Aritmética II

Adolfo Quirós

COMPLEMENTOS PARA LA FORMACIÓN DISCIPLINAR
EN MATEMÁTICAS
Curso 2012-2013

Lo que teníamos pendiente del otro día

¿Hay más números reales que números racionales?

¿Números complejos?

¿Números algebraicos?

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

¿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

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

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, $0 \leq r < 12$ $\iff$ $12|m-n$. Se escribe $m \equiv n \bmod 12$ o $m \equiv n\,(12)$.

EJEMPLOS : $12 \equiv 0 \equiv 24 \equiv -12 \equiv -36 \bmod 12$

$19 \equiv 7 \equiv 31 \equiv -5 \equiv -17 \bmod 12$

$\equiv \bmod 12$ define una **relación de equivalencia** y cualquier entero se puede **representar** por un número en $\{0, \ldots, 11\}$, 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, $0 \leq r < N$
$\iff$ $N | m - n$. Ponemos $m \equiv n \bmod N$ o $m \equiv n\,(N)$.

EJEMPLOS: $23 \equiv 3 \bmod 10$, $\quad -7 \equiv 3 \bmod 10$,

$28 \equiv 2 \bmod 13$, $\quad -28 \equiv 11 \bmod 13$.

Todo entero es equivalente módulo N a un número en $\{0, \ldots, N-1\}$, los restos al dividir entre N.
Este conjunto, visto así, se denota por $\mathbb{Z}/N$.

Los restos módulo N se pueden **sumar**:
$8 + 9 \equiv 17 \equiv 4 \bmod 13, \quad 13 + 22 \equiv 35 \equiv 5 \bmod 30.$

restar:
$11 - 5 \equiv 6 \bmod 13, \quad 3 - 8 \equiv -5 \equiv 8 \bmod 13,$
$13 - 22 \equiv -9 \equiv 21 \bmod 30.$

multiplicar:
$11 \cdot 5 \equiv 55 \equiv 3 \bmod 13, \quad 13 \cdot 22 \equiv 286 \equiv 16 \bmod 30.$

pero no siempre se puede **dividir**:
$x \equiv \frac{2}{3} \bmod 6 \iff 3 \cdot x \equiv 2 \bmod 6.$

PROPOSICIÓN.

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

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

$$a_0 - a_1a_2a_3a_4a_5a_6 - a_7a_8a_9a_{10}a_{11}a_{12}$$

tal que

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

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

Los códigos de barras detectan errores.

¿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?

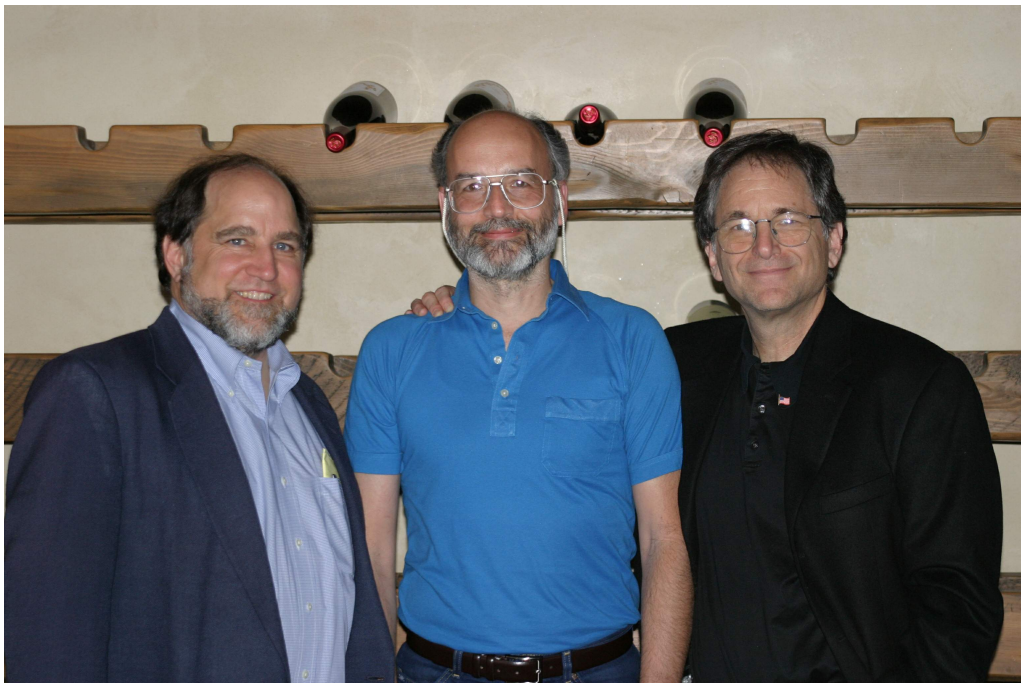
¿Y de dos dígitos en posiciones consecutivas?

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

Otra aplicación: criptografía de clave pública

El otro día vimos que encontrar dos números primos p y q de 150 cifras es fácil. Pero si nos dan un número n de 300 cifras y nos dicen que es producto de dos de esos p, q no vamos a ser capaces de factorizarlo.

Esta es la base del criptosistema RSA.



R. Rivest, A. Shamir, L. Adleman (2003)

Otra aplicación: criptografía de clave pública

El otro día vimos que encontrar dos números primos p y q de 150 cifras es fácil. Pero si nos dan un número n de 300 cifras y nos dicen que es producto de dos de esos p, q no vamos a ser capaces de factorizarlo.

Esta es la base del criptosistema RSA.

A. Shamir, R. Rivest, L. Adleman (1977)

$\mathcal{M}$ = mensajes en claro; $\mathcal{C}$ = mensajes cifrados

Función para cifrar $f_e : \mathcal{M} \longrightarrow \mathcal{C}$. Tiene que ser **inyectiva**.
Depende de una clave para cifrar **e**.

La correspondiente función para descifrar $f_d^{-1} : \mathcal{C} \longrightarrow \mathcal{M}$
depende de una clave para descifrar **d**.

Normalmente si se conoce e se conoce d, y viceversa, y por tanto hay que mantener ambas secretas.

Imaginad ahora que la función f_e es de un sólo sentido: sabemos que tiene inversa pero no sabemos cómo calcularla.

Dicho de otro modo: conocer la clave para cifrar e no permite averiguar la clave para descifrar d.

Entonces yo puedo **PUBLICAR** la clave e.

Quien quiera enviarme un mensaje m lo cifrará y, en lugar de m, me enviará $c := f_e(m)$.

Sólo yo conozco d y sólo yo puedo leer

$$f_d^{-1}(c) = f_d^{-1}(f_e(m)) = m.$$

¿Cómo funciona RSA? 1. Las claves

1. Cada usuario $A, B, C, \ldots$ encuentra dos primos grandes p, q [fácil].

2. Encuentra un entero e con $mcd(e, (p-1)(q-1)) = 1$ y calcula d tal que

$$ed \equiv 1 \bmod (p-1)(q-1),$$

es decir, $ed = 1 + k(p-1)(q-1)$ [fácil, Algoritmo de Euclides].

3. Calcula n=pq.

4. Publica su clave para cifrar $(\mathbf{n}, \mathbf{e})$ y mantiene oculta la clave para descifrar **d**.

5. Para escribirle, se transforman los mensajes en enteros $m, 0 \leq m \leq n-1$, es decir, elementos de $\mathbb{Z}/n$.
6. La función para cifrar es $f_e(m) = m^e \bmod n$ [fácil].
7. La función para descifrar es $f_d^{-1}(c) = c^d \bmod n$ [fácil, siempre que conozcamos d].
8. Gracias al Pequeño Teorema de Fermat

$$f_d^{-1}(f_e(m)) = m^{ed} \equiv m \bmod n.$$

9. Para romper la clave [encontrar d a partir de (n, e)] hay que calcular $(p-1)(q-1)$, lo que requiere factorizar $n = pq$. ¡IMPOSIBLE!

UN EJEMPLO: LA ESTRUCTURA

- Partimos de mensajes escritos en un alfabeto de 30 letras para los que damos equivalentes numéricos:
  A=0, B=1, C=2, D=3, E=4, F=5, G=6, H=7, I=8, J=9, K=10, L=11, M=12, N=13,Ñ=14, O=15, P=16, Q=17, R=18, S=19, T=20, U=21, V=22, W=23, X=24, Y=25, Z=26, espacio en blanco=27, ¿=28, ?=29
- Los mensajes en claro van a ser digrafos =palabras de 2 letras=números de 2 cifras en base 30.
- Los mensajes cifrados serán trigrafos =palabras de 3 letras=números de 3 cifras en base 30.
- Necesitamos que $900 = 30^2 < n < 30^3 = 27000$ para que

$$\mathcal{M} \subset \mathbb{Z}/n \xrightarrow{f_e} \mathbb{Z}/n \subset \mathcal{C}$$

Adolfo publica la clave $(n, e) = (24613, 6943)$ y recibe ZVQ. ¿Qué le dicen?

1. Factorizar $n = 24613$. [PISTA: son dos factores próximos. TÉCNICA: método de Fermat, $n = x^2 - y^2$.]

$$n = 151 \cdot 163$$

2. Calcular $d = 1/e \bmod (p-1)(q-1)$.[TÉCNICA: Algoritmo de Euclides.]

$$d = 1/6943 \bmod 24300 = 7.$$

3. $ZVQ = 26 \cdot 30^2 + 22 \cdot 30 + 17 = 24077 < 30^3 = 27000$.
4. $f_d^{-1}(ZVQ) = 24077^7 \bmod 24613 = 578 < 30^2 = 900$.
5. $578 = 19 \cdot 30 + 8 =$**SÍ**.

UN PRIMO REALMENTE GRANDE

$$2^{57885161} - 1$$

- Tiene 17.425.170 cifras.
- Es el primo más grande conocido.
- Se descubrió el 25 de enero de 2013.