Criptografía

Estímulo del Talento Matemático

Real Academia de Ciencias

30 de julio de 2003

La aritmética del reloj

Fijamos un cierto número natural: por ejemplo, 12. Y "contamos" como si estuviéramos con un reloj de manecillas. Las posibles "horas" son, por ejemplo, los números del 0 al 11.

Escribe aquí la "hora" $\longrightarrow$	0	6	11	12	15	123	-11

Lo que estamos haciendo es dividir (división entera) el número en cuestión entre 12, y quedarnos con el resto.

Podemos cambiar el reloj; por ejemplo, para el reloj de **dos** posiciones (que solo marca ceros y unos):

Escribe aquí la "hora" $\longrightarrow$	0	6	11	12	15	123	-11

O para el de **cinco**:

Escribe aquí la "hora" $\longrightarrow$	0	6	11	12	15	123	-11

En general, elegiremos un número n y diremos que estamos trabajando **módulo** n.

Operaciones módulo n

Sumar:

$3+3$	$\equiv$	(mod 7)	$9+13$	$\equiv$	(mod 10)
$-6+7$	$\equiv$	(mod 4)	$11+13$	$\equiv$	(mod 53)
$14+3$	$\equiv$	(mod 7)	$9+9$	$\equiv$	(mod 2)

Multiplicar:

3×3	$\equiv$	(mod 7)	9×13	$\equiv$	(mod 10)
-6×7	$\equiv$	(mod 4)	11×13	$\equiv$	(mod 53)
14×3	$\equiv$	(mod 7)	9×9	$\equiv$	(mod 2)

¿Y dividir? Ya sabemos que, dentro de los enteros, no siempre se puede dividir. Pensemos en los racionales: ¿qué quiere decir que

$$\frac{12}{3}=4? \quad \text{En realidad, es } 12\times\frac{1}{3}=4$$

Lo especial del $1/3$ es que es el número racional tal que $3\times\frac{1}{3}=1$.

Ahora estamos módulo 7. Encontrar los números x tales que

$$1x\equiv 1 \quad 2x\equiv 1 \quad 3x\equiv 1 \quad 4x\equiv 1 \quad 5x\equiv 1 \quad 6x\equiv 1 \quad 7x\equiv 1$$

¿Y si fuera módulo 6?

$$1x\equiv 1 \quad 2x\equiv 1 \quad 3x\equiv 1 \quad 4x\equiv 1 \quad 5x\equiv 1 \quad 6x\equiv 1$$

¿Sabrías decir cuándo un número m tiene inverso módulo n?

Cálculo de potencias

Queremos calcular cantidades del tipo 2^{45}, 14^{346}, $(-13)^{23}$ módulo un cierto n.

Por ejemplo, calculemos 2^{45} módulo 9.

$$\begin{array}{lccccccccc} & 2 & 2^2 & 2^3 & 2^4 & 2^5 & 2^6 & 2^7 & \cdots \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ \text{módulo } 9 \longrightarrow & & & & & & & & \end{array}$$

¿Ocurre algo que simplifique el cálculo? Veamos otros ejemplos:

$$\begin{array}{lccccccccc} & 2 & 2^2 & 2^3 & 2^4 & 2^5 & 2^6 & 2^7 & \cdots \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ \text{módulo } 7 \longrightarrow & & & & & & & & \end{array}$$

$$\begin{array}{lccccccccc} & 5 & 5^2 & 5^3 & 5^4 & 5^5 & 5^6 & 5^7 & \cdots \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ \text{módulo } 7 \longrightarrow & & & & & & & & \end{array}$$

¿Ocurrirá siempre, sea cual sea la cuenta que hagamos?

Periodicidad y patrones

Suma. Estamos en módulo 7. Y calculamos

$2+0\equiv$	$3+0\equiv$	$5+0\equiv$
$2+1\equiv$	$3+1\equiv$	$5+1\equiv$
$2+2\equiv$	$3+2\equiv$	$5+2\equiv$
$2+3\equiv$	$3+3\equiv$	$5+3\equiv$
$2+4\equiv$	$3+4\equiv$	$5+4\equiv$
$2+5\equiv$	$3+5\equiv$	$5+5\equiv$
$2+6\equiv$	$3+6\equiv$	$5+6\equiv$
$2+7\equiv$	$3+7\equiv$	$5+7\equiv$
$2+8\equiv$	$3+8\equiv$	$5+8\equiv$

Ahora en módulo 12:

$2+0\equiv$	$3+0\equiv$	$5+0\equiv$
$2+1\equiv$	$3+1\equiv$	$5+1\equiv$
$2+2\equiv$	$3+2\equiv$	$5+2\equiv$
$2+3\equiv$	$3+3\equiv$	$5+3\equiv$
$2+4\equiv$	$3+4\equiv$	$5+4\equiv$
$2+5\equiv$	$3+5\equiv$	$5+5\equiv$
$2+6\equiv$	$3+6\equiv$	$5+6\equiv$
$2+7\equiv$	$3+7\equiv$	$5+7\equiv$
$2+8\equiv$	$3+8\equiv$	$5+8\equiv$
$2+9\equiv$	$3+9\equiv$	$5+9\equiv$
$2+10\equiv$	$3+10\equiv$	$5+10\equiv$
$2+11\equiv$	$3+11\equiv$	$5+11\equiv$
$2+12\equiv$	$3+12\equiv$	$5+12\equiv$
$2+13\equiv$	$3+13\equiv$	$5+13\equiv$

Producto. En módulo 7, de nuevo, calculamos

$2 \times 0 \equiv$	$3 \times 0 \equiv$	$5 \times 0 \equiv$
$2 \times 1 \equiv$	$3 \times 1 \equiv$	$5 \times 1 \equiv$
$2 \times 2 \equiv$	$3 \times 2 \equiv$	$5 \times 2 \equiv$
$2 \times 3 \equiv$	$3 \times 3 \equiv$	$5 \times 3 \equiv$
$2 \times 4 \equiv$	$3 \times 4 \equiv$	$5 \times 4 \equiv$
$2 \times 5 \equiv$	$3 \times 5 \equiv$	$5 \times 5 \equiv$
$2 \times 6 \equiv$	$3 \times 6 \equiv$	$5 \times 6 \equiv$
$2 \times 7 \equiv$	$3 \times 7 \equiv$	$5 \times 7 \equiv$
$2 \times 8 \equiv$	$3 \times 8 \equiv$	$5 \times 8 \equiv$

Ahora en módulo 12:

$2 \times 0 \equiv$	$3 \times 0 \equiv$	$5 \times 0 \equiv$
$2 \times 1 \equiv$	$3 \times 1 \equiv$	$5 \times 1 \equiv$
$2 \times 2 \equiv$	$3 \times 2 \equiv$	$5 \times 2 \equiv$
$2 \times 3 \equiv$	$3 \times 3 \equiv$	$5 \times 3 \equiv$
$2 \times 4 \equiv$	$3 \times 4 \equiv$	$5 \times 4 \equiv$
$2 \times 5 \equiv$	$3 \times 5 \equiv$	$5 \times 5 \equiv$
$2 \times 6 \equiv$	$3 \times 6 \equiv$	$5 \times 6 \equiv$
$2 \times 7 \equiv$	$3 \times 7 \equiv$	$5 \times 7 \equiv$
$2 \times 8 \equiv$	$3 \times 8 \equiv$	$5 \times 8 \equiv$
$2 \times 9 \equiv$	$3 \times 9 \equiv$	$5 \times 9 \equiv$
$2 \times 10 \equiv$	$3 \times 10 \equiv$	$5 \times 10 \equiv$
$2 \times 11 \equiv$	$3 \times 11 \equiv$	$5 \times 11 \equiv$
$2 \times 12 \equiv$	$3 \times 12 \equiv$	$5 \times 12 \equiv$
$2 \times 13 \equiv$	$3 \times 13 \equiv$	$5 \times 13 \equiv$

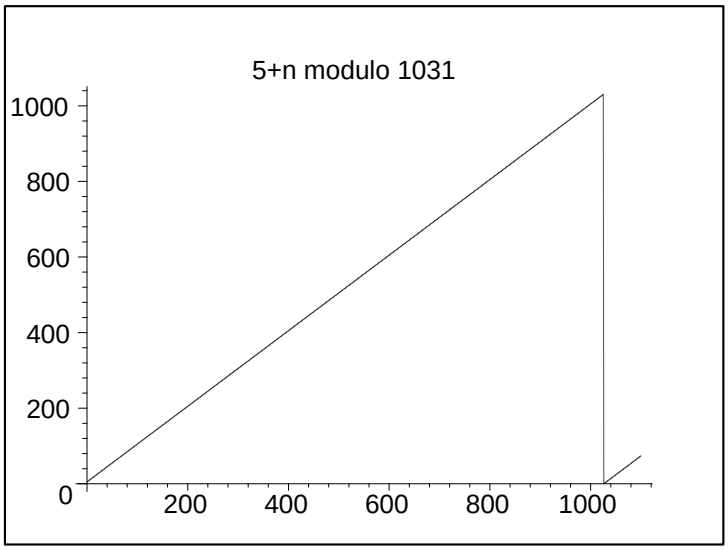
Vamos con las **potencias**. En módulo 7, de nuevo, calculamos

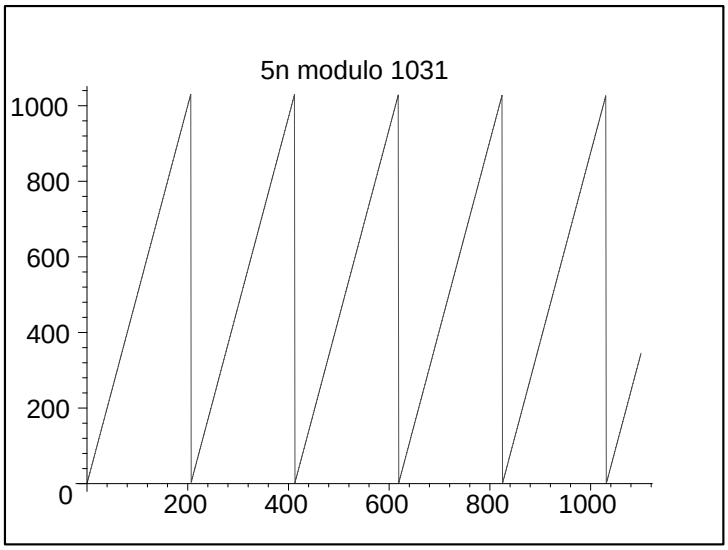
$2^0 \equiv$	$3^0 \equiv$	$5^0 \equiv$	$6^0 \equiv$
$2^1 \equiv$	$3^1 \equiv$	$5^1 \equiv$	$6^1 \equiv$
$2^2 \equiv$	$3^2 \equiv$	$5^2 \equiv$	$6^2 \equiv$
$2^3 \equiv$	$3^3 \equiv$	$5^3 \equiv$	$6^3 \equiv$
$2^4 \equiv$	$3^4 \equiv$	$5^4 \equiv$	$6^4 \equiv$
$2^5 \equiv$	$3^5 \equiv$	$5^5 \equiv$	$6^5 \equiv$
$2^6 \equiv$	$3^6 \equiv$	$5^6 \equiv$	$6^6 \equiv$
$2^7 \equiv$	$3^7 \equiv$	$5^7 \equiv$	$6^7 \equiv$
$2^8 \equiv$	$3^8 \equiv$	$5^8 \equiv$	$6^8 \equiv$

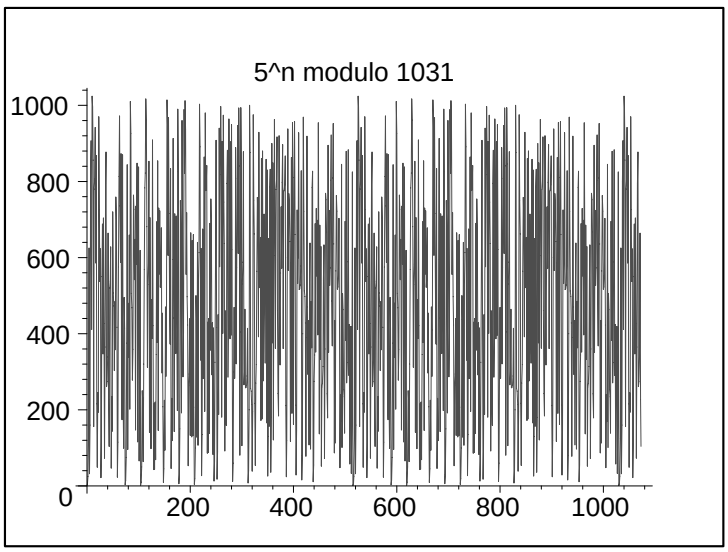
En módulo 12:

$2^0 \equiv$	$3^0 \equiv$	$5^0 \equiv$	$7^0 \equiv$
$2^1 \equiv$	$3^1 \equiv$	$5^1 \equiv$	$7^1 \equiv$
$2^2 \equiv$	$3^2 \equiv$	$5^2 \equiv$	$7^2 \equiv$
$2^3 \equiv$	$3^3 \equiv$	$5^3 \equiv$	$7^3 \equiv$
$2^4 \equiv$	$3^4 \equiv$	$5^4 \equiv$	$7^4 \equiv$
$2^5 \equiv$	$3^5 \equiv$	$5^5 \equiv$	$7^5 \equiv$
$2^6 \equiv$	$3^6 \equiv$	$5^6 \equiv$	$7^6 \equiv$
$2^7 \equiv$	$3^7 \equiv$	$5^7 \equiv$	$7^7 \equiv$
$2^8 \equiv$	$3^8 \equiv$	$5^8 \equiv$	$7^8 \equiv$
$2^9 \equiv$	$3^9 \equiv$	$5^9 \equiv$	$7^9 \equiv$
$2^{10} \equiv$	$3^{10} \equiv$	$5^{10} \equiv$	$7^{10} \equiv$
$2^{11} \equiv$	$3^{11} \equiv$	$5^{11} \equiv$	$7^{11} \equiv$
$2^{12} \equiv$	$3^{12} \equiv$	$5^{12} \equiv$	$7^{12} \equiv$
$2^{13} \equiv$	$3^{13} \equiv$	$5^{13} \equiv$	$7^{13} \equiv$

El aspecto de las gráficas:







Un par de resultados que luego serán útiles:

(Pequeño) Teorema de Fermat. Si p es un número primo, entonces

$$a^p \equiv a \pmod{p}$$

para cualquier a.

Si a es un múltiplo de p, no nos dice gran cosa.

Pero si no lo es, entonces tenemos que

$$a^{p-1} \equiv 1 \pmod{p}.$$

¿Cómo interpretas esto en términos de la periodicidad?

El caso de un módulo general (no necesariamente) primo es más delicado, claro.

Teorema de Euler. Si a es **primo** con el módulo m, entonces

$$a^{\phi(m)} \equiv 1 \pmod{m},$$

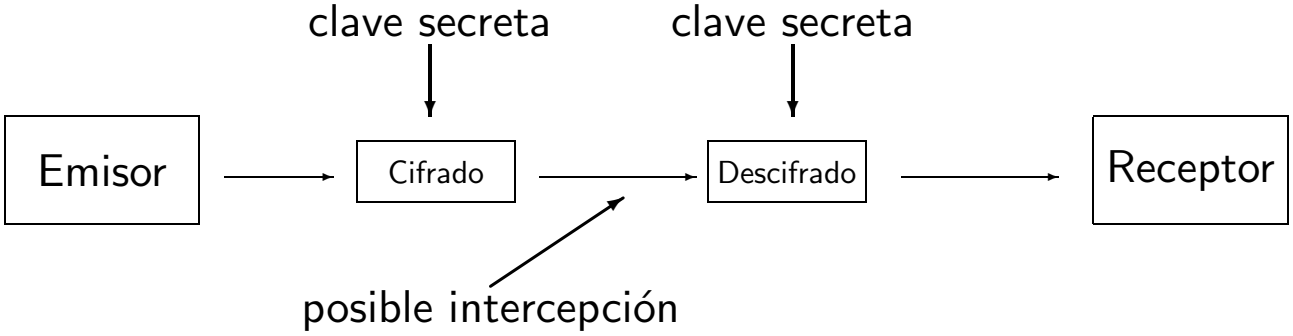
donde $\phi(m)$ es la **función de Euler**, que cuenta cuántos números más pequeños que m son primos con m.

¿Cuánto vale $\phi(p)$ si p es primo?

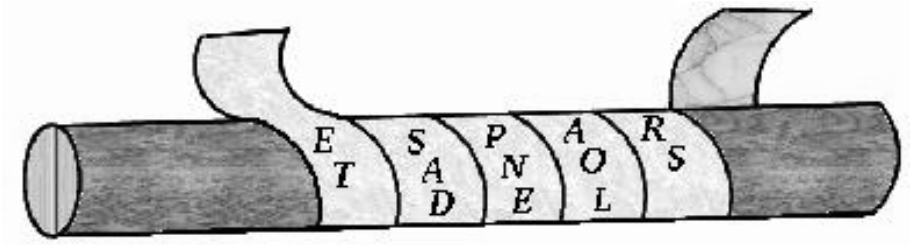
Criptografía clásica

Las comunicaciones confidenciales son necesarias. . . pero todos deseamos **descubrir secretos**.

Desde la Antigüedad se han creado **sistemas de cifrado** (criptosistemas) y, por supuesto, métodos para descifrar.

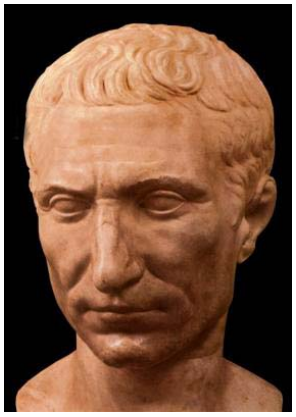


Primer aparato criptográfico de la historia: el **escítalo**.



Ejemplo ¿Te atreves a descifrar el siguiente mensaje cifrado con un escítalo NSNCO I TFLEAA? (ojo: entre las dos primeras palabras hay dos espacios en blanco)

Criptosistema de César



Sustituimos cada letra del mensaje por la que se encuentra tres posiciones más allá en el alfabeto.

En términos más matemáticos, adjudicamos

$$A = 0, B = 1, \ldots, Y = 25, Z = 26\,.$$

Y cifrar una letra x del mensaje es hacer $f(x) = x + 3$ módulo 27. La **clave secreta** es el número 3.

¿Se podría cifrar con otra clave k? ¿Qué valores puede tomar k?

Ejemplo:

1. Cifra la frase AVE CESAR, usando $k = 5$.

2. Descifra ÑÑÑHJXH YL YHPFL (sabiendo que se ha utilizado el 3 como clave) ¿Y si no supiéramos que la clave es 3?

3. Eres un espía e intentas descifrar los siguientes mensajes:

KDV GHVFXELHUWR HO VHFUHWR

GSQ HMID GERSQIW TSV FEQHE ZMIQXS IQ TSTE E XSHE

Si tienes dificultades, piensa en qué letras son las más frecuentes en castellano.

Observa que cada letra ha de poder ser descifrada de manera única. Una vez identificada una letra, ¿es difícil descifrar el resto del mensaje?

Criptografía de clave pública

Hoy en día estamos en la era de las comunicaciones: correo electrónico, Internet, llamadas vía satélite, TV por cable, banca electrónica, etc.

La **criptografía clásica o simétrica**, plantea dos **problemas** fundamentales:

- el **número de claves** necesarias en un sistema de n usuarios es $\frac{n(n-1)}{2}$.
  Por ejemplo, si $n = 100000$, se necesitarían $50000 \times 99999 = 4999950000$, es decir, casi 5000 millones de claves.
- **Intercambio** seguro de claves.

En los años 70 surge un tipo nuevo y revolucionario de criptografía, en el que cada usuario dispone de una clave PÚBLICA (para cifrar) y otra clave PRIVADA (para descifrar). Esta nueva criptografía se llama de **clave pública o asimétrica**.

¿Puedes imaginar por qué se utilizan los adjetivos simétrica y asimétrica según el tipo de criptografía?

Ahora:

- n usuarios necesitan n claves privadas. (Si $n = 100000$, compara con la criptografía clásica).
- No hace falta intercambio.

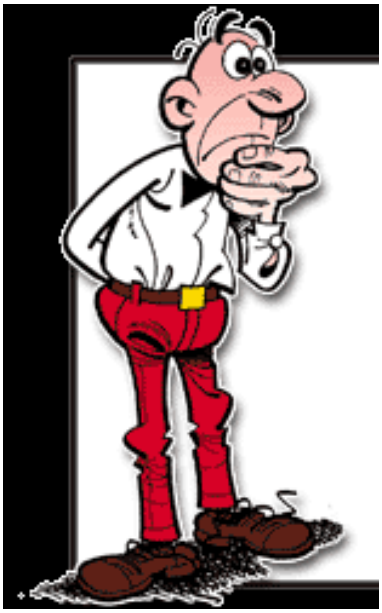
Intercambio de claves

Diffie y Hellman presentaron un sistema de **intercambio de claves**. Con este sistema, dos personas que no comparten ninguna información pueden ¡en una discusión pública! acordar una clave secreta. . . **paradójico**, ¿no?

Mortadelo y Filemón, los dos superagentes de la T.I.A quieren acordar una clave, que utilizarán para mandarse mensajes secretos.

¡Pero la temible organización A.B.U.E.L.A. está al acecho!

Mortadelo y Filemón consultan al Profesor Bacterio, que les muestra qué deben hacer.



Para empezar, se ponen de acuerdo en un número primo p y un entero s menor que p (p y s pueden hacerse públicos).

1. Mortadelo escoge un entero $a < p$ y calcula

$$\alpha = s^a \pmod{p}.$$

Filemón escoge un entero $b < p$ y calcula

$$\beta = s^b \pmod{p}.$$

Cada uno envía el resultado de sus cálculos (α y β) al otro.

2. Ahora, Mortadelo calcula

$$\beta^a \equiv s^{ba} \pmod{p}$$

y Filemón calcula

$$\alpha^b \equiv s^{ab} \pmod{p}.$$

3. Los dos han obtenido el mismo valor $k = s^{ab}$ que constituye la **clave secreta** con la que van a comunicarse.

Los malvados de la A.B.U.E.L.A. quieren obtener la clave secreta que han acordado Mortadelo Y Filemón, y para eso espían las comunicaciones.

Saben, primero, los valores de s y p (pues son públicos), y conocen también el mecanismo que se está utilizando.

Pero, por supuesto, no saben qué elecciones de a y b han hecho Mortadelo y Filemón. Pero, interceptando la comunicación, obtienen los valores de α y β.

Si a partir de ellos logran obtener a y b, habrán roto la seguridad del sistema (con ellos, pueden calcular k). ¡El mundo en peligro!

Pero claro, para esto necesitarían calcular el "logaritmo" (discreto). Fijémonos en el siguiente cálculo, donde s y p son públicos:

$$\alpha \equiv s^a \pmod{p}.$$

Si conocemos a, calcular α es muy sencillo.

Pero si lo que tenemos es α, ¿cómo obtenemos a?

Ya hemos visto que este problema es difícil, pero para convencerte otra vez, compara el cálculo 4^4 módulo 11 con el de encontrar un a tal que $4^a \equiv 3$ módulo 11.

Ya hemos solucionado el problema del intercambio de claves, pero todavía queda el asunto del número de claves necesarias.

En la próxima sesión veremos cómo se pueden conseguir las dos cosas a la vez, y diseñaremos un sistema de **criptografía de clave pública** cuyo nombre quizás os sonará: RSA.