Taller de Talento Matemático

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

Congruencias II

(20 de noviembre de 2009)

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

En la sesión de *Congruencias* del curso pasado, que puedes encontrar en nuestra web www.unizar.es/ttm, aprendimos a operar en *aritmética modular* o *aritmética del reloj*. Luego lo usamos para aprender a ser espías.

Hoy repasaremos cómo se opera en esta aritmética, veremos algunas aplicaciones 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 $1 \times 1 \equiv 1 \pmod 6$ y $5 \times 5 \equiv 1 \pmod 6$, 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. Algunas aplicaciones

Hay muchas aplicaciones de las congruencias y la aritmética del reloj.

2.1. NIF.

El NIF español se obtiene añadiendo una *letra de control* al DNI. Para hacerlo, dado un número de DNI, por ejemplo el 17.003.989, se calcula el resto de dividir este número por 23. Esto es, se calcula x entre 0 y 22 tal que

$$17003989 \equiv x \pmod{23}$$

(piensa en un reloj de 23 horas). La letra que se asigna depende del resto de acuerdo a la tabla siguiente:

$x =$	0	1	2	3	4	5	6	7	8	9	10	11
letra:	T	R	W	A	G	M	Y	F	P	D	X	B
$x =$	12	13	14	15	16	17	18	19	20	21	22	
letra:	N	J	Z	S	Q	V	H	L	C	K	E	

Fíjate que no se usan las letras I, O ni U (en parte, porque pueden confundirse con números).

Ejercicio 3. ¿Qué letra corresponde al DNI 17.003.989? ¿Y al tuyo?

Esta letra de control permite detectar errores. Imagina que al decir por teléfono tu NIF te equivocas en uno de los números. La persona que lo recibe puede hacer el cómputo anterior, darse cuenta de que la letra que le sale a ella no coincide con la que tú le has dicho y pedirte que se lo vuelvas a decir.

2.2. ISBN.

Un proceso un poquito más complicado se utiliza para el código ISBN (**I**nternational **S**tandar **B**ook **N**umber) de los libros. Hasta el 1 de enero de 2007, un número ISBN constaba de 10 dígitos divididos en 4 partes de longitud variable: identificador de grupo (país, área geográfica o área lingüística), de editor, de título y un dígito de control. Una vez determinados los 9 primeros dígitos, por ejemplo `0 8536 1072`, se calcula el número x entre 0 y 10 que verifique

$$\begin{aligned}(\mathbf{0}\times 1)+(\mathbf{8}\times 2)+(\mathbf{5}\times 3)+(\mathbf{3}\times 4)+(\mathbf{6}\times 5)+&\\ +(\mathbf{1}\times 6)+(\mathbf{0}\times 7)+(\mathbf{7}\times 8)+(\mathbf{2}\times 9)\equiv x \pmod{11}&\end{aligned}$$

Si x no es 10, entonces el último dígito del ISBN es x. Si, por el contrario, x es 10, en lugar de un último dígito se añade una letra `X`.

Ejercicio 4. Calcula el último dígito del ISBN anterior. Busca en tu casa libros cuyo ISBN acabe en `X` (aproximadamente uno de cada 11 libros lo hace). Coge varios libros y comprueba que el último dígito (o letra) de su ISBN es correcto.

Sin embargo, a partir del 1 de enero de 2007, se utilizan 13 dígitos, siendo el último ($0 \leq x_{13} \leq 9$) de nuevo un dígito de control, que se obtiene mediante la fórmula

$$x_{13} \equiv -\sum_{i=1}^{6}(x_{2i-1} + 3x_{2i}) \pmod{10}.$$

Como puedes apreciar, ahora se obtiene el dígito de control mediante una congruencia módulo 10, por lo que ya no hace falta el símbolo `X`.

2.3. El primo más grande conocido.

El número primo más grande conocido es $2^{43112609} - 1$, descubierto el 23 de agosto de 2008 con ordenadores del Departamento de Matemáticas de la Universidad de California en Los Ángeles (UCLA), dentro de un gran proyecto internacional que funciona gracias a la ayuda de muchos voluntarios en todo el mundo, que ponen sus ordenadores personales a trabajar en el proyecto. Este número primo tiene casi 13 millones de dígitos, y es el primer primo con más de 10 millones de dígitos conocido (eso le ha reportado un premio de 50.000 dólares a UCLA). El 12 de abril de este año 2009 se ha descubierto el segundo primo más grande conocido hasta el momento: $2^{42643801} - 1$.

El número estimado de partículas elementales de todo el universo es inferior a 2^{300}, esto da ideal del tamaño de estos números.

Ejercicio 5. ¿Cuál es el último dígito de este primo? ¿Y los dos últimos dígitos?

3. 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: $2+4 \equiv 6 \pmod{8}$. Así obtenemos la secuencia:

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

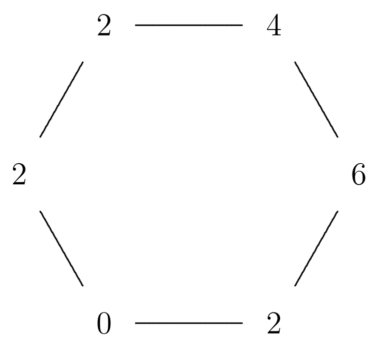
El cuarto número lo obtenemos sumando módulo 8 los dos últimos ($4 + 6 \equiv 2 \pmod{8}$):

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

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

Ejercicio 7. Repite el ejercicio 6, pero módulo 5 y módulo 6, en lugar de módulo 8.

Ejercicio 8. ¿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 las URL

`http://primes.utm.edu/largest.html`

`http://www.geom.uiuc.edu/~addingto/number_bracelets/number_bracelets.html`

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: C.

4: `X`.

5: 1 y 11.

6: 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.

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

8: 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).