 1! + b! + c! \leq 155$, és a dir $99 \leq b! + c! \leq 154$. Com que $b!, c! \in \{1, 2, 6, 24, 120\}$ les úniques solucions possibles corresponen a $(b, c) \in \{(4, 5), (5, 4)\}$. Tal i com volíem veure, d'aquestes dues possibilitats, l'única que proporciona una solució de (12) és la primera ja que

$$145 = 1! + 4! + 5!.$$

3.4 Identitats algebraiques

Llistarem a continuació unes quantes identitats clàssiques que recorden a les ternes pitagòriques. Totes es poden demostrar senzillament expandint els dos costats i comprovant que coincideixen. No farem aquests càlculs. N'hi ha moltes més a la plana web [47].

3.4.1 Identitats de Bramagupta–Fibonacci:

$$\begin{aligned}(a^2 + b^2)(c^2 + d^2) &= (a\,c + b\,d)^2 + (a\,d - b\,c)^2 \\ &= (a\,c - b\,d)^2 + (a\,d + b\,c)^2,\end{aligned}$$

també són conegudes com identitats de Diofant. Per exemple, pel cas particular $(a, b, c, d) = (1, 4, 2, 7)$ diuen que $(1^2 + 4^2)(2^2 + 7^2) = 30^2 + 1^2 = 26^2 + 15^2$. Brahmagupta les va desenvolupar, juntament amb altres identitats similars, per a estudiar certes equacions diofàntiques (equacions on els coeficients i les incògnites només prenen valors enters). Quan a, b, c i d són reals admeten una prova molt senzilla usant propietats del producte i la norma de números complexos, $|a + b\,\mathrm{i}|^2 = a^2 + b^2$, que es desenvolupa de la forma següent. Sabem que

$$(a + b\,\mathrm{i})(c + d\,\mathrm{i}) = (a\,c - b\,d) + (a\,d + b\,c)\,\mathrm{i},$$

fet que implica que

$$|a + b\,\mathrm{i}|^2\,|\,c + d\,\mathrm{i}|^2 = |(a\,c - b\,d) + (a\,d + b\,c)\,\mathrm{i}|^2\,.$$

Per tant

$$(a^2 + b^2)(c^2 + b^2) = (a\,c - b\,d)^2 + (a\,d + b\,c)^2.$$

Partint de

$$(a - b\,\mathrm{i})(c + d\,\mathrm{i}) = (a\,c + b\,d) + (a\,d - b\,c)\,\mathrm{i}$$

obtenim l'altra igualtat buscada.

3.4.2 Identitats de Ramanujan

Més endavant dedicarem una secció sencera, la 3.15, a Ramanujan. Aquí presentarem dues de les seves identitats. La primera és:

$$\left(3\,a^2+5\,a\,b-5\,b^2\right)^3+\left(4\,a^2-4\,a\,b+6\,b^2\right)^3+\left(5\,a^2-5\,a\,b-3\,b^2\right)^3 = \left(6\,a^2-4\,a\,b+4\,b^2\right)^3.$$

Quan $a=b=1$ dóna lloc a la bonica igualtat $3^3+4^3+5^3=6^3$. Una segona, d'un tipus semblant, és:

$$\left(a^2+9\,a\,b-b^2\right)^3+\left(12\,a^2-4\,a\,b+2\,b^2\right)^3 = \left(9\,a^2-7\,a\,b-b^2\right)^3+\left(10\,a^2+2\,b^2\right)^3.$$

En aquest cas, de nou quan $a=b=1$, dóna la famosa igualtat $1^3+12^3=9^3+10^3=1729$, associada a una l'anomenada *anècdota del taxi*, basada en una conversa entre Ramanujan i Hardy, vegeu [44]. Recordem-la breument: resulta que quan en Hardy va anar a visitar a Ramanujan a l'hospital en el que estava ingressat li va comentar que havia arribat en un taxi que tenia un número de matrícula avorrit, el 1729. Ell de seguida li va contestar que no, que 1729 era un número molt interessant ja que de fet era l'enter més petit que es podia posar de dues maneres diferents com a suma de dos cubs d'enters positius. Si s'admeten enters negatius hi ha valors molt més petits. Per exemple, $6^3+(-5)^3=4^3+3^3=91$.

Les dues identitats que hem donat formen part d'una família més general d'identitats amb quatre cubs. Una també semblant, atribuïda a Viète és:

$$\left(a^4-2\,a\,b^3\right)^3+\left(a^3b+b^4\right)^3=\left(b^4-2\,a^3\,b\right)^3+\left(a\,b^3+a^4\right)^3.$$

Sobre la pregunta natural sobre quin és l'enter més petit $T(3)$ que es pot posar de tres (o més) maneres com a suma dos cubs positius, tenim que és

$$87\,539\,319=436^3+167^3=423^3+228^3=414^3+255^3.$$

En general, el números $T(k)$ s'anomenen *taxicabs* en anglès, i se sap que $T(1)=2=1^3+1^3$, $T(2)=1729$ i $T(3)=87\,539\,319$. Es coneixen només per a $k\le 6$. Si admetem valors negatius de nou tenim un valor més petit:

$$4104=16^3+2^3=15^3+9^3=(-12)^3+18^3,$$

vegeu de nou [44].

3.5 Una identitat involucrant arrels quadrades

Demostrarem que per a tot $x>y>0$ es compleix la identitat

$$\sqrt{x\pm y}=\sqrt{\frac{x}{2}+\frac{\sqrt{x^2-y^2}}{2}}\pm\sqrt{\frac{x}{2}-\frac{\sqrt{x^2-y^2}}{2}}\,, \tag{13}$$

extreta de [31]. Si la intentem demostrar elevant al quadrat a ambdós costats, els càlculs es fan força pesats que se simplifiquen força si usem uns canvis de variables adients per al problema. Si introduïm $t > s > 0$ com $s = \sqrt{x^2 + y^2}$ i $t = x + y$, aleshores

$$x = \frac{t^2 + s^2}{2t} \quad \text{i} \quad y = \frac{t^2 - s^2}{2t}. \tag{14}$$

Substituint,

$$\sqrt{x+y} = \frac{t}{\sqrt{t}},\ \sqrt{x-y} = \frac{s}{\sqrt{t}} \quad \text{i} \quad \sqrt{\frac{x}{2} \pm \frac{\sqrt{x^2-y^2}}{2}} = \frac{t \pm s}{2\sqrt{t}}.$$

A partir d'aquestes igualtats és immediat obtenir (13).

Els canvis de variable de la forma (14) s'usen en molts contextos i se solen dir *parametritzacions racionals*, veure per exemple [22] i les seves referències.

3.6 L'aproximació de π d'Arquimedes

El mètode ideat per Arquimedes consisteix a aproximar π pels perímetres dels polígons regulars de $6 \cdot 2^n$ costats, circumscrits i inscrits a la circumferència de diàmetre 1, que denotarem per q_n i p_n, respectivament. Aleshores, $p_n < \pi < q_n$ i $\lim_{n\to\infty} q_n = \lim_{n\to\infty} p_n = \pi$.

Començarem calculant p_n. El perímetre de l'hexàgon inscrit és $p_0 = 3$ ja que el costat és igual al radi. Si anomenen x el costat d'un polígon regular, volem saber quin serà el costat y del polígon regular que té el doble de costats. Per obtenir y en funció de x ens basarem en la Figura 9.

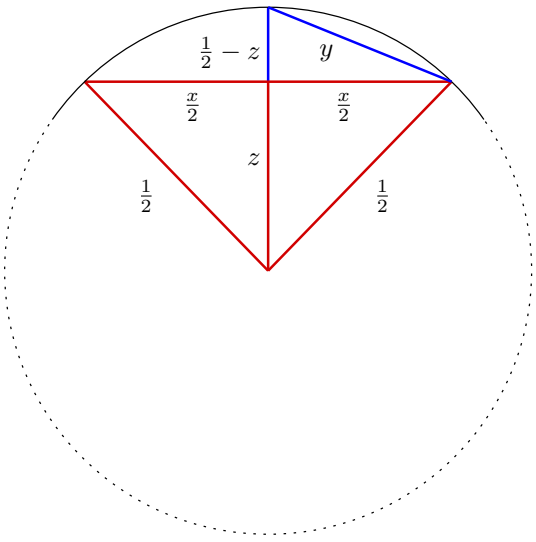


Figura 9: Càlcul dels costats d'un polígon

L'aplicació del Teorema de Pitàgores dos cops diu que

$$\frac{x^2}{4}+z^2=\frac{1}{4},\qquad \frac{x^2}{4}+\left(\frac{1}{2}-z\right)^2=y^2.$$

Operant a la segona fórmula, $\frac{x^2}{4}+\frac{1}{4}+z^2-z=y^2$, i usant la primera, $\frac{1}{2}-z=y^2$. Com que $z=\sqrt{\frac{1-x^2}{4}}$, concloem que $y=\sqrt{\frac{1}{2}\left(1-\sqrt{1-x^2}\right)}$.

Per tant, si anomenem ℓ_n el costat del polígon amb $6\cdot 2^n$ costats, tindrem $\ell_0=1/2$, $p_0=3$, i a partir d'aquí

$$\ell_{n+1}=\sqrt{\frac{1}{2}\left(1-\sqrt{1-(\ell_n)^2}\right)},\qquad p_{n+1}=6\cdot 2^{n+1}\,\ell_{n+1},$$

amb $\lim_{n\to\infty} p_n=\pi$.

El càlcul efectiu de ℓ_{n+1} a partir de ℓ_n produeix errors de càlcul, ja que en fer l'operació $\sqrt{\frac{1}{2}\left(1-\sqrt{1-(\ell_n)^2}\right)}$, amb ℓ_n cada cop més petit, s'han de restar números molt propers. Per tant, és convenient desracionalitzar l'última expressió usant la identitat:

$$\left(1-\sqrt{1-(\ell_n)^2}\right)\frac{1+\sqrt{1-(\ell_n)^2}}{1+\sqrt{1-(\ell_n)^2}}=\frac{(\ell_n)^2}{1+\sqrt{1-(\ell_n)^2}},$$

on el fet que ℓ_n sigui cada cop més petit influeix menys en la precisió del càlcul.

El resultat final és que si definim

$$\ell_0=\frac{1}{2},\qquad p_0=3,$$
$$\ell_{n+1}=\frac{\ell_n}{\sqrt{2\left(1+\sqrt{1-(\ell_n)^2}\right)}},\qquad p_{n+1}=6\cdot 2^{n+1}\,\ell_{n+1}.$$

obtenim una manera efectiva de calcular una successió $\{p_n\}$ que compleix $\lim_{n\to\infty} p_n=\pi$. En particular tenim que $p_0=\underline{3}$, $p_1=\underline{3.1}0\ldots$, $p_2=\underline{3.1}30\ldots$, $p_3=\underline{3.1}39\ldots$, $p_4=\underline{3.1415}0\ldots$, $p_{15}=\underline{3.1415926535}4,\ldots$.

Hi ha una expressió diferent pels càlculs d'Arquimedes, veure [18, Cap. 1] pels detalls, que calcula simultàniament q_n i p_n. Es verifica que

$$q_{n+1}=\frac{2\,q_n\,p_n}{q_n+p_n},\quad p_{n+1}=\sqrt{q_{n+1}\,p_n},\quad q_0=2\sqrt{3},\quad p_0=3.$$

A més, $q_{n+1}-p_{n+1}<(q_n-p_n)/3$. Per exemple, prenent el polígon amb 96 costats ($n=4$) obtenim $p_4=\underline{3.1415}0\ldots=p_4<\pi<q_4=\underline{3.1415}27\ldots$ i recuperem les fites clàssiques d'Arquimedes

$$3+\frac{10}{71}<p_4<\pi<q_4<3+\frac{10}{70}.$$

3.7 Fórmula de Viète

Demostrarem la fórmula de Viète per a calcular π,

$$\frac{2}{\pi} = \frac{\sqrt{2}}{2} \cdot \frac{\sqrt{2+\sqrt{2}}}{2} \cdot \frac{\sqrt{2+\sqrt{2+\sqrt{2}}}}{2} \cdot \frac{\sqrt{2+\sqrt{2+\sqrt{2+\sqrt{2}}}}}{2} \cdots$$

amb una prova semblant a la de la secció anterior. En aquesta demostració usarem àrees en lloc de longituds.

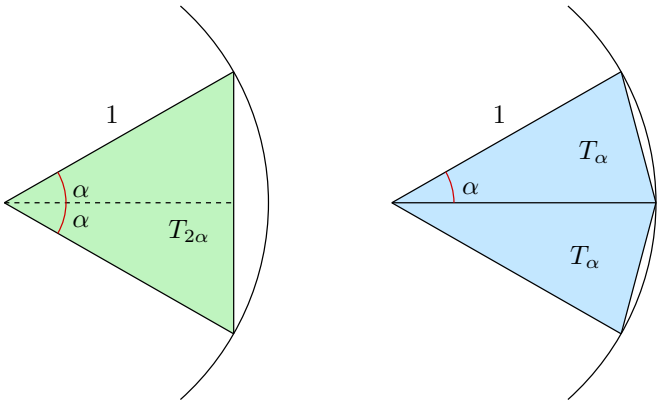


Figura 10: Sectors circulars

En primer lloc observem, usant la Figura 10, que l'àrea $T_{2\alpha}$ d'un triangle d'angle 2α, amb $0 < \alpha < \pi/2$, dins d'un disc de radi 1 és $T_{2\alpha} = \sin(\alpha)\cos(\alpha) = \sin(2\alpha)/2$. Per tant, si anomenem A_n l'àrea del polígon inscrit de 2^{n+1} costats corresponent tenim que $A_1 = 2$ i es compleix que

$$\frac{A_n}{A_{n+1}} = \frac{T_{2\alpha}}{2T_\alpha} = \frac{\sin(\alpha)\cos(\alpha)}{\sin(\alpha)} = \cos(\alpha),$$

on $\alpha = \pi/2^{n+1}$.

Així, si definim $d_n = 2\cos\left(\pi/2^{n+1}\right)$, usant la igualtat $2\cos(x/2) = \sqrt{2+2\cos(x)}$ obtenim que $d_{n+1} = \sqrt{2+d_n}$. Així,

$$d_1 = \sqrt{2}\,,\ d_2 = \sqrt{2+\sqrt{2}}\,,\ d_3 = \sqrt{2+\sqrt{2+\sqrt{2}}}\,,\ \ldots$$

i arribem a que,

$$A_{n+1} = \frac{2}{d_n}A_n \implies A_n = A_1\prod_{j=1}^{n-1}\frac{2}{d_j} \implies 2\prod_{j=1}^{\infty}\frac{2}{d_j} = \pi,$$

resultat equivalent a la fórmula de Viète, vegeu també la Figura 11.

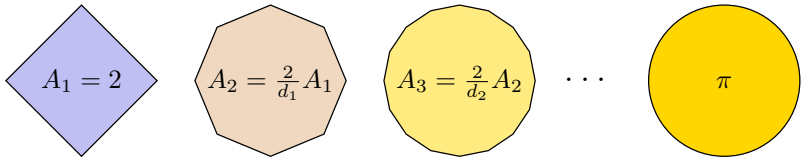


Figura 11: Visió gràfica de la fórmula de Viéte

3.8 Proves d'identitats per derivació

Usarem només el fet de que si la derivada d'una funció derivable és idènticament zero aleshores la funció és constant. Recordem que aquest resultat ha estat provat a la Secció 1.2.6 com a conseqüència del Teorema del valor mitjà.

3.8.1 La identitat trigonomètrica fonamental

Una de les relacions més conegudes a matemàtiques, que com ja hem vist és equivalent al Teorema de Pitàgores, és $\cos^2(x) + \sin^2(x) = 1$. Observem que si considerem la funció $f(x) = \cos^2(x) + \sin^2(x)$ aleshores

$$f'(x) = -2\cos(x)\sin(x) + 2\sin(x)\cos(x) = 0.$$

Per tant $\cos^2(x) + \sin^2(x) = f(x) \equiv f(0) = \cos^2(0) + \sin^2(0) = 1$. D'alguna manera la prova té molta "trampa" ja que la propietat que volem provar s'usa també en el càlcul de les derivades. A continuació, en farem un parell més, molt més interessants.

3.8.2 Una identitat d'Euler

Euler va demostrar que

$$\arctan\left(\frac{1}{x}\right) = \arctan\left(\frac{1}{x+y}\right) + \arctan\left(\frac{y}{x^2+x\,y+1}\right), \qquad (15)$$

per a tot $x > 0$ i y tals que $x+y > 0$ i $x^2+x\,y+1 > 0$. Anem a fer una prova usant el mateix mètode de derivació. Per a cada x considerem la funció de la variable y

$$f_x(y) = \arctan\left(\frac{1}{x}\right) - \arctan\left(\frac{1}{x+y}\right) - \arctan\left(\frac{y}{x^2+x\,y+1}\right).$$

Aleshores, si derivem la funció f_x obtenim

$$\frac{\mathrm{d}}{\mathrm{d}y} f_x(y) = 0 + \frac{1}{(x+y)^2+1} - \frac{1}{(x+y)^2+1} = 0.$$

Per exemple,

$$\frac{\mathrm{d}}{\mathrm{d}y}\arctan\left(\frac{y}{x^2+x\,y+1}\right)=\frac{\frac{1}{x^2+x\,y+1}-\frac{x\,y}{(x^2+x\,y+1)^2}}{\frac{y^2}{(x^2+x\,y+1)^2}+1}=\cdots=\frac{1}{(x+y)^2+1}.$$

Per tant

$$\begin{aligned}&\arctan\left(\frac{1}{x}\right)-\arctan\left(\frac{1}{x+y}\right)-\arctan\left(\frac{y}{x^2+x\,y+1}\right)\\&\qquad=f_x(y)\equiv f_x(0)=\arctan\left(\frac{1}{x}\right)-\arctan\left(\frac{1}{x}\right)-\arctan(0)=0\end{aligned}$$

i com a conseqüència s'obté (15).

Prenent $x=1$ i $y=1$ en la identitat d'Euler (15) obtenim la fórmula

$$\frac{\pi}{4}=\arctan\left(\frac{1}{2}\right)+\arctan\left(\frac{1}{3}\right),$$

que va ser utilitzada pel mateix Euler per aproximar π, usant el primers termes de la sèrie de Taylor de l'arctangent, per tal d'obtenir aproximacions de $\arctan(1/2)$ i $\arctan(1/3)$.

De fet, el número π que hi ha a la cúpula de la Sala π al "Palais de la découverte" de París es va calculat amb una fórmula similar obtinguda per Machin al 1706,

$$\frac{\pi}{4}=4\arctan\left(\frac{1}{5}\right)-\arctan\left(\frac{1}{239}\right),\tag{16}$$

vegeu la Figura 12. Aquesta fórmula va ser usada per W. Shanks en 1873 per trobar "a mà" 707 decimals de π. Aquest era el màxim nombre de xifres decimals de π de l'època.

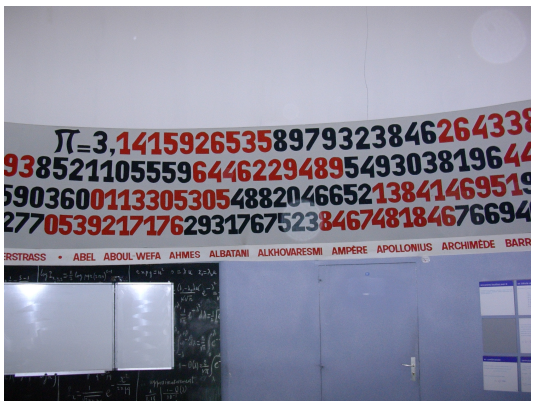


Figura 12: Cúpula de la Sala π

Es van posar a la Sala π l'any 1937 amb motiu d'una Exposició Universal. L'any 1944 en D. F. Ferguson, ja amb una "calculadora mecànica", va veure que només 527 eren correctes i l'any 1950 es van corregir. Avui en dia visitar aquesta sala és quasi una obligació per a tots els matemàtics que van a París.

Per exemple, usant que per a $|x| < 1$,

$$\arctan(x) = \sum_{n=0}^{\infty} \frac{(-1)^n\, x^{2n+1}}{2n+1},$$

podem definir

$$\Pi(m) = 16 \sum_{n=0}^{m} \frac{(-1)^{2n+1}}{(2n+1)5^{2n+1}} - 4 \sum_{n=0}^{[m/3]} \frac{(-1)^{2n+1}}{(2n+1)239^{2n+1}},$$

on $[m/3]$ és la part entera de $m/3$, i sabem que $\lim_{m\to\infty} \Pi(m) = \pi$. En particular, $\Pi(2) \approx 3.141621$ amb $|\pi - \Pi(2)| < 3 \times 10^{-5}$,

$$|\pi - \Pi(10)| < 6 \times 10^{-17}, \qquad |\pi - \Pi(100)| < 10^{-143},$$
$$|\pi - \Pi(300)| < 9 \times 10^{-424}, \qquad |\pi - \Pi(500)| < 2 \times 10^{-703}.$$

Com veiem, en Shanks va haver de calcular molt. Quan es va detectar l'error als seus càlculs ell ja havia mort i es va estalviar el disgust de veure que havia errat.

Derivant, també es poden demostrar fórmules com

$$\arctan(x) + \arctan\left(\frac{1}{x}\right) = \operatorname{sgn}(x)\frac{\pi}{2}, \quad x \neq 0,$$

o també,

$$\arctan(x) - \frac{1}{2}\arctan\left(\frac{2x}{1-x^2}\right) = \begin{cases} \pi/2, & \text{si } x > 1, \\ 0, & \text{si } |x| < 1, \\ -\pi/2, & \text{si } x < -1, \end{cases}$$

o moltes d'altres similars i útils per a calcular π, vegeu per exemple [23].

3.9 Una prova de la fórmula de Machin

És clar que la fórmula de Machin (16) es pot demostrar a partir de la fórmula de la tangent de la suma de dos angles. Donem a continuació una prova diferent i més elegant basada en les propietats dels números complexos. Fent uns quant càlculs obtenim

$$\frac{(5+\mathrm{i})^4}{239+\mathrm{i}} = \frac{476+480\,\mathrm{i}}{239+\mathrm{i}} = \frac{(476+480\,\mathrm{i})(239-\mathrm{i})}{57122} = 2(1+\mathrm{i}),$$

o de manera similar $(5+\mathrm{i})^4(239-\mathrm{i}) = 2^2\,13^4(1+\mathrm{i})$. Aleshores, la fórmula (16) es redueix a igualar els arguments de les dues bandes en qualsevol d'aquestes expressions.

De manera similar, a partir de la igualtat $(7+\mathrm{i})^5(79+3\mathrm{i})^2 = 2^3\,5^{10}(1+\mathrm{i})$ obtenim una altra fórmula de tipus Machin

$$\frac{\pi}{4} = 5\arctan\left(\frac{1}{7}\right) + 2\arctan\left(\frac{3}{79}\right).$$

Des d'aquest punt de vista és clar que la dificultat està en trobar noves fórmules de tipus Machin i no pas en demostrar que són certes. Una amb 4 termes molt útil, ja que els valors on s'avalua l'arctangent són molt petits, és

$$\frac{\pi}{4} = 12\arctan\left(\frac{1}{49}\right) + 32\arctan\left(\frac{1}{57}\right) - 5\arctan\left(\frac{1}{239}\right) + 12\arctan\left(\frac{1}{110443}\right),$$

que prové de la igualtat

$$(49+\mathrm{i})^{12}(57+\mathrm{i})^{32}(239-\mathrm{i})^5(110443+\mathrm{i})^{12} = 2^{30}\,5^{96}\,13^{32}\,1201^{12}(1+\mathrm{i}).$$

3.10 Un producte infinit telescòpic

Anem a demostrar que

$$P = \prod_{n=2}^{\infty}\left(1-\frac{1}{n^2}\right) = \frac{1}{2}.$$

Per a fer-ho, partim del fet que

$$P = \lim_{m\to\infty} P_m \quad \text{on} \quad P_m = \prod_{n=2}^{m}\left(1-\frac{1}{n^2}\right).$$

Ara bé

$$\begin{aligned}
P_m &= \prod_{n=2}^{m}\left(1-\frac{1}{n^2}\right) = \prod_{n=2}^{m}\left(1+\frac{1}{n}\right)\left(1-\frac{1}{n}\right)\\
&= \prod_{n=2}^{m}\left(\frac{n+1}{n}\right)\left(\frac{n-1}{n}\right) = \prod_{n=2}^{m}\left(\frac{n+1}{n}\right)\prod_{n=2}^{m}\left(\frac{n-1}{n}\right)\\
&= \left(\frac{3}{2}\frac{4}{3}\frac{5}{4}\cdots\frac{m}{m-1}\frac{m+1}{m}\right)\left(\frac{1}{2}\frac{2}{3}\frac{3}{4}\cdots\frac{m-2}{m-1}\frac{m-1}{m}\right)\\
&= \left(\frac{\cancel{3}}{2}\frac{\cancel{4}}{\cancel{3}}\frac{\cancel{5}}{\cancel{4}}\cdots\frac{\cancel{m}}{\cancel{m-1}}\frac{m+1}{\cancel{m}}\right)\left(\frac{1}{\cancel{2}}\frac{\cancel{2}}{\cancel{3}}\frac{\cancel{3}}{\cancel{4}}\cdots\frac{\cancel{m-2}}{\cancel{m-1}}\frac{\cancel{m-1}}{m}\right) = \frac{m+1}{2m}.
\end{aligned}$$

Per tant $\lim_{m\to\infty} P_m = \lim_{m\to\infty} (m+1)/(2m) = 1/2$, com volíem demostrar. Aquest tipus de productes infinits s'anomenen *telescòpics* ja que presenten un comportament similar a las sèries telescòpiques que ja han aparegut en aquest treball a la Secció 1.1.9.

3.11 Identitat de Chu–Vandermonde

La igualtat següent va ser provada pel matemàtic francés Alexandre Vandermonde (1735–1796). Sembla ser que ja era coneguda pel matemàtic xinés Chu Shi-Chieh a principis del segle XIV. Involucra números combinatoris dels que parlarem amb més detall a la Secció 4.3.

Proposició 3.1. *Per a tot $m, n, k \in \mathbb{N}$ amb $0 \le k \le m+n$ es compleix*

$$\binom{m+n}{k} = \sum_{j=0}^{k} \binom{m}{j}\binom{n}{k-j}. \tag{17}$$

Prova. El resultat és conseqüència del famós Binomi de Newton aplicat a $(1+x)^\ell$:

$$(1+x)^\ell = \sum_{i=0}^{\ell} \binom{\ell}{i} x^i,$$

per a diferents valors de ℓ. Observi's que aquest resultat ens permet identificar el coeficient de x^i de $(1+x)^\ell$ amb el número combinatori $\binom{\ell}{i}$. Així, com que $(1+x)^{m+n} = (1+x)^n(1+x)^m$, tenim que el coeficient de x^k de $(1+x)^{m+n}$ és el terme de l'esquerra de (17) i el de la dreta prové de buscar el terme de x^k del producte de les expansions respectives de $(1+x)^m$ i $(1+x)^n$. Precisament aquest terme s'obté sumant per a cada j entre 0 i k el producte del coeficient de x^j de $(1+x)^m$ pel coeficient de x^{k-j} de $(1+x)^n$. □

3.12 Càlcul enginyós d'una primitiva

Per calcular la primitiva següent,

$$\int \frac{\cos(x)}{\sin(x)+\cos(x)}\,\mathrm{d}x,$$

es podria usar el típic canvi trigonomètric $y = \tan(x/2)$, transformant-la en una integral racional i usar a continuació les tècniques ben conegudes per trobar-ne una primitiva. Veiem a continuació una manera més enginyosa de fer-ho.

Tenim que

$$\begin{aligned}\int \frac{\sin(x)+\cos(x)}{\sin(x)+\cos(x)}\,\mathrm{d}x &= \int \mathrm{d}x = x + C_1,\\ \int \frac{\cos(x)-\sin(x)}{\sin(x)+\cos(x)}\,\mathrm{d}x &= \int \frac{(\sin(x)+\cos(x))'}{\sin(x)+\cos(x)}\,\mathrm{d}x\\ &= \ln|\sin(x)+\cos(x)| + C_2.\end{aligned}$$

Sumant

$$\int \frac{2\cos(x)}{\sin(x)+\cos(x)}\,\mathrm{d}x = x + \ln|\sin(x)+\cos(x)| + (C_1+C_2).$$

Per tant

$$\int \frac{\cos(x)}{\sin(x)+\cos(x)}\,\mathrm{d}x = \frac{1}{2}\left(x + \ln|\sin(x)+\cos(x)|\right) + C.$$

3.13 Fórmula de Laisant

El matemàtic francès Charles-Ange Laisant va donar al 1905 una fórmula que permet calcular les primitives de la inversa d'una funció en termes de la primitiva de la funció ([34]). Aquest resultat es coneix com *fórmula de Laisant* i el demostrarem a la proposició següent.

Proposició 3.2. *Sigui $f(x)$ una funció invertible, amb derivada contínua, i F tal que $F'(x) = f(x)$. Aleshores les primitives de $f^{-1}(y)$ són de la forma $y\,f^{-1}(y) - F\big(f^{-1}(y)\big) + K$, amb $K \in \mathbb{R}$.*

Prova. Fixem un interval (a,b). Usant la fórmula d'integració per parts amb $u(x) = x$ i $v(x) = f(x)$, vegeu la fórmula (11) en la Secció 2.8, tenim

$$\int_a^b x\,f'(x)\,\mathrm{d}x = x\,f(x)\Big|_a^b - \int_a^b f(x)\,\mathrm{d}x. \tag{18}$$

Fent el canvi de variables $x = f^{-1}(y)$ en la integral de l'esquerra obtenim

$$\int_{f(a)}^{f(b)} f^{-1}(y)\,\mathrm{d}y = x\,f(x)\Big|_a^b - \int_a^b f(x)\,\mathrm{d}x. \tag{19}$$

Prenent $b = f^{-1}(t)$ arribem a

$$\int_{f(a)}^{t} f^{-1}(y)\,\mathrm{d}y = t\,f^{-1}(t) - F\big(f^{-1}(t)\big) + K_a,$$

on K_a no depèn de t. Aquesta fórmula és equivalent al que volíem demostrar. □

Veiem uns quants exemples d'aplicació:

$$\int \ln(y)\,\mathrm{d}y = y\,\ln(y) - \exp(\ln(y)) + K = y\ln(y) - y + K,$$
$$\int \arccos(y)\,\mathrm{d}y = y\,\arccos(y) - \sin(\arccos(y)) + K,$$
$$\int \arctan(y)\,\mathrm{d}y = y\,\arctan(y) - \ln|\arctan(y)| + K.$$

La fórmula de Laisant també és certa relaxant les hipòtesis sobre f, consulteu [32, 37]. Per exemple, també es compleix si f és continua i invertible.

3.14 Àrea sota la campana de Gauss

A [9] es calcula d'onze maneres diferents l'àrea sota la campana de Gauss. Anem a provar que

$$I = \int_0^\infty \mathrm{e}^{-x^2}\,\mathrm{d}x = \frac{\sqrt{\pi}}{2},$$

amb una de les demostracions més senzilles, deguda a Laplace. S'assembla a la més famosa, deguda a Poisson, que també consisteix a relacionar-la amb una integral doble. La diferencia principal és que Poisson la calcula fent un canvi a coordenades polars, mentre que en la prova de Laplace el canvi de variables que s'usa és per a integrals d'una variable.

Figura 13: Gauss i la seva campana al bitllet de 10 marcs alemanys.

Tenim que

$$I^2 = \left(\int_0^\infty \mathrm{e}^{-x^2}\,\mathrm{d}x\right)\left(\int_0^\infty \mathrm{e}^{-y^2}\,\mathrm{d}y\right) = \int_0^\infty \left(\int_0^\infty \mathrm{e}^{-(x^2+y^2)}\,\mathrm{d}x\right)\mathrm{d}y$$
$$\overset{(\star)}{=} \int_0^\infty \left(\int_0^\infty y\,\mathrm{e}^{-y^2(t^2+1)}\,\mathrm{d}t\right)\mathrm{d}y \overset{(\bullet)}{=} \int_0^\infty \left(\int_0^\infty y\,\mathrm{e}^{-y^2(t^2+1)}\,\mathrm{d}y\right)\mathrm{d}t.$$

A $(\star)$ hem fet el canvi de variable $x = y\,t$ en la integral entre parèntesi i a $(\bullet)$ hem canviat l'ordre d'integració usant el Teorema de Fubini. Finalment,

com que quan $a > 0$,

$$\int_0^\infty y\,\mathrm{e}^{-a\,y^2}\,\mathrm{d}y = -\frac{1}{2\,a}\mathrm{e}^{-a\,y^2}\Big|_0^\infty = \frac{1}{2\,a},$$

obtenim

$$\begin{aligned} I^2 &= \int_0^\infty \left(\int_0^\infty y\,\mathrm{e}^{-y^2(t^2+1)}\,\mathrm{d}y\right)\mathrm{d}t \\ &= \int_0^\infty \frac{1}{2(t^2+1)}\,\mathrm{d}t = \frac{1}{2}\arctan(t)\Big|_0^\infty = \frac{\pi}{4}, \end{aligned}$$

com volíem demostrar.

3.15 Ramanujan

Srinivasa Ramanujan (1887–1920) va ser un matemàtic indi, amb molt poca formació acadèmica, que va fer contribucions substancials a la matemàtica. La seva intuïció i habilitat per trobar noves igualtats matemàtiques encara fascina i intriga a la comunitat científica. Simplificant, potser es podria dir que Ramanujan ha estat la persona amb més habilitat del món en fer càlculs.

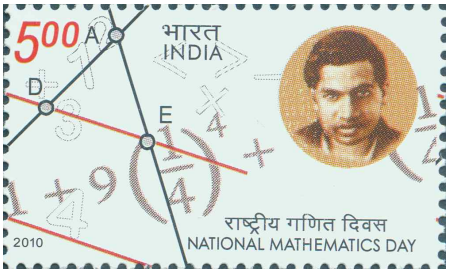


Figura 14: Segell i cartell de la pel·lícula dedicats a Ramanujan

Fa poc temps una pel·lícula *L'home que coneixia l'infinit*, vegeu la Figura 14, va ajudar a donar a conèixer la seva obra entre el gran públic.

Presentarem a continuació dues de les seves igualtats. La primera la va deduir quan anava a l'escola:

$$\sqrt{1+2\sqrt{1+3\sqrt{1+4\sqrt{1+5\sqrt{\cdots}}}}} = 3.$$

i no és molt difícil de demostrar. Per a provar-la definim

$$\begin{aligned} f(n) := n(n+2) &= n\sqrt{(n+2)^2} = n\sqrt{n^2+4\,n+4} \\ &= n\sqrt{1+(n+1)(n+3)} = n\sqrt{1+f(n+1)}\,. \end{aligned}$$

Substituint quan $n = 1$ tenim

$$\begin{aligned} 3 = f(1) &= \sqrt{1+f(2)} = \sqrt{1+2\sqrt{1+f(3)}} \\ &= \sqrt{1+2\sqrt{1+3\sqrt{1+f(4)}}} = \sqrt{1+2\sqrt{1+3\sqrt{1+4\sqrt{1+f(5)}}}} \\ &= \sqrt{1+2\sqrt{1+3\sqrt{1+4\sqrt{1+5\sqrt{1+f(6)}}}}} = \cdots, \end{aligned}$$

tal i com volíem veure.

La segona és una de les 17 fórmules que va donar per calcular π.

$$\frac{1}{\pi} = \frac{\sqrt{8}}{9801} \sum_{n=0}^{\infty} \frac{(4n)!\,(1103 + 26390\,n)}{(n!)^4\, 396^{4n}}.$$

Aquesta fórmula és molt útil computacionalment, profunda matemàticament i difícil de demostrar.

Ens limitarem a comprovar la seva eficàcia. Si definim $P(m) = 1/Q(m)$, on

$$Q(m) = \frac{\sqrt{8}}{9801} \sum_{n=0}^{m} \frac{(4n)!\,(1103 + 26390\,n)}{(n!)^4\, 396^{4n}},$$

obtenim:

$$\begin{aligned} P(0) &= \frac{9801\sqrt{2}}{4412} \approx \underline{3.1415927}300\ldots, & |\pi - P(0)| &< 10^{-7}, \\ P(1) &= \frac{2510613731736\sqrt{2}}{1130173253125}, & |\pi - P(1)| &< 10^{-15}, \\ & & |\pi - P(2)| &< 10^{-23}, \\ & & |\pi - P(3)| &< 10^{-31}, \\ & & |\pi - P(10)| &< 10^{-87}, \\ & & |\pi - P(100)| &< 10^{-806}, \\ & & |\pi - P(200)| &< 10^{-1604}, \\ & & |\pi - P(300)| &< 10^{-2403}. \end{aligned}$$

Per tenir més informació sobre aquesta i altres fórmules similars es pot consultar [5].

4 Altres Mètodes

Com ja hem comentat, en aquesta secció inclourem exemples de proves basades en el principi de les caselles, en el mètode del descens infinit de Fermat, proves combinatòries, proves per invariància o paritat, proves geomètriques i proves sense paraules.

4.1 El principi de les caselles o de Dirichlet

Aquest principi enunciat de manera informal diu que si hi ha més coloms que caselles, i tots els coloms entren en una de les caselles, en una de les caselles hi ha com a mínim dos coloms, vegeu-ne una il·lustració a la Figura 15.

Figura 15: Il·lustració del mètode de les caselles

De fet, aquest resultat es pot demostrar de manera senzilla usant reducció a l'absurd, però per tal de sistematitzar-ho és costum dir que s'utilitza aquest principi quan la situació ho permet.

Usant-lo, es poden demostrar resultats força interessants des del punt de vista teòric, com per exemple el Teorema d'aproximació de Dirichlet que afirma que per a tot número real $x \in \mathbb{R}$ hi ha infinits números racionals $p/q \in \mathbb{Q}$ tals que

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{q^2},$$

vegeu una prova a [21]. En aquest treball ens limitarem a donar algunes aplicacions més senzilles. Per veure més exemples podeu consultar moltes de les referencies donades a la introducció, com per exemple [24, pp. 105–112].

4.1.1 Punts dins d'un quadrat

Proposició 4.1. *Si posem 10 punts dins d'un quadrat de mida* 1 *aleshores dos d'ells estan a distancia més petita o igual que* $\sqrt{2}/3$.

Prova. El resultat és una conseqüència molt directa del principi de les caselles. Dividim el quadrat en 9 quadradets de mida $1/3 \times 1/3$. Aleshores per l'esmentat principi hi ha com a mínim dos punts (*que són els coloms*) dins d'un mateix quadradet. Finalment, aquest dos punts estan a una distància inferior a la diagonal del quadradet que, pel Teorema de Pitàgores val $\sqrt{2}/3$, vegeu la Figura 16. □

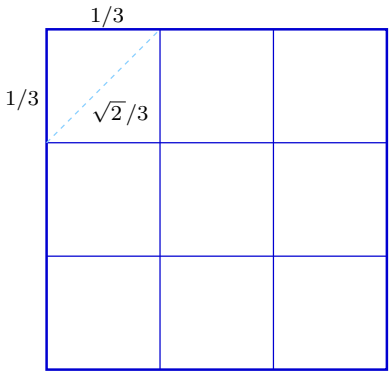


Figura 16: Quadrat 1×1 dividit en 9 quadrats iguals de mida $1/3 \times 1/3$

Si es pensa el problema sense usar el principi de les caselles ben aviat es té la sensació que el valor $\sqrt{2}/3$ segurament es pot reduir. És més, si els dos punts que comparteixen quadradet estan a distància $\sqrt{2}/3$ aleshores ocupen dos vèrtexs oposats del quadradet i no és difícil veure que no és possible posar 8 punts més mantenint aquesta distància, com la mínima entre els 10 punts. De fet, aquesta qüestió està molt relacionada amb l'anomenada *d'empaquetament de discs dins d'un quadrat*, que en poques paraules consisteix a posar k discs iguals i disjunts dins d'un quadrat de manera que ocupin l'àrea màxima possible, vegeu [11, Cap. D].

4.1.2 Sumes coincidents

Demostrarem que *donats 10 números naturals, de com a molt dues xifres, sempre hi ha dos subconjunts disjunts, no buits, d'aquests 10 números que tenen la mateixa suma.*

Per a provar-ho, les caselles del colomar seran els valors possibles de les sumes de tots els conjunts formats per, com a molt, 10 números menors que 100. Aquestes sumes van des de 1 fins a $90 + 91 + \cdots + 99 = 945$. Qualsevol conjunt format per 10 números naturals té $2^{10} = 1024$ parts (vegeu la Secció 4.3.3), que seran els coloms, i la suma de tots els elements de cada part dirà a quina casella del colomar va aquesta part. Com que el nombre total de valors possibles de les sumes és 945, és segur que hi ha dues parts diferents que tenen la mateixa suma. Si aquests dos subconjunts són disjunts, ja hem provat el que volíem. Però, encara que els subconjunts triats no ho siguin, es poden treure els elements comuns a tots dos, obtenint dues parts d'ells, més petites, disjuntes, no buides, i de la mateixa suma, tal i com volíem demostrar.

De fet, fixat qualsevol enter positiu m, es pot plantejar el problema següent: *Quina és la quantitat mínima k_m, de números naturals, tal que si agafem k_m números de com a molt m xifres, sempre hi ha dos subconjunts*

disjunts, no buits, d'aquests k_m números que tenen la mateixa suma? Argumentant com abans, aquest valor k_m és més petit o igual que el mínim enter positiu $k = K_m$ tal que

$$2^k > \sum_{j=1}^{k} (10^m - j) = k \cdot 10^m - \frac{k(k+1)}{2}.$$

Tot i que aquesta equació no es pot resoldre explícitament per a m arbitrari, no és difícil, per a un m donat, trobar el valor K_m. Recordem que $k_m \leq K_m$. A la Taula 1 hi ha els valors per a $m \leq 10$. Observi's que precisament $K_2 = 10$ correspon al problema plantejat a l'inici d'aquesta secció.

m	1	2	3	4	5	6	7	8	9	10
K_m	6	10	14	18	22	25	29	32	36	39

Taula 1: Valors de K_m en funció del nombre màxim de xifres m. Recordem que $k_m \leq K_m$.

4.1.3 Repunits

Si considerem tots els múltiples de 3:

$$3, 6, 9, 12, 15, \ldots, 105, 108, 111, 114, 117, \ldots$$

Els de 13:

$$13, 26, 39, \ldots, 1300, \ldots, 111098, 111111, 111124, \ldots$$

i els de 27:

$$27, 54, 81, \ldots, 111111111111111111111111111, \ldots$$

$(27 \times 411522633744855967078189 3 = 111111111111111111111111111)$.

Anomenarem repunits als números naturals formats per n xifres, totes iguals a 1 i els denotarem com r_n, vegeu també la Figura 17. Així,

$$27 \times 411522633744855967078189 3 = r_{27}.$$

De manera similar, per exemple:

$$\begin{aligned} 87 \times (&127713920817369093231162196679438058748403575989 7 \\ &828863346104725415070242656449553) = r_{84}, \\ 177 \times (&627746390458254865034526051475204017576898932831 13 \\ &622096672944130571249215317011927181418706842435655 \\ &994978028876333961079723791588198367859384808537 35 \\ &09102322661644695543) = r_{174}. \end{aligned}$$

Figura 17: Repunits arreu

Clarament, si un número és parell o acaba en 5 cap dels seus múltiples pot ser un repunit. Però a partir del que hem vist és natural preguntar-se si és cert que tot número natural acabat en 1, 3, 7 o 9 té un múltiple que és un repunit. Es pot demostrar que és cert usant el principi de les caselles.

Proposició 4.2. *Tot número natural acabat en* $1, 3, 7$ *o* 9 *té un múltiple que és un repunit.*

Prova. Sigui n un número natural sota les hipòtesis de la proposició. Aleshores:

- Agafem n caselles i les numerem com $0, 1, 2, \ldots, n-1$.
- Ara agafem $n+1$ "coloms", que són els $n+1$ repunits següents:

$$1,\ 11,\ 111,\ 1111,\ r_5 = 11111,\ r_6, \ldots,\ r_n,\ r_{n+1}.$$

- Finalment posem el repunit r_m a la casella número k_m, on $0 \le k_m \le n-1$ és la resta de dividir r_m entre n. És a dir:

$$r_m = 111\cdots111 = n \times q_m + k_m, \quad 0 \le k_m \le n-1.$$

Si algun repunit, per exemple r_j, cau a la casella 0 ja tenim el resultat desitjat ja que

$$r_j = 111\cdots111 = n \times q_j.$$

Si no, pel principi de les caselles, com que hi ha n caselles i $n+1$ coloms, hi ha una casella, per exemple la número i que conté com a mínim dos repunits $r_u > r_v$. Aleshores

$$r_u = n \times q_u + i, \quad \text{i} \quad r_v = n \times q_v + i,$$

fets que impliquen

$$r_u - r_v = n \times (q_u - q_v).$$

Com que r_u i r_v són repunits es té que

$$\begin{aligned} r_u - r_v &= 111\cdots111000\cdots000 = 111\cdots111 \times 10^\ell \\ &= 111\cdots111 \times 2^\ell \times 5^\ell = r_w \times 2^\ell \times 5^\ell, \end{aligned}$$

per a un cert repunit r_w. Finalment

$$n \times (q_u - q_v) = r_w \times 2^\ell \times 5^\ell,$$

però, com que per les hipòtesis, ni 2 ni 5 són divisors de n, obtenim que $n \times q = r_w$ amb

$$q = \frac{q_u - q_v}{2^\ell \times 5^\ell} = \frac{q_u - q_v}{10^\ell},$$

tal i com volíem demostrar. □

4.1.4 Zeros finals als números de Fibonacci

Anem a demostrar el fet següent, força sorprenent.

Proposició 4.3. *Per a tot natural m hi ha un número de Fibonacci que acaba, com a mínim, amb m zeros*

Prova. El que volem provar serà cert si demostrem el resultat següent: *Per a tot $m \in \mathbb{N}$ prenem $k = 10^m$ i siguin $\overline{F_n}, n \in \mathbb{N}$, el números de Fibonacci mòdul k. Aleshores hi ha un $N \in \mathbb{N}$ tal que $\overline{F_N} = 0$.*

Per tal d'aplicar el principi de les caselles introduïm les dues aplicacions $\Phi, \Phi^{-1} : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ donades per

$$\Phi(p, q) = (q, p + q), \quad \Phi^{-1}(p, q) = (q - p, p).$$

Clarament $\Phi \circ \Phi^{-1} = \Phi^{-1} \circ \Phi = \mathrm{Id}$ i, per tant, una és la inversa de l'altra. De fet, a partir de la seva definició és clar que

$$\Phi(F_{n-1}, F_n) = (F_n, F_{n+1}) \quad n \geq 1.$$

En aquest cas agafem com a coloms els $k^2 + 1$ elements de $\mathbb{Z}^2$:

$$\Phi^p(1, 1) = (F_{p+1}, F_{p+2}), \quad p = 0, \ldots, k^2.$$

Les caselles seran el k^2 elements de $(\mathbb{Z}/k\mathbb{Z})^2$, és a dir associarem a cada element $(F_{p+1}, F_{p+2}) \in \mathbb{Z}^2$ el corresponent $(\overline{F_{p+1}}, \overline{F_{p+2}}) \in (\mathbb{Z}/k\mathbb{Z})^2$. Com que hi ha més coloms que caselles sabem que existiran $i, j \in \mathbb{N}$, amb $i > j \geq 0$ tals que

$$\begin{aligned} \overline{\Phi^i(1, 1)} = \overline{\Phi^j(1, 1)} &\Longrightarrow \overline{\Phi^{i-j}(1, 1)} = \overline{\Phi^0(1, 1)} = \overline{(1, 1)} \\ &\Longrightarrow \Phi^N(\overline{1}, \overline{1}) = (\overline{1}, \overline{1}) \quad \text{amb} \quad N = i - j, \end{aligned}$$

on a la primera implicació hem aplicat Φ^{-j} a la primera igualtat i l'última Φ és la induïda a $(\mathbb{Z}/k\mathbb{Z})^2$ per les que hem definit a dalt. Per tant tenim que

$$(\overline{F_{N+1}}, \overline{F_{N+2}}) = \Phi^N(\overline{1}, \overline{1}) = (\overline{1}, \overline{1}) \Longrightarrow \overline{F_N} = \overline{F_{N+2}} - \overline{F_{N+1}} = \overline{1} - \overline{1} = 0,$$

ja que $\overline{F_N} + \overline{F_{N+1}} = \overline{F_{N+2}}$, tal i com volíem demostrar. □

De fet, a la demostració anterior es podrien haver agafat menys *coloms*, ja que, a partir de la definició dels números de Fibonacci, és clar que, per a tota parella (F_n, F_{n+1}), la situació en què ambdós números són parells mai es pot donar. Per tant, a priori ja se sap que una quarta part de les caselles (elements de $(\mathbb{Z}/k\mathbb{Z})^2$) quedaran sempre buides.

També és clar a partir de la prova que, per a cada m, hi ha infinits números de Fibonacci que acaben en com a mínim m zeros.

Per curiositat, tenim per exemple que, per a tot número natural n, F_{15n} acaba com a mínim amb un 0: $F_{15} = 610$, $F_{30} = 832040$. A més,

$$F_{150} = 9969216677189303386214405760200$$

és el més petit que acaba en 00. Finalment, per a $k = 1, 2, 3, 4$, $F_{75\times 10^k}$ acaba amb $k + 2$ zeros.

4.2 Mètode del descens infinit de Fermat

Sembla ser que aquest mètode ja va ser usat pels matemàtics pitagòrics per a demostrar la irracionalitat del número d'or, vegeu la secció següent. Fermat el va redescobrir i al 1659 va escriure: "Com que els mètodes usuals que surten als llibres són inadequats per a demostrar aquestes difícils proposicions, he descobert un mètode especial ... que anomenaré descens infinit". Tot i que aquest mètode es pot aplicar en altres contextos, un exemple prou clar del seu funcionament és el següent: si es vol demostrar que una certa equació no té solucions enteres positives és suficient provar que l'existència d'una solució positiva n_1 força la existència d'una altra solució positiva més petita n_2, donant lloc a una cadena infinita de desigualtats de la forma $n_1 > n_2 > \cdots > n_m > \cdots > 0$, cosa del tot impossible en els números naturals.

D'alguna manera, mentre inducció consisteix en un ascens infinit de pas 1 i serveix per demostrar afirmacions, el mètode del descens infinit consisteix a usar la impossibilitat d'un descens (amb pas variable) dins els números enters positius i se sol usar per arribar a una contradicció. A continuació trobarem un quants exemples de la seva utilització.

4.2.1 Irracionalitat del número d'or

Recordem que el número d'or (o raó àuria) $\varphi = \left(1 + \sqrt{5}\right)/2$ és la solució més gran de l'equació de segon grau $x^2 = x + 1$. Aquest número apareix en molts llocs a les matemàtiques, l'art i la natura, veure [2]. Per exemple, és present quan construïm un pentàgon regular i la seva estrella de cinc puntes associada, vegeu la Figura 18.

Pel Teorema de Thales tenim que

$$\frac{\varphi}{1} = \frac{\varphi + 1}{\varphi} \Longrightarrow \varphi^2 = \varphi + 1,$$

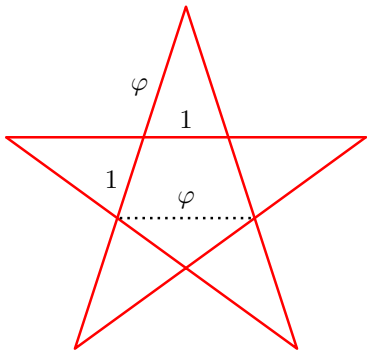


Figura 18: Estrella regular de cinc puntes

ja que, comparant angles, no és difícil argumentar que la base puntejada φ del triangle gran coincideix amb el costat de l'estrella regular.

Proposició 4.4. *El número d'or φ és irracional.*

Prova. Suposarem que φ és un número racional $\varphi = \frac{m}{n}$, amb m i n enters i arribarem a contradicció usant el mètode del descens infinit.

Sota aquesta suposició, com que φ compleix $x^2 = x + 1$, tenim que

$$m^2 = m\,n + n^2 \quad \text{amb } (m, n) \in \mathbb{N}^2. \tag{20}$$

Anem a demostrar en primer lloc que tant m com n han de ser números parells. Per a fer-ho descartem cas per cas totes les altres possibilitats:

- Si m i n són ambdós senars aleshores m^2, n^2 i $m\,n$ són els tres senars. Per tant (20) no es pot complir.
- Si m és senar i n és parell aleshores m^2 és senar i tant $m\,n$ com n^2 són els dos parells. Aleshores, de nou (20) no es pot complir.
- El cas m parell i n senar es pot descartar argumentant com en el cas anterior.

Per tant si (m, n) compleix (20) aleshores hi ha un $(m_1, n_1) \in \mathbb{N}^2$ tal que $m = 2m_1$ i $n = 2n_1$. A més,

$$m^2 = mn + n^2 \Longrightarrow 4m_1^2 = 4m_1\,n_1 + 4n_1^2 \Longrightarrow m_1^2 = m_1\,n_1 + n_1^2.$$

En resum si $(m, n) \in \mathbb{N}^2$ és una solució qualsevol de (20) aleshores es té $(m_1, n_1) \in \mathbb{N}^2$ amb $0 < n_1 < n = 2n_1$ que també ho és. Aquest procés es pot repetir indefinidament obtenint una seqüència infinita de números naturals complint $n > n_1 > n_2 > \cdots > n_k > \cdots > 0$, arribant a la contradicció desitjada. □

De fet, amb un argument similar al de la prova de la proposició anterior també es podria haver demostrat la irracionalitat de φ per reducció a l'absurd d'una manera encara més senzilla. Aquest argument consistiria a prendre els números naturals m i n de l'inici de la prova primers entre si. Seguint el mateix estudi de cassos possibles obtendríem que m i n tenen 2 com a factor en comú, arribant a la contradicció desitjada.

4.2.2 Una circumferència sense punts racionals

Demostrarem:

Proposició 4.5. *La circumferència $x^2+y^2=3$ no té punts $(x,y)\in\mathbb{Q}^2$.*

Prova. Si suposem que hi ha algun punt amb coordenades racionals a la circumferència podem suposar que aquest és $(p/r, q/r)$ amb p, q i r enters no negatius. Com que $\sqrt{3}$ és irracional, com es pot provar per exemple de manera similar a la prova de que $\sqrt{2}$ ho és, vegeu la Secció 1.4.4, tenim també que $p\,q\neq 0$, ja que, si no, tindríem una arrel quadrada racional de 3. Així, suposem per tal d'arribar a contradicció que

$$p^2+q^2=3r^2,\quad p,q,r\in\mathbb{N}.$$

Observem que qualsevol número natural s'escriu, per a un cert $n\in\mathbb{N}\cup\{0\}$, d'una de les 3 formes següents: $3n+1$, $3n-1$ o $3n$. Ara bé,

$$(3n\pm 1)^2=3\big(3n^2\pm 2n\big)+1\quad\text{i}\quad(3n)^2=3\big(3n^2\big). \tag{21}$$

Per tant, com que p^2+q^2 és un múltiple de 3, obligatòriament p i q també ho han de ser i aleshores $p=3p'$ i $q=3q'$ amb $p',q'\in\mathbb{N}$. Com a conseqüència

$$(3p')^2+(3q')^2=3r^2\Longrightarrow 3(p')^2+3(q')^2=r^2.$$

Usant de nou (21), com que r^2 és un múltiple de 3, obtenim que r també ho és i per tant $r=3r'$, amb $r'\in\mathbb{N}$. Finalment,

$$3(p')^2+3(q')^2=r^2=(3r')^2\Longrightarrow(p')^2+(q')^2=3(r')^2,$$

demostrant que si $(x,y,z)=(p,q,r)$ és una solució a $\mathbb{N}^3$ de $x^3+y^3=3z^3$ també ho és $(p',q',r')=(p/3,q/3,r/3)$. Iterant aquesta construcció arribem a la contradicció desitjada que ens dona el mètode del descens infinit. □

4.2.3 El número $\sqrt{2}$ és irracional, segona prova

Provarem de nou aquest resultat usant el mètode del descens infinit.

Prenem $(p,q)\in\mathbb{R}^2$, amb $p,q>0$ i tals que $\sqrt{2}=p/q$. És clar que

$$\sqrt{2}=\frac{p}{q}=\frac{2q-p}{p-q}\quad\text{i}\quad\frac{5}{4}<\frac{p}{q}<\frac{6}{4},$$

ja que $p(p-q) = q(2q-p)$ i $\sqrt{2} \approx 1.4142$. Aleshores, com que $4p/6 < q < 4p/5$, obtenim

$$0 < p - \frac{5}{4}q < p - q < \frac{6}{4}q - q < q,$$

i com a conseqüència $2q-p > 0$. Suposem ara, per tal d'arribar a contradicció, que $(p,q) \in \mathbb{N}^2$ amb p i q primers entre si. Aleshores $\sqrt{2} = p/q \in \mathbb{Q}$ i $\sqrt{2} = (2q-p)/(p-q) \in \mathbb{Q}$ amb $0 < p-q < q$. Com que podem repetir aquest procés indefinidament, això ens porta a la contradicció desitjada, proporcionada pel mètode del descens infinit.

4.3 Proves combinatòries

En poques paraules una prova combinatòria consisteix a comptar de dues maneres diferent els elements d'un cert conjunt triat adequadament. Igualant aquestes dues maneres de comptar s'obté el resultat que es vol demostrar.

Ens centrarem en aquesta secció en el càlcul i propietats del número combinatori $\binom{n}{k}$, on $0 \leq k \leq n$, amb $k, n \in \mathbb{N}$, que denota el nombre de subconjunts diferents de k elements que té un conjunt de n elements. Només usarem que, donat un conjunt de m elements diferents, aquests es poden ordenar de $m! = m(m-1)\cdots 2\cdot 1$ maneres ja que el primer pot ser qualsevol dels m, pel segon lloc només queden $m-1$ possibilitats, pel tercer $m-2$ i així successivament.

4.3.1 Números combinatoris

Anem a demostrar que

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots 1}.$$

Per a fer-ho, comptarem de dues formes diferents la quantitat de maneres en que es poden ordenar n objectes diferents. Per a fixar idees podem pensar que hi ha n persones i les volem posar en una filera de totes les maneres possibles.

- Per una banda, comptant de manera directa, sabem que es poden ordenar de $n!$ maneres.

- Per l'altra, per a aquest valor k, triem k persones qualssevol. Aleshores hi ha $\binom{n}{k}$ maneres de triar aquestes k persones. Per a cadascuna d'aquestes maneres posarem en primer lloc aquestes k persones i en segon lloc les altres $n-k$. Les primeres k persones es poden ordenar entre elles de $k!$ formes, mentre que les altres $n-k$ ho poden fer de $(n-k)!$ formes. Per tant, en total hi ha $\binom{n}{k}k!(n-k)!$ maneres de fer-ho.

En conclusió, igualant les dues formes de comptar arribem a

$$n! = \binom{n}{k} k!(n-k)!,$$

tal i com volíem demostrar.

4.3.2 Una propietat dels números combinatoris

Demostrarem la propietat fonamental

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}, \quad 1 \le k \le n, \tag{22}$$

que permet construir el conegut a occident com a triangle de Pascal o de Tartaglia, veure la Figura 19 tot i aquest triangle ja es coneixia molt abans a l'Índia i Xina.

Figura 19: Triangle de Pascal

Per això comptarem de dues maneres el nombre de subconjunts de k elements d'un conjunt amb $n+1$ elements:

- Per una banda hi ha $\binom{n+1}{k}$ subconjunts.
- Per l'altra, els comptem de la manera següent. Marquem un dels elements del conjunt. Aleshores, de subconjunts de k elements n'hi ha de dos tipus: els que el contenen i els que no. Del primer tipus n'hi ha tants com subconjunts de $k-1$ elements d'un conjunt de n, és a dir $\binom{n}{k-1}$. Del segon tipus n'hi ha tants com subconjunts de k elements d'un conjunt de n, és a dir $\binom{n}{k}$. En total en tenim $\binom{n}{k-1} + \binom{n}{k}$.

Igualant les dues expressions obtenim (22).

4.3.3 Un cas particular del binomi de Newton

Demostrem la igualtat

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n.$$

que també es pot provar directament aplicant el binomi de Newton a la igualtat òbvia $2^n = (1+1)^n$.

En la prova que donem comptarem de nou de dues maneres el nombre total de subconjunts d'un conjunt de n elements.

- L'expressió de l'esquerra de la fórmula es correspon a comptar els subconjunts de $0, 1, \ldots, n-1$ i n elements, respectivament i sumar-los.
- Per altra banda, veurem que 2^n és precisament el nombre total de subconjunts i en conseqüència la igualtat quedarà demostrada. Per a demostrar-ho llistem de forma ordenada els n elements del conjunt: $[a_1, a_2, \ldots, a_{n-1}, a_n]$. Un subconjunt, $\mathcal{C}$, estarà format per uns quants elements d'aquesta llista. Aleshores associem a aquest $\mathcal{C}$ una llista ordenada de 0's i 1's construïda de la manera següent: cada a_j es canvia per un 1 si $a_j \in \mathcal{C}$ i per un 0 en cas contrari. Per tant hi ha tants subconjunts con tires diferents de 0's i 1's amb longitud n, és a dir 2^n.

4.3.4 Una igualtat combinatòria més

Demostrarem que

$$\binom{2n}{n} = \binom{n}{0}^2 + \binom{n}{1}^2 + \cdots + \binom{n}{n-1}^2 + \binom{n}{n}^2.$$

Donat un conjunt amb $2n$ elements comptarem de dues maneres quants subconjunts de n elements té.

- Per una banda hi ha $\binom{2n}{n}$ subconjunts.
- Per l'altra banda, "pintem" n elements de color vermell i n elements de color blau. Ara, cada subconjunt amb n elements en tindrà k de vermells i $n-k$ de blaus, per a un cert $k, 0 \leq k \leq n$. Per a cada k fixat, podem triar k elements vermells de $\binom{n}{k}$ maneres i $n-k$ elements blaus de $\binom{n}{n-k}$ maneres. Així, com que per definició $\binom{n}{k} = \binom{n}{n-k}$, per a cada k hi ha $\binom{n}{k}\binom{n}{n-k} = \binom{n}{k}^2$ possibilitats. Variant k des de 0 fins a n obtenim un total de $\sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k} = \sum_{k=0}^{n} \binom{n}{k}^2$ subconjunts.

Igualant les dues maneres de comptar obtenim la fórmula desitjada.

4.4 Proves per invariància o paritat

En aquestes proves és essencial la paritat o invariància de certes quantitats involucrades en el problema, trobareu altres exemples a [17, Sec. 1 & 2] o [24, pp. 279–296].

4.4.1 Dues equacions diofàntiques

Anem a demostrar que les úniques solucions enteres positives de les dues equacions $2^n \pm 1 = m^2$, són $2^3 + 1 = 3^2$ i $2^1 - 1 = 1^2$.

Comencem per $2^n + 1 = m^2$. Clarament no té solucions enteres si $n = 1$. Si $n \geq 2$ i m és parell tampoc en té ja que $2^n + 1$ és senar i m^2 és parell. Finalment, si $m = 2k + 1$ és senar, l'equació s'escriu com $2^n = 4k(k + 1)$ o, equivalentment, $2^{n-2} = k(k + 1)$. Per tant, o bé $k = 1\,(m = 3)$ i $n = 3$ i tenim una solució, o bé k i $k + 1$ són ambdós parells, fet que és impossible.

Quan considerem $2^n - 1 = m^2$, òbviament $n = m = 1$ és una solució. Si $n \geq 2$ de nou no té solucions quan m és parell ja que $2^n - 1$ és senar i m^2 parell. Si $m = 2k + 1$ és senar tenim $2^n = 4k(k + 1) + 2$, o equivalentment, $2^{n-1} = 2k(k+1)+1$, situació també impossible ja que el número de l'esquerra de la igualtat és parell i el de la dreta és senar.

4.4.2 Una illa plena de camaleons

En una illa viuen 6000 camaleons, 3000 verds, 2000 blaus i 1000 grocs. Aquests camaleons ni es reprodueixen, ni moren, ni poden deixar la illa. Es van movent per la illa i sempre van sols. A més, mai es troben més de dos camaleons alhora, i quan se'n troben dos passa el següent:

- Si els dos tenen colors diferents, els dos adopten el tercer color.
- Si els dos tenen el mateix color, tots dos canvien de color, agafant colors diferents.

Dos camaleons verds a punt de transformar-se en un de blau i un de groc.

Anem a demostrar que en cap moment tots els camaleons tindran el mateix color.

Per a provar-ho designarem per (v, b) la quantitat de camaleons verds i blaus, respectivament, que hi ha en un cert instant. Observem que no cal parlar mai del nombre de camaleons grocs ja que sempre és $6000 - v - b$.

Quan hi ha una distribució (v, b) i dos camaleons es troben denotarem per $T(v, b)$ la nova distribució immediatament després. Aquest funció T ve

definida per les regles anteriors, tal i com es detalla a continuació:

$$T(v,b) = \begin{cases} (v-1, b-1), & \text{quan es troben un verd i un blau,} \\ (v-1, b+2), & \text{quan es troben un verd i un groc,} \\ (v+2, b-1), & \text{quan es troben un blau i un groc,} \\ (v-2, b+1), & \text{quan es troben dos verds,} \\ (v+1, b-2), & \text{quan es troben dos blaus,} \\ (v+1, b+1), & \text{quan es troben dos grocs.} \end{cases}$$

Un cop introduïda T, el nostre problema es redueix a demostrar que per a cap $n \in \mathbb{N}$, $T^n(v,b) \in \{(6000,0),(0,6000),(0,0)\}$, on $T^n = T \circ T^{n-1}$, i $T^0(v,b) = (v,b) = (3000,2000)$.

Per a fer-ho, definim la funció $H(v,b) = v - b$ i anem a demostrar que a $\mathbb{Z}/3\mathbb{Z}$ es compleix la igualtat següent

$$\overline{H(v,b)} = \overline{H(T(v,b))}, \tag{23}$$

on com és habitual la barra indica la classe a $\mathbb{Z}/3\mathbb{Z}$. Només cal veure la igualtat anterior en cadascuna de les sis possibilitats per T. Per exemple, per a la primera d'elles

$$\overline{H(T(v,b))} = \overline{(v-1)-(b-1)} = \overline{v-b} = \overline{H(v,b)}$$

i, per a la segona,

$$\overline{H(T(v,b))} = \overline{(v-1)-(b+2)} = \overline{v-b-3} = \overline{v-b} = \overline{H(v,b)}.$$

Ometem els detalls per a les quatre possibilitats restants. Així, sabem que per a tot n

$$\overline{H(T^n(3000,2000))} = \overline{H(3000,2000)} = \overline{1000} = \overline{1}.$$

Com que

$$\overline{H(6000,0)} = \overline{H(0,6000)} = \overline{H(0,0)} = \overline{0} \neq \overline{1},$$

el resultat queda provat.

En general, amb n camaleons, v_0 verds, b_0 blaus i $n - v_0 - b_0$ grocs, per tal que sigui possible que tots acabin sent dels mateix color, cal que $\overline{v_0 - b_0} \in \{\overline{n}, \overline{-n}, \overline{0}\}$.

De fet, en un llenguatge més matemàtic, el que estem estudiant són propietats del *semi-sistema dinàmic* donat per l'aplicació T. Els punts $T^n(v,b)$ formen la *semi-òrbita positiva* del punt (v,b). Una funció H complint la relació (23), però sense considerar-la a $\mathbb{Z}/3\mathbb{Z}$, és a dir complint $H(T(u,v)) = H(u,v)$, s'anomena *integral primera del sistema* i és un fet ben conegut que el coneixement d'una integral primera sempre ajuda molt a entendre l'evolució d'un sistema dinàmic.

4.4.3 Moviments de cavall

Demostrarem un resultat d'impossibilitat de certs moviments d'un cavall a un tauler d'escacs.

Proposició 4.6. *Si hi ha un cavall a una cantonada d'un tauler d'escacs és impossible que el cavall es mogui passant exactament un cop per cadascuna de les caselles i acabi a la cantonada oposada.*

Prova. La prova es basa en observar que cada cop que un cavall fa un moviment, la nova casella a la que va a parar té color contrari a la casella en què estava. Per tant, si un cavall fa una seqüència de n moviments consecutius podem assegurar que quan n és parell el color de la casella final coincideix amb el de la seva casella inicial, mentre que si és senar el color ha canviat. Com que el total de caselles del tauler és 64, el camí que es vol demostrar que és impossible té $n = 63$ moviments i la casella inicial i la final tindrien colors diferents. Això impossibilita que sigui la cantonada oposada a la cantonada inicial ja que ambdues són del mateix color. □

El que sí que hi ha són passeigs del cavall amb 63 moviments recorrent totes les caselles del tauler. I fins i tot, passeigs que amb 64 moviments les recorren totes, tornant a la casella inicial. Aquests moviments s'anomenen *periòdics*. Un exemple de moviment periòdic s'il·lustra a la Figura 20, extreta de l'entrada "Knight's tour" de la Wikipedia.

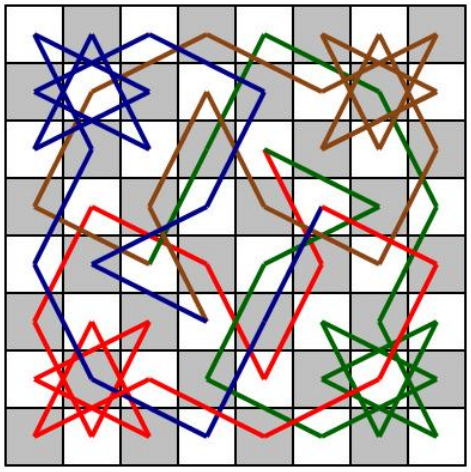


Figura 20: Moviment periòdic d'un cavall

4.4.4 Quadrats i dòminos

Demostrarem un resultat d'impossibilitat de recobriment d'una figura amb dòminos.

Proposició 4.7. *Un quadrat de mida $n \times n$ al que li hem tret dos quadrats de mida 1×1 situats a dues cantonades oposades no es pot pavimentar amb "dòminos" de mida 2×1.*

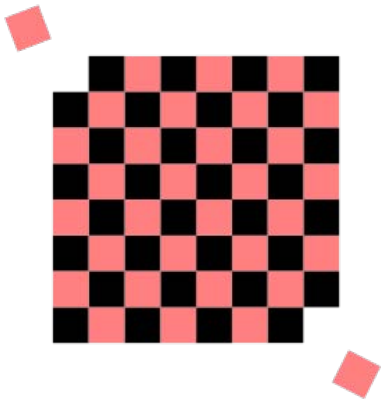


Figura 21: Quadrat 8×8 escapçat

Prova. Quan n és senar el resultat és trivialment cert, ja que $n^2 - 2$ és senar i per tant no és divisible per 2. Quan $n = 2k$ és parell, la prova està basada en un argument de paritat. Vegeu la Figura 21 com a il·lustració del cas $n = 8$. Pensem que els n^2 quadrats 1×1 del quadrat inicial estan acolorits com a un tauler d'escacs. Per tant, quan traiem els dos quadradets que hem dit, estem traient dos quadradets acolorits amb el mateix color. Com a conseqüència, la figura que hem d'emplenar té $2k^2$ quadrats 1×1 d'un color i $2k^2 - 2$ de l'altre. Com que, posem com posem un dòmino de mida 2×1, sempre cobreix un quadrat de cada color, és impossible recobrir aquest quadrat escapçat amb dòminos de mida 2×1, tal i com volíem demostrar. □

4.4.5 Impossibilitat d'un cert puzle

Provarem el resultat següent:

Proposició 4.8. *Donada la Taula 2,*

1	1	1	1
1	1	1	1
1	1	1	1
1	-1	1	1

Taula 2: Taula amb 1's i -1's

fent les modificacions següents:

(a) Canviar tots els signes d'una fila,

(b) Canviar tots els signes d'una columna,

(c) Canviar tots els signes d'una línia paral·lela a una de les diagonals (en particular, podem canviar el signe de cada una les caselles de les quatre cantonades),

mai es podrà aconseguir que tots els números siguin 1*'s.*

Prova. La demostració es basa en tenir en compte que el producte dels números que ocupen les 8 caselles de la vora que no són a les 4 cantonades és un *invariant* de tots els moviments possibles i per tant sempre serà -1. Cadascuna d'aquestes transformacions o bé canvia de signe exactament 2 de les 8 caselles, o bé no en canvia cap. Com a conseqüència, el resultat queda demostrat. □

Aquesta demostració d'impossibilitat recorda una de similar, però més difícil, per a un puzle famós (el joc del 15, vegeu la Figura 22) que demana passar, només lliscant el quadradets, d'una posició en la que el números estan ordenats com $1, 2, 3, \ldots, 13, 15, 14$ a un segona en la que estan ben ordenats.

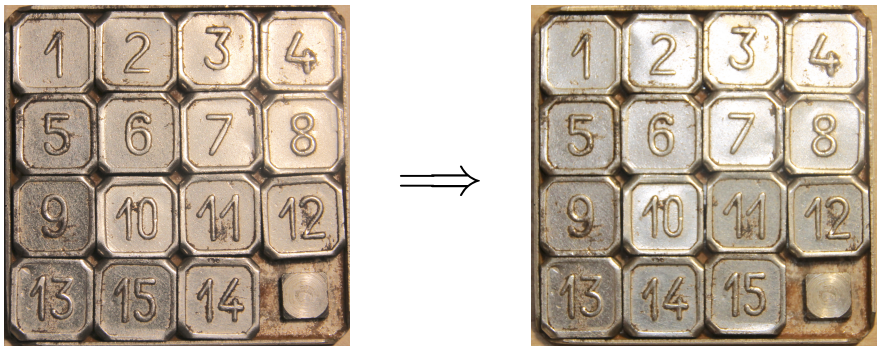


Figura 22: Joc del 15

4.4.6 Permutacions i productes

Proposició 4.9. *Sigui $m_1, m_2, \ldots, m_n$ una permutació de $1, 2, \ldots, n$. Aleshores, si n és senar, el producte $P = (m_1 - 1)(m_2 - 2) \cdots (m_n - n)$ és parell.*

Prova. Suposem, per tal d'arribar a contradicció, que el producte fos senar. Aleshores, tots els factors haurien de ser senars. Per una banda la suma S de

tots aquest factors és senar, en ser una suma d'un nombre senar de números senars, però per altra banda,

$$S = \sum_{j=1}^{n}(m_j - j) = \sum_{j=1}^{n} m_j - \sum_{j=1}^{n} j = 0,$$

ja que els m_j són una permutació de tots el números entre 1 i n. Per tant hem obtingut la contradicció desitjada. □

4.4.7 Matrius de 1's i -1's

Proposició 4.10. *Per a $k \in \mathbb{N}$ considerem una matriu $(2k+1) \times (2k+1)$ on cadascun dels seus elements és o bé un 1 o un -1. Sigui f_i el producte de tots els elements de la fila i-èssima i c_j el producte de tots els elements de la columna j-èssima. Aleshores $S = \sum_{j=1}^{2k+1}(f_j + c_j) \neq 0$.*

Prova. Suposem, per tal d'obtenir una contradicció, que $S = 0$. Per tenir aquest resultat a la suma hi ha d'haver el mateix nombre de termes positius que de negatius. Si entre tots els f_i n'hi ha exactament n de negatius aleshores entre tots els c_j n'hi ha d'haver $2k+1-n$ de negatius. Com que n i $2k+1-n$ tenen paritat diferent tenim $\prod_{i=1}^{2k+1} f_i = -\prod_{j=1}^{2k+1} c_j$ fet que dóna lloc a la contradicció desitjada ja que $\prod_{i=1}^{2k+1} f_i = \prod_{j=1}^{2k+1} c_j \neq 0$ és el producte de tots els elements de la matriu. □

4.5 Proves geomètriques

Hi ha moltíssims problemes de l'anomenada geometria clàssica que es podrien haver inclòs en aquesta secció. En podem trobar un bon recull en els llibres dedicats a les Olimpíades Matemàtiques citats a la introducció i en especial a [8]. La majoria dels problemes que hem triat no són purament geomètrics ja que tenen alguna petita component diferent.

4.5.1 Cercle inscrit i circumscrit

Donat un triangle equilàter demostrarem a continuació que *si l'àrea del cercle inscrit és A, aleshores la del cercle circumscrit és $S = 4A$*. La prova és conseqüència de la construcció de la Figura 23 on es mostra que $A = \pi r^2$ i $S = \pi(2r)^2 = 4\pi r^2 = 4A$.

De fet, que el cercle inscrit al triangle gran talla el radi puntejat del seu cercle circumscrit, que suposem de mida $2r$, just al seu punt mig és conseqüència, per exemple, de que tots els triangles rectangles formats per dues ratlles puntejades i una contínua tenen un dels seus angles igual a $\pi/6$.

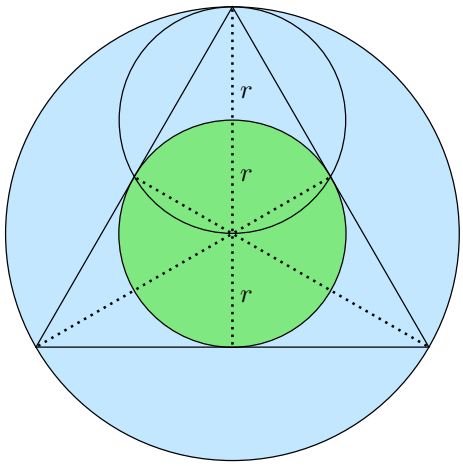


Figura 23: Cercles inscrit i circumscrit a un triangle equilàter

4.5.2 Quadrats i triangles

Els problemes de partir figures planes en subfigures amb certes propietats són molts clàssics, tant dins de la geometria com de la matemàtica recreativa. Demostrarem el resultat següent.

Proposició 4.11. *(i) Per a tot $n \geq 6$, un quadrat es pot partir en n quadrats més petits, no necessàriament iguals.*

(ii) Per a tot $n \geq 6$, un triangle equilàter es por partir en n triangles equilàters més petits, no necessàriament iguals.

Prova. (i) La prova usa inducció i recorda a la que hem usat a la Secció 2.9 quan estudiàvem el problema dels bitllets. Primer demostrem que el problema té solució per a $n = 6, 7$ i 8. Això és conseqüència de les particions que es mostren a la Figura 24.

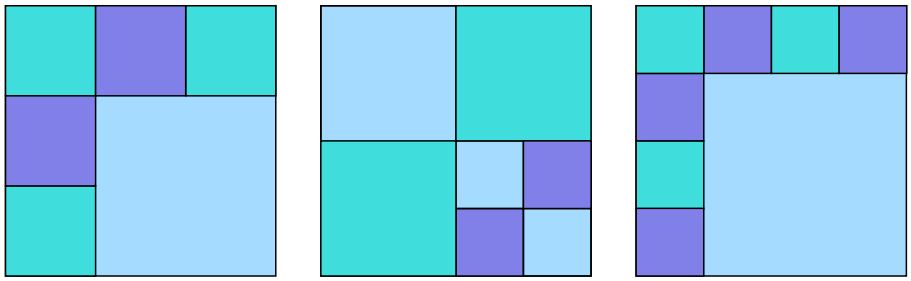


Figura 24: Partició d'un quadrat en 6, 7 o 8 quadrats

Ara bé, com que cada quadrat es pot dividir de manera trivial en 4 quadrats iguals és clar que donada qualsevol partició en m quadrats en podem

aconseguir una amb $m+3$ quadrats, senzillament dividint un quadrat qualsevol en quatre (mireu la partició de la cantonada inferior dreta del quadrat del mig de la figura). Per tant, a partir de les tres llavors aconseguim fàcilment particions per a tot $n \geq 9$:

$$6 \to\ 9 \to 12 \to 15 \to 18 \to 21 \to 24 \to 27 \to 30 \to 33 \to \cdots$$
$$7 \to 10 \to 13 \to 16 \to 19 \to 22 \to 25 \to 28 \to 31 \to 34 \to \cdots$$
$$8 \to 11 \to 14 \to 17 \to 20 \to 23 \to 26 \to 29 \to 32 \to 35 \to \cdots$$

(ii) La prova pel cas de triangles equilàters és exactament igual i es basa en les tres particions mostrades a la Figura 25 d'un triangle equilàter en 6, 7 o 8 triangles equilàters. □

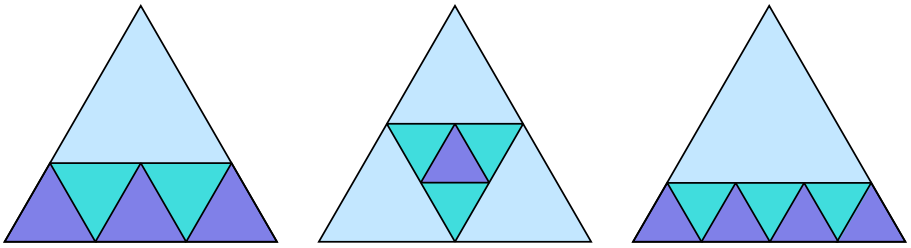


Figura 25: Partició d'un triangle equilàter en 6, 7 o 8 triangles equilàters

4.5.3 Sempre es pot construir un triangle

Proposició 4.12. *Donats $k \geq 3$ segments, amb longituds més grans que 1 i menors que F_k, el k-èssim número de Fibonacci, sempre n'hi ha, com a mínim, tres amb els que es pot construir un triangle.*

Prova. Ordenem els segments en funció de la seva longitud

$$1 < x_1 \leq x_2 \leq x_3 \leq \cdots \leq x_{k-1} \leq x_k < F_k.$$

Recordem que, donats 3 segments amb longituds $a \leq b \leq c$, es pot construir un triangle amb aquests costats si, i només si, $a + b > c$. Suposarem, per tal d'arribar a contradicció, que no es pot construir cap triangle amb els k segments donats. A partir d'aquesta suposició demostrarem seguidament, per inducció, que $x_j > F_j$ per a $j = 1, 2, \ldots, k$.

Com que, per hipòtesi, $F_1 = 1 < x_1$ i $F_2 = 1 < x_1 \leq x_2$ tenim la desigualtat que volem demostrar per a $j = 1, 2$. Suposem-la certa fins a $j = m$, per a un cert $m < k$. Aleshores, com que no es pot construir cap triangle amb els segments $x_{m-1} \leq x_m \leq x_{m+1}$, tenim que

$$x_{m+1} \geq x_{m-1} + x_m > F_{m-1} + F_m = F_{m+1},$$

tal i com volíem demostrar. Per tant, tenim la contradicció desitjada: $F_k > x_k > F_k$. □

4.5.4 La distància més curta

Presentem un dels resultats d'optimització més famosos, amb la demostració clàssica que s'atribueix a Heró d'Alexandria (segle I). A la Figura 26, donats A i B, volem determinar quin és el punt Q sobre la recta ℓ que fa que la distància $AQ + QB$ sigui la més curta possible.

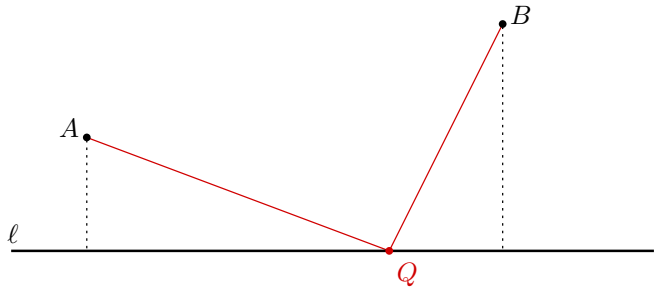


Figura 26: Plantejament d'un problema d'optimització

Si comencem a posar coordenades, a calcular distàncies usant el Teorema de Pitàgores i a derivar l'expressió que ens interessa per trobar el seu mínim, entrem en càlculs pesats que, tot i que permeten resoldre el problema, perden de vista la seva interpretació geomètrica. Per altra banda, a partir de la construcció de la Figura 27, es veu clarament quin ha de ser el punt Q.

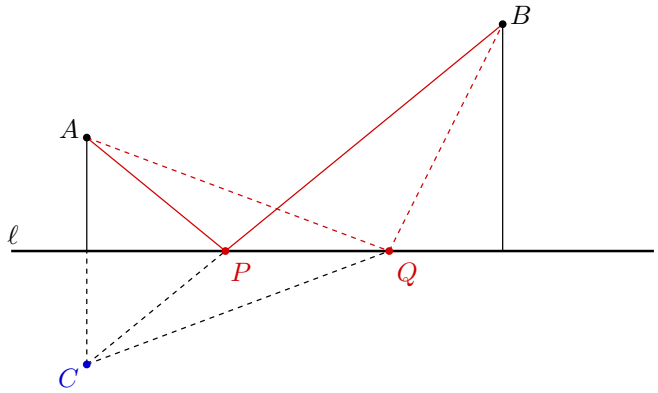


Figura 27: Resolució d'Herò d'un problema d'optimització

Sigui C el punt simètric de A respecte a la recta ℓ. Aleshores $Q = P$ on P és el tall entre el segment CB i la recta ℓ. El motiu és simple: sigui Q qualsevol punt diferent de P a ℓ. Si considerem la distància $AQ+QB$ aquesta coincidirà amb la distància $CQ+QB$ que és més gran que $CP+PB$, ja que la distància més curta entre dos punts, C i B, és sempre la línia recta. Com que la distància $CP+PB$ coincideix amb la distància $AP+PB$, el problema queda resolt, ja que hem provat que la distància $AQ + QB$, per a $Q \neq P$, és

més gran que $AP + PB$.

4.5.5 El Teorema de Viviani

Aquest resultat va ser provat per Viviani al segle XVII.

Teorema 4.13. *Si P és un punt interior d'un triangle equilàter aleshores la suma de les distancies de P als tres costats del triangle AB, BC i CA no depèn de P i val l'alçada h del triangle.*

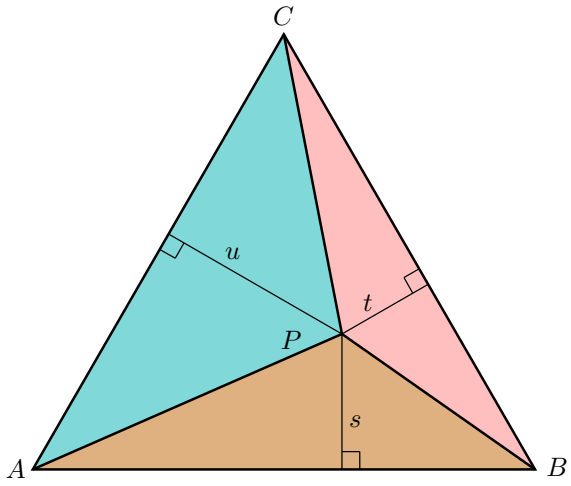


Figura 28: Teorema de Viviani: $s + t + u$ és constant.

Prova. Si a és el costat del triangle i h la seva alçada, per una banda sabem que la seva àrea és $a\,h/2$. De fet, pel Teorema de Pitàgores, $h = \sqrt{3}\,a/2$ però no necessitarem aquest valor en la prova. Per l'altra banda, l'àrea total del triangle, és igual a la suma de les àrees dels tres triangles en que es pot dividir, APB, BPC i CPA, vegeu la Figura 28. Aquestes àrees són $a\,s/2$, $a\,t/2$ i $a\,u/2$. Per tant $s + t + u = h$, tal i com volíem veure. □

4.5.6 Fórmula d'Heró

El següent resultat permet calcular l'àrea A d'un triangle en funció dels seus costats, a, b i c, i se sol atribuir a Heró d'Alexandria (segle I) tot i que hi ha autors que pensen que Arquimedes (segle III a. C.) ja la coneixia, veure [10, Cap. 3].

Proposició 4.14. *L'àrea A d'un triangle amb costats a, b i c és*

$$\begin{aligned} A &= \frac{1}{4}\sqrt{(a+b+c)(-a+b+c)(a-b+c)(a+b-c)} \\ &= \sqrt{s(s-a)(s-b)(s-c)}, \end{aligned}$$

on $s = (a+b+c)/2$.

Prova. Seguint [40], dividim el triangle en dos triangles rectangles mitjançant una alçada, vegeu la Figura 29.

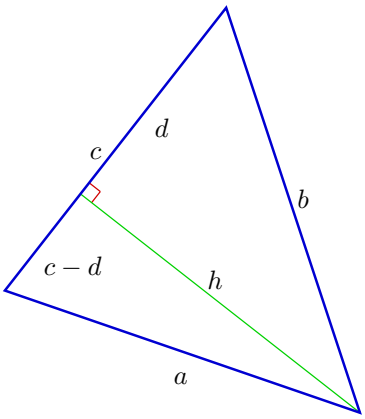


Figura 29: Triangle dividit en dos triangles rectangles.

Aplicant el Teorema de Pitàgores als dos triangles resultants tenim que $a^2 = h^2 + (c-d)^2$ i $b^2 = h^2 + d^2$. Restant les dues igualtats obtenim que $a^2 - b^2 = c^2 - 2\,c\,d$ i per tant, $d = (-a^2+b^2+c^2)/(2c)$. Finalment, substituint aquest valor de d a la segona igualtat tenim

$$\begin{aligned} h^2 = b^2 - d^2 = b^2 - \left(\frac{-a^2+b^2+c^2}{2c}\right)^2 &= \frac{(2\,b\,c)^2 - (-a^2+b^2+c^2)^2}{4c^2} \\ &= \frac{\big(2\,b\,c - a^2 + b^2 + c^2\big)\big(2\,b\,c + a^2 - b^2 - c^2\big)}{4c^2} \\ &= \frac{\big((b+c)^2 - a^2\big)\big(a^2 - (b-c)^2\big)}{4c^2} \\ &= \frac{(b+c+a)(b+c-a)(a+b-c)(a-b+c)}{4c^2}, \end{aligned}$$

on hem usat vàries vegades $u^2 - v^2 = (u+v)(u-v)$. Per tant

$$A = \frac{c\,h}{2} = \frac{1}{4}\sqrt{(a+b+c)(-a+b+c)(a-b+c)(a+b-c)}\,,$$

tal i com volíem demostrar. □

4.6 Proves sense paraules

Les proves basades en figures, també anomenades *proves sense paraules* són un recurs usat per molts professors a les seves classes. Sovint en moltes d'aquests figures ja hi ha tots els ingredients d'una demostració "formal". En presentem a continuació unes quantes. Per a veure una selecció més extensa podeu consultar [21] i les seves referències.

4.6.1 Fórmula de Nichomacus, segona prova

La igualtat

$$1^3 + 2^3 + \cdots + (n-1)^3 + n^3 = \big(1 + 2 + \cdots + (n-1) + n\big)^2.$$

es pot deduir de la Figura 30.

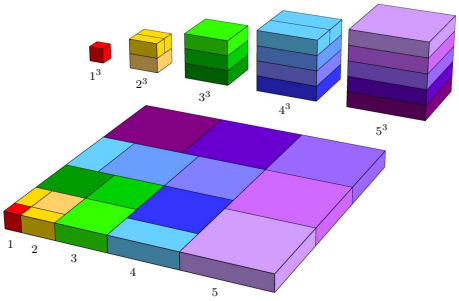


Figura 30: Suma dels primers cubs

4.6.2 Suma d'una sèrie geomètrica

La Figura 31, que dóna una prova de la fórmula

$$\frac{4}{9} + \left(\frac{4}{9}\right)^2 + \left(\frac{4}{9}\right)^3 + \cdots \left(\frac{4}{9}\right)^n + \cdots = \frac{4}{5},$$

s'ha extret de [16].

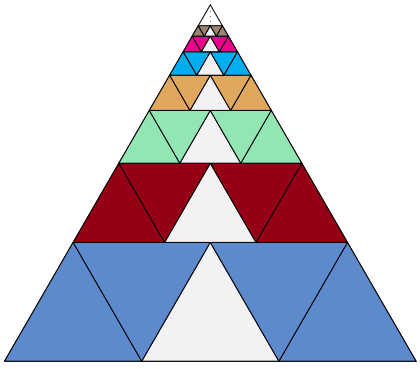


Figura 31: Suma d'una sèrie geomètrica

4.6.3 Derivada d'una sèrie geomètrica

Recordem que la suma d'una sèrie geomètrica amb raó $-1 < r < 1$, és

$$\sum_{n=0}^{\infty} r^n = 1 + r + r^2 + \cdots + r^n + \cdots = \frac{1}{1-r}.$$

A partir del resultat anterior, es pot demostrar que la igualtat també es manté derivant als dos costats respecte a r. Així es compleix

$$\sum_{n=0}^{\infty} n\, r^{n-1} = 1 + 2r + 3r^2 + \cdots + n\, r^{n-1} + \cdots = \frac{1}{(1-r)^2}.$$

Pel cas particular $r = 1/2$ s'obté

$$\sum_{n=0}^{\infty} n \left(\frac{1}{2}\right)^{n-1} = 1 + 2\left(\frac{1}{2}\right) + 3\left(\frac{1}{4}\right) + 4\left(\frac{1}{8}\right) + \cdots + n\left(\frac{1}{2}\right)^{n-1} + \cdots = 4,$$

a partir de la Figura 32.

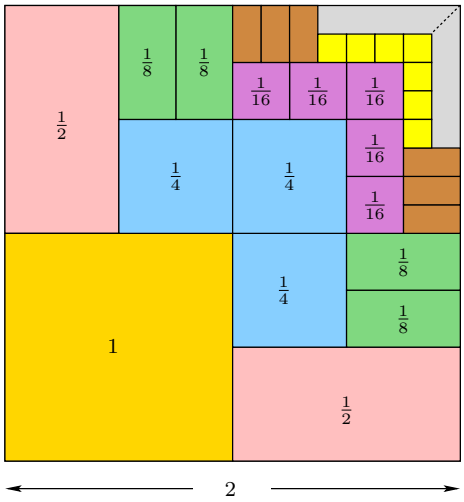


Figura 32: Suma de la derivada d'una sèrie geomètrica

4.6.4 Una desigualtat i una igualtat

A partir de la Figura 33 és clar que si $a, b > 0$ amb $a + b = 1$, aleshores $(a+1)(b+1) \geq 9\, a\, b$.

Per tant hem demostrat

$$a, b > 0,\ a + b = 1 \Longrightarrow \left(1 + \frac{1}{a}\right)\left(1 + \frac{1}{b}\right) \geq 9.$$

La igualtat es dona quan $a = b = 1/2$. De fet, si s'elimina la condició $a + b = 1$, la mateixa figura serveix per a demostrar que

$$(2a + b)(2b + a) = 9\, a\, b + 2(b - a)^2 \geq 9\, a\, b.$$

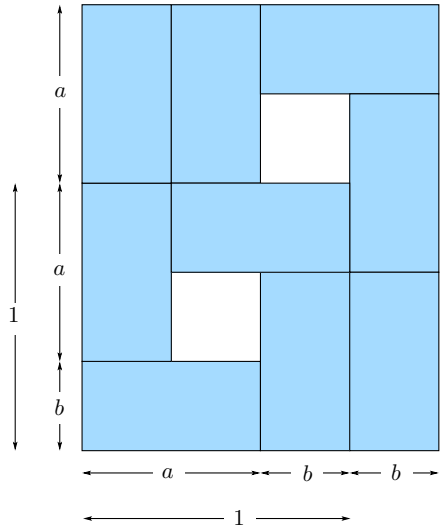


Figura 33: Prova d'una desigualtat i una igualtat

4.6.5 Teorema de Pitàgores

Si els catets de cada triangle rectangle de la Figura 34 són $b \geq a$, i la seva hipotenusa és c, aleshores el quadrat gran de costat $2c$ s'ha dividit en vuit triangles d'àrea $b\,c/2$, dos quadrats d'àrea a^2, dos d'àrea b^2 i dos més d'àrea $(b-a)^2$ (que són els més petits de tots en aquesta figura). Igualant les àrees arribem a

$$8\frac{a\,b}{2} + 2a^2 + 2(b-a)^2 + 2b^2 = (2c)^2.$$

Simplificant l'expressió obtenim el Teorema de Pitàgores: $a^2 + b^2 = c^2$.

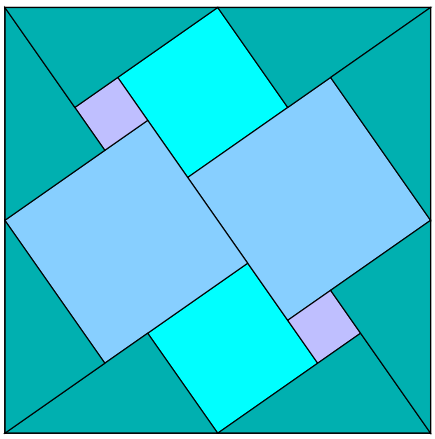


Figura 34: Una partició del quadrat que porta a provar el Teorema de Pitàgores

4.6.6 Una fórmula de tipus Machin

La fórmula

$$\frac{\pi}{4} = \arctan\left(\frac{1}{2}\right) + \arctan\left(\frac{1}{5}\right) + \arctan\left(\frac{1}{8}\right).$$

va ser demostrada l'any 1844 per Strassnitzky. Una prova sense paraules s'obté a partir de la Figura 35.

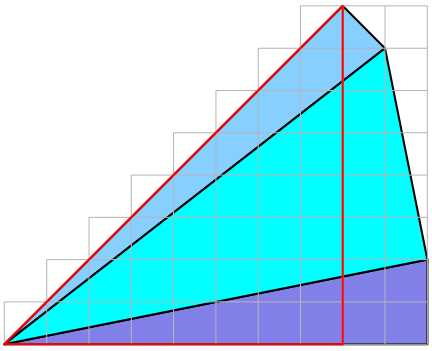


Figura 35: Una fórmula de tipus Machin

5 Epíleg: demostracions falses

No m'he pogut resistir a acabar aquest treball sense parlar de les "demostracions falses". El seu nom és en si mateix un oxímoron ja que l'objectiu final de les demostracions és presentar resultats certs. Òbviament aquestes "demostracions" no són demostracions, però si que són un bon recurs de motivació i de foment del pensament crític. Recullo a continuació algunes de les meves preferides. També es coneixen com fal·làcies matemàtiques.

Figura 36: Figures impossibles

Els "errors" comesos en cadascuna de les seccions següents estan comentats en la Secció final § 5.8. S'ha fet així per facilitar que el lector pensi per ell mateix on són els errors d'argumentació.

5.1 Prova de que $2 = 3$ calculant amb números

Aquesta primera "demostració" és la més senzilla de totes. Es basa en la cadena següent d'igualtats.

$$\begin{aligned} 4-10 = 9-15 &\Longrightarrow 4-10+\frac{25}{4} = 9-15+\frac{25}{4} \\ &\Longrightarrow \left(2-\frac{5}{2}\right)^2 = \left(3-\frac{5}{2}\right)^2 \Longrightarrow \sqrt{\left(2-\frac{5}{2}\right)^2} = \sqrt{\left(3-\frac{5}{2}\right)^2} \\ &\Longrightarrow 2-\frac{5}{2} = 3-\frac{5}{2} \Longrightarrow 2 = 3. \end{aligned}$$

5.2 Prova de que $2 = 1$ usant expressions algebraiques

Continuem amb una demostració falsa conceptualment també bastant senzilla. Prenem $a = b \neq 0$. Aleshores tenim les implicacions següents.

$$\begin{aligned} a = b &\Longrightarrow a^2 = a\,b \Longrightarrow a^2 - b^2 = a\,b - b^2 \Longrightarrow (a+b)(a-b) = b(a-b) \\ &\Longrightarrow (a+b)\cancel{(a-b)} = b\cancel{(a-b)} \Longrightarrow a+b = b \Longrightarrow 2b = b \Longrightarrow 2 = 1. \end{aligned}$$

5.3 Prova de que $m + 1 < m$ usant logaritmes

De nou farem una "cadena d'implicacions" que ens portaran al resultat fals.

$$\begin{aligned} \left(\frac{1}{2}\right)^{m+1} < \left(\frac{1}{2}\right)^m &\Longrightarrow \ln\left(\frac{1}{2}\right)^{m+1} < \ln\left(\frac{1}{2}\right)^m \\ &\Longrightarrow (m+1)\ln\left(\frac{1}{2}\right) < m\,\ln\left(\frac{1}{2}\right) \\ &\Longrightarrow (m+1)\ln\cancel{\left(\frac{1}{2}\right)} < m\,\ln\cancel{\left(\frac{1}{2}\right)} \Longrightarrow m+1 < m. \end{aligned}$$

5.4 Prova de que $2 = 1$ usant derivades

$$\begin{aligned} x^2 = \underbrace{x+x+\cdots+x}_{x \text{ cops}} &\Longrightarrow \frac{\mathrm{d}}{\mathrm{d}x}(x^2) = \frac{\mathrm{d}}{\mathrm{d}x}\underbrace{(x+x+\cdots+x)}_{x \text{ cops}} \\ &\Longrightarrow 2x = \underbrace{1+1+\cdots+1}_{x \text{ cops}} = x \Longrightarrow 2 = 1. \end{aligned}$$

5.5 Prova de que $0 = 1$ usant integrals

És clar que $(\sin^2(x))' = 2\sin(x)\cos(x)$ i $(\cos^2(x))' = -2\cos(x)\sin(x)$, on la prima denota la derivada respecte de x. Per tant

$$\int 2\sin(x)\cos(x)\,\mathrm{d}x = \sin^2(x) \;\text{ i }\; \int 2\sin(x)\cos(x)\,\mathrm{d}x = -\cos^2(x).$$

Restant ambdues igualtats obtenim

$$0 = \sin^2(x) - (-\cos^2(x)) = \sin^2(x) + \cos^2(x) = 1.$$

5.6 Prova de que $1 = -1$ usant números complexos

Observem la cadena "d'igualtats"

$$1 = \sqrt{1} = \sqrt{(-1)\times(-1)} = \sqrt{-1}\times\sqrt{-1} = \mathrm{i}\times\mathrm{i} = \mathrm{i}^2 = -1.$$

5.7 Prova de que $1 = 2$ usant fraccions contínues

Anem a fer dues cadenes d'igualtats:

$$1 = \frac{2}{3-1} = \frac{2}{3-\dfrac{2}{3-1}} = \frac{2}{3-\dfrac{2}{3-\dfrac{2}{3-1}}} = \cdots = \frac{2}{3-\dfrac{2}{3-\dfrac{2}{3-\dfrac{2}{3-\cdots}}}},$$

$$2 = \frac{2}{3-2} = \frac{2}{3-\dfrac{2}{3-2}} = \frac{2}{3-\dfrac{2}{3-\dfrac{2}{3-2}}} = \cdots = \frac{2}{3-\dfrac{2}{3-\dfrac{2}{3-\dfrac{2}{3-\cdots}}}}.$$

Com que les dues expressions de la dreta són iguals, el mateix passa amb les de l'esquerra i per tant $1 = 2$.

5.8 Explicacions de les "errades"

Donem a continuació una breu explicació dels arguments erronis que han portat a les "demostracions falses".

• L'error a la Secció 5.1 consisteix en un mal ús de l'arrel quadrada. De fet si no es posa cap signe davant d'ella s'entén que dóna un valor positiu, és a dir $\sqrt{x^2} = |x|$. Per tant $\sqrt{\left(2-\frac{5}{2}\right)^2} = \left|2-\frac{5}{2}\right| = \frac{1}{2}$. Una "demostració" amb un error similar és:

$$\cos^2(x) + \sin^2(x) = 1 \Longrightarrow \cos(x) = \sqrt{1-\sin^2(x)}$$
$$\overset{x=\pi}{\Longrightarrow} -1 = \sqrt{1} \Longrightarrow -1 = 1.$$

• En la cadena d'implicacions de la Secció 5.2 l'error està en la cancel·lació de $a-b$ en ambdós costats del producte ja que $a-b=0$.

• Com a la secció anterior, l'error en la Secció 5.3 de nou està en una mala cancel·lació. Aquesta vegada de $\ln(1/2)$. En aquest cas com que aquest valor és negatiu, quan el cancel·lem la desigualtat s'inverteix.

• En la Secció 5.4 es juga amb l'ambigüitat de la igualtat

$$x^2 = \underbrace{x + x + \cdots + x}_{x \text{ cops}},$$

ja que l'expressió de la dreta no està ben definida i és simplement $x \times x$ i és clar que està mal derivada.

• En la prova de la Secció 5.5 l'error prové de donar per fet que la resta de les dues integrals ha de donar 0. De fet, s'obliden les constants d'integració en el càlcul de primitives. Així, per exemple, $2\int \sin(x)\cos(x)\,\mathrm{d}x = \sin^2(x) + c$ per a $c \in \mathbb{R}$, i el correcte és que en restar-les hem d'obtenir una constant, i això és el que passa tal i com es pot apreciar a la figura 37.

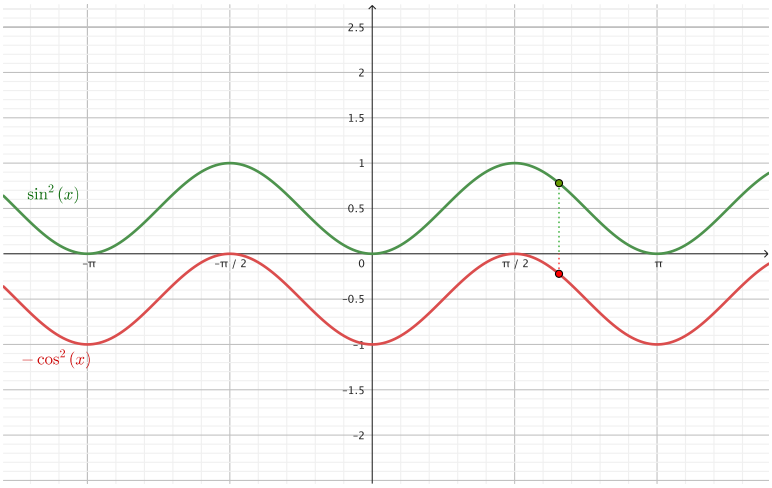


Figura 37: Les funcions $\sin^2(x)$ i $-\cos^2(x)$ difereixen en cada punt d'una constant. El gràfic conté un enllaç que porta a una construcció dinàmica (GeoGebra) on també es mostra com les dues funciones tenen rectes tangents paral·leles en cada punt.

• El problema en la "demostració" de la Secció 5.6 prové de l'ús de la igualtat $\sqrt{a\,b} = \sqrt{a}\,\sqrt{b}$ quan a i b són números complexos, ja que l'arrel quadrada no és una funció ben definida a $\mathbb{C}$. Una "prova" amb un error semblant, però ara oblidant que tot número complex no nul té 4 arrels quartes, és

$$\mathrm{i} = \sqrt{-1} = (-1)^{2/4} = \left((-1)^2\right)^{1/4} = 1^{1/4} = 1.$$

A més, si usem exponents complexos arribem sovint a resultats falsos degut a que donen lloc a funcions multivaluades. Per exemple

$$\mathrm{e}^{2\pi\mathrm{i}} = 1 \Longrightarrow \left(\mathrm{e}^{2\pi\mathrm{i}}\right)^{\mathrm{i}} = 1^{\mathrm{i}} \Longrightarrow \mathrm{e}^{-2\pi} = 1,$$

o també,

$$\mathrm{e} = \mathrm{e}^{\frac{2\pi\mathrm{i}}{2\pi\mathrm{i}}} = (\mathrm{e}^{2\pi\mathrm{i}})^{\frac{1}{2\pi\mathrm{i}}} = 1^{\frac{1}{2\pi\mathrm{i}}} = 1.$$

• El problema amb la "prova" de la Secció 5.7 és l'ambigüitat de la notació en l'ús dels punts suspensius. Clarament, aquest punts volen representar el valor que obtenim per pas al límit. Més concretament, si denotem $f(x) = \frac{2}{3-x}$, l'expressió de la dreta de la primera igualtat és L_1 on

$$L_1 = \lim_{n\to\infty} x_n \quad \text{on} \quad x_{n+1} = f(x_n),\ x_1 = 1,$$

i la quantitat de la dreta de la segona cadena d'igualtats és L_2 on

$$L_2 = \lim_{n\to\infty} y_n \quad \text{on} \quad y_{n+1} = f(y_n),\ y_1 = 2.$$

És fàcil veure que $L_1 = 1$ i $L_2 = 2$ són els dos punts fixos de f, és a dir les dues solucions de $f(x) = x$. Només podríem assegurar que els dos límits són iguals si ambdós límits existissin i el punt fix fos únic. En aquest cas els límits existeixen ja que de fet són successions constants, però hi ha dos límits diferents.

Agraïments

L'autor vol agrair Gregori Guasp, Toni Guillamon i Joan Torregrosa pels seus suggeriments sobre una versió prèvia d'aquest article. Treball recolzat per l'Agència Espanyola de Investigació via el projecte PID2019-104658GB-I00, pel programa Severo Ochoa i María de Maeztu per Centres i Unitats d'Excel·lencia en I&D (CEX2020-001084-M) i pel projecte 2021-SGR-113 d l'AGAUR, Generalitat de Catalunya.

Índex

Referències

[1] M. Aigner, G. M. Ziegler, EL LIBRO de las demostraciones. Nivola Libros y Ediciones, S.L., 2005.

[2] A. Alonso T. Bermúdez, *De conejos y números. La sorprendente sucesión de Fibonacci.* Gaceta de la Real Sociedad Matemática Española **5** (2002), 175–196.

[3] C. Alsina, R. B. Nelsen, Charming Proofs: A Journey into Elegant Mathematics, Dolciani Mathematical Expositions **42**, 2010. AMS/MAA Press.

[4] T. Andreescu, R. Gelca, Mathematical Olympiad Challenges. Birkhäuser Boston, MA, 2009.

[5] N. D. Baruah, B. C. Berndt, H. H. Chan, *Ramanujan's series for* $1/\pi$: *a survey*, Amer. Math. Monthly **116** (2009), 567–587.

[6] A. Bogomolny, *Cut The Knot.* https://www.cut-the-knot.org/front.shtml

[7] M. Chamberland, Single digits. In praise of small numbers. Princeton University Press, Princeton, NJ, 2015.

[8] E. Chen, Euclidean geometry in mathematical Olympiads. With 248 illustrations. MAA Problem Books Series. Washington, DC: Mathematical Association of America, MAA Press, 2016.

[9] K. Conrad, *The Gaussian integral*. http://www.math.uconn.edu/~kconrad/blurbs/analysis/gaussianintegral.pdf

[10] H. S. M. Coxeter, S. L. Greitzer, Geometry Revisited, Math. Assoc. Amer. 1967.

[11] H. T. Croft, K. J. Falconer, R. K. Guy, Unsolved problems in geometry. Problem Books in Mathematics. Unsolved Problems in Intuitive Mathematics, II. Springer-Verlag, New York, 1991.

[12] D. R. Curtiss, *Recent extensions of Descartes' rule of signs*. Annals of Mathematics **19** (1918), 251–278.

[13] B. A. Davey, Maths delivers! Proofs by induction. The University of Melbourne on behalf of the Australian Mathematical Sciences Institute (AMSI), 2013

[14] W. Dunham, El universo de las matemáticas: un recorrido alfabético por los grandes teoremas, enigmas y controversias, Ed. Pirámide, 1995.

[15] W. Dunham, Viaje a través de los genios. Biografías y teoremas de los grandes matemáticos. Ed. Pirámide, 2002.

[16] T. Edgar, *Sums of Powers of* 4/9. Math. Mag. **89** (2016) 191.

[17] A. Engel, Problem-solving strategies, Springer, 1998.

[18] P. Eymard, J-P. Lafon, The number π. Traduït de la versió francesa de 1999 per S. S. Wilson. American Mathematical Society, Providence, RI, 2004.

[19] D. Fomin, S. Genkin, I. Itenberg, Mathematical circles (Russian experience). Providence, Rhode Island: Americal Mathematical Society, 1996.

[20] A. Gasull, *Gemmes matemàtiques*. Mat. Mat. **2019**, treball no. 2, pp. 88, 2019.

[21] A. Gasull, *55 proves sense paraules*. Mat. Mat. **2022**, treball no. 2, pp. 61, 2022.

[22] A. Gasull, J. T. Lázaro, J. Torregrosa, *Rational parameterizations approach for solving equations in some dynamical systems problems*. Qual. Theory Dyn. Syst., 18, (2019) 583–602.

[23] A. Gasull, F. Luca, J. L. Varona, *Three essays on Machin's type formulas*. Pendent de publicació a Indag. Math.
DOI: 10.1016/j.indag.2023.07.002

[24] J. Grané (Editor), Sessions de Preparació per a l'Olimpíada Matemàtica. Publicacions Electròniques de la Societat Catalana de Matemàtiques, 2004.

[25] S. L. Greitzer, Olimpiadas matemáticas internacionales. La Totuga de Aquiles 2, Ed. DLS-EULER, Madrid, 1994.

[26] M. de Guzmán, Aventuras matemáticas. Una ventana hacia el caos y otros episodios. Ed. Pirámide, Madrid 2004.

[27] R. Hammack, BOOK OF PROOF, 2003. Disponible a https://www.people.vcu.edu/~rhammack/BookOfProof/BookOfProof.pdf

[28] R. Honsberger, Mathematical gems from elementary combinatorics, number theory, and geometry. The Dolciani Mathematical Expositions, **1**. The Mathematical Association of America, Buffalo, N.Y. 1973.

[29] R. Honsberger, Mathematical gems. II. Dolciani Mathematical Expositions, **2**. The Mathematical Association of America, Washington, D.C. 1976.

[30] R. Honsberger, Mathematical gems. III. The Dolciani Mathematical Expositions, **9**. Mathematical Association of America, Washington, D.C. 1985.

[31] D. J. Jeffrey, A. D. Rich, Computer Algebra Systems: A Practical Guide. Chapter: *Simplifying square roots of square roots by denesting*, John Wiley & Sons, Chichester, UK, 1999.

[32] E. Key, *Disks, Shells, and Integrals of Inverse Functions*. The College Mathematics Journal **25** (1994) 136–138.

[33] S. G. Krantz, The History and Concept of Mathematical Proof, 2007

[34] C. A. Laisant, *Intégration des fonctions inverses*. Nouvelles Annales de Mathématiques, Journal des candidats aux Écoles Polytechnique et Normale **5** (1905) 253–257.

[35] M. Macho Stadler, *Mapas, colores y números*, Descubrir las matemáticas hoy: Sociedad, Ciencia, Tecnología y Matemáticas **2006** (2008) 41–68

[36] J. Neunhäuserer, 12^2 *beautiful mathematical theorems with short proofs*. Preprint.

[37] F. D. Parker, *Integrals of inverse functions*. The American Mathematical Monthly. **62** (1955) 439–440.

[38] G. Polya, Mathematical Discovery. On Understanding, Learning, and Teaching Problem Solving. Combined Edition. John Wiley & Sons, 1981.

[39] H. Rademacher, O. Toeplitz, Números y figuras. Alianza Editorial. Madrid 1970.

[40] C. H. Raifaizen, *A Simpler Proof of Heron's Formula*. Mathematics Magazine. **44** (1971), 27–28.

[41] J. Ramírez Alfonsín, The Diophantine Frobenius problem. Oxford Univ. Press., 2005.

[42] M. A. Rincón Ortega, E. Letón Molina, Tipos de demostraciones, http://www.minixmodular.ia.uned.es, Madrid, 2021

[43] D. O. Shklarsky, N. N. Chentzov, I .M. Yaglom, The USSR Olympiad problem book: selected problems and theorems of elementary mathematics, 3a edició. Dover, New York, 1993.

[44] J. H. Silverman, *Taxicabs and sums of two cubes*. Am. Math. Monthly **100** (1993) 331–340.

[45] T. B. Soulami, Les olympiades de mathématiques: Réflexes et stratégies. Ed. Ellipses, Paris, 1999.

[46] P. Zeitz, The art and craft of problem solving. 3rd edition. John Wiley & Sons, 2017. Hi ha una traducció en castellà "El arte y el oficio de resolver problemas" d'en C. de Armas García.

[47] A Collection of Algebraic Identities, https://www.scribd.com/document/72611415/A-Collection-of-Algebraic-Identities

Tots els enllaços eren operatius el 2 de juny de 2023.

Departament de Matemàtiques
Universitat Autònoma de Barcelona
Centre de Recerca Matemàtica
Armengol.Gasull@uab.cat

Publicat el 19 d'octubre de 2023