Aritmética I

Eugenio Hernández

COMPLEMENTOS DE MATEMÁTICAS PARA LA EDUCACIÓN SECUNDARIA
Curso 2017-2018

Una fórmula bien conocida

Demostrar que para todo número natural $n \geq 1$

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

Demostración por inducción.

El principio de inducción se basa en los **Axiomas de Peano**, que caracterizan el conjunto $\mathbb{N}$ de los números naturales.

Axiomas de Peano (relación $=$, más...)

1. $0 \in \mathbb{N}$.
2. Existe una función $S : \mathbb{N} \to \mathbb{N}$. Es decir, para cada $n \in \mathbb{N}$ existe un único $S(n) \in \mathbb{N}$, el **sucesor de** n.
3. Para todo $n \in \mathbb{N}$, $S(n) \neq 0$
4. $S(m) = S(n) \Longrightarrow m = n$. Es decir, S es inyectiva.
5. **El axioma de inducción** Si $K \subset \mathbb{N}$ es un subconjunto tal que
   - $0 \in K$,
   - para todo $n \in \mathbb{N}$, si $n \in K \Longrightarrow S(n) \in K$,

   entonces $\mathbb{N} = K$.

¿Qué podemos demostrar por inducción?

Por inducción podemos demostrar **fórmulas**:

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

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

$$\sum_{k=1}^{n} (k \cdot k!) = (n+1)! - 1.$$

Desigualdades: Para todo entero $n > 4$ se tiene $2^n > n^2 + 1$. (Ejercicio)

Teoremas: Si A es un conjunto finito con $Card(A) = n$ entonces A tiene 2^n subconjuntos.

Y también podemos demostrar por inducción

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.

- ¿Y $n = 0$?
- ¿$n = 1$?
- ¿Qué es un primo? ¿Es 1 primo?
- ¿Y si $n \in \mathbb{Z}$ es quizás negativo?

Descomposición en la práctica

Ejemplos: $n_1 = 1306800$; $n_2 = 1327103$

$$n_1 = 2^4 \cdot 3^3 \cdot 5^2 \cdot 11^2$$

$$n_2 = 1151 \cdot 1153$$

No es sólo cuestión de tamaños, pero el tamaño importa.

- **¿Es fácil encontrar primos?** **SÍ**
- **¿Es fácil factorizar?** **NO**

DEFINICIÓN VS CÁLCULO

- **¿Cómo se definen** $(m, n) := m.c.d.(m, n)$ **y** $[m, n] := m.c.m.(m, n)$**?**
- **¿Cómo se calculan** (m, n) **y** $[m, n]$

Ejemplo 1:

$$m_1 = 1306800 = 2^4 \cdot 3^3 \cdot 5^2 \cdot 11^2, \quad n_1 = 292500 = 2^2 \cdot 3^2 \cdot 5^4 \cdot 13$$

Ejemplo 2:

$$m_2 = 1292573, \qquad n_2 = 1285667$$

¿Cómo calculo (m_2, n_2) si no puedo factorizar?

¡Usando el Algoritmo de Euclides!

Algoritmo de Euclides.

Lema 1

Si a y b son dos números naturales no nulos tales que $a = qb + r$, entonces $(a, b) = (b, r)$

Lema 2

Si a y b son dos números naturales no nulos tales que $b|a$ (es decir, b divide a a), entonces $(a, b) = b$

Ejercicio 1: Usar los lemas 1 y 2 para hallar el máximo común divisor de 441 y 24 sin factorizar los números.

Ejercicio 2: Usar los lemas 1 y 2 para hallar el máximo común divisor de $5k + 3$ y $3k + 2$, donde k es cualquier número entero positivo.

Algoritmo de Euclides.

Sean $m, n \in \mathbb{N}$ (digamos $m > n$). Dividamos sucesivamente con restos pequeños:

$$
\begin{array}{ll}
m = q_1 n + r_1, & 0 \leq r_1 < n \\
n = q_2 r_1 + r_2, & 0 \leq r_2 < r_1 < n \\
r_1 = q_3 r_2 + r_3, & 0 \leq r_3 < r_2 < r_1 < n \\
\ldots & \ldots \\
\text{En algún momento} & \\
r_{k-2} = q_k r_{k-1} + r_k, & 0 \leq r_k < \cdots < r_3 < r_2 < r_1 < n \\
r_{k-1} = q_{k+1} r_k + 0 &
\end{array}
$$

Pero entonces, por los lemas 1 y 2:

$$(m.n) = (n, r_1) = (r_1, r_2) = \cdots = (r_{k-2}, r_{k-1}) = (r_{k-1}, r_k) = r_k.$$

Ejercicio 3: usar el algoritmo de Euclides para hallar el máximo común divisor de los números

$$m = 1292573, \qquad \text{y} \qquad n = 1285667$$

Infinitos

Dos demostraciones por reducción al absurdo. Supongamos que el conjunto de los primos fuese finito:

$$\mathcal{P} = \{p_1, p_2, \ldots, p_s\}.$$

PRIMERA DEMOSTRACIÓN (EUCLIDES; BASADA EN LA EXISTENCIA DE FACTORIZACIÓN)

$$p_1 p_2 \ldots p_s + 1.$$

SEGUNDA DEMOSTRACIÓN (BASADA EN LA FACTORIZACIÓN ÚNICA)

$$\prod_{i=i}^{s} \frac{p_i}{p_i - 1} = \sum_{k=1}^{\infty} \frac{1}{k}.$$

¿Cuántos números primos hay?

- ¿Menos que enteros?
- ¿Más o menos que pares?
- ¿Más o menos que cuadrados?
- ¿Menos que racionales?
- ¿Menos que reales?

Empresas Turísticas Hilbert.

El Sr. Hilbert tiene un hotel cuyas habitaciones están numeradas usando TODOS los números naturales. Es una noche de tormenta y el hotel está lleno. Llega un viajero aterido de frío buscando refugio. ¿Podrá el Sr. Hilbert acomodarle (sin hacer compartir habitación a los huéspedes)?

Tras alojar al viajero, el Sr. Hilbert vuelve a recepción y descubre que le esperan los viajeros de uno de los autobuses que gestiona él mismo. Los autobuses de Hilbert tienen asientos numerados usando TODOS los números naturales, y este autobús en concreto ha llegado completamente lleno. ¿Podrá el Sr. Hilbert acomodar en su hotel a todos los pasajeros del autobús (de nuevo, sin hacer compartir habitación a los huéspedes)?

La paradoja de Galileo

En su libro *Discorsi e dimostrazioni matematiche intorno a due nuove scienze* (1638), Galileo Galilei emparejó los números 1, 2, 3, 4 , ... con los cuadrados 1, 4, 9 , 16, ...; cada núnero genera un cuadrado distinto -el 2 genera el 4, el 3 el 9, el 4 el 16, etc.- y a su vez cada cuadrado viene generado por un único número.

Podemos emparejar los números con sus cuadrados concluyendo que habrá tantos cuadrados como números; pero es de todo punto obvio que los números cuadrados son solo una parte de los enteros y, en consecuencia, concluimos que hay más números que cuadrados -el todo es mayor que la parte-.

Nos encontramos con la paradoja de que los números son, a la vez, tantos y más que los cuadrados. Galileo concluia que los ”atributos de *mayor, menor e igual* no se aplican a los infinitos”.

Antonio Machado. *Juan de Mairena*. (1936). **Los enigmas de lo infinito.**

La serie par es la mitad de la serie total de los números. La serie impar es la otra mitad.
Pero la serie par y la serie impar son —ambas— infinitas.
La serie total de los números es también infinita. ¿Será entonces doblemente infinita que la serie par y que la serie impar?
No parece aceptable, en buena lógica, que lo infinito pueda duplicarse, como, tampoco, que pueda partirse en mitades.
Luego la serie par y la serie impar son ambas, y cada una, iguales a la serie total de los números.
No es tan claro, pues, como vosotros pensáis, que el todo sea mayor que la parte.
Meditad con ahínco, hasta hallar en qué consiste lo sofístico de este razonamiento.
Y cuando os hiervan los sesos, avisad.

¿Cuándo tienen dos conjuntos la misma cantidad de elementos?

Si son pequeños, contamos. Pero si son grandes, es más rápido emparejar.

Definición

Diremos que dos conjuntos A y B tienen el mismo cardinal (la misma cantidad de elementos), o son equipotentes, $A \approx B$, si existe una biyección $A \longleftrightarrow B$ entre el conjunto A y el conjunto B.

Definición

Un conjunto es numerable si tiene el mismo cardinal que el conjunto de los números naturales. El cardinal de los conjuntos numerables se denota por $\aleph_0$.

Algunos ejemplos de conjuntos numerables.

- (El Hotel de Hilbert) Los naturales con/sin el 0.
- (Juan de Mairena) Los números pares.
- (Galileo) Los cuadrados.
- (El autobus de Hilbert que llega al hotel de Hilbert) Los enteros.
- (Nuestra primera pregunta) ¿Y los números primos?

Hay infinitos primos, los naturales son «el infinito más pequeño», los primos están dentro de los naturales,...
Cualquier subconjunto infinito de un conjunto numerable es numerable, ¡porque no puede ser más pequeño!
En particular, el conjunto $\mathcal{P}$ de primos es **numerable**. Es decir

- $Card(\mathcal{P}) = \aleph_0$.
- Hay la misma cantidad de primos que de naturales, o que de pares, o que de cuadrados, o que de enteros.

¿Cuántos divisores tiene un número natural n?

Está relacionado con la descomposición de n como producto de primos.

Sea $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$. ¿Cómo son sus divisores?

$$d \text{ divide a } n \iff d = p_1^{f_1} p_2^{f_2} \dots p_r^{f_r}, \text{ con } 0 \leq f_i \leq e_i.$$

¿Cuántos de estos d hay?

$$(e_1 + 1)(e_2 + 1) \dots (e_r + 1).$$

En esta cuenta hemos usado que la factorización como producto de primos es ÚNICA. ¿Lo es realmente?