Taller de Talento Matemático

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

Congruencias II

(21 de octubre de 2005)

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

En la sesión de *Congruencias* del curso pasado, que puedes encontrar en http://www.unizar.es/ttm/2004-05/congruencias.pdf, aprendimos a operar en *aritmética modular* o *aritmética del reloj*. Luego lo usamos para aprender a ser espías, y para calcular la letra del NIF, así como el último dígito del código ISBN de los libros.

Hoy repasaremos cómo se opera en esta aritmética y nos ejercitaremos con ella haciendo *pulseras modulares*.

1. Repaso de la aritmética del reloj

Si son las 6 en nuestro reloj y transcurren 7 horas, el reloj marcará la una. Esto lo expresamos así:

$$6 + 7 \equiv 1 \pmod{12},$$

que se lee "6 más 7 es *congruente* con 1 módulo 12".

Si en lugar de dividir medio día en 12 periodos (horas) lo hiciéramos en 6 periodos tendríamos, por ejemplo:

$$3 + 5 \equiv 2 \pmod{6}, \qquad 5 \times 2 \equiv 4 \pmod{6}.$$

Las tablas de "sumar y multiplicar módulo 6" son las siguientes:

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

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

Observemos que los números 1 y 5 tienen "inverso módulo 6" (pues $1 \times 1 \equiv 1$ (mód 6) y $5 \times 5 \equiv 1$ (mód 6), luego el inverso de 1 es 1 y el de 5 es 5).

Ejercicio 1. Calcula las tablas de sumar y multiplicar módulo 5:

+	0	1	2	3	4
0					
1					
2					
3					
4					

×	0	1	2	3	4
0					
1					
2					
3					
4					

¿Qué números tienen inverso módulo 5?

Ejercicio 2. Dado un número natural $n \geq 2$ arbitrario. ¿Qué números entre 1 y n tienen inverso módulo n?

2. PULSERAS MODULARES

Fijemos un número, por ejemplo 8. Para hacer una pulsera módulo 8 elegimos dos números del 0 al 7, por ejemplo 2 y 4. Ahora obtenemos un tercer número sumando estos dos números módulo 8: $2+4 \equiv 6$ (mód 8). Así obtenemos la secuencia:

$$2 \quad 4 \quad 6.$$

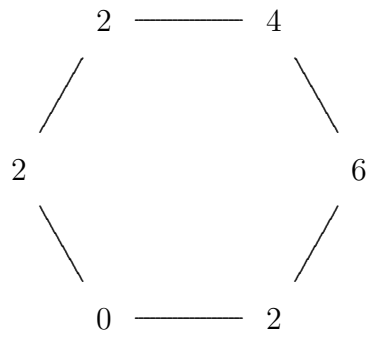
El cuarto número lo obtenemos sumando módulo 8 los dos últimos ($4 + 6 \equiv 2$ (mód 8)):

$$2 \quad 4 \quad 6 \quad 2,$$

y repetimos el proceso hasta que nos vuelvan a aparecen nuestros dos primeros números consecutivamente:

$$2 \quad 4 \quad 6 \quad 2 \quad 0 \quad 2 \quad 2 \quad 4.$$

Nuestra *pulsera modular* es



Si eres artista, puedes asignar colores a los números del 0 al 7 y crear así pulseras con cuentas de colores.

Observa que si hubiéramos comenzado con los números 4 y 6, o con 6 y 2, o 2 y 0, o 0 y 2, o 2 y 2, habríamos obtenido la misma pulsera.

Ejercicio 3. Obtén todas las pulseras módulo 8. ¿Cuántas hay? ¿Qué longitud tienen?

Ejercicio 4. Repite el ejercicio 3, pero módulo 5 y módulo 6, en lugar de módulo 8.

Ejercicio 5. ¿Por qué siempre obtienes la repetición del primer par de números? En otras palabras, ¿por qué termina siempre el proceso?

Observa que, en todos los casos, las longitudes de todas las pulseras son divisores de la longitud de la pulsera más larga. Esto no es casualidad, pero hacen falta más matemáticas de las que sabes ahora para probar esto. Estas matemáticas son las mismas que se utilizan para calcular cosas como el número posible de moléculas de determinado tipo.

* * * * * *

Para saber y practicar más, puedes entrar en la URL

`http://www.math.csusb.edu/faculty/susan/number_bracelets/INDEX.HTM`

Soluciones de algunos ejercicios:

2: Tienen inverso aquellos números m, con $1 \leq m < n$, cuyo máximo común divisor con n es 1. ¿Por qué?

3: Hay cuatro pulseras de longitud 12, dos pulseras de longitud 6, una de longitud 3, además de la pulsera trivial (la que empieza con 0 y 0) que, por convenio, se considera que tiene longitud 1.

4: Módulo 5 hay sólo tres pulseras, de longitudes 20, 4 y 1. Módulo 6 hay cuatro pulseras de longitudes 24, 8, 3 y 1.

5: Puedes pensar en cada paso del proceso como una regla para obtener un par de números a partir del par anterior: $(a, b) \xrightarrow{D} (b, c)$, con $c \equiv a + b \pmod{n}$, siendo n el módulo elegido. Así, por ejemplo, la primera pulsera que hemos creado equivale a:

$$(2,4) \xrightarrow{D} (4,6) \xrightarrow{D} (6,2) \xrightarrow{D} (2,0) \xrightarrow{D} (0,2) \xrightarrow{D} (2,2) \xrightarrow{D} (2,4),$$

repitiéndose el par $(2, 4)$.

Esta regla tiene su regla inversa: $(a, b) \xleftarrow{I} (b, c)$, donde $a \equiv c - b \pmod{n}$. Dado cualquier par de los que aparecen al hacer una pulsera, el par siguiente se obtiene aplicando la regla D y el anterior aplicando la regla I.

Puesto que sólo hay n^2 pares de números entre 0 y $n-1$, al aplicar la regla D un número de veces suficiente (por ejemplo n^2 veces) al par inicial, habrá necesariamente algún par (a, b) que se repita. Además, el primer par que se repita ha de ser el primero, pues si dos pares coinciden, y ninguno de ellos es el primer par, también lo hacen los pares anteriores (basta aplicar la regla I).