MAT^2
MATerials MATemàtics
Volum 2026, treball no. 1, 71 pp. ISSN: 1887-1097
Publicació electrònica de divulgació del Departament de Matemàtiques
de la Universitat Autònoma de Barcelona
www.mat.uab.cat/web/matmat

101 microdemostraciones

Armengol Gasull, Juan Luis Varona

En este trabajo damos ejemplos de distintos tipos de demostraciones. Su denominador común es que las pruebas de los resultados son muy cortas.

La motivación para escribir este trabajo ha sido presentar demostraciones de resultados variados que puedan ser intercaladas por los profesores en sus clases, que sean muy rápidas y formativas y que, al mismo tiempo, muestren la elegancia y la potencia del razonamiento matemático.

La mayoría de las pruebas que incluimos no son originales y las hemos seleccionado de entre la gran cantidad de material existente en recopilaciones de demostraciones. Por ejemplo, se pueden consultar los libros [1, 2, 5, 7, 8, 15, 16, 17, 18, 23, 27, 28, 30, 37], los libros dedicados a las Olimpiadas Matemáticas [3, 6, 9, 13, 14, 33, 34], o la página web [4]. Algunas de las pruebas presentadas también aparecen en trabajos anteriores de los autores [11, 12, 35].

Las pruebas están agrupadas en secciones teniendo en cuenta el tipo de demostración utilizada: razonamientos directos, equivalencias, contrarrecíproco, reducción al absurdo, existencia de invariantes, pruebas geométricas, inducción, congruencias, cálculos, pruebas sin palabras o principio del palomar. A veces, la clasificación de una prueba en una de las categorías anteriores (o en otras que podíamos haber añadido) no es cien por cien clara. De hecho, en las demostraciones matemáticas es usual que aparezcan varios de los tipos descritos encadenados. Como el uso de congruencias no es muy común, la sección correspondiente tiene una introducción mucho más amplia que el resto de tipos de demostración.

Las 101 pruebas que presentamos están numeradas y cada una de ellas tiene un nombre, seguido de un enunciado enmarcado en una caja coloreada; a continuación, se presenta la prueba en sí y, en ocasiones, algunos comentarios sobre la misma. La idea es presentar demostraciones que, explicadas con una cantidad razonable de detalles, ocupen, en la mayoría de los casos, menos de media página; en todo caso, nunca más de una página. Casi siempre, las demostraciones pueden leerse de manera independiente unas de otras.

La relevancia de los resultados que incluimos en esta recopilación es muy diversa. Algunos de ellos son resultados matemáticos importantes, o que históricamente han tenido mucho interés. Otros son, simplemente, bonitos. En cualquier caso, hemos incluido pruebas de los resultados que nos marcaron de jóvenes cuando nuestros profesores nos las explicaron. Por ejemplo, el teorema de Pitágoras, que $0.9999\ldots = 1$, la fórmula para resolver ecuaciones de segundo grado, la suma de las progresiones aritmética y geométrica, y la suma de los ángulos de un triángulo. Les dedicamos este trabajo a ellos y aprovechamos para defender la idea de incluir, siempre que sea posible, demostraciones en los currículums de los alumnos de secundaria.

El trabajo pretende ser de interés para profesores de enseñanza secundaria y de primeros cursos de enseñanza universitaria, así como para lectores con ganas de aprender matemáticas. Pretendemos que la lectura de esta selección de demostraciones no requiera conocimientos matemáticos avanzados, tanto para entender sus enunciados como sus correspondientes demostraciones.

Razonamientos directos

En esta sección agruparemos varias demostraciones basadas principalmente en cadenas de deducciones. Las etiquetamos con este nombre ya que pretenden seguir el camino más natural y sencillo para llegar al resultado deseado y usan simplemente razonamientos directos.

1. Huecos sin números primos

Dado $m \in \mathbb{N}$, existen m números consecutivos no primos.

Podemos considerar

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

Entonces, para cada $k \in \{2, 3, \ldots, m, m+1\}$, $(m+1)!+k$ es divisible por k, ya que $(m+1)!$ contiene el factor k.

2. Un irracional elevado a otro

Existen dos números irracionales x e y tales que x^y es racional.

Sea $z = \sqrt{2}^{\sqrt{2}}$. Si z es racional, ya hemos terminado tomando $x = y = \sqrt{2}$. Si no, como

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = 2,$$

podemos tomar $x = z$ e $y = \sqrt{2}$ (que $\sqrt{2}$ es irracional lo vemos en la prueba 27).

Obsérvese que la prueba no es constructiva ni aclara si z es racional o no. De hecho, del teorema de Gelfond-Schneider (probado en 1934, de manera independiente, por Alexander Gelfond y Theodor Schneider), que es un resultado mucho más complicado, se deduce inmediatamente que z es trascendente y, por tanto, irracional (que un número α sea trascendente significa que no existe ningún polinomio $P(t)$ con coeficientes enteros tal que $P(\alpha) = 0$, y los racionales no son trascendentes pues $p/q \in \mathbb{Q}$ es raíz de $P(t) = qt - p$).

3. El último teorema de Fermat con matrices

El último teorema de Fermat no es cierto con matrices.

Recordemos que el último teorema de Fermat, que fue enunciado por el famoso matemático en 1637 y probado por Andrew Wiles en 1995, afirma que, para $n > 2$, no hay soluciones enteras positivas x, y, z de la ecuación $x^n + y^n = z^n$.

Mostraremos algunos ejemplos que son soluciones de la ecuación de Fermat con matrices de enteros, pero no es mucho lo que se conoce en general (véase, por ejemplo, [29, sección XIII.9]). Si permitimos que las matrices tengan determinante nulo, encontrar contraejemplos matriciales al último teorema de Fermat es muy sencillo (sobre todo, si usamos matrices nilpotentes, es decir, matrices que elevadas a una cierta potencia dan la matriz 0), así que vamos a prescindir de ese caso.

Un contraejemplo para todo $n = 2m + 1$, $m \geq 1$, es

$$\begin{pmatrix} 1 & (2m+1)^m \\ 0 & 1 \end{pmatrix}^n + \begin{pmatrix} -1 & 0 \\ (2m+1)^{m-1} & -1 \end{pmatrix}^n = \begin{pmatrix} 0 & 2m+1 \\ 1 & 0 \end{pmatrix}^n.$$

Un contraejemplo para un n par es el siguiente:

$$\begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}^4 + \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}^4 = \begin{pmatrix} 0 & 1 \\ c & 0 \end{pmatrix}^4,$$

donde (a, b, c) es una terna pitagórica, es decir, $a^2 + b^2 = c^2$. De manera similar, se pueden construir contraejemplos $k \times k$, $k \geq 3$, con $k = m + 1$ y $n = km$. Así, por ejemplo, para $m = 2$ tenemos $k = 3$ y $n = 6$, y se cumple

$$\begin{pmatrix} 0 & a & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^6 + \begin{pmatrix} 0 & b & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^6 = \begin{pmatrix} 0 & c & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^6.$$

Además, si para un valor de n fijado hay contraejemplos con matrices 2×2 y 3×3, se pueden construir contraejemplos $k \times k$ (para cualquier k mayor) sin más que formar matrices compuestas con esas matrices 2×2 y 3×3 en la diagonal (por ejemplo, usando una matriz 2×2 y otra 3×3 obtendríamos una 5×5).

4. Resto al dividir entre 24

Para cualquier número primo $p \geq 5$, el resto de la división de p^2 entre 24 es 1.

El resultado es equivalente a demostrar que $p^2 - 1 = (p + 1)(p - 1)$ es múltiplo de 24. Para probar este hecho, observemos lo siguiente:

- $p + 1$ y $p - 1$ son dos pares consecutivos; en consecuencia, uno es múltiplo de 4 y el otro de 2.
- Si tomamos la terna $p-1, p, p+1$, seguro que o bien $p-1$ o bien $p+1$ es múltiplo de 3.

Por lo tanto,

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

para algún $k \in \mathbb{N}$, tal como queríamos ver.

5. Suma de una progresión aritmética

Sea $a_1, a_2, a_3, \ldots, a_n$ una progresión aritmética, con $a_{k+1} = a_k + d$ para $1 \leq k < n$. Entonces,

$$a_1 + a_2 + a_3 + \cdots + a_n = \frac{a_1 + a_n}{2}\, n.$$

Como $a_{k+1} = a_k + d$ (y, por tanto, $a_{j-1} = a_j - d$), es obvio que

$$a_1 + a_n = a_2 + a_{n-1} = a_3 + a_{n-2} = \cdots = a_n + a_1.$$

Llamando S a la suma cuyo valor queremos encontrar, podemos escribir

$$\begin{aligned} S &= a_1 + \ a_2 \ + \ a_3 \ + \cdots + a_n, \\ S &= a_n + a_{n-1} + a_{n-2} + \cdots + a_1. \end{aligned}$$

Sumando esas dos expresiones obtenemos $2S = (a_1 + a_n)n$, de donde se sigue la fórmula buscada.

6. Suma de una progresión geométrica

Sea $r \neq 1$ un número real (o complejo). Entonces,

$$\sum_{n=0}^{N} r^n = \frac{1 - r^{N+1}}{1 - r} \qquad \text{y, si } |r| < 1, \qquad \sum_{n=0}^{\infty} r^n = \frac{1}{1 - r}.$$

Si denotamos $S_N = \sum_{n=0}^{N} r^n$, tenemos

$$\begin{aligned} S_N &= 1 + r + r^2 + \cdots + r^{N-1} + r^N, \\ rS_N &= \quad r + r^2 + \cdots + r^{N-1} + r^N + r^{N+1}. \end{aligned}$$

Restando estas dos expresiones, $S_N - rS_N = 1 - r^{N+1}$, así que

$$S_N = \frac{1 - r^{N+1}}{1 - r}.$$

Finalmente, si la razón r cumple $|r| < 1$, entonces $r^{N+1} \to 0$ cuando $N \to \infty$, con lo cual

$$\sum_{n=0}^{\infty} r^n = \lim_{N \to \infty} S_N = \frac{1}{1 - r}.$$

7. Números perfectos

Sea un entero $p > 1$ tal que $2^p - 1$ es primo. Entonces, $n = 2^{p-1}(2^p - 1)$ es un número perfecto (es decir, n es la suma de sus divisores propios).

Si usamos $\sigma(n)$ para denotar la suma de los divisores de n (incluido el propio n), que un entero $n > 1$ sea perfecto equivale a que $\sigma(n) = 2n$.

En nuestro caso, al ser $2^p - 1$ primo, los divisores de $n = 2^{p-1}(2^p - 1)$ son $1, 2, 2^2, \ldots, 2^{p-1}$, y $1 \cdot (2^p - 1), 2 \cdot (2^p - 1), 2^2 \cdot (2^p - 1), \ldots, 2^{p-1} \cdot (2^p - 1)$. Entonces, utilizando la fórmula para la suma de una progresión geométrica (prueba 6),

$$\begin{aligned} \sigma(n) &= 1 + 2 + 2^2 + \cdots + 2^{p-1} + (1 + 2 + 2^2 + \cdots + 2^{p-1})(2^p - 1) \\ &= \frac{2^p - 1}{2 - 1} + \frac{2^p - 1}{2 - 1}(2^p - 1) = 2^p(2^p - 1) = 2n, \end{aligned}$$

tal como queríamos comprobar.

Aunque no es estrictamente necesario para la demostración que hemos dado, conviene mencionar que, si $2^p - 1$ es primo, también p es primo (lo veremos más adelante, prueba 24), lo cual es un requisito importante para intentar encontrar números perfectos. Los primeros números perfectos son 6, 28 y 496, que se corresponden con $p = 2$, 3 y 5; pero $2^{11} - 1$ no es primo, así que $2^{10}(2^{11} - 1)$ no es perfecto.

El resultado sobre números perfectos que hemos probado es de Euclides. Además, aunque no lo menciona expresamente, seguro que se dio cuenta de que, si $2^p - 1$ no es primo, $n = 2^{p-1}(2^p - 1)$ no es perfecto (si $2^p - 1$ no es primo, razonando como antes resulta obvio que $\sigma(n) > 2n$). En 1747, Euler encontró una caracterización de los números perfectos que es «casi» el recíproco del resultado de Euclides; lo que Euler demostró es que cualquier número perfecto par es de esa forma (la demostración no es complicada, pero requiere usar algunas propiedades de la función σ, y se puede ver, por ejemplo, en [35, sección 7.2]). No se sabe si existe algún número perfecto impar; posiblemente este es el problema matemático más antiguo cuya respuesta aún no se conoce.

8. Serie armónica

La serie

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \cdots$$

es divergente.

Esta es la demostración que realizó Nicolás de Oresme hacia 1360, que solo necesita agrupar los términos de la serie de manera adecuada:

$$\begin{aligned}\sum_{n=1}^{\infty} \frac{1}{n} &= 1 + \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right) + \cdots \\ &\geq 1 + \frac{1}{2} + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}\right) + \cdots \\ &= 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \cdots,\end{aligned}$$

que es claramente divergente.

9. Serie telescópica

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

Es un ejemplo típico de serie telescópica, un procedimiento ideado por Pietro Mengoli alrededor de 1650:

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{1}{n(n+1)} &= \sum_{n=1}^{\infty}\left(\frac{1}{n}-\frac{1}{n+1}\right) = \lim_{N\to\infty}\sum_{n=1}^{N}\left(\frac{1}{n}-\frac{1}{n+1}\right)\\ &= \lim_{N\to\infty}\left(\left(1-\frac{1}{2}\right)+\left(\frac{1}{2}-\frac{1}{3}\right)+\cdots+\left(\frac{1}{N}-\frac{1}{N+1}\right)\right)\\ &= \lim_{N\to\infty}\left(1+\left(-\frac{1}{2}+\frac{1}{2}\right)+\left(-\frac{1}{3}+\frac{1}{3}\right)+\cdots+\left(-\frac{1}{N}+\frac{1}{N}\right)-\frac{1}{N+1}\right)\\ &= \lim_{N\to\infty}\left(1-\frac{1}{N+1}\right)=1.\end{aligned}$$

10. Límites iterados en una sucesión

$$\lim_{n\to\infty}\lim_{m\to\infty}\frac{n}{m+n}\neq\lim_{m\to\infty}\lim_{n\to\infty}\frac{n}{m+n}.$$

A la izquierda, $\lim_{m\to\infty}\frac{n}{m+n}=0$ para cada n, luego el límite doble de la izquierda vale 0. A la derecha, $\lim_{n\to\infty}\frac{n}{m+n}=1$ para cada m, luego el límite doble de la derecha vale 1.

11. Límites iterados en una función

$$\lim_{m\to\infty}\lim_{n\to\infty}\cos^{2n}(m!\,\pi x)=\begin{cases}1, & \textit{si } x \textit{ es racional,}\\ 0, & \textit{si } x \textit{ es irracional.}\end{cases}$$

Si $x=p/q$ es racional (con $q>0$), entonces $m!\,\pi x$ es un múltiplo entero de π cuando $m\geq q$, así que $\cos(m!\,\pi x)=\pm1$, y $\cos^{2n}(m!\,\pi x)=1$ para cualquier n. Eso implica, claramente, que el límite doble vale 1.

Si x no es racional, entonces $m!\,\pi x$ no será nunca un múltiplo entero de π (aquí estamos usando que π es irracional, que lo veremos en la prueba 35), así que $|\cos(m!\,\pi x)|<1$ y $\cos^{2n}(m!\,\pi x)$ tiende a 0 cuando $n\to\infty$, luego el límite doble también tiende a 0.

12. Función constante

Las únicas funciones $f:\mathbb{R}\to\mathbb{R}$ *que cumplen*

$$f(y)-f(x)\leq(y-x)^2$$

son las constantes.

Si intercambiamos el papel de x e y también se cumple $f(x) - f(y) \leq (y-x)^2$, así que $|f(y) - f(x)| \leq (y-x)^2$, y, por tanto,

$$\frac{|f(y) - f(x)|}{|y-x|} \leq |y-x|.$$

Escribiendo $y = x+h$ y tomando límites cuando $h \to 0$ obtenemos $f'(x) = 0$ (para cualquier $x \in \mathbb{R}$), así que f es una función constante.

13. Teorema del punto fijo

Si, para alguna constante $c < 1$, una función $f : \mathbb{R} \to \mathbb{R}$ cumple

$$|f(y) - f(x)| \leq c|y-x|, \qquad x, y \in \mathbb{R},$$

entonces f tiene un único punto fijo.

Una función como la del enunciado se denomina *contractiva*, con lo cual el resultado que estamos mostrando, que en matemáticas tiene importantes consecuencias, se denomina teorema del punto fijo para aplicaciones contractivas. Usando la definición de continuidad es inmediato que cualquier función contractiva es continua. Obviamente, tiene que ser $c \geq 0$ y el caso $c = 0$ es trivial.

Además, usando normas o distancias en vez de valores absolutos, el correspondiente teorema del punto fijo es igualmente cierto si, en vez de en $\mathbb{R}$, tomamos funciones definidas en $\mathbb{C}$, en $\mathbb{R}^n$ o en un espacio de Banach (y la demostración es, esencialmente, la misma).

Dado $x \in \mathbb{R}$ cualquiera, sea la sucesión $\{x_k\}_{k=0}^{\infty}$ definida tomando $x_0 = x$ y $x_k = f(x_{k-1})$, para $k \geq 1$. Entonces,

$$|x_{k+1} - x_k| \leq c|x_k - x_{k-1}| \leq c^2|x_{k-1} - x_{k-2}| \leq \cdots \leq c^k|x_1 - x_0|.$$

Con esto, para enteros positivos distintos n y m cualesquiera (podemos suponer $m > n$), utilizando la desigualdad triangular y la fórmula para la suma de una progresión geométrica (prueba 6) tenemos

$$\begin{aligned} |x_m - x_n| &\leq \sum_{k=n}^{m-1} |x_{k+1} - x_k| \leq \sum_{k=n}^{m-1} c^k |x_1 - x_0| \\ &= |x_1 - x_0| c^n \sum_{k=0}^{m-n-1} c^k \leq |x_1 - x_0| c^n \sum_{k=0}^{\infty} c^k = \frac{c^n}{1-c} |x_1 - x_0| =: I_n. \end{aligned}$$

Para cada $\varepsilon > 0$ que elijamos, existe un N tal que $I_n < \varepsilon$ cuando $n \geq N$ (recordar que $c < 1$). Entonces $|x_m - x_n| < \varepsilon$ para $n, m \geq N$, y la sucesión $\{x_k\}_{k=0}^{\infty}$ es de Cauchy, con lo cual tiene límite, $x^* = \lim_{k\to\infty} x_k$. En consecuencia, como f es continua,

$$f(x^*) = f\left(\lim_{k\to\infty} x_k\right) = \lim_{k\to\infty} f(x_k) = \lim_{k\to\infty} x_{k+1} = x^*,$$

y x^* es un punto fijo.

Que no puede haber dos puntos fijos es obvio, pues si x^* y x^{**} fuesen puntos fijos tendríamos

$$|x^* - x^{**}| = |f(x^*) - f(x^{**})| \leq c|x^* - x^{**}|,$$

lo cual es imposible por ser $c < 1$.

El lector interesado puede consultar [25] para ver otra demostración, incluso algo más breve, del mismo resultado. En ella, la prueba de que la sucesión $\{x_k\}_{k=0}^{\infty}$ es de Cauchy es diferente.

14. Teorema de Jacobi sobre rotaciones irracionales

Sea $\mathbb{S}^1 := \{z \in \mathbb{C} : |z| = 1\}$ *la circunferencia de radio* 1, $\alpha \in \mathbb{R}$ *y* $\lambda = e^{2\pi\alpha i}$. *El conjunto* $\mathcal{O} := \{\lambda^n : n \geq 0\} \subset \mathbb{S}^1$ *es denso en* $\mathbb{S}^1$ *si y solo si* $\alpha \notin \mathbb{Q}$.

Cuando $\alpha = p/q \in \mathbb{Q}$, es claro que el conjunto $\mathcal{O}$ es finito ya que, como $\lambda^q = e^{2\pi pi} = 1$, entonces $\mathcal{O} = \{\lambda^n : 0 \leq n \leq q\}$. En particular, no puede ser denso.

Supongamos ahora que $\alpha \notin \mathbb{Q}$ y demostremos su densidad. En primer lugar observemos que, en este caso, $\lambda^m \neq \lambda^n$ cuando $m \neq n$. En efecto, si para $m > n$ coincidiesen, λ cumpliría $\lambda^{m-n} = 1$, así que λ sería una raíz de la unidad, lo cual no es cierto (las raíces k-ésimas de la unidad son $e^{2\pi ji/k}$, con $j = 0, 1, \ldots, k-1$).

Por lo tanto, el conjunto $\mathcal{O}$ es infinito y, como $\mathbb{S}^1$ es compacto, $\mathcal{O}$ tiene un punto de acumulación en $\mathbb{S}^1$. En consecuencia, para todo $\varepsilon > 0$ hay dos puntos de $\mathcal{O}$, digamos λ^p y λ^q, con $p > q$, que están a distancia menor que ε. Como multiplicar o dividir por λ corresponde a una rotación rígida que no cambia la distancia entre puntos (es decir, es una isometría), tenemos que la distancia entre λ^k y 1, donde $k = p - q \in \mathbb{N}$, es también menor que ε. Finalmente, usando de nuevo la propiedad de isometría, se sigue que el subconjunto de $\mathcal{O}$ formado por los puntos λ^{jk}, $j \geq 0$, es tal que dos puntos consecutivos están a distancia menor que ε. Por lo tanto, ya solo usando estos puntos tenemos un recubrimiento de $\mathbb{S}^1$ con intervalos de medida menor que ε, y $\mathcal{O}$ es denso, tal y como queríamos probar.

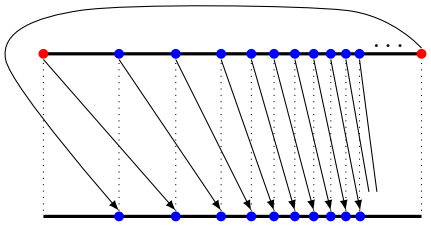
El resultado que hemos demostrado se puede interpretar también en el lenguaje de sistemas dinámicos: si se toma el sistema dinámico discreto generado por $f(z) = \lambda z$, que va de $\mathbb{S}^1$ a $\mathbb{S}^1$, la órbita (positiva) de 1 es $f^n(1) = \lambda^n$, $n \geq 0$, que coincide con $\mathcal{O}$, y llena densamente $\mathbb{S}^1$ si y solo si α es irracional.

15. Una aplicación biyectiva entre $[0,1]$ y $(0,1)$

Existe una aplicación biyectiva entre $[0,1]$ *y* $(0,1)$.

Aunque de entrada puede parecer sorprendente, hay aplicaciones biyectivas entre el intervalo cerrado $[0,1]$ y el intervalo abierto $(0,1)$. Eso sí, las diferencias topológicas entre ellos hacen que estas aplicaciones no puedan ser continuas. Damos a continuación una aplicación f explícita y biyectiva.

Fijada una sucesión estrictamente creciente de puntos en $(0,1)$, $x_1 < x_2 < \cdots < x_n < \cdots$, con límite 1, definimos $f : [0,1] \to (0,1)$ tomando $f(1) = x_1$, $f(0) = x_2$, $f(x_n) = x_{n+2}$ para todo $n \geq 1$, y $f(x) = x$ en cualquier otro caso. Esta aplicación f, que es, evidentemente, una biyección, se ilustra en la siguiente figura:

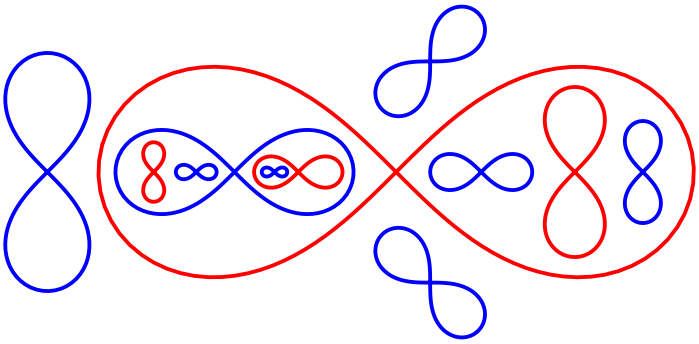


Por lo general, construir una biyección explícita entre dos conjuntos, para los que se sospecha que existe, es un trabajo complicado. Hay un resultado que nos permite probar su existencia sin necesidad de construirla, el teorema de Cantor-Bernstein-Schröder, véase [1, capítulo 19]. Este teorema nos dice que, si para dos conjuntos S y T existe una aplicación inyectiva de S a T y otra de T a S, entonces hay una tercera aplicación entre los dos que es biyectiva. Para los dos conjuntos del enunciado, esas dos aplicaciones inyectivas son muy fáciles de construir: la identidad $\mathrm{id}(x) = x$ entre $(0,1)$ y $[0,1]$, y $g(x) = (2x+1)/4$ entre $[0,1]$ y un subconjunto de $(0,1)$.

16. Curvas con forma de infinito

En el plano, no es posible tener un número no numerable de curvas disjuntas con «forma de infinito».

Antes de dar la demostración, debemos aclarar que el enunciado alude a configuraciones como la que sigue (pero con infinitas curvas de ese tipo, a las que llamamos, simplemente, «infinitos»):



Además, un conjunto se denomina *numerable* si existe una aplicación biyectiva entre ese conjunto y los números naturales, o entre ese conjunto y cualquier otro que se sabe que es numerable (como $\mathbb{Q}$ o $\mathbb{Q}^n$ para cualquier n fijo), y *no numerable* en caso contrario (como $\mathbb{R}$). Una vez precisado el enunciado, vamos con la demostración.

Tomemos una configuración con infinitos infinitos, $\mathcal{I}$. A cada infinito, $I \in \mathcal{I}$, le podemos asociar un par de puntos con coordenadas racionales $(p_1, p_2), (q_1, q_2) \in \mathbb{Q}^2$ de manera que cada uno de ellos esté dentro de cada una de las dos componentes conexas acotadas de $\mathbb{R}^2 \setminus I$. Así construimos la aplicación $f : \mathcal{I} \to \mathbb{Q}^4$ definida como $f(I) = (p_1, p_2, q_1, q_2)$. Observemos que si $I, J \in \mathcal{I}$ y $I \neq J$, entonces una de las componentes conexas acotadas de $\mathbb{R}^2 \setminus I$ es disjunta con una de las componentes conexas acotadas de $\mathbb{R}^2 \setminus J$. Por lo tanto, $f(I) \neq f(J)$ y f es inyectiva. Como consecuencia, $\mathcal{I}$ está en correspondencia biyectiva con un subconjunto de $\mathbb{Q}^4$ y, por lo tanto, es numerable.

La demostración es fácil de adaptar para conjuntos C cuya forma sea tal que $\mathbb{R}^2 \setminus C$ tenga, como mínimo, dos componentes conexas acotadas. Por otro lado, colocar en el plano un número no numerable de curvas disjuntas con «forma de cero» es sencillo. Basta tomar las circunferencias $C_r = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = r^2\}$, con $r \in (0, 1)$ (que los reales del intervalo $(0, 1)$ no forman un conjunto numerable se ve en la prueba 31).

Equivalencias

Hay numerosos resultados matemáticos que afirman que determinadas propiedades o expresiones son equivalentes. A menudo, comprobar eso requiere un tipo de argumentos en una dirección, y otros en la dirección contraria. Presentamos aquí unos pocos resultados en los que se usan argumentos que funcionan, a la vez, en ambas direcciones.

17. Un número más su inverso

Para todo $x > 0$ se cumple que $x + 1/x \geq 2$.

Basta observar lo siguiente:

$$x + 1/x \geq 2 \iff x^2 + 1 \geq 2x \iff x^2 - 2x + 1 \geq 0 \iff (x-1)^2 \geq 0.$$

18. Ecuación cuadrática

Las soluciones de $ax^2 + bx + c = 0$, *con* $a \neq 0$, *son* $x = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.

Tenemos la siguiente cadena de equivalencias:

$$\begin{aligned} ax^2 + bx + c = 0 &\iff x^2 + \frac{b}{a}x + \frac{c}{a} = 0 \\ &\iff \left(x + \frac{b}{2a}\right)^2 - \frac{b^2}{4a^2} + \frac{c}{a} = 0 \iff \left(x + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2} \\ &\iff x + \frac{b}{2a} = \pm\frac{\sqrt{b^2 - 4ac}}{2a} \iff x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}, \end{aligned}$$

que demuestra el resultado deseado.

19. Raíces complejas de un polinomio

Sea $P(z)$ *un polinomio con coeficientes reales. Entonces,* $\alpha = a + bi \in \mathbb{C}$ *(con* $a, b \in \mathbb{R}$*) es raíz si y solo si su conjugado* $\overline{\alpha} = a - bi$ *es raíz.*

Si tenemos dos números complejos z y w, es inmediato comprobar que

$$\overline{z + w} = \overline{z} + \overline{w} \qquad \text{y} \qquad \overline{z \cdot w} = \overline{z} \cdot \overline{w}$$

(basta escribir ambos complejos en su forma $x + yi$ y operar). Como consecuencia, si el polinomio es $P(z) = a_k z^k + a_{k-1} z^{k-1} + \cdots a_1 z + a_0$, al conjugar tendremos

$$\begin{aligned} \overline{P(z)} &= \overline{a_k}(\overline{z})^k + \overline{a_{k-1}}(\overline{z})^{k-1} + \cdots + \overline{a_1 z} + \overline{a_0} \\ &= a_k(\overline{z})^k + a_{k-1}(\overline{z})^{k-1} + \cdots + a_1\overline{z} + a_0 = P(\overline{z}). \end{aligned}$$

Entonces,

$$P(\alpha) = 0 \iff \overline{P(\alpha)} = 0 \iff P(\overline{\alpha}) = 0,$$

tal como queríamos demostrar.

20. Una ecuación diferencial

Sea $f : \mathbb{R} \to \mathbb{R}$ *una función derivable, y* $a \in \mathbb{R}$. *Entonces,* f *es solución de la ecuación diferencial* $f'(x) = af(x)$ *si y solo si* $f(x) = ce^{ax}$ *para una cierta* $c \in \mathbb{R}$.

Sea $F(x) = e^{-ax} f(x)$, función también derivable, con lo cual

$$\begin{aligned} F'(x) &= \left(e^{-ax} f(x)\right)' = -ae^{-ax} f(x) + e^{-ax} f'(x) \\ &= e^{-ax}\left(f'(x) - af(x)\right). \end{aligned}$$

Entonces, sin más que usar que una función es constante si y solo si su derivada es 0, tenemos

$$f'(x) = af(x) \iff F'(x) = 0 \iff F(x) = c \iff f(x) = ce^{ax}$$

para un cierto $c \in \mathbb{R}$, tal y como queríamos demostrar.

Aunque la ecuación diferencial considerada es una de las más sencillas, no por eso es menos importante. Por ejemplo, la ley de Malthus sobre crecimiento de poblaciones o la ley de desintegración radiactiva se reducen a ella.

Contrarrecíproco

El contrarrecíproco de una implicación lógica «Si P, entonces Q» es una proposición equivalente «Si no Q, entonces no P». Se utiliza como método de demostración indirecta pues, para demostrar «Si P, entonces Q», a menudo es más sencillo demostrar su contrarrecíproco.

21. Raíz de un irracional

Si $x > 0$ es irracional, entonces $\sqrt[n]{x}$ también lo es.

Lo que queremos demostrar es que $0 < x \notin \mathbb{Q} \Longrightarrow \sqrt[n]{x} \notin \mathbb{Q}$. Su contrarrecíproco

$$\sqrt[n]{x} = p/q \in \mathbb{Q} \implies x = (p/q)^n \in \mathbb{Q}$$

es claramente cierto.

22. Un cuadrado par

Si $n \in \mathbb{N}$ y $n^2 \in \mathbb{N}$ es par, entonces n también es par.

Es mucho más sencillo demostrar el contrarrecíproco: *si n es impar entonces n^2 es impar*. Para hacerlo escribimos $n = 2m+1$, con $m \in \mathbb{N}$. Entonces $n^2 = 2(2m^2 + 2m) + 1$ es impar, tal como queríamos probar.

23. Test de primalidad

Si un entero $n \geq 2$ no tiene divisores primos menores o iguales que $\sqrt{n}$, entonces n es primo.

El contrarrecíproco de este resultado es así: *si $n \geq 2$ es compuesto, tiene algún divisor primo menor o igual que $\sqrt{n}$*. Y esto es fácil de comprobar. Si n es compuesto, su descomposición en factores tiene, al menos, dos primos p y q (pueden ser iguales). Y no pueden ser ambos mayores que $\sqrt{n}$, porque entonces $pq > n$.

24. Primos de Mersenne

Sea un entero $n > 1$ tal que $2^n - 1$ es primo. Entonces, n es primo.

Es más sencillo probar el contrarrecíproco: *si n es un número compuesto, $2^n - 1$ no es primo.*

Comencemos observando la siguiente igualdad entre polinomios:

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1), \quad n > 1.$$

Si $n = rs$ y tomamos $y = x^r$, resulta claro que $y - 1 = x^r - 1$ divide a $x^n - 1 = y^s - 1$. En el caso del número $2^n - 1$ con n compuesto, se podrá poner $n = rs$ para ciertos números enteros $r, s > 1$. Con esto, tomando $x = 2$ en el polinomio anterior, $2^r - 1$ divide a $2^n - 1$, luego $2^n - 1$ no puede ser primo, y ya hemos probado el resultado.

El recíproco no es cierto: el primer contraejemplo es $2^{11} - 1 = 23 \cdot 89$. Los números de la forma $2^p - 1$, con p primo, se denominan números de Mersenne; y, si son primos, primos de Mersenne. El nombre alude a Marin Mersenne, quien los estudió en el siglo XVII.

Por descontado, lo mismo se puede probar para números de la forma $a^n - 1$ con cualquier entero $a > 1$, y con la misma demostración. Pero el caso más famoso es el que se corresponde con $a = 2$. La razón es que existe un test especializado muy rápido para probar la primalidad de los números de la forma $2^p - 1$ (el test de Lucas-Lehmer), lo cual permite encontrar primos enormemente grandes. Además, son los números $2^p - 1$ los que están relacionados con los números perfectos (prueba 7).

25. Densidad en $\mathbb{R}$

Dados dos números reales $x < y$, siempre hay un número racional, uno irracional y uno trascendente en el intervalo $\mathcal{I} = (x, y)$.

Recordemos, para empezar, que un número real α se llama *algebraico* si hay un polinomio P no trivial, con coeficientes en $\mathbb{Z}$ (o en $\mathbb{Q}$, es equivalente),

y tal que $P(\alpha) = 0$. En particular, todos los números racionales $p/q \in \mathbb{Q}$ son algebraicos ya que son ceros de $P(t) = qt - p$. Los números que no son algebraicos se llaman *trascendentes*. Un famoso número trascendente es π. Esta propiedad de π fue demostrada por Ferdinand von Lindemann en 1882. Se sabe que tanto los números racionales como los algebraicos son numerables. En cambio, los irracionales y los trascendentes no lo son, y, en consecuencia, constituyen la mayoría de los números.

Veamos primero la existencia de un racional en $\mathcal{I}$. Sea $n \in \mathbb{N}$ tal que $1/n < y - x$. Tomamos $j \in \mathbb{Z}$ como el mayor entero tal que $j/n \leq x$. Demostremos que $(j+1)/n \in \mathcal{I}$. Por la maximalidad de j sabemos que $(j+1)/n > x$. Además, $(j+1)/n = j/n + 1/n < j/n + y - x \leq y$, tal y como queríamos ver.

Para probar que hay un irracional (respectivamente, trascendente) en $\mathcal{I}$, aplicamos el resultado anterior a $(x/a, y/a)$, donde $a > 0$ es un irracional (respectivamente, trascendente). Ya sabemos que hay un racional p/q en ese intervalo. Entonces

$$\frac{x}{a} < \frac{p}{q} < \frac{y}{a} \implies x < r := \frac{ap}{q} < y.$$

Si $a \notin \mathbb{Q}$, claramente $r \notin \mathbb{Q}$ y el resultado queda probado para números irracionales. Si a es trascendente, veamos que r también lo es, concluyendo la demostración. Lo haremos probando el contrarrecíproco de la afirmación. Si r es algebraico, existe un polinomio P, no trivial y con coeficientes en $\mathbb{Q}$, tal que $P(r) = 0$. Si definimos $Q(t) = P(qt/p)$, tenemos otro polinomio no trivial y con coeficientes racionales tal que $Q(r) = P(a) = 0$, y por lo tanto a es también algebraico, demostrando el resultado deseado.

Reducción al absurdo

La reducción al absurdo es un método lógico y matemático para demostrar la veracidad de una tesis, asumiendo temporalmente que su opuesta es cierta. Si esta suposición conlleva una contradicción lógica o un absurdo, se concluye que la tesis original es verdadera.

26. Infinitos números primos

Existen infinitos números primos.

Damos la famosa y clásica demostración de Euclides. Si hubiera una cantidad finita, considerémoslos todos: $n_1, n_2, \ldots, n_k$. Entonces el número $n = n_1 n_2 \cdots n_k + 1$ o bien es primo, o bien tiene un divisor primo que no está en la lista, ya que n no es divisible por ninguno de los n_j.

En realidad, Euclides no tenía la noción de infinito que tenemos hoy, así que, en los *Elementos*, él redactó el resultado diciendo que «cualquier

conjunto finito de números primos no contiene todos los números primos». Esencialmente, esta es la demostración que hemos dado aquí. En la prueba 54 se ve cómo deducir la existencia de infinitos primos del resultado que allí se presenta. Y en [31] se recogen bastantes demostraciones más.

27. Irracionalidad de $\sqrt{2}$

El número $\sqrt{2}$ es irracional.

La demostración más habitual es suponer que $\sqrt{2} = p/q$, fracción irreducible, y llegar a un absurdo. Elevando al cuadrado, $p^2 = 2q^2$ par, así que p también será par, $p = 2m$ (de hecho, esto lo hemos visto en la prueba 22). Entonces, $4m^2 = 2q^2$, $q^2 = 2m^2$ par, y q también será par. Pero p y q no pueden ser ambos pares, ya que la fracción p/q era irreducible.

Presentamos asimismo una curiosa demostración, también por reducción al absurdo, que no es muy conocida. Como

$$\left(18 + 17\sqrt{2}\right)^3 + \left(18 - 17\sqrt{2}\right)^3 = 42^3,$$

y dado que $\sqrt{2} \neq \pm 18/17$, si se cumpliera que $\sqrt{2} \in \mathbb{Q}$ entraríamos en contradicción con el último teorema de Fermat (con exponente 3, un resultado de Euler). Ya hemos recordado este teorema en la prueba 3.

28. Irracionalidad de un logaritmo

El número $\log_2(3)$ es irracional.

Si fuera racional, $\log_2(3) = p/q$, con $p, q \in \mathbb{N}$. Entonces,

$$3 = 2^{\log_2(3)} = 2^{p/q} \implies 3^q = 2^p.$$

Igualdad imposible, ya que 3^q es impar y 2^p es par. La demostración se adapta fácilmente para probar que si m y n son primos entre sí, entonces $\log_n(m)$ es siempre irracional.

29. Irracionalidad de e

El número e es irracional.

La irracionalidad de e la probó Euler en 1737, utilizando fracciones continuas. La demostración que vamos a dar parte de la conocida serie $e = \sum_{k=0}^{\infty} 1/k!$, y es, esencialmente, la que dio Joseph Fourier alrededor de 1815. Aparte de eso, solo usa un hecho completamente elemental, al que a veces se alude con el nombre de principio fundamental de la teoría de números: que no existe ningún entero I que cumple $0 < I < 1$.

Supongamos que $e = m/n \in \mathbb{Q}$. Resulta obvio que

$$I := n!\left(\frac{m}{n} - \sum_{k=0}^{n} \frac{1}{k!}\right)$$

es un entero. Además, $e - \sum_{k=0}^{n} 1/k!$ es positivo. Entonces,

$$\begin{aligned}
0 < I &= n!\left(\frac{m}{n} - \sum_{k=0}^{n} \frac{1}{k!}\right) = n!\left(e - \sum_{k=0}^{n} \frac{1}{k!}\right) \\
&= n!\left(\frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \frac{1}{(n+3)!} + \frac{1}{(n+4)!} + \cdots\right) \\
&= \frac{n!}{(n+1)!}\left(1 + \frac{1}{n+2} + \frac{1}{(n+2)(n+3)} + \frac{1}{(n+2)(n+3)(n+4)} + \cdots\right) \\
&\le \frac{1}{n+1}\left(1 + \frac{1}{n+2} + \frac{1}{(n+2)^2} + \frac{1}{(n+2)^3} + \cdots\right) \\
&= \frac{1}{n+1} \cdot \frac{1}{1 - 1/(n+2)} = \frac{n+2}{(n+1)^2} < 1,
\end{aligned}$$

y hemos encontrado que I es un entero entre 0 y 1, lo cual es absurdo. Obsérvese que en el paso a la última línea hemos usado la fórmula para sumar una progresión geométrica, demostrada en la prueba 6.

30. Coseno de un grado

El número $\cos(1°)$ *es irracional.*

Como

$$\cos(n° + 1°) + \cos(n° - 1°) = 2\cos(1°)\cos(n°),$$

para $n = 1$ se cumple que

$$\cos(2°) = 2\cos^2(1°) - 1.$$

Si asumimos que $\cos(1°)$ es racional, esto implica que $\cos(2°)$ también sería racional y, repitiendo varias veces el mismo argumento, todos los $\cos(n°)$, $n \ge 1$, hasta $n = 30$, serían asimismo racionales. Sin embargo, $\cos(30°) = \sqrt{3}/2$, que es irracional, luego hemos llegado a una contradicción.

31. El argumento de la diagonal de Cantor

El conjunto de los números reales no es numerable

Recordemos que un conjunto es numerable si existe una aplicación biyectiva entre ese conjunto y los números naturales (y dar una biyección con los naturales es lo mismo que escribir todos los elementos del conjunto en

un cierto orden). Como la función $y = (2x-1)/(x-x^2)$ entre el intervalo $(0,1)$ y $\mathbb{R}$ es biyectiva, el resultado equivale a demostrar que $(0,1)$ no es un conjunto numerable.

La prueba que vamos a dar es de Georg Cantor, y utiliza lo que ahora conocemos como argumento de la diagonal de Cantor. Dio esta preciosa demostración en 1891, aunque el resultado lo había probado de otra forma mucho más complicada en 1874.

Cualquier número $r \in (0,1)$ tiene una expresión decimal de la forma

$$r = \sum_{j=1}^{\infty} \frac{d_j}{10^j} = 0.d_1 d_2 d_3 d_4 d_5 \ldots,$$

donde los dígitos d_j cumplen $d_j \in \{0,1,2,3,4,5,6,7,8,9\}$. No permitimos que haya infinitos $d_j = 9$ seguidos, con lo cual la expresión decimal de cada número es única (sin esta salvedad, puede ocurrir lo que se observa en la prueba 69).

Para demostrar la no numerabilidad del intervalo $(0,1)$ emplearemos reducción al absurdo. Supongamos que hemos logrado numerarlo, de tal manera que tenemos una sucesión $\{r_n\}_{n=1}^{\infty}$ en la que están todos los reales entre 0 y 1. De este modo, podemos escribir

$$\begin{aligned}
r_1 &= 0.d_1^1 d_2^1 d_3^1 d_4^1 d_5^1 \ldots,\\
r_2 &= 0.d_1^2 d_2^2 d_3^2 d_4^2 d_5^2 \ldots,\\
r_3 &= 0.d_1^3 d_2^3 d_3^3 d_4^3 d_5^3 \ldots,\\
r_4 &= 0.d_1^4 d_2^4 d_3^4 d_4^4 d_5^4 \ldots,\\
r_5 &= 0.d_1^5 d_2^5 d_3^5 d_4^5 d_5^5 \ldots,
\end{aligned}$$

y así sucesivamente. Recorriendo el cuadro anterior en diagonal, construyamos un número

$$r = 0.d_1 d_2 d_3 d_4 d_5 \ldots,$$

de forma que

$$d_1 \neq d_1^1, \quad d_2 \neq d_2^2, \quad d_3 \neq d_3^3, \quad d_4 \neq d_4^4, \quad d_5 \neq d_5^5, \quad \ldots$$

(de paso, no elegimos ningún $d_j = 0$ o $d_j = 9$, para que no pueda haber problemas con la no unicidad en la representación decimal, y para evitar que r sea 0 o 1). Ahora, por una parte, $r \in (0,1)$; y, por otra, este r no está en la lista ya que $d_j \neq d_j^j$ por construcción, luego $r \neq r_j$ para todos los j. Esto es un absurdo, que proviene de haber supuesto que el intervalo $(0,1)$ es un conjunto numerable.

32. Un conjunto y sus partes

No existe ninguna aplicación biyectiva entre un conjunto A (no vacío) y el conjunto de sus partes $\mathcal{P}(A)$.

Obsérvese que cuando A es finito, digamos que tiene n elementos, $\mathcal{P}(A)$ tiene 2^n elementos, y el resultado es trivial. Así que la demostración que sigue solo tiene interés solo cuando A es un conjunto infinito (aunque es válida en general).

Supongamos, para llegar a una contradicción, que A es un conjunto tal que existe una aplicación biyectiva f entre A y $\mathcal{P}(A)$. Definimos el siguiente subconjunto de A:

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

Como f es biyectiva, existe un $y \in A$ tal que $f(y) = B$. Ahora bien, si $y \in B$, por definición $y \notin f(y) = B$ y tenemos una contradicción. Por otra parte, si $y \notin B$, tenemos que $y \in f(y) = B$, de nuevo una contradicción. En ambos casos hemos llegado a la contradicción, así que la biyección f no puede existir.

33. Una ecuación diofántica

La ecuación

$$x^2 + y^2 + z^2 = 2xyz$$

no tiene soluciones en los enteros positivos.

Para ver que esa ecuación no tiene soluciones, usaremos el método de descenso infinito de Fermat. Este método es una técnica de demostración por contradicción que popularizó Pierre de Fermat, en el siglo XVII, para resolver problemas de la teoría de números. Las demostraciones que usan el método de descenso infinito entran en contradicción con el principio de buena ordenación en los números naturales, esto es, que todo subconjunto $A \subseteq \mathbb{N}$ de números naturales tiene un mínimo. Donde más empleó Fermat su método fue en el estudio de soluciones de ecuaciones diofánticas (ecuaciones en las que solo interesa conocer sus soluciones enteras); la propuesta en el enunciado es un ejemplo típico.

Dado que $2xyz$ es par, la suma $x^2 + y^2 + z^2$ también debe ser par, así que, si (x, y, z) es una solución, los tres serán pares o exactamente uno de ellos será par.

Si uno de ellos es par (supongamos que x) y los otros dos impares, escribiendo $x = 2u$, $y = 2v + 1$, $z = 2w + 1$, tendremos

$$4u^2 + (2v + 1)^2 + (2w + 1)^2 = 4u(2v + 1)(2w + 1).$$

En esta expresión, el lado derecho es divisible por 4, pero no así el lado izquierdo (basta expandir las dos potencias $(2v + 1)^2$ y $(2w + 1)^2$). Eso es imposible, luego los tres valores x, y, z deben ser pares.

Así pues, tomemos $x = 2x_1$, $y = 2y_1$, $z = 2z_1$, que serán soluciones de la ecuación

$$x_1^2 + y_1^2 + z_1^2 = 4x_1y_1z_1.$$

De esta ecuación, y con el mismo razonamiento que antes, también se deduce que los tres valores x_1, y_1, z_1 deben ser pares. Tomemos de nuevo $x_1 = 2x_2$, $y_1 = 2y_1$, $z_2 = 2z_1$ (luego $x_2 = x/4$, $y_2 = y/4$, $z_2 = z/4$), y su ecuación

$$x_2^2 + y_2^2 + z_2^2 = 8x_s y_s z_s.$$

Manteniendo este proceso, para cada s encontramos enteros $x_s = x/2^s$, $y_s = y/2^s$, $z_s = z/2^s$ que son solución de la ecuación

$$x_s^2 + y_s^2 + z_s^2 = 2^{s+1} x_s y_s z_s.$$

Pero esto es imposible, ya que un entero positivo no se puede dividir por 2 indefinidamente.

34. Irracionalidad de $\sqrt{k}$

Si $k \in \mathbb{N}$ no es un cuadrado perfecto, $\sqrt{k}$ es un número irracional.

En la prueba 27, ya hemos visto la irracionalidad de $\sqrt{2}$. Usando la descomposición única en factores primos, es fácil generalizarla a otros enteros. Aquí presentamos una prueba de la irracionalidad de $\sqrt{k}$ que ilustra muy bien el método de descenso infinito de Fermat.

Supongamos que $\sqrt{k}$ no es un entero, pero que sí es un racional, que se podrá expresar como $\sqrt{k} = m/n$ donde m y n son dos números naturales. Asimismo, sea $q = \lfloor \sqrt{k} \rfloor$ (es decir, el mayor entero menor que $\sqrt{k}$). Tomemos ahora $m' = m(\sqrt{k} - q)$ y $n' = n(\sqrt{k} - q)$. Al ser $0 < \sqrt{k} - q < 1$, es claro que $0 < m' < m$ y $0 < n' < n$. Además, m' y n' son enteros:

$$m' = m\sqrt{k} - mq = \left(n\sqrt{k}\right)\sqrt{k} - mq = nk - mq,$$
$$n' = n\sqrt{k} - nq = n\frac{m}{n} - nq = m - nq.$$

Así, cualesquiera que sean los números naturales m y n que hayamos usado para escribir $\sqrt{k} = m/n$, hemos encontrado otros dos números naturales m' y n', con $m' < m$ y $n' < n$, tales que

$$\sqrt{k} = \frac{m}{n} = \frac{m(\sqrt{k} - q)}{n(\sqrt{k} - q)} = \frac{m'}{n'}.$$

Pero el descenso infinito es imposible, así que esto contradice la asunción original de que $\sqrt{k}$ se puede expresar como cociente de dos números naturales.

35. Irracionalidad de π

El número π es irracional.

Reproducimos la demostración de Niven [24]. Supongamos, para llegar a contradicción, que $\pi = \frac{p}{q} \in \mathbb{Q}$. Entonces, definamos

$$f(x) := \frac{F(x)}{n!} := \frac{x^n(p-qx)^n}{n!} = \frac{\sum_{j=n}^{2n} c_j x^j}{n!},$$

para cierto $n \in \mathbb{N}$ que fijaremos más adelante y ciertos $c_j \in \mathbb{Z}$ que no es necesario especificar. Asimismo, introducimos el polinomio

$$G(x) = f(x) - f''(x) + f^{(4)}(x) + \cdots + (-1)^n f^{(2n)}(x).$$

Como $G''(x) + G(x) = f(x)$, se cumple que

$$\Big(G'(x)\operatorname{sen}(x) - G(x)\cos(x)\Big)' = G''(x)\operatorname{sen}(x) + G(x)\operatorname{sen}(x) = f(x)\operatorname{sen}(x),$$

y, como consecuencia,

$$\int_0^\pi f(x)\operatorname{sen}(x)\,\mathrm{d}x = \Big(G'(x)\operatorname{sen}(x) - G(x)\cos(x)\Big)\Big|_0^\pi = G(0) + G(\pi).$$

Probamos a continuación que $G(0) + G(\pi) \in \mathbb{Z}$. Comenzamos viendo que, para todo $j \in \mathbb{N}$, $f^{(j)}(0) \in \mathbb{Z}$ y $f^{(j)}(\pi) \in \mathbb{Z}$. Para $j < n$ y $j > 2n$, es claro que $F^{(j)}(0) = f^{(j)}(0) = 0$; y, para $n \le j \le 2n$,

$$f^{(j)}(0) = \frac{F^{(j)}(0)}{n!} = \frac{j!}{n!}c_j \in \mathbb{Z}.$$

Por simetría, es fácil ver que $f(x) = f(\frac{p}{q} - x)$. Derivando sucesivamente esta igualdad obtenemos que $f^{(j)}(x) = (-1)^j f^{(j)}(\frac{p}{q} - x)$ y, por tanto,

$$f^{(j)}(\pi) = f^{(j)}\left(\frac{p}{q}\right) = (-1)^j f^{(j)}(0) \in \mathbb{Z}.$$

Evaluando el polinomio $G(x)$ en $x = 0$ y en $x = \pi$, y utilizando lo que acabamos de probar, obtenemos que $G(0) + G(\pi) \in \mathbb{Z}$. Por lo tanto,

$$0 < I_n := \int_0^\pi f(x)\operatorname{sen}(x)\,\mathrm{d}x \in \mathbb{Z}.$$

Demostraremos, para terminar, que, para n suficientemente grande, I_n es menor que 1, lo cual es absurdo pues es un entero postivo. En efecto, como

$$0 < I_n = \int_0^\pi \frac{\big(x(p-qx)\big)^n}{n!}\operatorname{sen}(x)\,\mathrm{d}x \le \int_0^\pi \frac{1}{n!}\left(\frac{q^2}{4p}\right)^n \mathrm{d}x = \frac{\pi}{n!}\left(\frac{q^2}{4p}\right)^n,$$

se tiene que $\lim_{n\to\infty} I_n = 0$, y esto prueba el resultado.

36. Una propiedad de los subgrupos de $\mathbb{R}$

Sea $G \neq \{0\}$ un subgrupo de $(\mathbb{R}, +)$. Entonces, o bien existe un número real $a > 0$ tal que $G = a\mathbb{Z} := \{an : n \in \mathbb{Z}\}$, o bien la adherencia de G es todo $\mathbb{R}$.

Sea $a = \text{ínf}\{x \in G : x > 0\}$. Demostraremos que si $a = 0$ entonces G es denso en $\mathbb{R}$, y que si $a > 0$ entonces $G = a\mathbb{Z}$.

Como primer paso, veamos que $a \in G$. Cuando $a = 0$ es obvio, ya que $0 \in G$. Si $a > 0$, y suponemos que $a \notin G$, existirá una sucesión decreciente $\{b_n\}_n$ de elementos de G que tienden a a. En particular, tomando n suficientemente grande, podemos asegurar que $0 < a < b_{n+1} < b_n$ y además $0 < c := b_n - b_{n+1} < a$. Como $0 < c \in G$, y c es menor que a, llegamos a una contradicción con la definición de a. Por lo tanto, ya hemos demostrado que $a \in C$.

Para analizar las dos posibilidades, comencemos por el caso $a = 0$. Entonces, para todo $\varepsilon > 0$ existe $b \in (0, \varepsilon)$ tal que $b \in G$. Como G es subgrupo, $b\mathbb{Z} \subset G$; así pues, cualquier intervalo de longitud ε contendrá puntos de G, y en consecuencia G es denso en $\mathbb{R}$, tal y como queríamos ver.

Si $a > 0$, vamos a ver que $G = a\mathbb{Z}$. Como $a \in G$ y G es subgrupo, $a\mathbb{Z} \subset G$. Para concluir la prueba basta demostrar la inclusión contraria. Procedemos por reducción al absurdo. Sea $b \in G$, pero no en $a\mathbb{Z}$. Entonces existe un $n \in \mathbb{Z}$ tal que $an < b < a(n + 1)$, luego $0 < b - an < a$. Como $b - an \in G$, tenemos un elemento de G positivo y menor que a, contradiciendo el hecho de que a es el ínfimo de los elementos positivos de G. En consecuencia, $G = a\mathbb{Z}$.

Usando lo que hemos demostrado obtenemos sin dificultad el resultado de Leopold Kronecker que afirma que, si $\alpha \notin \mathbb{Q}$, entonces el conjunto de números $m + n\alpha$ con $m, n \in \mathbb{Z}$ es denso en $\mathbb{R}$. A partir del resultado de Kronecker no es difícil dar una prueba diferente del resultado de Jacobi presentado en la prueba 14.

37. Teorema fundamental del álgebra

Todo polinomio no constante tiene, al menos, una raíz en $\mathbb{C}$.

Con distinto grado de rigor, las primeras demostraciones de este importante resultado datan de la segunda mitad del siglo XVIII. Posiblemente, la primera demostración correcta la publicó Jean Robert Argand en 1806. Actualmente, hay unas cuantas demostraciones más, y la más corta es la que usa que, si un polinomio $P(z)$ no tiene raíces en $\mathbb{C}$, entonces la función $1/P(z)$ es entera (holomorfa en todo $\mathbb{C}$) y acotada, lo cual implica, por el teorema de Liouville en análisis complejo, que esa función es constante. Pero esos argumentos requieren más conocimientos matemáticos que los que aquí

estamos presuponiendo, así que vamos a dar una prueba alternativa que no necesita tantos prerrequisitos técnicos.

Sea $P(z)$ polinomio no constante. Entonces, puesto que $|P(z)| \to \infty$ cuando $|z| \to \infty$, $|P(z)|$ tiene en un cierto z_0 el mínimo global. Si $P(z_0) = 0$, ya está demostrado el resultado. En caso contrario, es decir, si $P(z_0) \neq 0$, definamos el polinomio

$$Q(z) := \frac{P(z)}{P(z_0)} = 1 + a_{j_1}(z - z_0)^{j_1} + a_{j_2}(z - z_0)^{j_2} + \cdots + a_{j_k}(z - z_0)^{j_k}$$

con $a_{j_1}, a_{j_2}, \ldots, a_{j_k}$ complejos no nulos y $1 \leq j_1 < j_2 < \cdots < j_k$ enteros (basta considerar el desarrollo de Taylor de $P(z)$ en $z = z_0$ y dividir por $P(z_0)$). Entonces, $|Q(z)|$ tiene el mínimo global en z_0, y su valor es 1. Denotemos $z = z_0 + h$, con $h \in \mathbb{C}$, $h \neq 0$. Observemos que $a_{j_1}(z - z_0)^{j_1}$ es, después del término independiente, el término dominante de $Q(z)$ cuando $h \to 0$, y tomemos $h \in \mathbb{C}$ de modo que $a_{j_1}(z - z_0)^{j_1}$ sea real y negativo. Entonces, para h suficientemente pequeño,

$$|Q(z)| \leq (1 + a_{j_1}h^{j_1}) + |h|^{j_1+1}|a_{j_2}h^{j_2-j_1-1} + \cdots + a_{j_k}h^{j_k-j_1-1}| < 1.$$

Comoquiera que $Q(z_0) = 1$, esta desigualdad contradice que $|Q(z)|$ tiene el mínimo global en z_0. En consecuencia, hemos probado el resultado.

Para concluir, merece la pena mencionar que, una vez que se ha probado que $P(z)$ tiene una raíz en un cierto z_0, podemos tomar el polinomio $P(z)/(z-z_0)$ y construir, fácilmente, una demostración por inducción (sobre el grado del polinomio) para probar que cualquier polinomio no constante tiene tantas raíces en $\mathbb{C}$ (contando su multiplicidad) como su grado.

38. Ceros de funciones analíticas

Sea f una función analítica real definida en un intervalo abierto $\mathcal{I}$. Entonces, o f es idénticamente 0, o sus ceros son aislados.

Recordemos que una función $f : \mathcal{I} \to \mathbb{R}$ que es derivable infinitas veces en todo punto se llama *analítica* si, para cada punto $x_0 \in \mathcal{I}$, existe un intervalo abierto $\mathcal{U}_{x_0}$ tal que, en él, la función coincide con su serie de Taylor, es decir,

$$f(x) = \sum_{k=0}^{\infty} \frac{f^{(k)}(x_0)}{k!}(x - x_0)^k, \quad x \in \mathcal{U}_{x_0}.$$

El resultado quedará demostrado si probamos que, suponiendo que f tiene un cero no aislado $x_0 \in \mathcal{I}$, entonces $f = 0$ en todo $\mathcal{I}$. Procedemos a demostrar esta última afirmación.

Si x_0 es un cero no aislado, podemos construir una sucesión de números reales $\{y_n\}_n$ que tienden monótonamente a x_0 y tales que $f(y_n) = 0$. Por el teorema de Rolle, intercalados entre ellos hay una nueva sucesión monótona

de ceros de f', que también tienden a x_0. Como f' es continua obtenemos que $f'(x_0) = 0$. Podemos repetir el mismo razonamiento empezando por f' y llegamos a que $f''(x_0) = 0$, y así sucesivamente, obteniendo que $f^{(k)}(x_0) = 0$ para todo k. Como f coincide con su serie de Taylor en $\mathcal{U}_{x_0}$, tenemos que $f(x) \equiv 0$ en $\mathcal{U}_{x_0}$.

Sea $\mathcal{J} \supset \mathcal{U}_{x_0}$ el intervalo abierto más grande en el que $f = 0$. Si $\mathcal{J} = \mathcal{I}$, el resultado queda probado. Supongamos ahora que $\mathcal{J} \subsetneq \mathcal{I}$, y vamos a llegar a una contradicción. Sea $z \in \overline{\mathcal{J}} \cap \mathcal{I}$ uno de los bordes de $\mathcal{J}$ (por descontado, $\overline{\mathcal{J}}$ denota la adherencia de $\mathcal{J}$), el cual, por continuidad, debe ser también un cero de f. Argumentando como con x_0, llegamos a que existe un intervalo abierto, entorno de z, $\mathcal{U}_z$, en el que $f = 0$. Por lo tanto, $f = 0$ sobre el intervalo abierto $\mathcal{J} \cup \mathcal{U}_z \supsetneq \mathcal{J}$, hecho que contradice la maximalidad de $\mathcal{J}$.

El resultado que hemos demostrado también es cierto para funciones analíticas de variable compleja (aunque requiere una demostración distinta), y no lo es para funciones infinitamente derivables, como muestra el clásico ejemplo $f(x) = e^{-1/x^2} \operatorname{sen}(1/x)$, si $x \neq 0$, y $f(0) = 0$, que se anula en $x = 0$ y en $x = 1/(m\pi)$ para todo $m \in \mathbb{Z} \setminus \{0\}$.

Existencia de invariantes

Las demostraciones por invariante son una técnica para resolver problemas identificando una característica que no cambia (invariante) tras aplicar ciertas operaciones permitidas. Lo más habitual es utilizarlo para probar que, tras algún proceso, cierto estado final no es posible, pues no satisface el invariante (así pues, se puede pensar que es un tipo de demostración por reducción al absurdo).

Los invariantes más comunes están relacionados con la paridad o con la conservación de colores, y pueden tener forma de ciclo (por ejemplo, alternando par/impar en un proceso).

39. Paseos de un caballo de ajedrez

Si un caballo está en una esquina de un tablero de ajedrez, es imposible que se mueva pasando exactamente una vez por cada una de las casillas y acabe en la esquina opuesta.

La prueba se basa en observar que cada vez que un caballo hace un movimiento, la casilla a la que llega tiene color contrario al de la casilla en la que estaba. Por tanto, si un caballo hace una secuencia impar de movimientos, al final estará en una casilla de color contrario al inicial. Como el total de casillas del tablero es 64, el camino deseado es imposible ya que la pieza necesita hacer 63 movimientos y dos esquinas opuestas del tablero son del mismo color.

Lo que sí es posible es dar paseos del caballo con 63 movimientos y recorriendo todas las casillas del tablero. E, incluso, paseos con 64 movimientos que las recorran todas, volviendo a la casilla inicial, pero esto ya es otra cuestión.

40. Cubrimiento de una cuadrícula

Una cuadrícula de tamaño $n \times n$ a la que se le han quitado dos esquinas opuestas no se puede cubrir con piezas de tamaño 2×1.

Si n es impar el resultado es obvio, pues la cuadrícula menos las dos esquinas tiene $n^2 - 2$ casillas, que no es múltiplo de 2.

Si n es par, pintemos las casillas blancas y negras de manera alternativa, como en un tablero de ajedrez, con lo cual las dos esquinas opuestas tendrán el mismo color; supongamos que ambas son blancas. Así, el tablero sin esas dos casillas tendrá $n^2/2$ casillas negras y $n^2/2 - 2$ casillas blancas. Y eso es imposible de cubrir con piezas de tamaño 2×1, pues una de tales piezas siempre cubre una casilla blanca y otra negra.

41. Un invariante en un proceso iterativo

Tenemos un proceso iterativo en el que, partiendo de un par (a, b) con $a, b \in \mathbb{Z}^+$, se pasa al par $(a, b-a)$ si $a < b$ o al par $(a-b, b)$ si $a > b$, y el proceso se detiene si $a = b$. Entonces, si partimos de $a = n(n^2-4)$ y $b = m(m^2-4)$, con $n, m \geq 3$, nunca llegaremos a $(1, 1)$.

En lo que sigue, usaremos $\mid$ con el significado de «divide a», Obsérvese que

$$d \mid a \quad \text{y} \quad d \mid b \quad \Longleftrightarrow \quad d \mid a \quad \text{y} \quad d \mid (b-a).$$

Entonces, como los divisores (a, b) y de $(a, b-a)$ son los mismos, $\mathrm{mcd}(a, b-a) = \mathrm{mcd}(a, b)$. Y, del mismo modo, $\mathrm{mcd}(a-b, b) = \mathrm{mcd}(a, b)$. Así pues, el máximo común divisor de a y b es un invariante del proceso.

En el caso $a = n(n^2-4)$ y $b = m(m^2-4)$, tenemos dos números de la forma $(k-2)k(k+2)$, donde al menos uno de esos tres factores es divisible por 3, así que $3 \mid \mathrm{mcd}(a, b)$. Pero $\mathrm{mcd}(1, 1) = 1$, así que no se puede llegar a $(1, 1)$ conservando el mcd en cada paso.

42. Algoritmo de Euclides

Sea $M = \{(m,n) \in \mathbb{N}^2 : m \geq n \geq 0, m \neq 0\}$ *y definamos la función* $F : M \to M$ *mediante*

$$F(m,0) = (m,0) \qquad y \qquad F(m,n) = (n, m - n\lfloor m/n \rfloor) \quad si\ n > 0$$

(nótese que $\lfloor m/n \rfloor$ *es el cociente de la división de* m *entre* n*, y* $m - n\lfloor m/n \rfloor$ *es el resto). Asimismo, denotemos* $F^0 = \mathrm{Id}$ *y* $F^j = F \circ F^{j-1}$*, para* $j \geq 1$*. Entonces, para cada* $(m,n) \in M$ *hay un* $k = k(m,n)$ *tal que* $F^k(m,n) = (\mathrm{mcd}(m,n), 0)$*.*

Introduzcamos dos funciones $V, W : M \to \mathbb{N}$ definidas como

$$V(m,n) = m + n, \qquad W(m,n) = \mathrm{mcd}(m,n).$$

Estas funciones cumplen lo siguiente:

(a) $V(F(m,n)) \leq V(m,n)$, y la desigualdad es estricta si $n \neq 0$;

(b) W es un invariante para F, es decir, $W(F(m,n)) = W(m,n)$.

La propiedad (a) es evidente, pues $F(m,n) = (m,n)$ si $n = 0$, y si $n \neq 0$, $V(F(m,n)) = m + n - n\lfloor m/n \rfloor < m + n = V(m,n)$.

Para demostrar (b), basta observar que, si d divide a m y a n, divide a ambas componentes de $F(m,n)$, y viceversa, con lo cual el máximo común divisor es el mismo.

Así pues, supongamos que partimos de $(m,n) \in M$. Si $n = 0$, no hay nada que probar, pues $\mathrm{mcd}(m,0) = m$ y podemos tomar $k(m,0) = 0$ (o 1, da lo mismo). En otro caso, por la propiedad (a), el valor V va decreciendo cada vez que aplicamos F, y esto sucede hasta que llegamos a un punto de la forma $(d,0)$ (a partir de entonces F se comporta como la función identidad). Pero, como, por la propiedad (b), W permanece invariante, $d = \mathrm{mcd}(m,n)$, y esto prueba el resultado.

Este procedimiento es una reformulación del algoritmo de Euclides para calcular el máximo común denominador en términos de invariantes e iteración de funciones. En el lenguaje de los sistemas dinámicos, V sería una especie de función de Lyapunov, ya que va decreciendo sobre los puntos de la iteración, y W sería una integral primera o invariante, ya que mantiene siempre su valor inicial.

43. Un cubo con vértices y caras numeradas

A cada uno de los ocho vértices de un cubo le asignamos un 1 *o un* -1*. Después, a cada una de sus seis caras le asignamos el producto de los números de sus vértices. Con estas reglas, es imposible hacerlo de manera que la suma de los catorce números sea* 0*.*

Supongamos que hemos asignado a los vértices valores iguales a 1 o -1. Si cambiamos el signo de un solo vértice, cambia el signo de ese mismo vértice y, al mismo tiempo, el signo de las tres caras que lo tienen en común. Por tanto, se producen 4 cambios de signo, lo que no altera el producto de todos los números (vértices y caras), que es un invariante ante cambios de signo de un vértice. Cuando todos los vértices son 1, también las caras valen 1, y el producto es 1; así pues, el invariante es 1. Además, es obvio que desde la posición inicial con todos los vértices iguales a 1, se puede pasar a cualquier otra en sucesivos pasos de un cambio de signo en un vértice.

Ahora bien, si la suma de los 14 números es igual a 0, eso es debido a que hay 7 de ellos iguales a 1 y otros 7 iguales a -1. En este caso, el producto de todos ellos sería -1, cosa que no puede ser, ya que hemos visto que el invariante es igual a 1.

44. Un alfabeto con tres letras

Supongamos que tenemos un alfabeto con tres letras a, b y c, y llamamos palabra a una concatenación finita de letras. Además, podemos transformar unas palabras en otras llevando a cabo, tantas veces como queramos, las siguientes transformaciones básicas (en cualquiera de los dos sentidos indicados por la flecha):

$$bc \leftrightarrow cb, \quad ab \leftrightarrow bba, \quad ac \leftrightarrow cca.$$

Con estas reglas, la palabra $abca$ no se puede transformar en $cabc$.

Este problema puede interpretarse en el marco de los lenguajes formales como un sistema de reescritura de palabras sobre el alfabeto $\{a, b, c\}$. Las reglas dadas permiten transformar localmente una palabra en otra, generando así una relación de equivalencia entre palabras. En este caso, se trata de ver que las palabras $abca$ y $cabc$ no son equivalentes. En general, con alfabetos y reglas de transformación arbitrarias, decidir si dos palabras son equivalentes es un problema computacional muy complicado.

Dada cualquier palabra P, vamos a asignarle un valor aritmético $V(P)$, y lo vamos a hacer de forma recursiva. Para ello, definimos $V(\emptyset) = 0$ (valor de la palabra de cero caracteres) y, recorriendo las palabras de izquierda a derecha,

$$V(aQ) = 2V(Q), \quad V(bQ) = 1 + V(Q), \quad V(cQ) = 1 + V(Q).$$

En particular, $V(a) = V(a\emptyset) = 2V(\emptyset) = 0$, $V(b) = V(b\emptyset) = 1 + V(\emptyset) = 1$, $V(c) = V(c\emptyset) = 1 + V(\emptyset) = 1$. Así, por ejemplo,

$$V(baccaba) = 1 + 2(1 + 1 + 2(1 + 0)) = 9.$$

Además, como $V(xQ)$ (con $x = a$, b o c) no depende de la palabra Q sino solo de su valor $V(Q)$, lo mismo ocurre con $V(yxQ)$, y así sucesivamente;

en general, si tenemos una parte fija F, $V(FQ)$ solo depende de $V(Q)$, no de Q. Por ejemplo, con la estructura de paréntesis del ejemplo anterior, y con $F = baccaba$, tendríamos

$$V(baccabaQ) = 1 + 2(1 + 1 + 2(1 + V(Q))).$$

En consecuencia, si efectuamos una transformación en el interior de una palabra, lo que hay a la izquierda de la transformación no tiene ninguna relevancia para ver si el valor de la palabra transformada cambia o permanece igual.

Con esta interpretación, las tres transformaciones permitidas no alteran el valor de una palabra, ya que

$$\begin{gathered} V(bcQ) = V(cbQ) = 1 + 1 + V(Q) = 2 + V(Q); \\ V(abQ) = 2(1 + V(Q)) = 2 + 2V(Q) = 1 + 1 + 2V(Q) = V(bbaQ); \\ V(acQ) = 2(1 + V(Q)) = 2 + 2V(Q) = 1 + 1 + 2V(Q) = V(ccaQ). \end{gathered}$$

Así pues, el valor aritmético de una palabra es un invariante que se conserva al aplicar transformaciones autorizadas.

Pero $V(abca) = 2(1 + 1 + 0) = 4$ y $V(cabc) = 1 + 2(1 + 1) = 5$, así que es imposible que la palabra *abca* se pueda transformar en *cabc*.

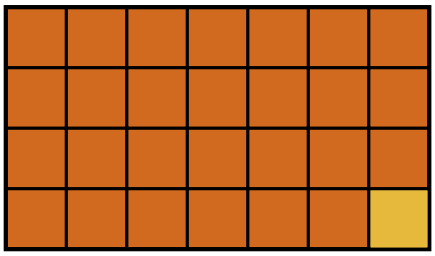
45. El juego de la tableta de chocolate

Hay numerosos juegos de estrategia entre dos jugadores en los que, si uno de ellos juega de manera inteligente, siempre va a ganar, independientemente de lo que haga su adversario. Eso ocurre, por ejemplo, cuando uno de los dos jugadores, con determinada estrategia, siempre puede conseguir, tras su jugada, e independientemente de la jugada previa del oponente, cierto tipo de posición que, a la postre, le va a permitir ganar el juego. Ese tipo de posición que garantiza la victoria hace el papel de invariante en el juego.

Una vez descubierta la estrategia ganadora, el juego entre dos jugadores inteligentes ya no tiene interés, y el interés es puramente matemático: descubrir la estrategia.

Uno de los juegos más conocidos de este tipo es el Nim (con sus múltiples variantes), pero aquí vamos a mostrar uno más sencillo, para poderlo explicar en pocas líneas. Es el denominado juego de la tableta de chocolate.

Supongamos que tenemos una tableta de chocolate rectangular pero con la particularidad de que la onza de una de las esquinas es de distinto color y está envenenada, como se muestra en el dibujo:



Dos jugadores, por turnos, partirán el chocolate por una línea horizontal o vertical (el corte es de toda la línea, de un lado a otro, como, de hecho, se hace en la realidad), con la intención de comerse uno de los trozos de chocolate que parten (el que no incluya la onza envenenada, claro). El jugador que se come la onza envenenada pierde. En estas circunstancias, lo que se tiene es lo siguiente:

En una tableta de chocolate rectangular con $n \times m$ onzas, el jugador que inicia el juego de la tableta de chocolate tiene una estrategia ganadora si $n \neq m$; y, si $n = m$, quien tiene una estrategia ganadora es el segundo jugador.

Vamos a usar A y B para designar a los dos jugadores. Supongamos que A, en su turno, se encuentra con que el trozo de tableta que recibe no es cuadrado. Entonces, puede cortar un trozo de tableta para transformarla en un cuadrado, y eso es lo que recibirá B. Haga lo que haga B, al cortar una o varias líneas a la vez, el trozo de tableta que dejará ya no será cuadrado, y eso es lo que recibirá A, que podrá volver a trasformarla en un cuadrado, y así sucesivamente.

Al cabo de cierto número de jugadas, y como los cuadrados son cada vez menores, el jugador B recibirá un trozo de tableta de tamaño 1×1, ¡la onza envenenada!, y habrá perdido la partida.

Así pues, transformar el trozo de tableta en una cuadrada es un invariante que permite que el jugador A gane la partida. ¿Y qué jugador es A, el que empieza la partida o el otro? Es obvio que, si la tableta original de tamaño $n \times m$ no es cuadrada, el que comienza la partida hace el papel de A, y ganará la partida si sigue la estrategia correcta. Y, si $n = m$, el que comienza la partida juega el papel de B, y será el que pierda (si el otro jugador aplica la estrategia).

Pruebas geométricas

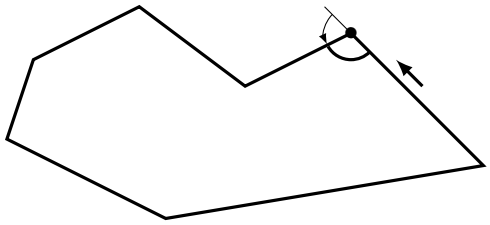
Esta sección se podría haber llenado con los innumerables problemas tratados por los matemáticos de la Grecia clásica. En cambio, nos hemos limitado a mostrar unos pocos ejemplos variados de la belleza de las demostraciones en las que las propiedades geométricas juegan un papel relevante.

46. Suma de los ángulos internos de un polígono

La suma de los ángulos internos de un polígono simple de n lados es $180° \cdot (n-2)$.

Por supuesto, existen numerosas demostraciones de este resultado, realizadas con técnicas diversas (por ejemplo, partiendo del resultado para el triángulo y haciendo inducción sobre el número de lados, o descomponiendo el polígono en triángulos). Vamos a dar una que es muy visual.

Supongamos que tenemos una hormiga que recorre los lados del polígono (que tiene que ser simple, es decir, que no se interseca a sí mismo), hasta volver al principio, como se ve a continuación; la hormiga está situada sobre la flecha, y recorre el polígono en esa dirección:



La hormiga recorre cada lado y, al llegar a cada vértice, gira para alinearse con el siguiente lado. Como se ve en el dibujo, el ángulo que gira la hormiga en cada vértice y el ángulo interior del polígono en ese vértice suman 180°. Para que la demostración también se pueda aplicar a polígonos no convexos, hay que tener en cuenta que, en un vértice en el que el ángulo interior es mayor que 180°, el ángulo de giro de la hormiga es negativo, de manera que su suma con el ángulo interior del polígono siga siendo 180°.

Al completar el recorrido y volver a la posición de partida, la hormiga ha dado una vuelta completa sobre sí misma, es decir, ha hecho un giro total de 360°.

Llamamos ahora I a la suma de los ángulos internos, y G a la suma de los giros que ha tenido que hacer. Por una parte, $G = 360°$, ya que ese es el giro total de la hormiga. Pero, por otra parte, como cada ángulo interno más cada giro suman 180°, y hay n vértices, es claro que $I + G = 180° \cdot n$. Así que $I = 180° \cdot n - 360° = 180° \cdot (n-2)$, tal y como queríamos probar.

47. Fórmula de Herón

El área de un triángulo de lados a, b y c es

$$A_T = \sqrt{s(s-a)(s-b)(s-c)}\,,$$

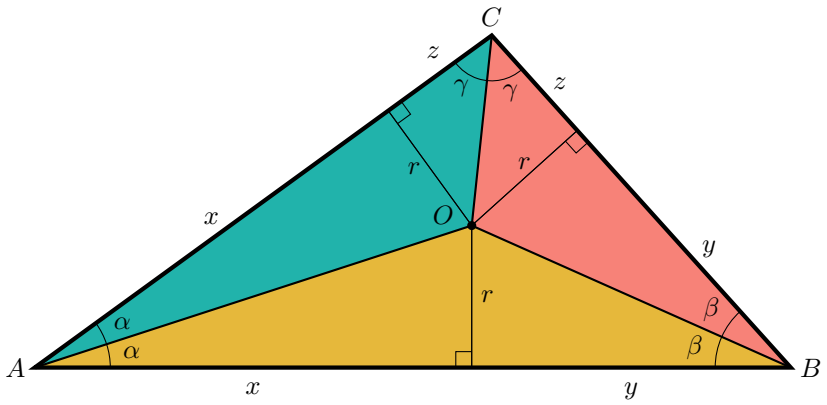
donde $s = (a+b+c)/2$ es el semiperímetro del triángulo.

De las distintas formas que hay para probar la fórmula de Herón, nosotros vamos a ver la que aparece en [22]. Utiliza que si α, β y γ son tres ángulos positivos tales que $\alpha+\beta+\gamma=\pi/2$, entonces

$$\tan(\alpha)\tan(\beta)+\tan(\beta)\tan(\gamma)+\tan(\gamma)\tan(\alpha)=1$$

(en este escrito, véase la prueba 88, donde se demuestra esa bonita identidad trigonométrica).

Llamemos A, B y C a los vértices del triángulo, 2α, 2β y 2γ a los correspondientes ángulos (para que $\alpha+\beta+\gamma=\pi/2$), y a, b y c a las longitudes de sus lados opuestos. Entonces, la situación descrita en el enunciado es como sigue:



Según se ve en el dibujo, el punto O es la intersección de las bisectrices de los ángulos del triángulo, los lados del triángulo son $a=y+z$, $b=x+z$ y $c=x+y$, y el semiperímetro es

$$s=x+y+z=x+a=y+b=z+c.$$

Además, el triángulo ABC se descompone en tres triángulos de altura r, con lo cual

$$\begin{aligned}A_T&=\text{Área}(ABC)=\text{Área}(OAB)+\text{Área}(OBC)+\text{Área}(OCA)\\&=\frac{x+y}{2}\,r+\frac{y+z}{2}\,r+\frac{x+z}{2}\,r=(x+y+z)r=sr.\end{aligned}$$

Con todo esto, aplicando la identidad de la suma de productos de tangentes a los ángulos α, β y γ de la figura, obtenemos

$$\begin{aligned}1&=\tan(\alpha)\tan(\beta)+\tan(\beta)\tan(\gamma)+\tan(\gamma)\tan(\alpha)\\&=\frac{r}{x}\cdot\frac{r}{y}+\frac{r}{y}\cdot\frac{r}{z}+\frac{r}{z}\cdot\frac{r}{x}=\frac{(x+y+z)r^2}{xyz}\\&=\frac{sr^2}{(s-a)(s-b)(s-c)}=\frac{A_T^2}{s(s-a)(s-b)(s-c)},\end{aligned}$$

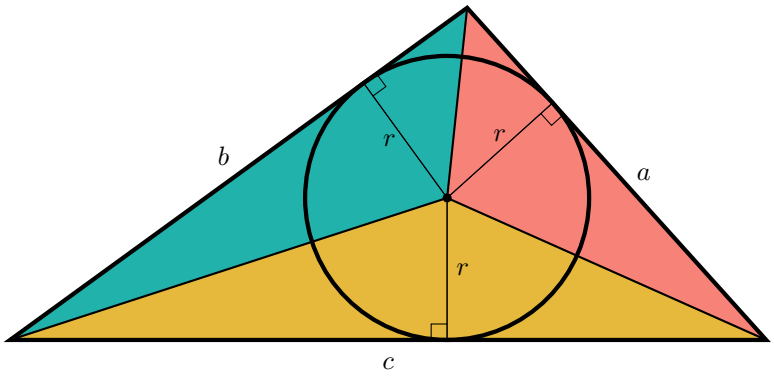
y despejando A_T se sigue el enunciado.

48. Círculo inscrito en un triángulo

Si $s = (a+b+c)/2$ es el semiperímetro de un triángulo de lados a, b y c, entonces el área de su círculo inscrito es

$$A_C = \frac{(s-a)(s-b)(s-c)}{s}\,\pi.$$

Como en la prueba anterior, un triángulo cualquiera de lados a, b y c puede ser dividido en tres triángulos tomando como bases sus lados y como altura el radio r del círculo inscrito, ya que el radio es perpendicular a la tangente. De hecho, este es el mismo gráfico que teníamos entonces, pero destacando distintos elementos:



Por lo tanto, si $s = (a+b+c)/2$ es el semiperímetro y r el radio del círculo inscrito, el área del triángulo es

$$A_T = \frac{ar}{2} + \frac{br}{2} + \frac{cr}{2} = \frac{a+b+c}{2}\,r = sr.$$

Comparando $A_T = sr$ con la fórmula de Herón $A_T = \sqrt{s(s-a)(s-b)(s-c)}$ (véase la prueba 47), es claro que

$$r = \sqrt{\frac{(s-a)(s-b)(s-c)}{s}}\,.$$

Para concluir, basta usar que el área del círculo es $A_C = \pi r^2$.

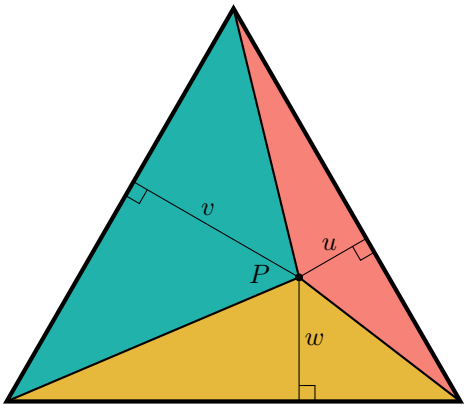
Resulta curioso observar que si el triángulo es un triángulo rectángulo de lados 3, 4 y 5, su semiperímetro es $s = 6$, y el radio del círculo inscrito es $\sqrt{(s-a)(s-b)(s-c)/s} = \sqrt{3\cdot 2\cdot 1/6} = 1$, con lo cual el círculo tiene área π.

Igual que ha ocurrido en esta prueba y en la anterior, la estrategia de descomponer un triángulo en tres triángulos cuyas bases son los lados del primer triángulo también sirve para establecer el siguiente resultado, que fue probado por Vincenzo Viviani en 1659:

49. Teorema de Viviani

Si P está en un triángulo equilátero, la suma de las distancias de P a los tres lados del triángulo no depende de P.

Observemos el dibujo:



Si ℓ es el lado del triángulo y h su altura, su área es $\ell h/2$. Así, $\ell h/2 = \ell u/2 + \ell v/2 + \ell w/2$. Por tanto, $u + v + w = h$.

50. Medias de dos números

Las medias armónica (**H**), *geométrica* (**G**), *aritmética* (**A**) *y cuadrática* (**Q**) *de dos números positivos a y b satisfacen*

$$\min\{a,b\} \le \mathbf{H} \le \mathbf{G} \le \mathbf{A} \le \mathbf{Q} \le \max\{a,b\},$$

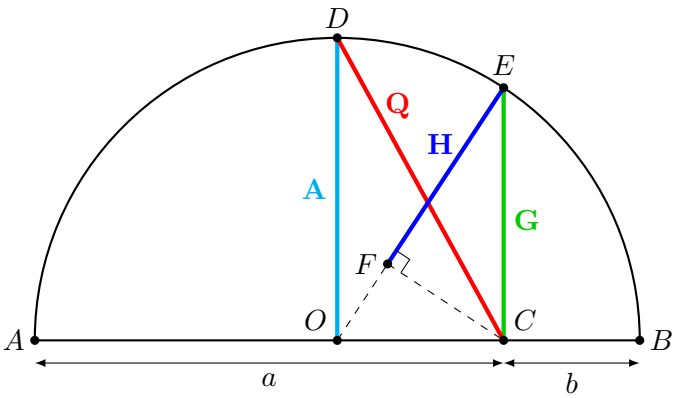
y las cuatro coinciden si y solo si $a = b$.

Las cuatro medias de los dos números a y b son, por definición,

$$\mathbf{H} = \frac{2}{\frac{1}{a}+\frac{1}{b}}, \quad \mathbf{G} = \sqrt{ab}, \quad \mathbf{A} = \frac{a+b}{2}, \quad \mathbf{Q} = \sqrt{\frac{a^2+b^2}{2}}$$

(por supuesto, la notación alude a la inicial de la palabra en inglés). Podemos suponer que $a \ge b$.

Construyamos lo que se ve en la figura. Tenemos que comprobar que las cuatro medias **H**, **G**, **A** y **Q** son las líneas marcadas con su correspondiente color (si $a = b$ entonces $C = O$ y todo es trivial, así que asumimos $a > b$ a partir de ahora):



Que $OD = \frac{a+b}{2} =: \mathbf{A}$ es obvio. Que $EC = \sqrt{ab} =: \mathbf{G}$ es el teorema de la altura aplicado al triángulo rectángulo AEB. Como $OC = (a+b)/2 - b = (a-b)/2$, el teorema de Pitágoras aplicado al triángulo rectángulo COD muestra que $CD = \sqrt{OC^2 + OD^2} = \sqrt{(a^2+b^2)/2} =: \mathbf{Q}$. Además, el teorema del cateto aplicado al triángulo rectángulo ECO nos dice que $EC^2 = OE \cdot EF$, con lo cual

$$EF = \frac{EC^2}{OE} = \frac{ab}{(a+b)/2} = \frac{2}{1/a + 1/b} =: \mathbf{H}.$$

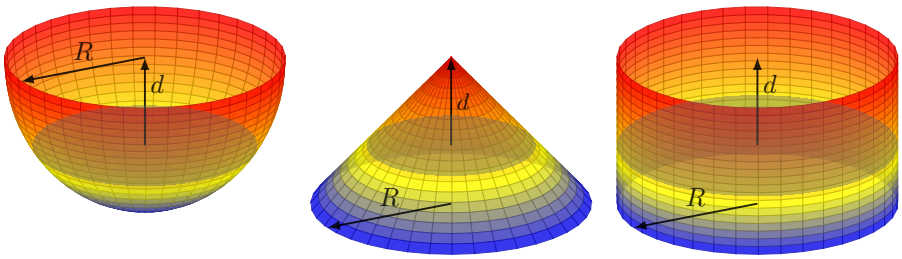
Finalmente, $b \leq \mathbf{H}$ y $\mathbf{Q} \leq a$ es inmediato a partir lo que se ve en la figura, y esto concluye la demostración.

51. Volumen de la esfera

El volumen de una esfera de radio R es $\frac{4\pi}{3}R^3$.

Incluimos la prueba de Arquímedes, que usa lo que hoy en día llamamos principio de Cavalieri, que a su vez es un caso particular del teorema de Fubini.

Consideremos una semiesfera, un cono y un cilindro, todos de altura R (y, en el caso del cono y el cilindro, con el radio de la circunferencia base también R), como en la figura:



Si los cortamos con el plano horizontal que está a distancia d de sus puntos más altos, obtenemos tres círculos. Sus radios respectivos son $\sqrt{R^2-d^2}$ (por el teorema de Pitágoras), d y R. Por lo tanto, las áreas de las tres secciones son $S=\pi(R^2-d^2)$, $T=\pi d^2$ y $U=\pi R^2$, y cumplen $S+T=U$. Como consecuencia,

$$\frac{\text{Volumen de la esfera}}{2}+\text{Volumen del cono}=\text{Volumen del cilindro}.$$

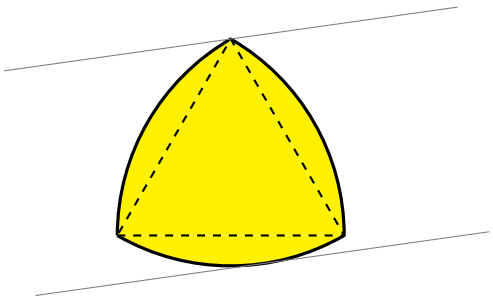
Así, el volumen V de la esfera satisface $V/2+\pi R^3/3=\pi R^3$. Despejando V obtenemos el resultado deseado.

52. El triángulo de Reuleaux

Existen conjuntos de anchura constante que no son el círculo.

En el plano, un conjunto de anchura constante es una figura convexa cuya anchura, medida por la distancia entre dos rectas paralelas tales que la figura esté completamente entre esas dos rectas y que cada una de ellas toque a la figura en un solo punto, es la misma independientemente de la dirección de esas dos paralelas. (Si la frontera de la figura es derivable en el punto de contacto, la recta será una tangente.)

Es obvio que el círculo tiene anchura constante (su diámetro). Para demostrar que hay otros conjuntos de anchura constante, basta construir uno. Aunque ya Euler en 1778 dio un ejemplo, la figura más conocida que tiene esa propiedad es el denominado triángulo de Reuleaux, que mostramos a continuación. Se obtiene partiendo de un triángulo equilátero de lado l y trazando, con centro en cada vértice, arcos de circunferencia de radio l entre los dos vértices opuestos, como se ve en la figura (la distancia entre las rectas paralelas siempre es l):



Debe su nombre a Franz Reuleaux, ingeniero mecánico alemán del siglo XIX, que los utilizó en sus diseños. Sin embargo, estas formas eran conocidas antes de su época; por ejemplo, por los diseñadores de ventanas góticas de las iglesias. Como se puede ver en [28, capítulo 25], hay muchos otros conjuntos de anchura constante.

Inducción

El principio de inducción es consecuencia de los axiomas de Peano para definir los números naturales (Giuseppe Peano, 1889). Establece que, si una propiedad es verdadera para cierto número entero n_0, y si, supuesto que la propiedad es verdadera para n, también lo sería para $n+1$, entonces la propiedad es verdadera para todos los números enteros mayores o iguales que n_0.

53. Suma de cuadrados

$$1^2+2^2+3^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6}.$$

Para $n=1$, el resultado es obvio. Supongámoslo cierto para $n=m$ y probémoslo para $n=m+1$. Por hipótesis de inducción,

$$1^2+2^2+3^2+\cdots+m^2+(m+1)^2=\frac{m(m+1)(2m+1)}{6}+(m+1)^2;$$

extrayendo $(m+1)$ factor común, eso queda como sigue:

$$(m+1)\frac{m(2m+1)+6(m+1)}{6}=\frac{(m+1)(m+2)(2m+3)}{6},$$

lo cual prueba el resultado.

Más adelante, en este mismo escrito, veremos una demostración sin palabras que permite evaluar $1^3+2^3+3^3+\cdots+n^3$ (prueba 89). De manera más general, el primero que encontró y demostró cómo sumar $1^p+2^p+3^p+\cdots+n^p$ para cualquier entero positivo p fue Jacob Bernoulli alrededor de 1700, usando los ahora denominados polinomios de Bernoulli (véase [36]).

54. Primos en la aplicación logística

Sea la sucesión $2,6,42,1806,\ldots$ *que se define iterando la aplicación logística:*

$$x_{n+1}=x_n(x_n+1),\quad x_1=2.$$

Entonces, cada número x_n *es divisible por, al menos,* n *números primos distintos.*

Vamos a demostrarlo por inducción sobre n. El resultado es cierto para $n=1$. Supongámoslo cierto para $n=m$ y probémoslo para $n=m+1$. Tenemos que x_m es divisible por m primos distintos. Además, para todo $1<k\in\mathbb{N}$, los números k y $k+1$ son coprimos, ya que si p divide a k y a $k+1$, también divide a su diferencia, que es 1. Así, x_m+1 contiene algún primo en su descomposición en factores primos que no aparece en la de x_m.

Por tanto, x_{m+1} es divisible, como mínimo, por $m+1$ números primos, como queríamos demostrar.

Como consecuencia de lo anterior, se sigue de manera obvia que existen infinitos primos. Esta prueba se debe a Saidak [32].

Una demostración muy similar se puede hacer con los números $x_n = 2^{2^n} - 1$. El paso de inducción es consecuencia de la igualdad $2^{2^{m+1}} - 1 = (2^{2^m} - 1)(2^{2^m} + 1)$, donde los factores son números impares consecutivos (y, por lo tanto, primos entre sí).

55. Una desigualdad entre senos

Para $x \in \mathbb{R}$ y $n \in \mathbb{N}$ se cumple que $|\operatorname{sen}(nx)| \leq n|\operatorname{sen}(x)|$.

Para $n = 0$ la desigualdad es cierta. Además, si es cierta para $n = m$ también lo es para $n = m + 1$:

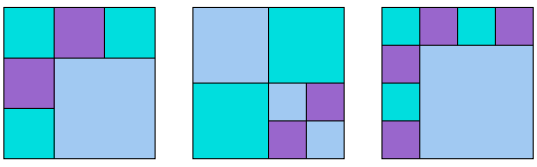
$$\begin{aligned} |\operatorname{sen}((m+1)x)| &= |\operatorname{sen}(mx)\cos(x) + \cos(mx)\operatorname{sen}(x)| \\ &\leq |\operatorname{sen}(mx)||\cos(x)| + |\cos(mx)||\operatorname{sen}(x)| \\ &\leq |\operatorname{sen}(mx)| + |\operatorname{sen}(x)| \\ &\leq m|\operatorname{sen}(x)| + |\operatorname{sen}(x)| = (m+1)|\operatorname{sen}(x)|. \end{aligned}$$

Es interesante observar que la desigualdad no es siempre cierta cuando $n \notin \mathbb{N}$. Por ejemplo, falla para $n = (2k+1)/2$ (con $k \in \mathbb{N}$) y $x = \pi$.

56. Subdivisión de un cuadrado en cuadrados

Para cualquier $n \geq 6$, un cuadrado se puede dividir en n cuadrados más pequeños, no necesariamente iguales.

Lo demostraremos por inducción. El resultado es cierto para $n = 6$, 7 y 8, véase la siguiente figura:



Ahora bien, como cada cuadrado se puede dividir de forma evidente en 4 cuadrados iguales, está claro que a partir de una partición en m cuadrados podemos conseguir otra con $m+3$ cuadrados, sin más que dividir el cuadrado que queramos en cuatro. Por lo tanto, a partir de las tres particiones de la figura podemos conseguir fácilmente particiones para todo $n \geq 9$, observando

los procesos de subdivisión

$$\begin{aligned} 6 &\to 9 \to 12 \to \cdots \to 3k, \\ 7 &\to 10 \to 13 \to \cdots \to 3k+1, \\ 8 &\to 11 \to 14 \to \cdots \to 3k+2, \end{aligned}$$

para todo $k \geq 2$.

El mismo resultado, con una demostración similar, puede probarse para triángulos equiláteros.

57. Pequeño teorema de Fermat

Sea p un primo y a un entero positivo. Entonces, $a^p - a$ es múltiplo de p. Y, si a no es divisible por p, $a^{p-1} - 1$ es múltiplo de p.

Comencemos observando que la primera parte implica la segunda, pues, dado que p primo divide a $a^p - a = (a^{p-1} - 1)a$, si p no divide a a debe dividir al otro factor.

Así pues, probemos que $a^p - a$ es múltiplo de p por inducción sobre a. Para $a = 1$ es trivial. Ahora, supuesto que a lo cumple, para $a+1$, desarrollando por el binomio de Newton, podemos escribir

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k = 1 + \sum_{k=1}^{p-1} \binom{p}{k} a^k + a^p;$$

entonces, teniendo en cuenta que

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!}, \qquad 1 \leq k \leq p-1,$$

es múltiplo de p (por ser primo, el p del numerador no se puede cancelar con ninguno de los factores del denominador), y que, por hipótesis de inducción, $a^p - a$ también es múltiplo de p, se sigue que

$$(a+1)^p - (a+1) = \sum_{k=1}^{p-1} \binom{p}{k} a^k + (a^p - a)$$

es múltiplo de p.

Este resultado, que tiene una gran relevancia en la teoría de congruencias, lo demostró Pierre de Fermat en 1636. Es un caso particular del denominado teorema de Euler-Fermat (véase, por ejemplo, [35, capítulo 3]).

58. Primos de Germain

No existen sucesiones infinitas de primos $p_0, p_1, \ldots$ con $p_{n+1} = 2p_n + 1$ para todo $n \geq 0$.

Es claro que, si tenemos números de esa forma, p_0 fija todos los demás. Así pues, sea $p_0 = p$, un primo. Probemos por inducción que $p_n = 2^n p + 2^n - 1$. Para $n = 0$ es obvio. Y, supuesto que se cumple para $n = m$, para $n = m + 1$ se tiene

$$p_{m+1} = 2p_m + 1 = 2(2^m p + 2^m - 1) + 1) = 2^{m+1}p + 2^{m+1} - 1,$$

tal como queríamos comprobar.

Para ver que no todos los p_n pueden ser primos, analicemos primero qué pasa si $p = 2$. En este caso, $p_1 = 5$, $p_2 = 11$, $p_3 = 23$, $p_4 = 47$ y $p_5 = 95 = 5 \cdot 19$, luego la sucesión que comienza en $p_0 = 2$ no da siempre primos.

En otro caso, vamos a usar que, si p primo no divide a a, entonces p divide a $a^{p-1} - 1$ (pequeño teorema de Fermat, prueba 57). Como $p_n = 2^n p + 2^n - 1$, para $n = p - 1$ tenemos $p_{p-1} = 2^{p-1}p + 2^{p-1} - 1$, y el resultado anterior con $a = 2$ asegura que p_{p-1} es divisible entre p, luego no es primo. En resumen, sea cual sea el primo p inicial, no todos los p_n pueden ser primos.

Un número primo p tal que $2p + 1$ también es primo se denomina primo de Germain (y, además, se dice que $2p + 1$ es un primo seguro). A principios del siglo XIX, Sophie Germain los utilizó en sus investigaciones sobre el último teorema de Fermat; actualmente, estos primos tienen gran importancia en criptografía. Por otra parte, aludiendo al matemático A. J. C. Cunningham (1842–1928), las cadenas de primos como la del enunciado se denominan cadenas de Cunningham (de primera clase); un ejemplo de cadena de Cunningham es 89, 179, 359, 719, 1439, 2879; el siguiente número, $2 \cdot 2879 + 1 = 5759$ ya no es primo. No se sabe si hay infinitos primos de Germain; lo que hemos probado en este apartado es que no puede haber una cadena de Cunningham infinita.

59. Fórmula de Binet

Los números G_n definidos como $G_0 = 0$, $G_1 = 1$ y $G_{n+1} = aG_n + bG_{n-1}$, con $\Delta = a^2 + 4b \neq 0$, son

$$G_n = \frac{u^n - v^n}{u - v} = \frac{u^n - v^n}{\sqrt{\Delta}}, \quad n \geq 0,$$

donde $u = \left(a + \sqrt{\Delta}\right)/2$ y $v = \left(a - \sqrt{\Delta}\right)/2$ son las dos raíces de de la ecuación $z^2 - az - b = 0$.

La fórmula debe su nombre a Jacques Philippe Marie Binet quien la dio, en 1843, cuando $a = b = 1$ y $G_n = F_n$ son los números de Fibonacci; pero De Moivre, Daniel Bernoulli y Euler ya la conocían en el siglo XVII.

Comenzamos probando por inducción que si $z \in \{u, v\}$, entonces $z^n = G_n z + bG_{n-1}$. La fórmula es claramente cierta para $n = 1$. Suponiéndola cierta para $n = m$, $z^m = G_m z + bG_{m-1}$, tenemos que

$$\begin{aligned} z^{m+1} &= G_m z^2 + bG_{m-1}z = G_m(az + b) + bG_{m-1}z \\ &= (aG_m + bG_{m-1})\, z + bG_m = G_{m+1}z + bG_m, \end{aligned}$$

tal y como queríamos ver. Por lo tanto, $u^n = G_n u + bG_{n-1}$ y $v^n = G_n v + bG_{n-1}$. Restando ambas ecuaciones obtenemos $u^n - v^n = G_n(u - v) = G_n\sqrt{\Delta}$, que es la fórmula deseada.

60. Raíces reales de polinomios

Un polinomio real con $n+1$ monomios tiene, como máximo, $2n+1$ raíces reales. Además, este resultado es óptimo.

Usaremos $p(x)$ para denotar el polinomio con $n + 1$ monomios. Demostremos en primer lugar que p tiene, como máximo, n raíces positivas, con una prueba que mezcla inducción y reducción al absurdo.

Si $n = 0$, el resultado es cierto ya que $p(x) = a_1 x^{k_1}$, con $a_1 \neq 0$, no tiene ninguna raíz positiva. Suponiéndolo cierto para $n = m$, vamos a demostrarlo cuando $n = m+1$. Sea un polinomio arbitrario con $n+1 = m+2$ monomios,

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

con $a_1 \cdot a_2 \cdots a_{m+1} \cdot a_{m+2} \neq 0$ y $k_1 > k_2 > \cdots > k_{m+1} > k_{m+2} \geq 0$.

Si ese polinomio tuviera $m + 2$ raíces positivas (o más), tomemos $q(x) = p(x)/x^{k_{m+2}}$, que tiene el mismo número de raíces positivas que $p(x)$. Entonces $q'(x)$ tendría $m + 1$ monomios y, por el teorema de Rolle, como mínimo $m + 1$ raíces reales positivas (una entre cada dos raíces consecutivas de p). Este hecho estaría en contradicción con la hipótesis de inducción. Así pues, hemos probado el resultado sobre la cantidad de raíces positivas.

El resultado para raíces negativas es consecuencia del resultado para raíces positivas simplemente considerando el polinomio $r(x) = p(-x)$. Con esto, para raíces reales en general basta usar que puede haber n positivas, n negativas y la raíz $x = 0$. Finalmente, para ver que la cantidad $2n + 1$ no se puede mejorar para ningún n podemos tomar $p(x) = x \prod_{j=1}^{n}(x^2 - j^2)$.

Usando, además, que si un polinomio tiene una raíz de multiplicidad $k \geq 2$, su derivada la mantiene con multiplicidad $k-1$, se puede precisar un poco más el resultado. Concretamente, un polinomio real con $n+1$ monomios tiene como máximo n raíces positivas (teniendo en cuenta su multiplicidad), como máximo n raíces negativas (también teniendo en cuenta su multiplicidad), y

eventualmente el cero (con cualquier multiplicidad). Omitimos los detalles de esta prueba.

Merece la pena comentar que lo que hemos demostrado es una versión débil de la famosa regla de Descartes. Esta regla asegura que la cantidad de raíces positivas de un polinomio (teniendo en cuenta su multiplicidad) es, como máximo, el número de cambios de signo de la lista ordenada de los coeficientes del polinomio, y tiene su misma paridad.

Congruencias

Una herramienta muy útil y sencilla, pero que generalmente no se explica en las matemáticas preuniversitarias (ni en la mayoría de los estudios de ingeniería), es el uso de congruencias. Aquí solo veremos unos pocos ejemplos, pero, en el mundo actual, resulta prácticamente omnipresente, pues se aplica en criptografía y en teoría de códigos, así que las comunicaciones electrónicas descansan, en una gran medida, en la teoría de congruencias.

En realidad, todo lo que se hace en términos de congruencias se puede redactar, también, usando divisibilidad; pero los resultados son mucho más cómodos de probar si se usa el lenguaje de las congruencias, cuya notación moderna fue introducida por Carl Friedrich Gauss en su libro *Disquisitiones Arithmeticae* en 1801 (Fermat y Euler, por ejemplo, probaron unos cuantos resultados que ahora son clave en la teoría de congruencias, pero los enunciaron en términos de divisibilidad). Como queremos que este escrito se pueda seguir sin tener conocimientos especializados, vamos a comenzar, al contrario que en otras secciones, dando una pequeña introducción de la teoría de congruencias (que también se conoce con el nombre de aritmética modular). Esta introducción puede ser ignorada por los lectores con formación matemática. Por otra parte, para profundizar en el estudio de las congruencias, se puede consultar [35, capítulos 3 y 4].

Sea m un entero positivo. Decimos que dos enteros a y b son *congruentes* módulo m si tienen el mismo resto al dividir por m, y se expresa

$$a \equiv b \pmod{m}$$

(cuidado: aunque el entero sea negativo, al dividir por m hay que quedarse con un resto positivo, y ese resto al hacer la división será un número entre 0 y $m-1$). Por ejemplo,

$$22 = 2\cdot 9 + 4, \quad 94 = 10\cdot 9 + 4, \quad 4 = 0\cdot 9 + 4, \quad -23 = -3\cdot 9 + 4,$$

así que $22 \equiv 94 \equiv 4 \equiv -23 \pmod{9}$.

También podemos decir que dos enteros a y b son congruentes módulo m si m divide a $a-b$. Esto es equivalente a la definición que hemos dado al principio pues, si tomamos

$$a = a_1 m + r, \quad b = b_1 m + s,$$

tendremos $a-b=(a_1-b_1)m+(r-s)$, luego resulta evidente que m divide a $a-b$ si y solo si los dos restos r y s coinciden.

Como ya hemos mencionado, usar congruencias es muy útil en muchos problemas aritméticos, sobre todo cuando aparecen cuestiones de divisibilidad. Según cómo sea el problema, a veces resulta más natural pensar en la primera definición que hemos dado (coincidencia de resto al dividir por m), y otras veces en la segunda (m divide a la resta).

Al efectuar congruencias módulo m, los únicos números importantes son $0,1,2,\ldots,m-1$, pues cualquier otro número entero es equivalente a uno de esos. Por ejemplo, módulo 5 tenemos

$$\begin{aligned}
\cdots &\equiv -15 \equiv -10 \equiv -5 \equiv 0 \equiv 5 \equiv 10 \equiv 15 \equiv 20 \equiv \cdots \pmod 5,\\
\cdots &\equiv -14 \equiv -9 \equiv -4 \equiv 1 \equiv 6 \equiv 11 \equiv 16 \equiv 21 \equiv \cdots \pmod 5,\\
\cdots &\equiv -13 \equiv -8 \equiv -3 \equiv 2 \equiv 7 \equiv 12 \equiv 17 \equiv 22 \equiv \cdots \pmod 5,\\
\cdots &\equiv -12 \equiv -7 \equiv -2 \equiv 3 \equiv 8 \equiv 13 \equiv 18 \equiv 23 \equiv \cdots \pmod 5,\\
\cdots &\equiv -11 \equiv -6 \equiv -1 \equiv 4 \equiv 9 \equiv 14 \equiv 19 \equiv 24 \equiv \cdots \pmod 5.
\end{aligned}$$

Todos los números de la misma línea son, esencialmente, el mismo, así que los consideramos agrupados y basta quedarse con un representante de todos ellos; normalmente, los representantes elegidos son $0,1,2,3,4$, pero daría igual si fuesen otros (a veces, estas agrupaciones se denotan $\widehat{0},\widehat{1},\widehat{2},\widehat{3},\widehat{4}$ o $[0],[1],[2],[3],[4]$, pero no hace falta que lo hagamos). Al quedarnos con el representante módulo m (y considerar a todos sus congruentes agrupados con él), los enteros $\mathbb{Z}$ se distribuyen en paquetes (que se denominan clases de equivalencia), y esto se denota así:

$$\mathbb{Z}_m=\{0,1,2,\ldots,m-1\}.$$

Las congruencias se comportan muy bien con sumas y productos, ya que

$$\begin{aligned}
&a\equiv b \pmod m, \qquad c\equiv d \pmod m\\
&\quad\Longrightarrow\quad a+c\equiv b+d \pmod m, \qquad a\cdot c\equiv b\cdot d \pmod m.
\end{aligned}$$

Vamos a comprobarlo para el producto (con la suma es similar): tenemos $a=a_1m+r$, $b=b_1m+r$, $c=c_1m+s$, $d=d_1m+s$, con lo cual

$$\begin{aligned}
a\cdot c&=(a_1m+r)(c_1m+s)=(a_1c_1m+rc_1+sa_1)m+rs\equiv rs \pmod m,\\
b\cdot d&=(b_1m+r)(d_1m+s)=(b_1d_1m+rd_1+sb_1)m+rs\equiv rs \pmod m;
\end{aligned}$$

luego, efectivamente, $a\cdot c\equiv b\cdot d \pmod m$. Este buen comportamiento es crucial, pues permite definir las operaciones suma y producto en $\mathbb{Z}_m$, ya que lo que sale al operar no depende del representante elegido. Así, usando el lenguaje de las estructuras algebraicas, se dice que $\mathbb{Z}_m$ es un anillo; y, de paso, se emplea también la notación $\mathbb{Z}/m\mathbb{Z}$, que se corresponde con la de un anillo cociente (aunque aquí no la usaremos).

Un resultado muy importante de la teoría de congruencias es el pequeño teorema de Fermat (prueba 57). Con este lenguaje, lo que tenemos es que, si p primo, entonces $a^p \equiv a \pmod{p}$; y que, además, $a^{p-1} \equiv 1 \pmod{p}$ si $a \not\equiv 0 \pmod{p}$ (allí lo hemos probado para $a \geq 1$, pero resulta inmediato extenderlo para cualquier $a \in \mathbb{Z}$).

Con congruencias se puede restar, pero no siempre se puede dividir (multiplicar por el inverso respecto al producto). Es más, también puede ocurrir que el producto de dos números no nulos sea nulo módulo m; por ejemplo, $2 \cdot 3 \equiv 0 \pmod{6}$. Si p es un primo, cualquier $a \in \mathbb{Z}_p \setminus \{0\}$ tiene inverso multiplicativo (además, esto impide que haya divisores de cero): por el pequeño teorema de Fermat, el producto de a y a^{p-2} en $\mathbb{Z}_p$ es 1 (en la práctica, hay procedimientos mucho más efectivos para encontrar el inverso de a en $\mathbb{Z}_p$, pero no nos vamos a preocupar por eso). Así pues, cuando p es un primo, $\mathbb{Z}_p$ tiene estructura de cuerpo (y estos cuerpos se suelen denotar $\mathbb{F}_p$).

61. Un criterio de divisibilidad

Sea $m \geq 1$ y q un divisor de $10^m - 1$. Dado $N = \sum_{j=0}^{k} d_j 10^{mj}$, tomemos $N' = \sum_{j=0}^{k} d_j$. En estas circunstancias, $q \mid N$ si y solo si $q \mid N'$.

Recordemos que la notación $a \mid b$ significa «a divide a b». Además, con notación de congruencias, tenemos

$$q \mid (10^m - 1) \quad \Longleftrightarrow \quad 10^m \equiv 1 \pmod{q}.$$

En consecuencia, $10^{mj} = (10^m)^j \equiv 1^j \equiv 1 \pmod{q}$ para todo j. Así pues,

$$\begin{aligned} N &= a_k 10^{km} + a_{k-1} 10^{(k-1)m} + \cdots + a_2 10^{2m} + a_1 10^m + a_0 \\ &\equiv a_k + a_{k-1} + \cdots + a_2 + a_1 + a_0 \equiv N' \pmod{q}, \end{aligned}$$

luego $q \mid N$ si y solo si $q \mid N'$.

Tomando $m = 1$ obtenemos las muy conocidas reglas de divisibilidad por 3 y 9:

- Un número es divisible por 3 si y solo si la suma de sus dígitos es divisible por 3.
- Un número es divisible por 9 si y solo si la suma de sus dígitos es divisible por 9.

Tomando $m = 3$, y como $1000 - 1 = 3^3 \cdot 37$, obtenemos un criterio de divisibilidad por 37. Apliquémoslo a un número concreto:

$$37 \mid 64\,975\,256 \iff 37 \mid (64 + 975 + 256) \iff 37 \mid 1295 \iff 37 \mid 296,$$

y, al final, la veracidad de $37 \mid 296$ hay que comprobarla efectuando la división.

62. Otro criterio de divisibilidad

Sea $m \geq 1$ y q un divisor de $10^m + 1$. Dado $N = \sum_{j=0}^{k} d_j 10^{mj}$, tomemos $N' = \sum_{j=0}^{k} (-1)^j d_j$. En estas circunstancias, $q \mid N$ si y sólo si $q \mid N'$.

Con notación de congruencias,

$$q \mid (10^m + 1) \quad \Longleftrightarrow \quad 10^m \equiv -1 \pmod{q}.$$

En consecuencia, $10^{mj} = (10^m)^j \equiv (-1)^j \pmod{q}$ para todo k. Así pues,

$$\begin{aligned} N &= a_k 10^{km} + a_{k-1} 10^{(k-1)m} + \cdots + a_2 10^{2m} + a_1 10^m + a_0 \\ &\equiv (-1)^k a_k + (-1)^{k-1} a_{k-1} + \cdots + (-1)^2 a_2 - a_1 + a_0 \equiv N' \pmod{q}, \end{aligned}$$

luego $q \mid N$ si y solo si $q \mid N'$.

Tomando $m = 1$ obtenemos el criterio de divisibilidad por 11: un número es divisible por 11 si y solo si la diferencia entre la suma de las cifras que ocupan los lugares pares y la suma de las cifras de lugares impares es múltiplo de 11. Así, por ejemplo:

$$11 \mid 135\,802\,458 \iff 11 \mid \big((8 + 4 + 0 + 5 + 1) - (5 + 2 + 8 + 3)\big),$$

y eso es cierto pues $(8 + 4 + 0 + 5 + 1) - (5 + 2 + 8 + 3) = 0$.

Tomando $m = 3$ tenemos $1001 = 7 \cdot 11 \cdot 13$. De este modo surge la regla de divisibilidad por 7, que se aplica de manera similar a la que acabamos de mostrar para 11 pero tomando grupos de tres cifras:

$$7 \mid 86\,419\,746 \iff 7 \mid \big((86 + 746) - 419\big) \iff 7 \mid 413.$$

El mismo criterio sirve para analizar la divisibilidad por 13 (por supuesto, también se puede aplicar a la divisibilidad por 11, pero obviamente es mucho más sencillo el que hemos obtenido con $m = 1$).

63. Suma de enteros elevados a un primo

Sean tres enteros x, y, z, y p un primo. Entonces,

$$(x + y + z)^p - (x^p + y^p + z^p)$$

es múltiplo de p.

Apliquemos el pequeño teorema de Fermat en su forma $a^p \equiv a \pmod{p}$. Entonces,

$$x^p \equiv x \pmod{p}, \qquad y^p \equiv y \pmod{p}, \qquad z^p \equiv z \pmod{p};$$

y, a su vez,

$$(x+y+z)^p \equiv x+y+z \pmod{p}.$$

De aquí que

$$x^p+y^p+z^p \equiv x+y+z \equiv (x+y+z)^p \pmod{p},$$

lo que equivale a decir que p divide a $(x+y+z)^p-(x^p+y^p+z^p)$.

Por descontado, el resultado es igualmente cierto si, en lugar de tres enteros, tenemos cualquier otra cantidad, y la demostración es la misma.

64. Una ecuación diofántica exponencial

Si n y m son enteros y $m>2$, entonces $3^m \pm 1 \neq 2^n$.

Supongamos que $3^m \pm 1 = 2^n$. Como $m \geq 3$, $3^m \pm 1 \geq 26$, luego forzosamente debería ser $n \geq 4$. En particular, se cumplirá $3^m \pm 1 \equiv 0 \pmod{8}$. Además, $3^2 \equiv 1 \pmod{8}$.

Con este trabajo previo, para 3^m+1 tenemos:

- si $m=2k+1$, $3^m+1 = 3(3^2)^k+1 \equiv 3\cdot 1+1 \equiv 4 \not\equiv 0 \pmod{8}$;
- si $m=2k$, $3^m+1 = (3^2)^k+1 \equiv 1\cdot 1+1 \equiv 2 \not\equiv 0 \pmod{8}$;

así pues, $3^m+1=2^n$ no tiene solución.

Analicemos ahora 3^m-1:

- si $m=2k+1$, $3^m-1 = 3(3^2)^k-1 \equiv 3\cdot 1-1 \equiv 2 \not\equiv 0 \pmod{8}$;
- si $m=2k$, $3^m-1 = 3^{2k}-1 = (3^k+1)(3^k-1)$, y eso no puede tener la forma 2^n pues 3^k+1 y 3^k-1 no pueden ser potencias de 2 a la vez (salvo con $k=1$ que da $m=2$, prohibido por las hipótesis).

65. Una ecuación modular

Si p es primo, entonces $x^2 \equiv 1 \pmod{p}$ si y solo si $x \equiv \pm 1 \pmod{p}$.

La implicación «si» es evidente, o sea que analicemos la parte «solo si». Supongamos que $x^2 \equiv 1 \pmod{p}$, es decir, p divide a $x^2-1=(x-1)(x+1)$. Como p es primo, deberá dividir a uno de los dos factores $x-1$ o $x+1$, y por tanto $x \equiv 1 \pmod{p}$ o $x \equiv -1 \pmod{p}$.

El resultado no es cierto en aritmética módulo m si m no es primo. Por ejemplo, $3^2 \equiv 1 \pmod{8}$ y $4^2 \equiv 1 \pmod{15}$.

66. Teorema de Wilson

Si p es primo, entonces $(p-1)! \equiv -1 \pmod{p}$.

Basándose en lo que observaba en un número grande de casos, John Wilson conjeturó que, si p era primo, $(p-1)!+1$ siempre iba a ser divisible por p. La demostración la dio Joseph-Louis Lagrange en 1773, pocos años después de que Wilson lo intuyera. A decir verdad, esta propiedad ya había sido observada, a principios del siglo XI, por el matemático persa Abu Ali al-Hasan ibn al-Haytham (a quien, por diversas circunstancias de su vida, además de como al-Haytham también se le conoce como al-Basri y al-Misri, así como por su nombre latinizado Alhazen o Alhacén).

El resultado es claramente cierto cuando $p = 2$ o $p = 3$, así que supongamos $p \geq 5$. Como p es primo, cualquier $a \in \{1, 2, \ldots, p-1\}$ tiene inverso $a^{-1} \in \{1, 2, \ldots, p-1\}$ tal que $aa^{-1} \equiv 1 \pmod{p}$. Por el resultado de la prueba 65, $a = a^{-1}$ si y solo si $a = 1$ o $a = p-1$. De este modo, podemos partir el conjunto $\{2, 3, \ldots, p-2\}$ en $(p-3)/2$ pares de enteros $\{a_j, a_j^{-1}\}$ tales que $a_j a_j^{-1} \equiv 1 \pmod{p}$ para $j = 1, 2, \ldots, (p-3)/2$. En consecuencia,

$$\begin{aligned}(p-1)! &= 1 \cdot 2 \cdot 3 \cdots (p-2)(p-1) \\ &= (p-1) \prod_{j=1}^{(p-3)/2} a_j a_j^{-1} \equiv p-1 \equiv -1 \pmod{p},\end{aligned}$$

tal como queríamos probar.

Es interesante comentar que el inverso del teorema de Wilson también es cierto: *Si un entero $n > 1$ verifica $(n-1)! \equiv -1 \pmod{n}$, entonces n es primo.* En efecto, si n no fuera primo, existiría un primo $q < n$ que divide a n, y también dividirá a $(n-1)!$, pues q es uno de los factores del factorial. Pero, por hipótesis, n divide a $(n-1)!+1$ (y, por tanto, también q), luego el primo q divide a 1, lo cual es imposible.

Así pues, se puede decir que el teorema de Wilson es un test de primalidad; pero no tiene utilidad práctica, pues calcular $(n-1)!$ requiere mucho más trabajo que buscar un divisor de n.

67. Polinomio generador de primos

No hay ningún polinomio $P(x)$ (no constante) con coeficientes enteros tal que $P(n)$ sea un número primo para todo $n \in \mathbb{N}$ (ni tampoco para todo n a partir de un cierto n_0).

La demostración de este resultado se remonta a 1752 y es debida a Christian Goldbach (la que ahora presentamos no es la original).

Supongamos que sí existe un polinomio tal que $P(n)$ es primo para cada $n \geq n_0$. Tomemos $a \geq n_0$ cualquiera y $p = P(a)$, que por hipótesis deberá ser primo.

Como las congruencias se conservan con sumas y productos, también se conservan con polinomios. Entonces, para cualquier $b \equiv a \pmod{p}$ se cumplirá que $P(b) \equiv P(a) \pmod{p}$. Por hipótesis, $P(b)$ también es primo, así que forzosamente $P(b) = p$.

Pero en la clase de a en $\mathbb{Z}_p$ existen infinitos elementos (todos los de la forma $b = a + kp$, $k \in \mathbb{Z}$, y nos quedamos con los $k \geq 0$ para que $b \geq n_0$), luego el polinomio $Q(x) = P(x) - p$ tiene infinitas raíces, lo cual es imposible. Una demostración de esta imposibilidad se explica en el último párrafo de la prueba 37.

Como curiosidad, comentemos que el polinomio $P(n) = n^2 + n + 41$, dado por Euler en 1772, proporciona valores primos para $0 \leq n \leq 39$. Por ejemplo, $P(0) = 41$, $P(39) = 1601$, pero $P(40) = 40^2 + 40 + 41 = 40 \cdot 41 + 41 = 41^2$.

68. Prueba del nueve

Para concluir esta sección, explicaremos el funcionamiento de una de las pruebas más usadas en la escuela primaria por los alumnos de nuestra generación y generaciones anteriores, hasta que aparecieron las calculadoras: la famosa *prueba del nueve*. De hecho, está ya descrita en el *Liber Abaci* de Fibonacci, publicado en 1202.

Esa prueba sirve para intentar detectar si hay errores en una suma, resta, multiplicación o división (e incluso en raíces cuadradas, cúbicas, etc.). Sin embargo, no es útil ni para asegurar que una operación es correcta, ni para localizar dónde está el error o errores cometidos, en caso de que los haya (con el lenguaje de la teoría de códigos, la prueba del nueve es un código detector de errores, pero no un código corrector de errores). En cualquier caso, su utilidad es incuestionable y los autores reconocen haberla usado de jóvenes cientos, si no miles, de veces.

Vamos a explicarla en el caso de la multiplicación; utilizando el lenguaje de las congruencias, es sencillísimo entender por qué funciona. Supongamos que tenemos tres enteros positivos a, b y c tales que $ab = c$. Entonces, también deberá cumplirse que $ab \equiv c \pmod{9}$. Y lo que realmente resulta útil es su contrarrecíproco:

$$ab \not\equiv c \pmod{9} \quad \Longrightarrow \quad ab \neq c.$$

La suerte, además, es que chequear la parte izquierda de la expresión anterior es muy cómodo. Como hemos visto en la prueba 61, cualquier entero (escrito en base 10) es congruente módulo 9 con la suma de sus dígitos; es más, no hace falta sumar los dígitos que sean 9, pues no contribuyen en nada a esa congruencia. Así, si $S(n)$ es la suma de todas las cifras de n (escrito en base 10) descartando las que sean 9, $S(n) \equiv n \pmod{9}$. Si $S(n)$ tiene más de un dígito, podemos hacer lo mismo, con lo cual $S(S(n)) \equiv S(n) \equiv n \pmod{9}$. Y así sucesivamente.

Si denotamos $S^0 = \mathrm{Id}$ y $S^k = S \circ S^{k-1}$, es claro que, para j suficientemente grande, $S^j(n) \in \{0, 1, 2, \ldots, 8\}$ y, a partir de entonces, $S^k(n) = S^j(n)$ para todo $k \geq j$. Llamemos $\mathcal{S}(n)$ a este número.

Con esta notación, la prueba del nueve para el producto es la siguiente:

Sean tres enteros positivos a, b y c. Entonces,

$$\mathcal{S}(\mathcal{S}(a) \cdot \mathcal{S}(b)) \neq \mathcal{S}(c) \implies a \cdot b \neq c.$$

Para la suma y la resta se comporta igual:

$$\mathcal{S}(\mathcal{S}(a) \pm \mathcal{S}(b)) \neq \mathcal{S}(c) \implies a \pm b \neq c$$

(por supuesto, puede haber más de dos sumandos). Y para la división, si usamos D, d, c y r para denotar, respectivamente, dividendo, divisor, cociente y resto, se tiene

$$\mathcal{S}(\mathcal{S}(d)\mathcal{S}(c) + \mathcal{S}(r)) \neq \mathcal{S}(D) \implies dc + r \neq D.$$

Con la práctica, se puede calcular $S(n)$ no sólo prescindiendo de los dígitos que sean 9, sino también de cualquier pareja de dígitos de n que sumen 9 (o emplear cualquier otro truco que conserve la congruencia, como sumar los dígitos cada vez que, haciendo sumas parciales, llegamos a un número de dos dígitos); el valor de $S(n)$ no va a ser el mismo, pero sí que va a ser un número congruente con él módulo 9, que es lo que importa para que el método funcione. Por descontado, el valor final $\mathcal{S}(n)$ sí que será el mismo.

Volviendo al caso de la multiplicación, vamos a ilustrar esto con un ejemplo de multiplicación incorrecta. Supongamos que queremos multiplicar $a = 47\,930\,216$ por $b = 394$ y sea c lo que hemos obtenido al multiplicar. Disponemos los números tal como se usa en el algoritmo de la multiplicación y, a la derecha, en un aspa, colocamos los valores que salen al aplicar $\mathcal{S}$ (para economizar espacio, en el aspa vamos a usar $\overline{n} := \mathcal{S}(n)$); además, hemos marcado en rojo dónde se han producido los errores al operar:

$$\begin{array}{r} 47930217 \\ \times \quad 394 \\ \hline 191720868 \\ 431371953 \\ 142790651 \\ \hline 18784505498 \end{array} \qquad \begin{array}{c} \overline{a} \\ \overline{\overline{a}\,\overline{b}} \times \overline{c} \\ \overline{b} \end{array}$$

Ahí, tenemos

$$\overline{a} = \mathcal{S}(a) = S(S(a)) = S(4+7+3+2+1+7) = S(24) = 6,$$
$$\overline{b} = \mathcal{S}(b) = S(394) = 3+4 = 7,$$
$$\overline{c} = \mathcal{S}(c) = S(S(c)) = S(1+8+7+8+4+5+5+4+8) = S(50) = 5.$$

Pero

$$\overline{\overline{a}\,\overline{b}} = \mathcal{S}(\mathcal{S}(a)\mathcal{S}(b)) = \mathcal{S}(6\cdot 7) = \mathcal{S}(42) = 6 \neq 5 = \mathcal{S}(c) = \overline{c},$$

lo cual prueba que nos hemos tenido que equivocar al hacer la multiplicación.

Cálculos

La habilidad calculando siempre ha sido una de las vertientes importantes dentro de las matemáticas. Es más, algunas personas asocian las matemáticas simplemente a los cálculos. En esta sección incluiremos algunos ejemplos de demostraciones en las que estos constituyen la parte esencial de las pruebas.

69. Número decimal periódico

Se cumple que $1 = 0.9999\ldots$.

Sea $x = 0.9999\ldots = 0.\overline{9}$. Entonces $10x = 9.\overline{9}$. Restando ambas expresiones obtenemos $9x = 9$, y por tanto $x = 1$.

70. Identidad de los cuatro cuadrados de Euler

Si dos números enteros son cada uno suma de cuatro cuadrados, entonces su producto es también la suma de cuatro cuadrados.

El resultado es muy sencillo con enteros que son suma de dos cuadrados en lugar de cuatro, y se reduce a la siguiente expresión que se suele denominar identidad de la suma de cuadrados de Diofanto:

$$(a^2+b^2)(c^2+d^2) = (ac+bd)^2 + (ad-bc)^2.$$

Con cuatro cuadrados, fue Euler en 1749 quien descubrió esta identidad, que puede comprobarse sin dificultad efectuando los cálculos de ambos miembros:

$$\begin{aligned}&\left(a_1^2+a_2^2+a_3^2+a_4^2\right)\left(b_1^2+b_2^2+b_3^2+b_4^2\right)\\ &\quad = \left(-a_1b_1+a_2b_2+a_3b_3+a_4b_4\right)^2 + \left(a_1b_2+a_2b_1+a_3b_4-a_4b_3\right)^2\\ &\qquad + \left(a_1b_3-a_2b_4+a_3b_1+a_4b_2\right)^2 + \left(a_1b_4+a_2b_3-a_3b_2+a_4b_1\right)^2.\end{aligned}$$

Las dos bonitas identidades que hemos mostrado se pueden interpretar también como la igualdad de normas al cuadrado, $|z|^2|w|^2 = |z\cdot w|^2$, donde z y w son dos números complejos en el primer caso, y son dos cuaterniones en el segundo (pero los cuaterniones no aparecieron hasta 1843, cuando los ideó William Hamilton como una forma de extender los complejos a cuatro dimensiones).

71. Indentidad de Chu-Vandermonde

Para enteros no negativos cualesquiera r, s, n, se cumple

$$\sum_{k=0}^{n} \binom{r}{k}\binom{s}{n-k} = \binom{r+s}{n},$$

donde estamos usando $\binom{p}{q} = 0$ si $q > p$ (enteros no negativos).

Esta expresión la probó Alexandre Vandermonde en 1772, pero ya la conocía el matemático chino Chu Shih-Chieh en 1303, por lo que actualmente se suele denominar identidad de Chu-Vandermonde.

En el desarrollo en potencias de $(1+x)^{r+s}$ usando el binomio de Newton, el coeficiente de x^n es $\binom{r+s}{n}$. Por otra parte, si hacemos

$$(1+x)^{r+s} = (1+x)^r(1+x)^s = \left(\sum_{k=0}^{\infty}\binom{r}{k}x^k\right)\left(\sum_{j=0}^{\infty}\binom{s}{j}x^j\right)$$

(obsérvese que los números combinatorios son 0 a partir de un término), el coeficiente de x^n al multiplicar las series es $\sum_{k=0}^{n}\binom{r}{k}\binom{s}{n-k}$.

72. Serie de Gregory

$$\operatorname{arc\,tan}(x) = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \cdots = \sum_{k=0}^{\infty}\frac{(-1)^k x^{2k+1}}{2k+1}, \quad |x| < 1.$$

Esta serie, que es el desarrollo de Taylor de la función arcotangente alrededor del origen, la encontró James Gregory en 1671, aunque ya la conocía el matemático indio Madhava de Sangamagrama en el siglo XIV.

Derivando la función $f(x) = \operatorname{arc\,tan}(x)$ y utilizando el desarrollo de la progresión geométrica de razón $r = -x^2$ (que converge para $|r| < 1$, véase la prueba 6), tenemos

$$f'(x) = \frac{1}{1+x^2} = \sum_{k=0}^{\infty}(-x^2)^k = \sum_{k=0}^{\infty}(-1)^k x^{2k}.$$

Integrando término a término (existen resultados que aseguran que esto está justificado dentro del radio de convergencia de la serie, que es 1),

$$f(x) = C + \sum_{k=0}^{\infty}(-1)^k\frac{x^{2k+1}}{2k+1},$$

donde C es la constante de integración. Como $\operatorname{arc\,tan}(0) = 0$, también $C = 0$, y esto prueba el resultado.

Con algo más de trabajo se puede demostrar que la serie también converge para $x = 1$, lo cual proporciona lo que tradicionalmente se denomina fórmula de Leibniz para π,

$$\frac{\pi}{4} = \arctan(1) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots .$$

Pero la convergencia de esta serie es muy lenta, lo cual hace que no sea útil para estimar π. Como vemos a continuación, John Machin encontró en 1706 cómo expresar $\pi/4$ como una suma de arcotangentes de valores más pequeños, con lo cual la convergencia de las correspondientes series era mucho más rápida, y sí resultaba útil para calcular π.

73. Fórmula de Machin

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

El nombre de esta bonita fórmula alude a John Machin, quien la demostró en 1706 (usando un procedimiento distinto al que aquí presentamos), y la utilizó para calcular cien decimales de π (con la ayuda del desarrollo de Taylor de la arcotangente, que había encontrado James Gregory en 1671, véase la prueba 72).

Calculando obtenemos que $(5+i)^4 \cdot (239-i) = 2^2 \cdot 13^4 \cdot (1+i)$. Igualando los argumentos de los números complejos involucrados, obtenemos la prueba.

74. Una identidad de Euler

Sean x, y dos números reales que cumplen $x > 0$, $x+y > 0$, $x^2+xy+1 > 0$. Entonces,

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

Para $x > 0$ fijado, consideremos

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

como función de la variable y. Derivando respecto a y,

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

Por tanto, $f_x(y)$ es una función que no depende de y, así que

$$f_x(y) \equiv f_x(0) = \arctan\left(\frac{1}{x}\right) - \arctan\left(\frac{1}{x}\right) - \arctan(0) = 0,$$

y como consecuencia se obtiene el resultado.

Tomando $x = y = 1$ en la identidad de Euler obtenemos la bonita fórmula

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

que fue utilizada por el mismo Euler para aproximar π, usando los primeros términos de la serie de Taylor de la arcotangente (pero esta fórmula es más lenta que la de Machin que hemos mostrado en la prueba 73).

75. Una expresión con raíces anidadas

$$\sqrt{-\sqrt{3}+\sqrt{3+8\sqrt{7+4\sqrt{3}}}} = 2.$$

Basta manipular la expresión de manera adecuada:

$$\begin{aligned}\sqrt{-\sqrt{3}+\sqrt{3+8\sqrt{7+4\sqrt{3}}}} &= \sqrt{-\sqrt{3}+\sqrt{3+8\sqrt{\left(2+\sqrt{3}\right)^2}}} \\ &= \sqrt{-\sqrt{3}+\sqrt{3+8\left(2+\sqrt{3}\right)}} = \sqrt{-\sqrt{3}+\sqrt{19+8\sqrt{3}}} \\ &= \sqrt{-\sqrt{3}+\sqrt{\left(4+\sqrt{3}\right)^2}} = \sqrt{-\sqrt{3}+\left(4+\sqrt{3}\right)} = \sqrt{4} = 2.\end{aligned}$$

En particular, esto muestra que una expresión que tiene un aspecto claramente irracional, puede no serlo, así que no podemos fiarnos de la primera impresión.

76. Comparación entre e^π y π^e

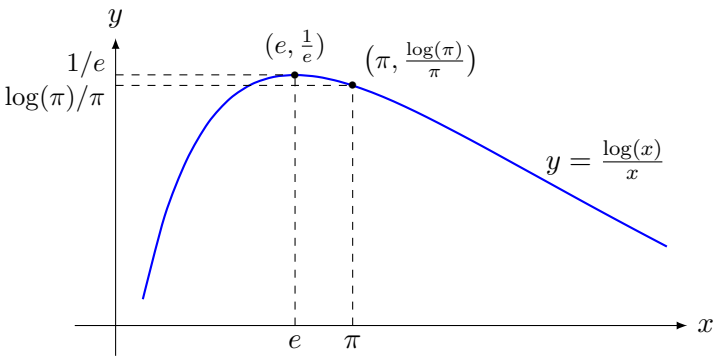
$$e^\pi > \pi^e.$$

Si se calculan e^π y π^e de manera aproximada, lo que se tiene es

$$e^\pi \sim 23.140\,692\,632\,779, \quad \pi^e \sim 22.459\,157\,718\,361.$$

Pero, por supuesto, no es eso lo que queremos, sino que se trata de demostrar que $e^\pi > \pi^e$ sin recurrir a una calculadora. Hay unas cuantas demostraciones muy bonitas de esta desigualdad. Presentamos tres de ellas.

La derivada de función $y = \log(x)/x$ es $y' = (1 - \log(x))/x^2$. De aquí se deduce que la función tiene su máximo en $x = e$. Gráficamente, tenemos lo siguiente:

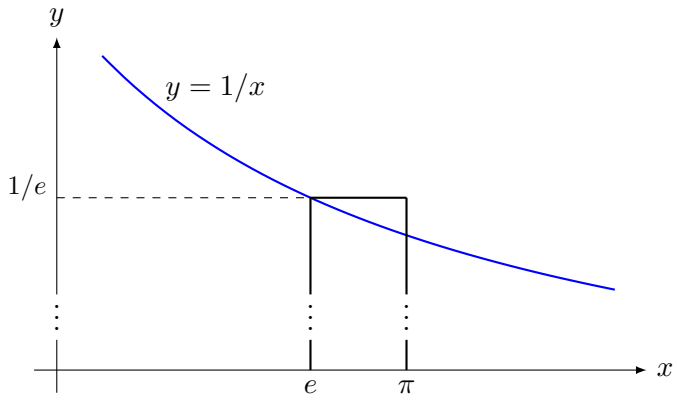


Así pues, $\frac{1}{e} > \frac{\log(\pi)}{\pi}$, con lo cual $\frac{\pi}{e} > \log(\pi)$ y $e^{\pi/e} > \pi$, de donde se sigue el resultado.

Una demostración alternativa, muy cortita, y que solo necesita usar que $e^x > 1 + x$ cuando $x > 0$, es la siguiente:

$$e^\pi = e^e \left(e^{\frac{\pi}{e}-1}\right)^e > e^e \left(\frac{\pi}{e} - 1 + 1\right)^e = \pi^e.$$

Finalmente, he aquí una tercera prueba, basada en el cálculo integral y con una interpretación más gráfica:



El área del rectángulo es mayor que el área bajo la curva entre e y π, así que

$$(\pi - e)\frac{1}{e} > \int_e^\pi \frac{1}{x}\,\mathrm{d}x = \log(\pi) - 1.$$

En consecuencia, $\pi/e > \log(\pi)$ y, de ahí, $e^\pi > \pi^e$.

77. Aproximación de π

Se cumple que

$$3 < \pi < \frac{22}{7} = 3.1428\ldots.$$

Las dos desigualdades se obtienen a partir de los siguientes cálculos, donde usamos que $\arctan(1) = \pi/4$:

$$0 < \int_0^1 \frac{(3x^2-1)^2}{1+x^2}\,\mathrm{d}x = \int_0^1 \left(9x^2 - 15 + \frac{16}{1+x^2}\right)\mathrm{d}x$$
$$= \left(3x^3 - 15x + 16\arctan(x)\right)\Big|_0^1 = 4(\pi - 3)$$

y

$$0 < \int_0^1 \frac{x^4(1-x)^4}{1+x^2}\,\mathrm{d}x = \int_0^1 \left(x^6 - 4x^5 + 5x^4 - 4x^2 + 4 - \frac{4}{1+x^2}\right)\mathrm{d}x$$
$$= \frac{1}{7} - \frac{2}{3} + 1 - \frac{4}{3} + 4 - \pi = \frac{22}{7} - \pi.$$

Tal como demostró Stephen K. Lucas en 2005 [20], con una integral algo más complicada también se puede probar que $\pi < 355/113 = 3.14159\ldots$, pues

$$\int_0^1 \frac{x^8(1-x)^8(25+816x^2)}{3164(1+x^2)}\,\mathrm{d}x = \frac{355}{113} - \pi$$

(para más detalles sobre aproximaciones de π, véase [10]).

78. Integral gaussiana

$$\int_{-\infty}^{\infty} e^{-x^2}\,\mathrm{d}x = \sqrt{\pi}\,.$$

Llamemos I a la integral. Por el teorema de Fubini,

$$I^2 = \int_{-\infty}^{\infty} e^{-x^2}\,\mathrm{d}x \cdot \int_{-\infty}^{\infty} e^{-y^2}\,\mathrm{d}y = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} e^{-x^2-y^2}\,\mathrm{d}x\,\mathrm{d}y.$$

Si hacemos el cambio de variable a coordenadas polares r y θ, donde $0 \le r < \infty$ y $0 \le \theta \le 2\pi$, con $x^2 + y^2 = r^2$ y $\mathrm{d}x\,\mathrm{d}y = r\,\mathrm{d}r\,\mathrm{d}\theta$, tenemos

$$I^2 = \int_0^{2\pi}\int_0^{\infty} re^{-r^2}\,\mathrm{d}r\,\mathrm{d}\theta = \int_0^{2\pi}\mathrm{d}\theta \cdot \int_0^{\infty} re^{-r^2}\,\mathrm{d}r$$
$$= 2\pi \cdot \left(-\frac{1}{2}e^{-r^2}\right)\Big|_0^{\infty} = 2\pi \cdot \frac{1}{2} = \pi,$$

luego $I = \sqrt{\pi}$.

79. Derivación bajo el signo integral

$$\int_0^1 \frac{\log(x)}{\sqrt[3]{x}}\,\mathrm{d}x = -\frac{9}{4}.$$

En el siguiente cálculo directo, el paso importante es que la «derivación bajo el signo integral» puede extraerse fuera del signo integral (en este caso, la justificación se sigue de que la derivada con respecto a p de la función x^p puede acotarse en valor absoluto, y para todo p en un entorno de $p=-1/3$, por una función independiente de p que es integrable Lebesgue en $[0,1]$):

$$\int_0^1 x^{-1/3}\log(x)\,\mathrm{d}x = \int_0^1 \frac{\partial}{\partial p}(x^p)\Big|_{p=-1/3}\mathrm{d}x = \frac{\partial}{\partial p}\left(\int_0^1 x^p\,\mathrm{d}x\right)\Big|_{p=-1/3}$$
$$= \frac{\partial}{\partial p}\left(\frac{1}{p+1}\right)\Big|_{p=-1/3} = \frac{-1}{(p+1)^2}\Big|_{p=-1/3} = \frac{-1}{(-1/3+1)^2} = \frac{-9}{4}.$$

De hecho, con esencialmente la misma prueba se puede ver que, para cualquier $a>-1$,

$$\int_0^1 x^a\log(x)\,\mathrm{d}x = \frac{-1}{(a+1)^2}.$$

80. Función generatriz

Sean F_n los números de Fibonacci, definidos como $F_1=F_2=1$ y $F_{n+2}=F_{n+1}+F_n$, $n\geq 1$. Entonces, para cierto $r>0$ se cumple

$$\sum_{n=1}^{\infty} F_n x^n = \frac{x}{1-x-x^2}, \qquad \textit{cuando} \quad |x|<r.$$

Los números de Fibonacci deben su nombre a Leonardo de Pisa, conocido como Fibonacci, que en su *Liber Abaci* (1202), destinado a difundir los números indoarábigos y su uso en el comercio, los introdujo en un problema redactado en términos de proliferación de conejos. Seguramente, su problema fue el primer modelo de ecología matemática. Es sorprendente el número de propiedades interesantes que tienen los números de Fibonacci; en este escrito aparecen varias veces más.

Denotemos $f(x)=\sum_{n=1}^{\infty} F_n x^n$. Como $F_n<2^n$ (por inducción: $F_{n-1}<2^{n-1}$, $F_{n-2}<2^{n-2}\Rightarrow F_n<2^{n-1}+2^{n-2}<2^n$), la serie es convergente al menos cuando $|x|<1/2$. Además,

$$f(x) = x+x^2+\sum_{n=3}^{\infty} F_n x^n = x+x^2+\sum_{n=3}^{\infty} F_{n-1}x^n+\sum_{n=3}^{\infty} F_{n-2}x^n$$
$$= x+x^2+x\sum_{n=3}^{\infty} F_{n-1}x^{n-1}+x^2\sum_{n=3}^{\infty} F_{n-2}x^{n-2}$$
$$= x+x^2+x(f(x)-x)+x^2 f(x);$$

por tanto, $f(x)(1-x-x^2)=x$, de donde se sigue el resultado.

Con algo más de esfuerzo se puede probar que la serie $f(x)$ (que se denomina función generatriz) tiene radio de convergencia $r=(\sqrt{5}-1)/2$ (el inverso de la razón áurea).

81. Números de Fibonacci y matrices

Si F_n son los números de Fibonacci (con $F_0 = 0$), entonces

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}, \quad n \geq 1.$$

Además, esta expresión permite dar un algoritmo que solo usa $O(\log n)$ pasos para calcular F_n.

El resultado que aquí presentamos está recogido de [21, miniatura 1]. Antes de comenzar, recordemos que, si f y g son dos funciones no negativas definidas sobre los naturales, la notación $f(n) = O(g(n))$ (que fue introducida por Edmund Landau) significa que, para alguna constante C, se cumple $f(n) \leq Cg(n)$ para todo n suficientemente grande.

La igualdad matricial del enunciado resulta inmediata usando inducción, ya que

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

Veamos ahora cómo construir el algoritmo de cálculo (usando lo que se denomina método de los cuadrados sucesivos, y que resulta muy útil siempre que se quiere elevar un número o una matriz a un exponente grande). Para $k \in \mathbb{N}$, introducimos de manera recurrente las matrices $N_{k+1} = N_k^2$, con $N_0 = M$. Es fácil ver, de nuevo por inducción, que $N_k = M^{2^k}$.

Entonces, dado $n \in \mathbb{N}$, lo expresamos en base 2 como

$$n = n_m 2^m + n_{m-1} 2^{m-1} + \cdots + n_1 2 + n_0 2^0,$$

donde $n_j \in \{0, 1\}$. Con esto,

$$M^n = (M^{2^m})^{n_m} (M^{2^{m-1}})^{n_{m-1}} \cdots (M^2)^{n_1} (M)^{n_0} = N_m^{n_m} N_{m-1}^{n_{m-1}} \cdots N_1^{n_1} N_0^{n_0},$$

igualdad que da lugar al algoritmo deseado. No abundamos en los detalles de por qué la cantidad de operaciones es logarítmica (la razón es que el número de dígitos de n es $O(\log n)$), pero en cualquier caso es claro que es mucho menor que usando directamente la recurrencia que define los números de Fibonacci, que requiere $O(n)$ pasos para llegar a F_n.

82. Desigualdad sujeta a condiciones

Cuando x, y, z son reales positivos que cumplen $x + y + z = 1$, entonces

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} \geq 9,$$

y esta desigualdad no se puede mejorar.

Recordemos que, si usamos $\langle\cdot,\cdot\rangle$ para denotar el producto escalar en un espacio de vectores, la desigualdad de Cauchy-Schwarz establece que $|\langle \mathbf{u},\mathbf{v}\rangle|^2 \le \langle \mathbf{u},\mathbf{u}\rangle \cdot \langle \mathbf{v},\mathbf{v}\rangle$. En nuestro caso,

$$\left(\sqrt{x}\cdot\frac{1}{\sqrt{x}}+\sqrt{y}\cdot\frac{1}{\sqrt{y}}+\sqrt{z}\cdot\frac{1}{\sqrt{z}}\right)^2 \le (x+y+z)\left(\frac{1}{x}+\frac{1}{y}+\frac{1}{z}\right).$$

En esta desigualdad, la expresión de la izquierda vale $3^2=9$; y, a la derecha, $x+y+z=1$. Así pues, $9 \le \frac{1}{x}+\frac{1}{y}+\frac{1}{z}$. En el caso $x=y=z=1/3$ se da la igualdad, luego la desigualdad no se puede mejorar.

83. Una suma trigonométrica

$$\sum_{k=1}^{m} \cot^2\left(\frac{k\pi}{2m+1}\right) = \frac{m(2m-1)}{3}.$$

Para comenzar, observemos que

$$\begin{aligned}\cos(n\theta)+i\,\mathrm{sen}(n\theta) &= e^{in\theta} = \left(e^{i\theta}\right)^n = (\cos(\theta)+i\,\mathrm{sen}(\theta))^n \\ &= \mathrm{sen}^n(\theta)\,(\cot(\theta)+i)^n = \mathrm{sen}^n(\theta)\sum_{k=0}^{n}\binom{n}{k} i^k \cot^{n-k}(\theta).\end{aligned}$$

Tomando $n=2m+1$ e igualando las partes imaginarias de la relación anterior, obtenemos

$$\begin{aligned}\mathrm{sen}\,((2m+1)\theta) &= \mathrm{sen}^{2m+1}(\theta)\sum_{j=0}^{m}\binom{2m+1}{2j+1}(-1)^j\cot^{2(m-j)}(\theta) \\ &= \mathrm{sen}^{2m+1}(\theta)P_m(\cot^2(\theta)),\end{aligned}$$

donde P_m es el polinomio (de grado m)

$$P_m(x) = \sum_{j=0}^{m}\binom{2m+1}{2j+1}(-1)^j x^{m-j}.$$

Por su definición, las m raíces de P_m son $x_k = \cot^2\left(k\pi/(2m+1)\right)$, $k=1,2,\ldots,m$. Ahora bien, si las m raíces de un polinomio $Q(x)=a_m x^m + a_{m-1}x^{m-1}+\cdots+a_0$, con $a_m\neq 0$, son $y_1,y_2,\ldots,y_m$, expandiendo

$$a_m x^m + a_{m-1}x^{m-1}+\cdots+a_0 = a_m(x-y_1)(x-y_2)\cdots(x-y_m)$$

e igualando el coeficiente de x^{m-1} se obtiene que $y_1+y_2+\cdots+y_m = -a_{m-1}/a_m$. Por lo tanto,

$$\sum_{k=1}^{m}\cot^2\left(\frac{k\pi}{2m+1}\right) = \sum_{k=1}^{m} x_k = -\frac{-\binom{2m+1}{3}}{\binom{2m+1}{1}} = \frac{m(2m-1)}{3},$$

tal y como queríamos ver.

84. El problema de Basilea

$$\sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{\pi^2}{6}.$$

El cálculo de esta suma fue propuesto por primera vez por Pietro Mengoli en 1644. Más adelante, Jacob Bernoulli se interesó por él, y de ahí proviene su nombre, ya que su residencia estaba en Basilea. Euler lo resolvió, por primera vez, en el año 1734.

Presentamos la prueba dada en [26], que se basa en la también interesante relación trigonométrica demostrada en la prueba 83:

$$\sum_{k=1}^{m} \cot^2\left(\frac{k\pi}{2m+1}\right) = \frac{m(2m-1)}{3}.$$

Para todo $0 < x < \pi/2$ se cumple que $\operatorname{sen}(x) < x < \tan(x)$; por lo tanto, tomando recíprocos y elevando al cuadrado, $\cot^2(x) < 1/x^2 < 1 + \cot^2(x)$. Sustituyendo $x = k\pi/(2m+1)$, con $k, m \in \mathbb{N}$ cumpliendo $1 \le k \le m$, y sumando, se obtiene

$$\sum_{k=1}^{m} \cot^2\left(\frac{k\pi}{2m+1}\right) < \frac{(2m+1)^2}{\pi^2} \sum_{k=1}^{m} \frac{1}{k^2} < m + \sum_{k=1}^{m} \cot^2\left(\frac{k\pi}{2m+1}\right).$$

Multiplicando las desigualdades por $\pi^2/(2m+1)^2$ y usando el valor de la suma trigonométrica anterior, llegamos a

$$\frac{m(2m-1)}{3(2m+1)^2}\pi^2 < \sum_{k=1}^{m} \frac{1}{k^2} < \left(m + \frac{m(2m-1)}{3}\right)\frac{\pi^2}{(2m+1)^2} = \frac{2m(m+1)}{3(2m+1)^2}\pi^2.$$

Haciendo tender m a infinito se obtiene la suma deseada, dado que las fracciones de la izquierda y de la derecha tienden a $\pi^2/6$.

85. Divergencia de la suma de los inversos de los primos

La suma de los inversos de todos los números primos es una serie divergente.

La primera prueba de la divergencia de esta serie se debe a Euler y data de 1737. La que presentamos es atribuida a F. Gilfeather y G. Meisters en [19], y se inspira en la de Euler. Obviamente, el resultado implica que hay infinitos números primos.

Fijado $2 \le n \in \mathbb{N}$, denotemos por $\mathbf{P}_n$ el conjunto de todos los primos $p \le n$. Utilizando la fórmula de la suma de una progresión aritmética de razón $1/p$ (prueba 6) tenemos que

$$\prod_{p\in\mathbf{P}_n} \frac{p}{p-1} = \prod_{p\in\mathbf{P}_n} \frac{1}{1-1/p} = \prod_{p\in\mathbf{P}_n} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots\right).$$

Como todo entero positivo $k \leq n$ se descompone como producto de primos menores o iguales que n elevados a potencias enteras positivas, es seguro que $1/k$ aparece como un término del desarrollo del producto de la derecha de la igualdad. Por tanto,

$$\prod_{p\in\mathbf{P}_n} \frac{p}{p-1} > \sum_{k=1}^{n} \frac{1}{k}.$$

Tomando logaritmos en la desigualdad anterior, y teniendo en cuenta que el logaritmo es una función creciente,

$$\sum_{p\in\mathbf{P}_n} \big(\log(p) - \log(p-1)\big) > \log\left(\sum_{k=1}^{n} \frac{1}{k}\right).$$

Por otra parte,

$$\sum_{p\in\mathbf{P}_n} (\log(p) - \log(p-1)) = \sum_{p\in\mathbf{P}_n} \int_{p-1}^{p} \frac{1}{x}\,\mathrm{d}x < \sum_{p\in\mathbf{P}_n} \frac{1}{p-1} \leq \sum_{p\in\mathbf{P}_n} \frac{2}{p}.$$

Combinando las dos desigualdades anteriores llegamos a

$$\sum_{p\in\mathbf{P}_n} \frac{1}{p} > \frac{1}{2}\log\left(\sum_{k=1}^{n} \frac{1}{k}\right)$$

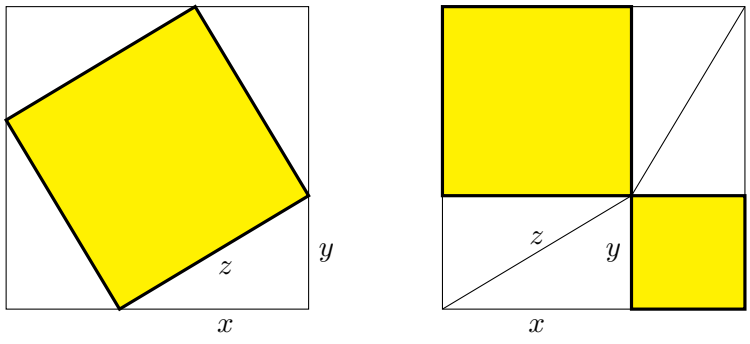
y, como la serie armónica es divergente (prueba 8), obtenemos el resultado.

Pruebas sin palabras

Mostramos ahora algunas demostraciones en las que, observando una figura y razonando sobre lo que se ve, ya no se requieren explicaciones adicionales. Por supuesto, todos los resultados que aquí presentamos tienen pruebas alternativas con lenguaje y notación matemática estándar.

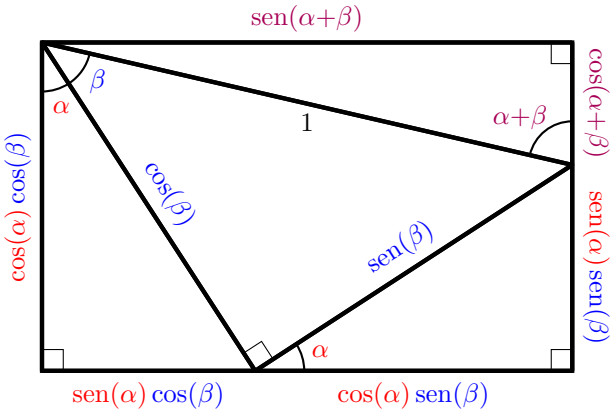
86. Teorema de Pitágoras

Si x e y son los dos catetos de un triángulo rectángulo, y z es la hipotenusa, entonces $x^2 + y^2 = z^2$.



87. Razones trigonométricas de la suma de ángulos

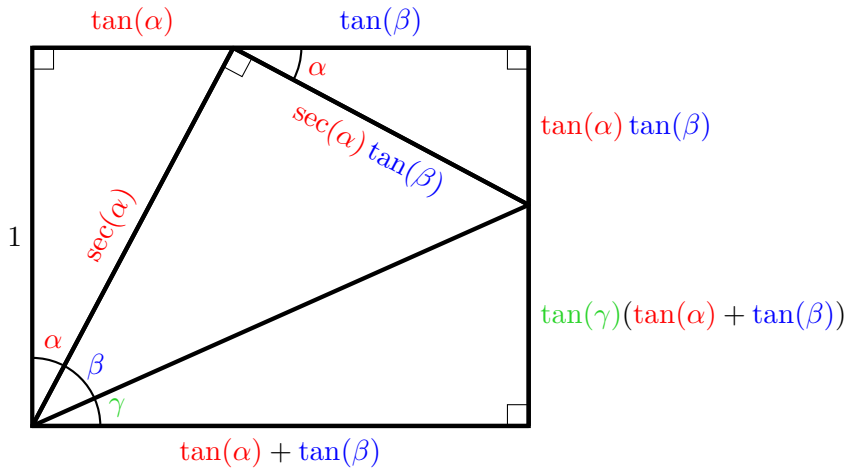
$$\operatorname{sen}(\alpha+\beta) = \operatorname{sen}(\alpha)\cos(\beta) + \cos(\alpha)\operatorname{sen}(\beta),$$
$$\cos(\alpha+\beta) = \cos(\alpha)\cos(\beta) - \operatorname{sen}(\alpha)\operatorname{sen}(\beta).$$



88. Una relación entre tangentes

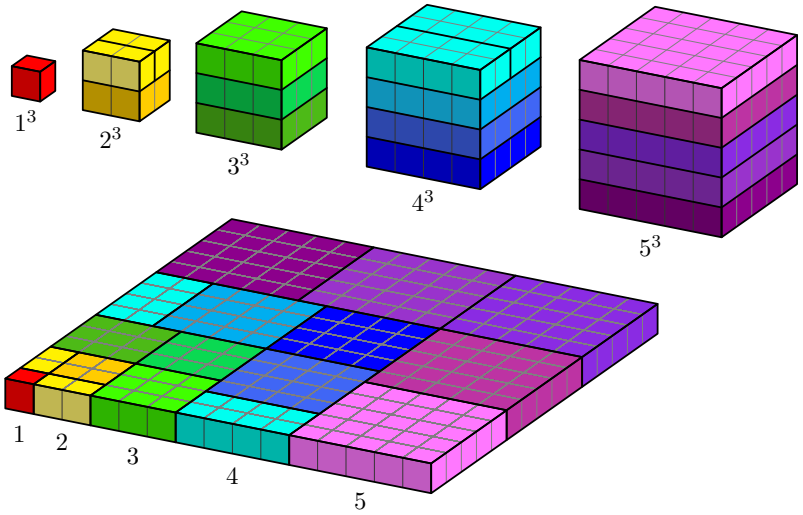
Si α, β y γ son tres ángulos positivos tales que $\alpha+\beta+\gamma = \pi/2$, entonces

$$\tan(\alpha)\tan(\beta) + \tan(\beta)\tan(\gamma) + \tan(\gamma)\tan(\alpha) = 1.$$



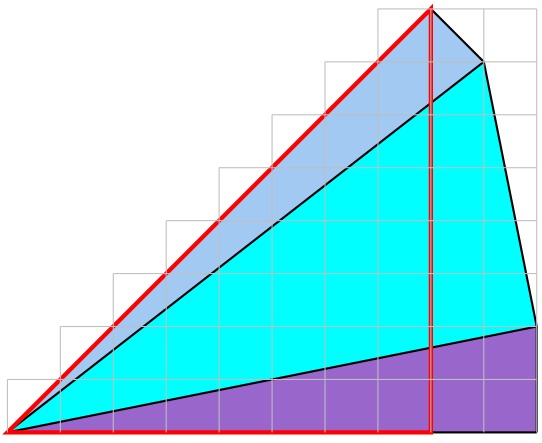
89. Teorema de Nicómaco

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



90. Otra fórmula de tipo Machin

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



Principio del palomar

El principio del palomar, también llamado principio de las casillas o principio de Dirichlet, establece que si n palomas se distribuyen en m palomares, y si $n > m$, entonces al menos habrá un palomar con más de una paloma. Aunque ya se había usado antes, debe su nombre a un tratado escrito en 1834 por Lejeune Dirichlet (en el que parece la prueba 95). Es una herramienta fundamental en combinatoria y teoría de conjuntos, útil para demostrar la existencia de algún elemento que satisface determinada propiedad sin especificar el elemento exacto que la cumple.

91. Contando cabellos

En Sabadell hay dos personas con la misma cantidad de cabello.

El número de cabellos de una persona es, como mucho, 200 000, y en Sabadell hay más de 200 000 habitantes. Por tanto, si los agrupamos en función de su cantidad de cabello, debe existir un grupo con al menos dos personas.

92. Un múltiplo formado por unos y ceros

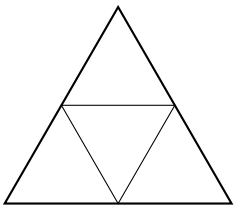
Todo número $n \in \mathbb{N}$ tiene un múltiplo formado solo por unos y ceros.

Tomamos $n + 1$ números: $1, 11, 111, 1111, \ldots$. Al dividirlos todos entre n hay dos, $p > q$, que tienen el mismo resto, ya que solo existen n restos. Finalmente, $p - q$ es el múltiplo buscado.

93. Puntos en un triángulo

Dados cinco puntos cualesquiera en un triángulo equilátero de lado 2, siempre podemos encontrar dos puntos que están a distancia menor o igual que 1.

Construyamos cuatro palomares a partir de una división adecuada del triángulo equilátero, como en la figura, donde el triángulo original se ha dividido en cuatro triángulos equiláteros de lado 1:



Por el principio de palomar hay al menos dos puntos en alguno de estos cuatro triángulos, y la distancia entre ellos no puede ser mayor que el lado del triángulo, luego están a distancia menor o igual que 1.

94. Elección de números en un conjunto

Dado $n \geq 1$, sea $C_n = \{1, 2, 3, \ldots, 2n\}$. Si se toman $n+1$ números cualesquiera del conjunto C_n, al menos habrá entre ellos dos elementos tal que uno divide al otro.

Definamos los conjuntos

$$T_j = \{\, (2j-1) \cdot 2^k \,:\, k = 0, 1, 2, 3, \ldots \}, \quad 1 \leq j \leq n$$

(observemos que, en un mismo T_j, cada número divide a todos los siguientes) y, asimismo,

$$\widetilde{T}_j = T_j \cap C_n, \quad 1 \leq j \leq n.$$

Es claro que estos n conjuntos $\widetilde{T}_j$ son disjuntos, y su unión es el conjunto de partida C_n.

Por el principio del palomar, si tomamos $n+1$ números de C_n, forzosamente habrá dos que estarán en un mismo $\widetilde{T}_j$. Y, si tenemos dos elementos en un mismo $\widetilde{T}_j$, el menor divide al mayor.

95. Aproximación por racionales

Para cualquier número real α y cualquier entero positivo n, existen enteros p y q, con $1 \leq q \leq n$ tales que

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{nq}.$$

Además, si α es irracional, existen infinitas fracciones p/q tales que

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Para $x \in \mathbb{R}$, usemos $\lfloor x \rfloor$ para denotar su parte entera, y $\{x\} = x - \lfloor x \rfloor$ para su parte fraccionaria; obsérvese que $\{x\} \in [0, 1)$.

Dividamos el intervalo $[0, 1)$ en n subintervalos

$$\left[0, \frac{1}{n}\right), \ \left[\frac{1}{n}, \frac{1}{n}\right), \ \ldots, \ \left[\frac{n-1}{n}, 1\right).$$

Entonces, dado $\alpha \in \mathbb{R}$ y las $n+1$ partes fraccionarias $\{j\alpha\}$, $0 \leq j \leq n$, habrá dos (llamémoslas $\{j\alpha\}$ y $\{k\alpha\}$, con $0 \leq j < k$) que estarán en el

mismo subintervalo; así pues,

$$|\{k\alpha\} - \{j\alpha\}| < \frac{1}{n}.$$

Expandiendo $\{k\alpha\} = k\alpha - \lfloor k\alpha \rfloor$ y $\{j\alpha\} = j\alpha - \lfloor j\alpha \rfloor$, se puede escribir como

$$|(k-j)\alpha - (\lfloor k\alpha \rfloor - \lfloor j\alpha \rfloor)| < \frac{1}{n}.$$

Llamando $q = k - j$ y $p = \lfloor k\alpha \rfloor - \lfloor j\alpha \rfloor$, tenemos $|q\alpha - p| < 1/n$, luego $|\alpha - p/q| < 1/(nq)$, tal como buscábamos.

Analicemos ahora el caso $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Precisamente por ser α irracional, nunca puede ocurrir que $|\alpha - p/q| = 0$, pues en ese caso sería $\alpha = p/q \in \mathbb{Q}$.

Para ver que existen infinitas fracciones p/q que aproximan α con un error menor que $1/q^2$, apliquemos el caso general para cada $n \geq 1$. Dado n, existen p_n y q_n, con $1 \leq q_n \leq n$ tales que $|\alpha - p_n/q_n| < 1/(nq_n)$. Además, los denominadores q_n cumplen $q_n \to \infty$ cuando $n \to \infty$ pues, de lo contrario, solo habría una cantidad finita de p_n y q_n posibles, con lo cual $|q_n\alpha - p_n|$ (que no se anula) estaría acotado inferiormente para algún $c > 0$, y tendríamos $c < |q_n\alpha - p_n| < 1/n$ para todo n, lo cual es imposible. Entonces, como $q_n \leq n$, $|\alpha - p_n/q_n| < 1/(q_n n) \leq 1/q_n^2$, y ya hemos concluido la prueba.

No es difícil probar que esa aproximación no es posible en el caso $\alpha \in \mathbb{Q}$.

Pruebas combinatorias

Presentamos ahora algunas demostraciones que usan fórmulas o razonamientos combinatorios, incluyendo aquí, en algunos casos, problemas relacionados con la teoría de grafos.

96. Suma de números combinatorios

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

Por un lado, 2^n es el número de subconjuntos de un conjunto con n elementos. Por otro, $\binom{n}{k}$ indica el número de subconjuntos de k elementos de dicho conjunto.

Esta igualdad también se puede demostrar fácilmente a partir del binomio de Newton ya que $2^n = (1+1)^n$.

97. Una igualdad combinatoria sencilla

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

De hecho, esta igualdad no es más que la identidad de Chu-Vandermonde cuando $r = s = n$ (prueba 71), pero la demostración que presentamos aquí es puramente combinatoria.

Dado un conjunto con $2n$ elementos, contaremos de dos formas distintas cuántos subconjuntos de n elementos tiene:

- Por un lado hay $\binom{2n}{n}$ subconjuntos.
- Por otro lado, «pintamos» n elementos de color rojo y n elementos de color azul. Ahora, cada subconjunto con n elementos tendrá k rojos y $n-k$ azules, para un cierto k, con $0 \leq k \leq n$. Para cada k fijado, podemos elegir k elementos rojos de $\binom{n}{k}$ modos y $n-k$ elementos azules de $\binom{n}{n-k}$ maneras. Así, como $\binom{n}{k} = \binom{n}{n-k}$, para cada k hay $\binom{n}{k}\binom{n}{n-k} = \binom{n}{k}^2$ posibilidades. Variando k desde 0 hasta n obtenemos un total de $\sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k} = \sum_{k=0}^{n} \binom{n}{k}^2$ subconjuntos.

Igualando las dos formas de contar obtenemos la fórmula deseada.

98. Paradoja del cumpleaños

En un grupo de 23 personas (o más), la probabilidad de que dos cumplan los años el mismo día es superior al 50 %.

Sea n el número de personas en el grupo (si $n > 365$, la probabilidad es del 100 % por el principio del palomar, así que podemos suponer que $n \leq 365$), y comencemos calculando la probabilidad del suceso contrario, que es más sencillo. Es decir, calcularemos la probabilidad de que las n personas celebren su cumpleaños en diferentes días, y lo haremos dividiendo el número de casos favorables entre el número de casos posibles (regla de Laplace). Dar un caso favorable equivale a dar una lista ordenada de n días distintos de entre los 365 días del año, luego el total de casos favorables es

$$365 \cdot 364 \cdots (365 - n + 1) = \frac{365!}{(365-n)!}.$$

Por otra parte, los casos posibles son todas las posibles listas ordenadas de n días, es decir, 365^n. Entonces, la probabilidad pedida es

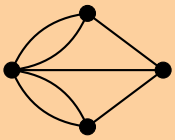
$$p_n = 1 - \frac{365!/(365-n)!}{365^n} = 1 - \frac{365!}{365^n (365-n)!}.$$

Para $n = 22$, la probabilidad es $p_{22} \sim 0.475\,695$; para $n = 23$, $p_{23} \sim 0.507\,297$. Para $n > 40$, la probabilidad es mayor del 90 %.

Conviene aclarar que el nombre paradoja del cumpleaños con el que se designa habitualmente a este resultado no es porque sea una paradoja matemática, sino porque, a simple vista, cabría esperar que iban a hacer falta muchas más de 23 personas para que la probabilidad de que dos de ellas compartan día de cumpleaños exceda el 50 %.

99. Camino euleriano en un grafo

En el grafo

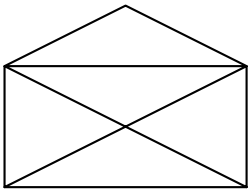


no hay ningún camino que, empezando en un vértice cualquiera, recorra todas las aristas una sola vez y regrese al vértice de partida.

En 1736, Euler modeló y resolvió el denominado problema de los puentes de Königsberg usando este grafo, lo cual supuso el nacimiento de la teoría de grafos, una nueva rama de las matemáticas. Un recorrido como el que se propone se conoce con el nombre de *ciclo euleriano*, así que lo que queremos es demostrar que, en ese grafo, no se puede encontrar un ciclo euleriano.

Si existiera un camino que recorra todas las aristas una sola vez, incluso sin exigir que el vértice inicial y final sean el mismo, los vértices intermedios necesariamente han de estar conectados a un número par de aristas (si llegamos a un vértice desde alguna arista, hay que salir de ese vértice por una arista diferente). Esto significa que el vértice inicial y el final son los únicos que podrían estar conectados a un número impar de aristas (si el recorrido debe comenzar y acabar en el mismo vértice, ese vértice tampoco puede tener un número impar de aristas). Pero el grafo del enunciado tiene cuatro vértices en los que inciden un número impar de aristas, luego tal recorrido no puede existir.

Aunque esto es más difícil de demostrar, el argumento de paridad del número de aristas que inciden en cada vértice es una condición necesaria y suficiente para la existencia de caminos eulerianos en un grafo.



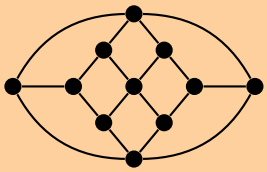
Como un pequeño homenaje a la madre del primer autor, tristemente fallecida mientras preparábamos este trabajo, incluimos un problema clásico con el que ella le tenía entretenido de pequeño. Le decía: *Nen, a veure si pots dibuixar aquest sobre sense aixecar el llàpis del paper i sense passar dos cops per la mateixa línia.*[1] Entretenimientos como este desarrollaron su interés por la resolución de problemas y seguramente le llevaron a dedicarse a las matemáticas.

Con todo lo que se ha explicado en esta prueba, es claro que es posible dibujar el sobre con las condiciones impuestas, y que hay que empezar a dibujar por uno de los vértices inferiores y acabar en el otro, ya que son los únicos a los que llegan un número impar de aristas.

[1] Niño, a ver si puedes dibujar este sobre sin levantar el lápiz del papel y sin pasar dos veces por la misma línea.

100. Camino hamiltoniano en un grafo

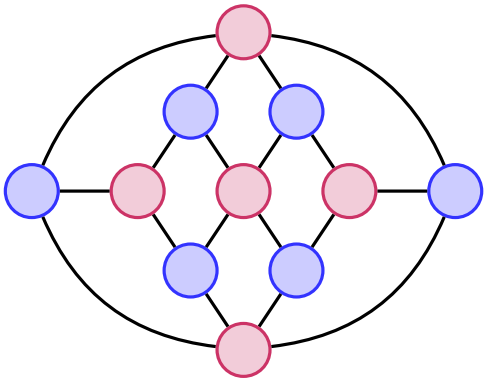
En el grafo



no hay ningún camino que, empezando en un vértice, recorra todos los demás sin repetir ninguno y regrese al vértice de partida.

Un camino como el que se requiere se denomina *ciclo hamiltoniano*. El nombre alude a William Rowan Hamilton (1805–65), quien inventó un juego cuyo objetivo era encontrar un camino que recorriera veinte ciudades, representadas como los vértices de un dodecaedro regular, siguiendo las aristas del dodecaedro. En honor al astrónomo Alexander Stewart Herschel, que realizó diversos estudios sobre ciclos hamiltonianos, el grafo que hemos mostrado se denomina grafo de Herschel. Así pues, lo que tenemos que probar es que, en el grafo de Herschel, no puede haber un ciclo hamiltoniano.

Utilizando dos colores, rojo y azul, coloreemos los vértices del grafo como se muestra a continuación:



Como se ve, hay 6 vértices azules y 5 rojos, y no hay ninguna arista que una dos vértices del mismo color. Así pues, cualquiera que sea el vértice por el que empecemos un camino, cada vez que recorremos una arista cambiamos de color.

Si empezamos en un vértice azul, tras recorrer los 11 vértices alternando colores acabaríamos en un vértice también azul, pero ya no podríamos regresar al de partida, pues no hay ninguna arista que una dos vértices azules. Si empezamos en un vértice rojo (solo hay 5) será peor: quedaremos atascados antes de completar el circuito.

En general, un grafo se denomina bipartito si los vértices se pueden pintar con dos colores de manera que ninguna arista une vértices del mismo color.

El mismo argumento que hemos usado con el grafo de Herschel prueba que, en un grafo bipartito con un número impar de vértices, nunca puede haber un ciclo hamiltoniano. Al contrario de lo que ocurre con los ciclos eulerianos, no se conoce ninguna condición necesaria y suficiente que caracterice la existencia de ciclos hamiltonianos en un grafo.

101. Lema de los apretones de manos

En una fiesta con un número impar de invitados, cada invitado estrecha la mano de todos sus conocidos. En estas circunstancias, siempre hay al menos un invitado que da una cantidad par de apretones de mano.

Formemos un grafo en el que los vértices son los invitados, que estarán unidos por una arista si se han dado la mano (quizás conviene aclarar que si un invitado no da la mano a nadie, se considera que da 0 apretones, que es un número par). Si sumamos el número de apretones de manos que ha dado cada invitado, el número total que obtendremos será el doble del número de aristas del grafo (pues cada apretón lo estaremos contando dos veces). Pero si cada invitado da un número impar de apretones, estaremos sumando una cantidad impar de números impares, y eso no puede ser el doble del número de aristas.

Agradecimientos

Agradecemos a Pilar Benito, Óscar Ciaurri, Ronaldo A. Garcia, Maria Jolis, Víctor Lanchares, Francesc Mañosas, Luis Fernando Mello, Gaspar Mora y Luis Navas su atenta lectura de versiones previas de este artículo, así como sus sugerencias. Algunas de las pruebas que hemos recogido nos las han proporcionado ellos.

Este trabajo está subvencionado por el Ministerio de Ciencia, Innovación y Universidades, Agencia Estatal de Investigación, proyectos PID2022-136613NB-I00 y PID2024-155593NB-C22.

Referencias

[1] M. Aigner, G. M. Ziegler, Proofs from THE BOOK, sexta edición, Springer, 2018. Existe traducción en castellano (de una edición anterior): EL LIBRO de las demostraciones, Nivola, 2005.

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

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

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

[5] M. Chamberland, Single digits. In praise of small numbers, Princeton University Press, Princeton, N.J., 2015.

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

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

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

[9] D. Fomin, S. Genkin, I. Itenberg, Mathematical circles (Russian experience), Mathematical World **7**, American Mathematical Society, Providence, R.I., 1996.

[10] A. Gasull, *Integració de funcions racionals i* π, Materials Matemàtics **2018**, treball no. 2, 28 pp., 2018.

[11] A. Gasull, *Gemmes matemàtiques*, Materials Matemàtics **2019**, treball no. 2, 88 pp., 2019.

[12] A. Gasull, *Mètodes de demostració*, Materials Matemàtics **2023**, treball no. 3, 85 pp., 2023.

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

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

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

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

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

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

[19] W. G. Leavitt, *The sum of the reciprocals of the primes*. Two-Year College Math. J. **10** (1979), pp. 198–199.

[20] S. K. Lucas, *Integral proofs that* $355/113 > \pi$, Australian Math. Soc. Gazette **32** (2005), pp. 263–266.

[21] J. Matoušek, Thirty-three Miniatures: Mathematical and Algorithmic Applications of Linear Algebra, Student Mathematical Library **53**, American Mathematical Society, Providence, R.I., 2010.

[22] R. B. Nelsen, *Heron's formula via proof without words*, College Math. J. **32** (2001), pp. 290–292.

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

[24] I. Niven, *A simple proof that* π *is irrational*. Bull. Amer. Math. Soc. **53** (1947), p. 509.

[25] R. S. Palais, *A simple proof of the Banach contraction principle*, J. Fixed Point Theory Appl. **2** (2007), pp. 221–223.

[26] I. Papadimitriou, *A simple proof of the formula* $\sum_{k=1}^{\infty} k^{-2} = \pi^2/6$. Amer. Math. Monthly **80** (1973), pp. 424–425.

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

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

[29] P. Ribenboim, 13 Lectures on Fermat's Last Theorem, Springer-Verlag, 1979.

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

[31] D. Sadornil, J. L. Varona, *Existen infinitos primos (desde Euclides hasta el siglo XXI)*, Gac. R. Soc. Mat. Esp. **24** (2021), pp. 301–324.

[32] F. Saidak, *A new proof of Euclides' theorem*, Amer. Math. Monthly **113** (2006), pp. 937–938.

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

[34] T. B. Soulami, Les olympiades de mathématiques: Réflexes et stratégies, 2.ª edición, Ellipses, 2007.

[35] J. L. Varona, Recorridos por la Teoría de Números, Electolibiris y Real Sociedad Matemática Española, Murcia, 2019.

[36] J. L. Varona, *Suma de potencias de enteros consecutivos*, Lva2 **1** (2024), pp. 73–80.

[37] P. Zeitz, The art and craft of problem solving, 3.ª edición, Wiley, 2017.

Armengol Gasull
Departament de Matemàtiques
Universitat Autònoma de Barcelona
armengol.gasull@uab.cat

Juan Luis Varona
Departamento de Matemáticas y Computación
Universidad de La Rioja
jvarona@unirioja.es
https://www.unirioja.es/cu/jvarona/

Publicat el 30 de març de 2026