Taller de Talento Matemático

http://www.unizar.es/ttm ttm@unizar.es

Congruencias I

(20 de octubre de 2006)

Alberto Elduque
Departamento de Matemáticas. Universidad de Zaragoza.
elduque@unizar.es

Hoy vamos a aprender a sumar y multiplicar de otra manera. Es lo que se conoce como *aritmética modular* o *aritmética del reloj*. La idea es muy simple, vamos a contar como lo hacemos con las horas en un reloj. Luego aplicaremos esta aritmética al cifrado y descifrado de mensajes.

1. Aritmética del reloj

Todos sabemos sumar y multiplicar números enteros, pero en los relojes ocurren cosas raras. Si son las 7 y transcurren 8 horas, el reloj marcará las 3. Sabemos que $7 + 8 = 15$, pero en un reloj cada vez que pasamos de 12 volvemos a empezar. Para indicar esta situación, escribiremos

$$7 + 8 \equiv 3 \pmod{12},$$

que se lee "7 más 8 es *congruente* con 3 módulo 12".

Al sumar números del modo anterior, se dice que estamos haciendo *aritmética del reloj* o *aritmética modular*.

De hecho, en un reloj hay sólo 12 horas, así que basta usar los números $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$ para designar las horas. El 12 pasa a ser el 0, el 13 el 1, ... Esto lo escribiremos así:

$$12 \equiv 0 \pmod{12}, \qquad 13 \equiv 1 \pmod{12}, \quad ...$$

De modo más general, diremos que dos números enteros a y b son *congruentes módulo* 12, y lo escribiremos

$$a \equiv b \pmod{12},$$

si la diferencia $a - b$ es un múltiplo de 12. En un reloj, dos números a y b, que sean congruentes módulo 12, representan la misma hora.

Ejercicio 1. Usa aritmética del reloj para calcular las sumas siguientes (el resultado debe de ser un número entre 0 y 11):

$$3 + 5 \equiv \_\_\_\_ \pmod{12}$$
$$7 + 6 \equiv \_\_\_\_ \pmod{12}$$
$$11 + 7 \equiv \_\_\_\_ \pmod{12}$$
$$7 + 13 \equiv \_\_\_\_ \pmod{12}$$
$$9 + 14 \equiv \_\_\_\_ \pmod{12}$$

En aritmética del reloj podemos sumar, restar y multiplicar. Incluso se puede dividir por algunos números.

Ya tienes práctica para la suma. Por ejemplo, para sumar 7 y 9, empezamos en la hora 0, adelantamos 7 horas y luego otras 9. Esto da $16 = 12 + 4$, luego el resultado es 4:

$$7 + 9 \equiv 4 \pmod{12}.$$

Para restar 7 y 9, comenzamos en 0 y primero adelantamos 7 horas para luego retrasar 9. Esto da $-2 = 10 - 12$, y el resultado es 10 ($-2 \equiv 10 \pmod{12}$):

$$7 - 9 \equiv 10 \pmod{12}.$$

De otro modo, el signo menos nos dice que debemos retrasar el reloj.

Ejercicio 2. Calcula, recordando que el resultado debe de ser un número entre 0 y 11:

$$11 + 11 \equiv \_\_\_\_ \pmod{12}$$
$$11 + 11 + 11 + 11 + 11 \equiv \_\_\_\_ \pmod{12}$$
$$7 + 7 + 7 + 7 + 7 + 7 + 7 + 7 + 7 + 7 \equiv \_\_\_\_ \pmod{12}$$
$$7 - 11 \equiv \_\_\_\_ \pmod{12}$$
$$54 - 29 \equiv \_\_\_\_ \pmod{12}$$
$$1 - 9 \equiv \_\_\_\_ \pmod{12}$$
$$-5 - 7 \equiv \_\_\_\_ \pmod{12}$$

La multiplicación es una suma repetida, luego sabiendo sumar también sabes multiplicar (ya has hecho 11×5 y 7×9 en el ejercicio anterior). Pero puedes operar de otra manera. Si deseas calcular, en aritmética del reloj, 9×15, puedes primero hacer la multiplicación normal: $9 \times 15 = 135$, ahora divides por 12 calculando el cociente y el resto: $135 = (12 \times 11) + 3$. Como dar 11 vueltas completas al reloj es como no hacer nada, nos queda

$$9 \times 15 \equiv 3 \pmod{12}.$$

Pero todavía lo podemos hacer más fácilmente:

$$9 \times 15 = 9 \times (12 + 3) = (9 \times 12) + (9 \times 3)$$

y dar 9 vueltas completas al reloj es no hacer nada. Por tanto,

$$9 \times 15 \equiv 9 \times 3 \pmod{12}$$

y claro,

$$9 \times 3 = 27 = (12 \times 2) + 3 \equiv 3 \pmod{12}.$$

Ejercicio 3.

$$\begin{aligned} 7 \times 6 &\equiv \_\_\_\_ \pmod{12} \\ 11 \times 11 &\equiv \_\_\_\_ \pmod{12} \\ 7^3 &\equiv \_\_\_\_ \pmod{12} \\ 7 \times (-5) &\equiv \_\_\_\_ \pmod{12} \\ (-5) \times (-14) &\equiv \_\_\_\_ \pmod{12} \end{aligned}$$

La división es la operación inversa de la multiplicación. Así, si nos planteamos cuánto vale 5 : 7 en la aritmética del reloj, lo que nos estamos planteando es encontrar un número x, entre 0 y 11 tal que

$$x \times 7 \equiv 5 \pmod{12}.$$

Ejercicio 4. ¿Existe tal x? ¿Qué número es?

Puesto que dividir por 7 equivale a multiplicar por el inverso de 7 (si existe):

Ejercicio 5. Resuelve la ecuación $7 \times y \equiv 1 \pmod{12}$. ¿Qué otros números (entre 0 y 11) tienen también un "inverso módulo 12"?

Lo que hemos hecho hasta ahora con un reloj "normal" (congruencias módulo 12), lo podemos hacer con relojes que tengan otro número de horas. Al fin y al cabo, nuestros antepasados (los babilonios) podrían haber decidido contar el tiempo de otra manera. Todo lo anterior tiene perfecto sentido para otros relojes.

Ejercicio 6.

$$7 + 6 \equiv \_\_\_\_ \pmod 5$$
$$32 - 3 \equiv \_\_\_\_ \pmod{15}$$
$$5 - 8 \equiv \_\_\_\_ \pmod 6$$
$$5 \times 14 \equiv \_\_\_\_ \pmod 7$$
$$5^3 \equiv \_\_\_\_ \pmod 8$$

Ejercicio 7. Haz las tablas de sumar y multiplicar módulo 7:

+	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

×	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

Comprueba que todo número $\neq 0$ tiene un inverso y, por tanto, puedes dividir por cualquier número no nulo.

Ejercicio 8. Haz lo mismo módulo 6:

+	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

×	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

¿Qué números tienen inverso? ¿Por qué ocurre esta diferencia entre la aritmética módulo 7 y la aritmética módulo 6?

2. Vamos a jugar a espías

Quizá todo lo anterior te haya parecido un juego, pero no es sólo eso. De hecho tiene multitud de aplicaciones. Ahora nos conformaremos con hablar de una de ellas: el cifrado y descifrado de mensajes.

Esto ya se usaba durante el Imperio Romano. El emperador deseaba transmitir órdenes a sus legiones, pero no quería que el enemigo, que podía interceptar a los mensajeros, se enterara del contenido de las órdenes.

Nosotros utilizaremos un método más complicado y seguro que el usado por los emperadores romanos, pero no tan sofisticado como los que se utilizan hoy en día, por ejemplo, cuando entramos en una *página segura* en internet (las que comienzan con `https://...` y se usan siempre que se vayan a hacer compras o actividades bancarias a través de la red). Estos sistemas más complejos también están basados en la aritmética del reloj.

Para simplificar, vamos a enviarnos mensajes que tengan sólo letras mayúsculas y espacios en blanco. Para ello, asignamos números a cada uno de estos símbolos como sigue:

A	B	C	D	E	F	G	H	I	J	K	L	M	
1	2	3	4	5	6	7	8	9	10	11	12	13	
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	_
14	15	16	17	18	19	20	21	22	23	24	25	26	0

(asignamos el número 0 al espacio en blanco)

Trabajaremos en la aritmética módulo 27. Primero buscamos un número sencillo a que tenga inverso módulo 27, por ejemplo $a = 4$ porque $4 \times 7 = 28 \equiv 1 \pmod{27}$; ahora tomamos otro número b, por ejemplo $b = 10$. Con estos números a y b podemos diseñar lo que se conoce como un *cifrado afín*.

Imagínate que quieres enviarle a Juan el siguiente mensaje:

`HOLA JUAN`

Seguimos los siguiente pasos para *cifrar* el mensaje:

(i) Traducimos nuestro mensaje en una secuencia de números, usando para ello la asignación anterior:

$$\texttt{HOLA JUAN} \quad \longrightarrow \quad (8, 15, 12, 1, 0, 10, 21, 1, 14).$$

(ii) Transformamos cada número x de la secuencia por el número y entre 0 y 26 que verifica

$$(a \times x) + b \equiv y \pmod{27}$$

(usaremos, como antes, $a = 4$ y $b = 10$):

$$\begin{array}{rcrcrcll}
\mathbf{8} & \mapsto & (4 \times \mathbf{8}) + 10 & = & 42 & \equiv & \mathbf{15} & (\text{mód } 27) \\
\mathbf{15} & \mapsto & (4 \times \mathbf{15}) + 10 & = & 70 & \equiv & \mathbf{16} & (\text{mód } 27) \\
\mathbf{12} & \mapsto & (4 \times \mathbf{12}) + 10 & = & 58 & \equiv & \mathbf{4} & (\text{mód } 27) \\
\mathbf{1} & \mapsto & (4 \times \mathbf{1}) + 10 & = & 14 & \equiv & \mathbf{14} & (\text{mód } 27) \\
\mathbf{0} & \mapsto & (4 \times \mathbf{0}) + 10 & = & 10 & \equiv & \mathbf{10} & (\text{mód } 27) \\
\mathbf{10} & \mapsto & (4 \times \mathbf{10}) + 10 & = & 50 & \equiv & \mathbf{23} & (\text{mód } 27) \\
\mathbf{21} & \mapsto & (4 \times \mathbf{21}) + 10 & = & 94 & \equiv & \mathbf{13} & (\text{mód } 27) \\
\mathbf{1} & \mapsto & (4 \times \mathbf{1}) + 10 & = & 14 & \equiv & \mathbf{14} & (\text{mód } 27) \\
\mathbf{14} & \mapsto & (4 \times \mathbf{14}) + 10 & = & 66 & \equiv & \mathbf{12} & (\text{mód } 27)
\end{array}$$

obteniendo así una nueva secuencia:

$$(8, 15, 12, 1, 0, 10, 21, 1, 14) \quad \longrightarrow \quad (15, 16, 4, 14, 10, 23, 13, 14, 12).$$

(iii) Traducimos ahora nuestra nueva secuencia de números en símbolos:

$$(15, 16, 4, 14, 10, 23, 13, 14, 12) \quad \longrightarrow \quad \texttt{OPDNJWMNL}$$

y éste es el mensaje que enviamos a Juan:

$$\texttt{OPDNJWMNL}$$

Si alguien intercepta nuestro mensaje se quedará muy sorprendido.

Juan tiene que recorrer el camino inverso para *descifrar* el mensaje que le llega:

(i) Traduce los símbolos a números:

$$\texttt{OPDNJWMNL} \quad \longrightarrow \quad (15, 16, 4, 14, 10, 23, 13, 14, 12).$$

(ii) Realiza, módulo 27, las operaciones inversas a cada número:

$$y \mapsto (y - b) : a$$

Para ello es muy importante que nuestro $a = 4$ tenga inverso, que es 7, así que dividir por a equivale a multiplicar por 7 (módulo 27):

$$\begin{array}{rcrcrcll}
\mathbf{15} & \mapsto & (\mathbf{15} - 10) \times 7 & = & 35 & \equiv & \mathbf{8} & (\text{mód } 27) \\
\mathbf{16} & \mapsto & (\mathbf{16} - 10) \times 7 & = & 42 & \equiv & \mathbf{15} & (\text{mód } 27) \\
\mathbf{4} & \mapsto & (\mathbf{4} - 10) \times 7 & = & -42 & \equiv & \mathbf{12} & (\text{mód } 27) \\
\mathbf{14} & \mapsto & (\mathbf{14} - 10) \times 7 & = & 28 & \equiv & \mathbf{1} & (\text{mód } 27) \\
\mathbf{10} & \mapsto & (\mathbf{10} - 10) \times 7 & = & 0 & \equiv & \mathbf{0} & (\text{mód } 27) \\
\mathbf{23} & \mapsto & (\mathbf{23} - 10) \times 7 & = & 91 & \equiv & \mathbf{10} & (\text{mód } 27) \\
\mathbf{13} & \mapsto & (\mathbf{13} - 10) \times 7 & = & 21 & \equiv & \mathbf{21} & (\text{mód } 27) \\
\mathbf{14} & \mapsto & (\mathbf{14} - 10) \times 7 & = & 28 & \equiv & \mathbf{1} & (\text{mód } 27) \\
\mathbf{12} & \mapsto & (\mathbf{12} - 10) \times 7 & = & 14 & \equiv & \mathbf{14} & (\text{mód } 27)
\end{array}$$

obteniendo una nueva secuencia:

$$(15, 16, 4, 14, 10, 23, 13, 14, 12) \quad \longrightarrow \quad (8, 15, 12, 1, 0, 10, 21, 1, 14).$$

(iii) Y finalmente traduce estos números a letras:

$$(8, 15, 12, 1, 0, 10, 21, 1, 14) \quad \longrightarrow \quad \texttt{HOLA JUAN}.$$

De este modo, Juan se entera del contenido de nuestro mensaje.

Ejercicio 9. Agrupaos en grupos de 6 o 7 personas divididas en dos subgrupos, poneos de acuerdo en qué números a y b vais a utilizar, y enviaos mensajes cifrados de un subgrupo a otro.

Si deseamos incluir signos de ortografía y letras mayúsculas y minúsculas, necesitaremos trabajar en aritmética módulo un número mayor que 27 y el proceso se hace más lento, salvo que utilicemos un ordenador.

* * * * * *

Si no te asusta el inglés, hay muchas páginas web donde poder practicar la aritmética del reloj. Puedes consultar, por ejemplo, las URLs

`http://www-math.cudenver.edu/~wcherowi/clockar.html`

`http://www.wou.edu/~burtonl/arithclock.html`

`http://www.shodor.org/interactivate/lessons/clock.html`

o muchas más que puedes encontrar con tu buscador favorito.

Soluciones de algunos ejercicios:
1: 8, 1, 6, 8, 11.
2: 10, 7, 3, 8, 1, 4, 0.
3: 6, 1, 7, 1, 10.
4: $x = 11$.
5: $y = 7$. Tienen inverso módulo 12 los números $1, 5, 7, 11$.
6: 3, 14, 3, 0, 5.