

ARITMÉTICA II

Adolfo Quirós

COMPLEMENTOS PARA LA FORMACIÓN DISCIPLINAR
EN MATEMÁTICAS
Curso 2010-2011

LA ÚLTIMA PREGUNTA DEL OTRO DÍA: ¿CUÁNTOS NÚMEROS PRIMOS HAY?

Si nos referimos al **cardinal** del conjunto \mathcal{P} de primos, que denotaremos por $Card(\mathcal{P})$ o por $\#\mathcal{P}$, hay los mismos que números naturales, \mathbb{N} , una cantidad **numerable**.

Este cardinal se denota por \aleph_0 y $Card(\mathcal{P}) = \aleph_0$ no significa otra cosa que la existencia de una biyección:

$$\mathbb{N} \longleftrightarrow \mathcal{P}.$$

Cualquier subconjunto infinito de un conjunto numerable es numerable, ¡porque no puede ser más pequeño!

Pero $\mathcal{P} \subsetneq \mathbb{N}$, y tiene sentido preguntarse: **¿cómo de denso es?**

¿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 enteros que números naturales?
(Ahora $\mathbb{N} \subset \mathbb{Z}$.)

¿Hay más números racionales que números enteros?

¿Hay más números reales que números racionales?

¿Números complejos?

¿Números algebraicos?

VOLVAMOS A LA DESCOMPOSICIÓN COMO PRODUCTO DE PRIMOS

PREGUNTA:

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

¿De cuántas maneras podemos descomponerlo?

Única no es: $30 = 2 \cdot 3 \cdot 5 = 3 \cdot 5 \cdot 2 = 2 \cdot 5 \cdot 3 = \dots$

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:

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

$$m = q_1 n + r_1,$$

$$r_1 = m - q_1 n = a_1 m + b_1 n$$

$$n = q_2 r_1 + r_2,$$

$$r_2 = n - q_2 r_1 = n - q_2(a_1 m + b_1 n) \\ = a_2 m + b_2 n$$

$$r_1 = q_3 r_2 + r_3,$$

$$r_3 = r_1 - q_3 r_2 = (a_1 m + b_1 n) - q_3(a_2 m + b_2 n) \\ = a_3 m + b_3 n$$

...

...

$$r_{k-2} = q_k r_{k-1} + r_k,$$

$$r_k = r_{k-2} - q_k r_{k-1} = \dots = a_k m + b_k n$$

$$r_{k-1} = q_{k+1} r_k + 0,$$

$$r_k = d = (m, n) = a_k m + b_k n = am + bn$$

EJEMPLO:

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

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

APLICACIÓN:

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.

Si ahora son las 7, ¿qué hora será dentro de 19 horas?

$$7 + 19 = 26 = 2 \cdot 12 + 2 = 2$$

Ignoramos los múltiplos de 12.

DEFINICIÓN:

Dos números enteros m, n son **congruentes módulo 12** \iff
Al dividirlos entre 12, m y n dan el mismo resto, $0 \leq r < 12$
 $\iff 12 \mid m - n$. Se escribe $m \equiv n \pmod{12}$ o $m \equiv n(12)$.

$$\begin{aligned} \text{EJEMPLOS : } \quad 12 &\equiv 0 \equiv 24 \equiv -12 \equiv -36 \pmod{12} \\ 19 &\equiv 7 \equiv 31 \equiv -5 \equiv -17 \pmod{12} \end{aligned}$$

$\equiv \pmod{12}$ define una **relación de equivalencia** y cualquier entero se puede **representar** por un número en $\{0, \dots, 11\}$, los restos al dividir entre 12.

ESTO SE PUEDE GENERALIZAR A OTROS MÓDULOS

SEA $N \geq 2$ UN ENTERO.

Dos números enteros m, n son **congruentes módulo N** \iff
Al dividirlos entre N , m y n dan el mismo resto, $0 \leq r < N$
 $\iff N \mid m - n$. Ponemos $m \equiv n \pmod N$ o $m \equiv n(N)$.

EJEMPLOS: $23 \equiv 3 \pmod{10}$, $-7 \equiv 3 \pmod{10}$,

$28 \equiv 2 \pmod{13}$, $-28 \equiv 11 \pmod{13}$.

Todo entero es equivalente módulo N a un número en $\{0, \dots, N - 1\}$, los restos al dividir entre N .

Este conjunto, visto así, se denota por \mathbb{Z}/N .

ARITMÉTICA MODULAR:

Los restos módulo N se pueden **sumar**:

$$8 + 9 \equiv 17 \equiv 4 \pmod{13}, \quad 13 + 22 \equiv 35 \equiv 5 \pmod{30}.$$

restar:

$$11 - 5 \equiv 6 \pmod{13}, \quad 3 - 8 \equiv -5 \equiv 8 \pmod{13},$$

$$13 - 22 \equiv -9 \equiv 21 \pmod{30}.$$

multiplicar:

$$11 \cdot 5 \equiv 55 \equiv 3 \pmod{13}, \quad 13 \cdot 22 \equiv 286 \equiv 16 \pmod{30}.$$

pero no siempre se puede **dividir**:

$$x \equiv \frac{2}{3} \pmod{6} \iff 3 \cdot x \equiv 2 \pmod{6}.$$

PROPOSICIÓN.

Existe $\frac{1}{n} \in \mathbb{Z}/N \iff (n, N) = 1$. En ese caso $\frac{1}{n} \pmod{N}$ se puede calcular usando la identidad de Bezout.

UNA APLICACIÓN: EL CÓDIGO DE BARRAS (VERSIÓN EAN=EUROPEAN ARTICLE NUMBER)

$$a_0 - a_1 a_2 a_3 a_4 a_5 a_6 - a_7 a_8 a_9 a_{10} a_{11} a_{12}$$

tal que

$$(a_0 + a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12}) + 3(a_1 + a_3 + a_5 + a_7 + a_9 + a_{11}) \equiv 0 \pmod{10}.$$

El dígito a_{12} es un **dígito de control**, c , que se pone para que la operación anterior sea un múltiplo de 10.

Halla el dígitos de control de los códigos de barras siguientes:

Leche Lauki entera: 8-414700-01101c

Leche Lauki semidesnatada: 8-414700-01102c

Coca-Cola: 5-449000-00099c

¿Son correctos los códigos de barras siguientes?

9-788748-290208

8-410240-210402

¿Es capaz el EAN de detectar cualquier error en un dígito? ¿Es capaz de corregirlo?

¿Es capaz de detectar el intercambio de dos dígitos?

¿Y de dos dígitos en posiciones consecutivas?

Sirve para alguna cosa más, útil en combinación con las barras en sí.

Halla el número borrado en los siguientes códigos de barras:

Vichy Catalán: 8-410?49-001107

Zumo Minute Made: 5-449000-03?895