Aritmética II

Eugenio Hernández

COMPLEMENTOS DE MATEMÁTICAS PARA LA EDUCACIÓN SECUNDARIA
Curso 2022-23

Más preguntas sobre cardinales

- Ya sabemos que hay igual de primos, de pares o de cuadrados que números naturales: **todos estos conjuntos son numerables, tienen cardinal $\aleph_0$.**

- ¿Qué hacer si llega al Hotel de Hilbert una flota de Hilbert de autobuses de Hilbert? Es decir, una flota de autobuses numerados $1, 2, 3, \ldots$ cada uno de ellos con asientos $1, 2, 3, \ldots$, todos ocupados. Como sabemos, el hotel está lleno.

- ¿Podremos alojar también, sin que nadie comparta habitación, a todos estos nuevos clientes?

¡Numérense!

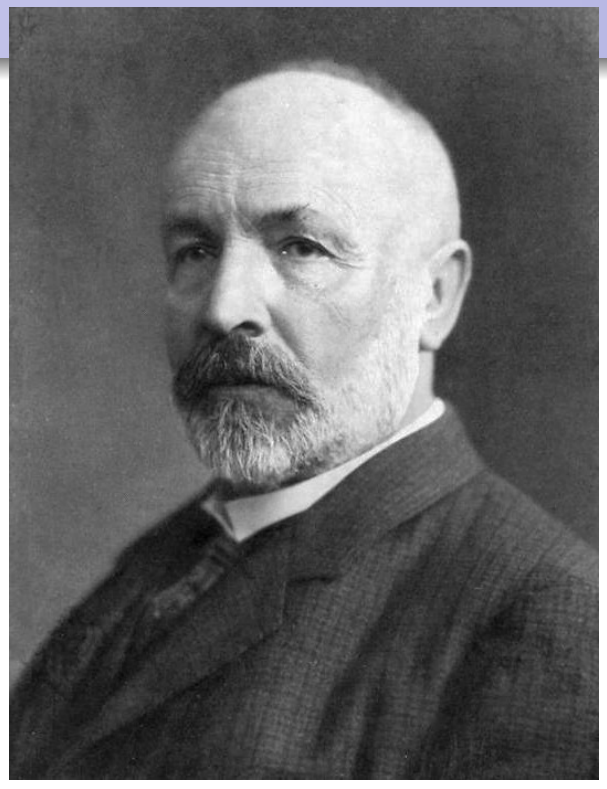
Llamamos h_i al huesped que ocupa en este momento la habitación i y llamemos $p_i^{(j)}$ al pasajero del asiento i en el autobús j. Los distribuimos en filas y columnas:

$$\begin{array}{ccccc} h_1 & h_2 & h_3 & h_4 & \cdots \\ p_1^{(1)} & p_2^{(1)} & p_3^{(1)} & p_4^{(1)} & \cdots \\ p_1^{(2)} & p_2^{(2)} & p_3^{(2)} & p_4^{(2)} & \cdots \\ p_1^{(3)} & p_2^{(3)} & p_3^{(3)} & p_4^{(3)} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \cdots \end{array}$$

La pregunta es: **¿podemos numerarlos?**

Pues sí (Los ordenados en diagonal comenzando por la esquina superior izquierda).

Paradojas del infinito



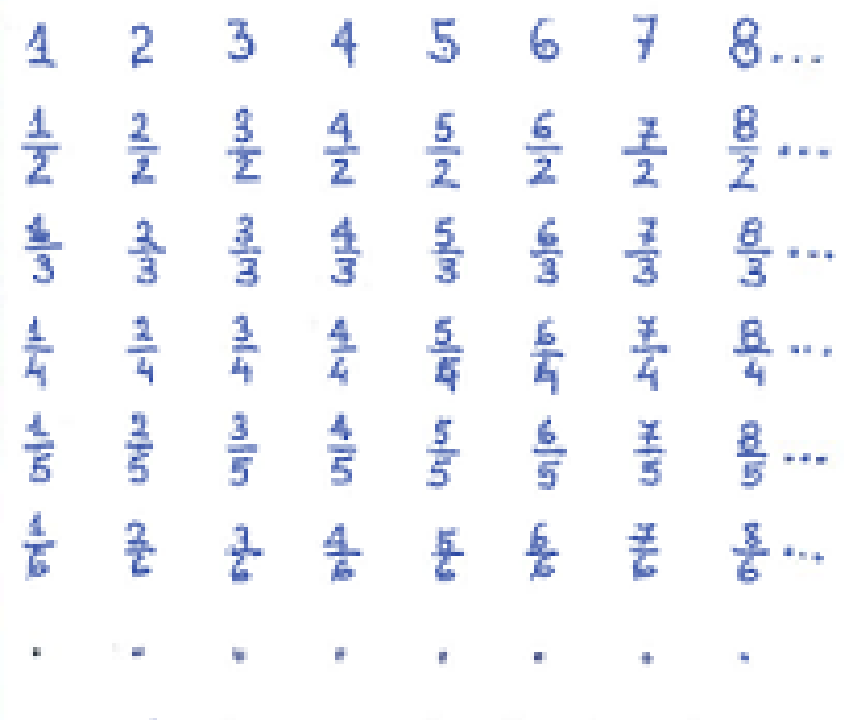
El matemático que más ha contribuido a entender las paradojas del infinito es Georg Cantor (San Petersburgo, 1845 - Halle, 1918). Su obra más conocida, *"Contribuciones a los fundamentos de la teoría de los números transfinitos"* fué publicada en 1915.

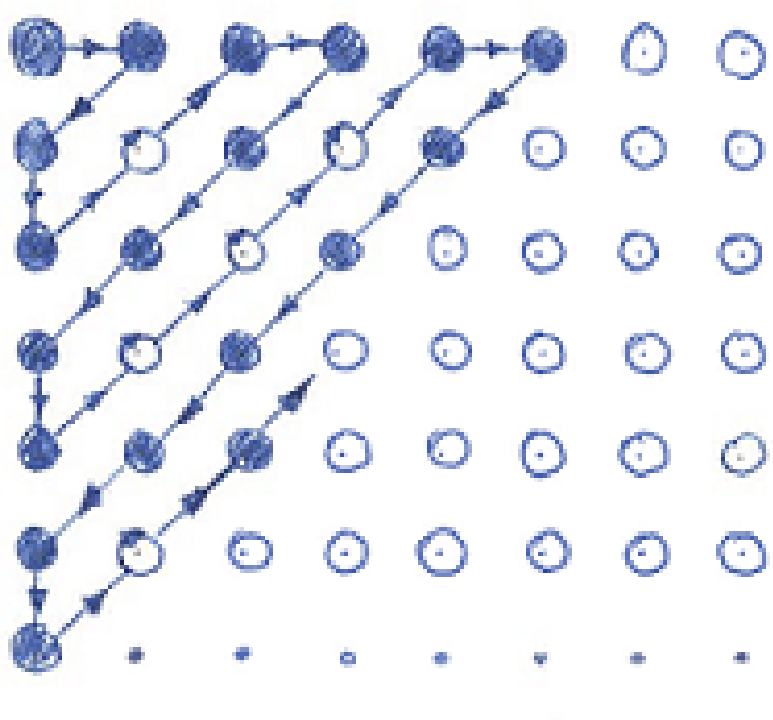
Un ejemplo muy sencillo de las paradojas del infinito es la igualdad

$$0,9999999..... = 0,\overline{9} = 1$$

¿Y LOS RACIONALES?

¿Hay más números racionales que números enteros?





- $\mathbb{Q}$ **es numerable:** Una ordenación de los números racionales positivos se describe en la figura de arriba:

$$1, 2, \frac{1}{2}, \frac{1}{3}, 3, 4, \frac{3}{2}, \frac{2}{3}, \frac{1}{4}, \frac{1}{5}, 5, 6, \frac{5}{2}, \frac{4}{3}, \frac{3}{4}, \frac{2}{5}, \frac{1}{6}, \frac{1}{7}, \frac{3}{5} \ldots$$

Números irracionales

Los números irracionales son densos en toda la recta de números reales. Pero aun quedan en la recta pequeños agujeritos que corresponden a los números irracionales, es decir, los números reales que no se pueden escribir como una fracción.

- $\sqrt{2} = 1,414213562\ldots$ es irracional. La demostración se puede hacer por reducción al absurdo
- $e = 2,718281828\ldots$ es irracional. Puede hacerse una demostración sencilla sabiendo que

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \ldots\ldots \frac{1}{n!} + \ldots$$

- $\pi = 3,141592654\ldots$ es irracional. Lo demostró Johann Heinrich Lambert (1728-1777) en 1761.

¿Hay conjuntos no numerables?

¿Es $\mathbb{R}$ numerable? NO. Lo demostró Cantor con el «argumento diagonal» siguiente:

Supongamos que $\mathbb{R} = \{x_1, x_2, x_3, x_4, \dots\}$ fuese numerable.
Fijémonos en los dígitos «de la diagonal» de los x_i

$$
\begin{aligned}
x_1 &= n_1, a_1^{(1)} a_2^{(1)} a_3^{(1)} a_4^{(1)} \dots \\
x_2 &= n_2, a_1^{(2)} a_2^{(2)} a_3^{(2)} a_4^{(2)} \dots \\
x_3 &= n_3, a_1^{(3)} a_2^{(3)} a_3^{(3)} a_4^{(3)} \dots \\
x_4 &= n_4, a_1^{(4)} a_2^{(4)} a_3^{(4)} a_4^{(4)} \dots \\
&\dots
\end{aligned}
$$

Construimos $y = 0, b_1 b_2 b_3 b_4 \dots$ tal que $b_i = 2$ si $a_i^{(i)} = 1$ y $b_i = 1$ si $a_i^{(i)} \neq 1$, de manera que $b_i \neq a_i^{(i)}$ y $b \neq x_i$ para todo i.
Entonces b es un número real pero $b \notin \{x_1, x_2, x_3, x_4, \dots\}$, contradicción. **Conclusión: $\mathbb{R}$ no es numerable.**
$|\mathbb{R}| = 2^{\aleph_0}$ **se llama cardinal del continuo.**

¿Es el intervalo $I = (0, 1)$ numerable?

Supongamos que los elementos de $I = (0, 1)$ se pudieran numerar como $x_1, x_2, x_3, \ldots, x_n \ldots$.

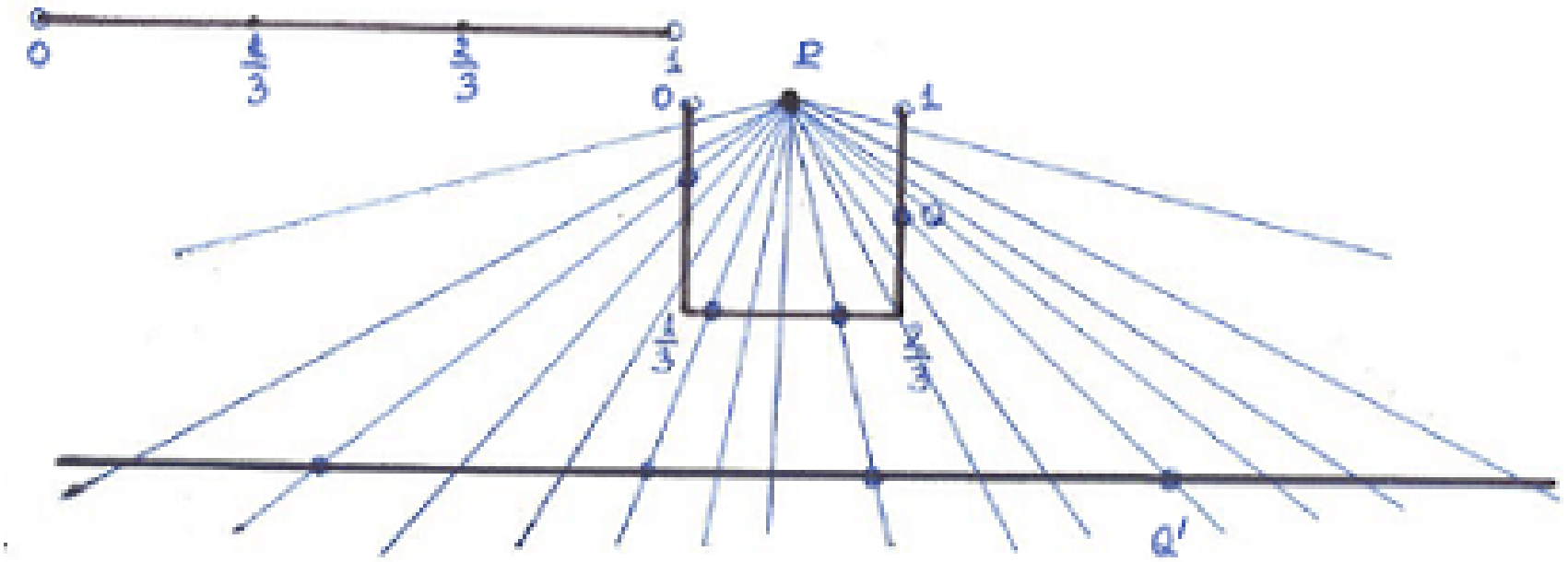
- Colocamos alrededor de x_1 un intervalo I_1 de longitud $1/10$.
- Colocamos alrededor de x_2 un intervalo I_2 de longitud $1/10^2$.
- .....
- Colocamos alrededor de x_n un intervalo I_n de longitud $1/10^n$.
- .....

Los intervalos $I_1, I_2, \ldots, I_n \ldots$ cubren $I = (0, 1)$ (y más). Pero esto es imposible porque $\sum_{n=1}^{\infty} |I_n| = \sum_{n=1}^{\infty} \frac{1}{10^n} = \frac{1}{9} < 1$.

Conclusión: $I = (0, 1)$ no es numerable.

El cardinal del intervalo $I = (0, 1)$.

El conjunto $I = (0, 1)$ está contenido en $\mathbb{R}$ y no es numerable. Luego $\aleph_0 < |I| \leq |\mathbb{R}| = 2^{\aleph_0}$. Sorprende que ambos, I y $\mathbb{R}$, tengan el mismo cardinal. El dibujo siguiente muestra una biyección entre $I = (0, 1)$ y $\mathbb{R}$:



Otra biyección entre $I = (0, 1)$ y $\mathbb{R}$ la da la función

$$y = f(x) = \tan\left(\frac{\pi}{2}(2x - 1)\right), \quad x \in (0, 1).$$

¿Hay conjuntos de otros tamaños?

$|\mathbb{R}| = 2^{\aleph_0}$ **se llama cardinal del continuo.**

- ¿Es $2^{\aleph_0}$ el cardinal siguiente a $\aleph_0$ o existe algún conjunto $\mathcal{S}$ con $\aleph_0 < |\mathcal{S}| < 2^{\aleph_0}$?

- **Hipótesis del continuo: No existe ningún conjunto $\mathcal{S}$ con $\aleph_0 < |\mathcal{S}| < 2^{\aleph_0}$.**

- **¿Es cierta o falsa la Hipótesis del continuo?**
  K. Gödel (1940): no se puede refutar. P. Cohen (1963): no se puede demostrar.
  La Hipótesis del Continuo es independiente de los axiomas de la Teoría de Conjuntos. Se pueden hacer matemáticas con ella o sin ella.

UNA NOCIÓN DISTINTA DE "TAMAÑO": LA DENSIDAD.

Puesto que *Pares* $\subset \mathbb{N}$, **¿Cómo de densos son los pares?**

$$\frac{\#\{n \in \mathbb{N} : n < x,\ n \text{ es par}\}}{\#\{n \in \mathbb{N} : n < x\}} \sim \frac{1}{2}.$$

¿Cómo de densos son los cuadrados?

$$\frac{\#\{n \in \mathbb{N} : n < x, n = m^2\}}{\#\{n \in \mathbb{N} : n < x\}} \sim \frac{\sqrt{x}}{x} = \frac{1}{\sqrt{x}}.$$

¿Cómo de densos son los primos?
Nos lo dice el **Teorema de los Números Primos:**

$$\frac{\#\{n \in \mathbb{N} : n < x,\ n \text{ es primo}\}}{\#\{n \in \mathbb{N} : n < x\}} = \frac{\pi(x)}{x} \sim \frac{x/\ln x}{x} = \frac{1}{\ln x}.$$

Volvamos a la descomposición en primos

Teorema Fundamental de la aritmética (Existencia)

Dado un entero $n > 1$ se puede escribir como

$$n = p_1 p_2 \dots p_r$$

donde $p_1, p_2, \dots . p_r$ son primos, no necesariamente distintos.

Pregunta:

¿Es única la descomposición de un número natural $n \geq 2$ como producto de primos?

Única no es, **pero es única salvo el orden.**

¿Demostración?

Algoritmo de Euclides extendido.

Identidad de Bezout.

Sean $m, n \in \mathbb{N}$ (digamos $m > n$) y sea $d = (m, n)$. El Algoritmo de Euclides permite escribir:

$$d = a \cdot m + b \cdot n \qquad \textbf{con} \quad a, b \in \mathbb{Z}.$$

$$
\begin{array}{ll}
m = q_1 n + r_1, & r_1 = m - q_1 n = a_1 m + b_1 n \\
n = q_2 r_1 + r_2, & r_2 = n - q_2 r_1 = n - q_2(a_1 m + b_1 n) \\
 & = a_2 m + b_2 n \\
r_1 = q_3 r_2 + r_3, & r_3 = r_1 - q_3 r_2 = (a_1 m + b_1 n) - q_3(a_2 m + b_2 n) \\
 & = a_3 m + b_3 n \\
\ldots & \ldots \\
r_{k-2} = q_k r_{k-1} + r_k, & r_k = r_{k-2} - q_k r_{k-1} = \cdots = a_k m + b_k n \\
r_{k-1} = q_{k+1} r_k + 0, & r_k = d = (m, n) = a_k m + b_k n = am + bn
\end{array}
$$

EJEMPLO:

Sean $m = 1292573, n = 1285667$ y $d = (m, n)$.
Encontrar enteros a, b tales que

$$d = a \cdot 1292573 + b \cdot 1285667.$$

COROLARIO 1:

Dos números enteros x e y, no nulos, son primos entre sí $\Leftrightarrow$ exiten $u, v \in \mathbb{Z}$ tales que $ux + vy = 1$.

COROLARIO 2:

Sean $p, x, y \in \mathbb{N}$ tales que p es primo y $p|xy$. Entonces $p|x$ ó $p|y$.

COROLARIO:

La descomposición de un número natural $n \geq 2$ como producto de primos es única salvo el orden.