# Aritmética I

Adolfo Quirós

COMPLEMENTOS PARA LA FORMACIÓN DISCIPLINAR EN MATEMÁTICAS
Curso 2012-2013

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

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

**Demostración por inducción.**

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

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. $S(m) = S(n) \implies m = n$. 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 $n \in K \implies S(n) \in K$,

   entonces $\mathbb{N} \subset K$.

# ¿QUÉ PODEMOS DEMOSTRAR POR INDUCCIÓN?

Por inducción podemos demostrar **fórmulas**:

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

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

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

**Desigualdades:** Para todo entero $n>4$ se tiene $2^n>n^2+1$.
**Teoremas:** Si $A$ es un conjunto finito con $Card(A)=n$ entonces $A$ tiene $2^n$ subconjuntos.
**Cosas extrañas:** Dado un conjunto $C$ de caballos todos los caballos de $C$ son del mismo color.

Y también

**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?

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

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

$$n_2 = 1151 \cdot 1153$$

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

- **¿Es fácil encontrar primos?**
- **¿Es fácil factorizar?**

### 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!**

**¿Menos que enteros?**

**¿Más o menos que pares?**

**¿Más o menos que cuadrados?**

**¿Menos que racionales?**

**¿Menos que reales?**

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)?

# GALILEO GALILEI. *Discorsi e dimostrazioni matematiche intorno a due nuove scienze* (1638)

**Salviati:** [...] Onde se io dirò, i numeri tutti, comprendendo i quadrati e i non quadrati, esser più che i quadrati soli, dirò proposizione verissima: non è così?

**Simplicio:** Non si può dir altrimenti.

**Salviati:** Interrogando io di poi, quanti siano i numeri quadrati, si può con verità rispondere, loro esser tanti quante sono le proprie radici, avvenga che ogni quadrato ha la sua radice, ogni radice il suo quadrato, né quadrato alcuno ha più d'una sola radice, né radice alcuna più d'un quadrato solo.

**Simplicio:** Così sta.

**Salviati:** Ma se io domanderò, quante siano le radici, non si può negare che elle non siano quante tutti i numeri, poiché non vi è numero alcuno che non sia radice di qualche quadrato; e stante questo, converrà dire che i numeri quadrati siano quanti tutti i numeri, poiché tanti sono quante le lor radici, e radici son tutti i numeri: e pur da principio dicemmo, tutti i numeri esser assai più che tutti i quadrati, essendo la maggior parte non quadrati.[...]

## 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

$$A \longleftrightarrow B.$$

(Así, un cardinal es una clase de equivalencia de conjuntos bajo esta relación. ).

### 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.

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 del Número Primo.**

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

Ya sabemos que hay igual de primos, de pares o de cuadrados que números naturales: **todos estos conjuntos son numerables**.

- **¿Hay más números racionales que números enteros?**
- ¿Cuál es el cardinal del producto de dos conjuntos numerables? ¿Y el cardinal de una unión numerable de conjuntos numerables? (¿Qué hacer si llega al Hotel de Hilbert una flota de Hilbert de autobuses de Hilbert?)
- Los segmentos $(0, 1), (-1, 1), (-2, 2), (a, b)$.
- Los segmentos $(0, 1), [0, 1), (0, 1], [0, 1]$.
- $(0, 1)$ vs. $\mathbb{R}$, la recta real.
- **¿Es $\mathbb{R}$ numerable? NO. Lo demostró Cantor con el «argumento diagonal».**

**¿Cuántos números complejos hay?**

**¿Cuántos números algebraicos?**

# El próximo día. . .

**¿Es la descomposición como producto de primos única?**