CAPÍTULO 6

6

ARITMÉTICA MODULAR - PARTE 1

Jorge Roldán López
Universidad de La Rioja

Palabras clave

- *Módulo*
- *Congruencia*
- *Divisibilidad*
- *Fermat*

Durante la resolución de muchos ejercicios de matemáticas necesitamos conocer la divisibilidad de un número. Desde la infancia empezamos a conocer los criterios para saber cuándo podemos dividir por números pequeños, aunque otros más grandes como el 7, 11 ó 13 igual no los recordamos o ni siquiera llegamos a conocerlos. Sin embargo, aunque útiles, las técnicas clásicas que nos permiten conocer cuándo un número es divisible por otro, pronto se quedan cortas. En este capítulo se introduce la aritmética modular con sus congruencias. Esta es una nueva técnica que lleva mucho más lejos esta idea y nos abre un abanico de potentes resultados para enfrentarnos a estos y otros problemas.

6.1 Introducción

A lo largo de nuestra vida es frecuente encontrarse con situaciones donde resulte conveniente conocer si un número entero es divisible por otro. Por ejemplo, para responder a la siguiente pregunta:

«¿Podemos repartir 112332 acciones de una empresa entre 33 accionistas sin que sobre ninguna?»

Dado que una acción no se puede partir, debemos estudiar si 112332 es divisible por 33. En este caso la respuesta es sí. No obstante, aunque en números pequeños la cuenta resulta viable, incluso mentalmente, el problema escala con fácilidad. Así pues, surge la pregunta de si podemos comprobarlo fácilmente sin necesidad de tener que hacer la cuenta completa.

Para aliviar la comprobación de si un número entero es divisible por otro existen los criterios de divisibilidad. Aunque pronto veremos que estas herramientas se quedan cortas y necesitaremos introducir nuevas.

6.2 Criterios de divisiblidad

El primer paso es tener claro qué entendemos por ser divisible o múltiplo. Un concepto que, aunque sencillo, tiene su propia notación matemática.

Definición 6.1 (Divisible o múltiplo)

Dados dos números enteros n y m. Decimos que un número n es divisible por m, o que m divide a n, o que n es múltiplo de m, y lo denotamos como $m|n$, cuando existe otro entero k tal que $n = m \cdot k$.

Una vez vistas todas las formas en las podemos expresarlo, podemos empezar a buscar criterios de divisibilidad. El criterio más conocido, y que se estudia desde niño, es el del número dos. Este nos dice que para que un número sea divisible por dos debe ser par. Aunque, como ya sabremos, esto se limita a estudiar la última cifra como nos indica el siguiente lema:

Lema 6.1 (Criterio de divisibilidad para 2)

Un número es divisible por 2 si y solo si el número en cuestión termina en un número par.

Conviene recordar por si acaso que el número cero es un número par. De hecho el cero es divisible por cualquier entero no nulo. En el caso del número 3, el criterio también es muy conocido y sencillo:

Lema 6.2 (Criterio de divisibilidad para 3)

Un número es múltiplo de 3 si y solo si la suma de sus cifras lo es también.

Así, como nos dice este lema, para comprobar si 291 231 398 172 es divisible por 3 basta calcular

$$2 + 9 + 1 + 2 + 3 + 1 + 3 + 9 + 8 + 1 + 7 + 2 = 48.$$

Aunque con esto puede ser suficiente para responder ya que sí, podemos seguir comprobando si 48 divisible por 3 calculando $4 + 8 = 12$. Y nuevamente podríamos hacer $1 + 2 = 3$ dejándolo ya muy claro. Es decir, todos estos criterios se pueden aplicar varias veces.

Sigamos ahora enunciando reglas para los siguientes números:

Lema 6.3 (Criterio de divisibilidad para 4)
Un número es divisible por cuatro si y solo si sus últimas dos cifras son un múltiplo de 4.

Lema 6.4 (Criterio de divisibilidad para 5)
Un número es divisible por 5 si y solo si termina en 0 o 5.

Lema 6.5 (Criterio de divisibilidad para 7)
Un número es divisible por 7 si y solo si al restar a dicho número sin la cifra de la unidades el doble de la cifra de las unidades da múltiplo de 7.

Este criterio es algo más complejo, así que para que termine de quedar claro vamos a ver un ejemplo.

Ejemplo 6.1 ¿Es divisible 127621 por 7? El primer paso es calcular $12762 - 2 \cdot 1 = 12760$. Como seguimos sin saberlo vamos a repetir este mismo paso hasta que ya sepamos responder. Ahora debemos hacer $1276 - 2 \cdot 0 = 1276$. El siguiente paso sería $127 - 2 \cdot 6 = 115$, seguido por $11 - 2 \cdot 5 = 1$. Llegados a este punto ya podemos decir sin dudarlo que la respuesta es no. 127621 no es divisible por 7 ya que 1 no lo es.

Sigamos con nuestra lista:

Lema 6.6 (Criterio de divisibilidad para 9)
Un número es divisible por 8 si y solo sus últimas 3 cifras son un múltiplo de 8.

Lema 6.7 (Criterio de divisibilidad para 9)
Un número es divisible por 9 si y solo si la suma de sus cifras lo es.

Lema 6.8 (Criterio de divisibilidad para 10)
Un número es divisible por 10 si y solo si termina en 0.

Lema 6.9 (Criterio de divisibilidad para 11)
Un número es divisible por 11 cuando la diferencia entre las cifras que ocupan posición par y las que ocupan posición impar es múltiplo de 11.

Lema 6.10 (Criterio de divisibilidad para 13)
Un número es divisible por 13 si y solo si al restar a dicho número sin la cifra de la unidades nueve veces la cifra de las unidades da múltiplo de 13.

Como podemos ver, hay criterios muy similares: el del 4 y el 8, el 3 y 9, el 7 y 13... Y así podríamos seguir dando criterios para más números, aunque no tiene mucho sentido. En cualquier caso, llegados a este punto podemos ver que no hemos puesto ni el criterio para el 6, ni respondido a la pregunta inicial de si 112332

es divisible por 33. Sin embargo, sí que sabemos responder con los criterios ya dados a ambas preguntas. Para ello vamos a hacer uso de la siguiente proposición:

Proposición 6.1

Un número n es divisible entre $a \cdot b$, siendo el $mcd(a, b) = 1$, si y solo si n es divisible por a y por b.

Así, un número es divisible por 6 si lo es por 2 y por 3 a la vez. Y, a su vez, 112332 es divisible por $33 = 3 \cdot 11$ si y solo si lo es por 3 y por 11. Y todos estos criterios de divisibilidad los conocemos ya de antes. Por tanto:

- $1 + 1 + 2 + 3 + 3 + 2 = 12$, luego es divisible por 3.
- $1 - 1 + 2 - 3 + 3 - 2 = 0$, luego es divisible por 11.

Nota: *Cuidado que esto necesita que el mcd sea 1 y de no ser así no podremos descomponerlo. Así 12 podemos descomponerlo como $3 \cdot 4$ y algo es divisible entre 12 si lo es entre 3 y entre 4, pero no podemos descomponerlo como 6 y 2 o como 3, 2 y 2.*

Ahora con todo esto claro ya somos capaces de poner a prueba estos criterios en los ejercicios propuestos 1., 2. y 3. del final del capítulo. No obstante, los criterios de divisibilidad presentan algunas pegas:

- Podemos no conocerlos.
- Pueden ser tediosos de aplicar.
- Podemos desconocer las cifras del número el cual queremos saber si es divisible.

Aunque para este último caso podemos encontrar alternativas en algunos casos para salir adelante como en el siguiente ejemplo:

Ejemplo 6.2 ¿Para qué x e y enteros el número $x^2 - y^2$ es divisible por 4?

El primer paso es darse cuenta que $x^2 - y^2 = (x + y)(x - y)$. Como queremos que $(x + y)(x - y)$ sea múltiplo de cuatro y por tanto par, necesitamos al menos que $x + y$ o $x - y$ sea uno de ellos par como mínimo. Veamos en el Cuadro 6.1 qué ocurre en función de si x e y son pares o impares.

x	y	$x + y$	$x - y$
Par	Par	Par	Par
Par	Impar	Impar	Impar
Impar	Par	Impar	Impar
Impar	Impar	Par	Par

Cuadro 6.1: Tabla de paridades de $x + y$ y de $x - y$.

Como podemos ver $x + y$ y $x - y$ tienen siempre la misma paridad. Y ambos son pares, como queremos, cuando x e y tienen la misma paridad. Y es más, como ambos son pares, su producto es directamente múltiplo de 4. Por tanto, la solución es que tanto x como y deben tener la misma paridad para que $x^2 - y^2$ sea múltiplo de 4.

Notar que parece que este mismo análisis se puede hacer sin esta descomposición en producto usando el Cuadro 6.2. Sin embargo, el resultado no queda claro que sea múltiplo de 4 directamente y habría que estudiar esos casos. Por ejemplo poniendo x e y como $2n$ y $2m$ o $2n + 1$ y $2m + 1$ en función de si son pares o impares.

x	y	x^2	y^2	x^2-y^2
Par	Par	Par	Par	Par
Par	Impar	Par	Impar	Impar
Impar	Par	Impar	Par	Impar
Impar	Impar	Impar	Impar	Par

Cuadro 6.2: Tabla de paridades de $x^2 - y^2$.

En cualquier caso, aunque hemos podido salir al paso en este ejemplo, existen otras preguntas que no podremos responder:

- ¿Es $7^n - 1$ múltiplo de 6?
- ¿Es $25^{3123} + 15$ divisible por 8?

Este último por ejemplo se trata de un número que tiene ¡4366 cifras! Son estos problemas los que en parte motivan la búsqueda de herramientas más potentes, como las que veremos en el siguiente capítulo.

6.3 Aritmética modular: definición y principales propiedades

Antes de introducir la aritmética modular, para evitar asustarnos ante un concepto nuevo, conviene darse cuenta que en el día a día cualquier persona hace uso de ella sin saberlo. Todo el mundo sabe que las 17:00 horas son las 5 de la tarde, o que las 21:00 son las 9. Incluso esto afecta a operaciones. Si a las 10 alguien nos dice que queda con nosotros en 5 horas, nos está citando a las 3. ¿Pero qué clase de brujería nos lleva a comparar el 17 con el 5 o el 21 con el 9 o nos dice que $10 + 5 = 3$? La respuesta es la aritmética modular, en este caso módulo 12. Como 17-12 = 5, decimos que ambas horas son "equivalentes" módulo 12. Y en el caso de la suma $10 + 5 = 15$ pero 15 es como 3.

Algo similar ocurre cuando trabajamos con ángulos. Un ángulo de $30°$ es equivalente a uno de $390°$, o uno de $\pi/6$ es equivalente a otro de $13\pi/6$ si hablamos del mismo ángulo en radianes. Esto se debe a que están en la misma posición y lo único que los diferencia es el número de vueltas que han dado para llegar ahí. De hecho, el siguiente ejemplo muestra que, en problemas trigonométricos, muchas veces todos estos ángulos son solución.

Ejemplo 6.3 Calcula α tal que $\operatorname{sen}\alpha = \dfrac{1}{\sqrt{2}} = \cos\alpha$. En este caso la solución es $\alpha = 45° + 360°k = \dfrac{\pi}{4} + 2\pi k$ siendo k un entero cualquiera que representa el número de vueltas.

Una vez hemos visto que hay situaciones habituales donde números aparentemente diferentes se comportan como "equivalentes", podemos perder el miedo e introducirnos en la aritmética modular. Si bien la idea es antigua, el lenguaje que vamos a emplear es relativamente nuevo y apareció en el siglo XIX de mano del genio matemático Carl Friedrich Gauss (1777–1855).

Definición 6.2 (Congruentes)

Dados tres números enteros n, m y k. Decimos que n y m son congruentes módulo k, y lo denotamos

$$n \equiv m \pmod{k}.$$

si al dividir n y m ambos por k obtenemos el mismo resto.

En otras palabras, $n \equiv m$ módulo k es equivalente a que $n - m$ sea múltiplo de k.

Nota: *Aunque toda congruencia se realiza módulo cierto natural, en aquellos contextos donde quede claro podremos omitir la escritura del módulo en el cual estamos trabajando para abreviar.*

Así tendríamos que

$$25 \equiv 4 \pmod 7,$$
$$15 \equiv 35 \pmod 2,$$
$$1605 \equiv 149 \pmod{13}$$
$$193\,183 \equiv 33\,261\,931 \pmod{12},$$
$$24 \equiv -1 \pmod 5.$$

Notar que la congruencia nos sirve directamente para comprobar o calcular cuál es el resto de dividir dos números:

Lema 6.11
Si al dividir m entre n da resto k entonces $m \equiv k \pmod n$.

Este lema también nos da el criterio general de divisibilidad en congruencias:

Corolario 6.1
Un número n es divisible por m si y solo si $n \equiv 0 \pmod m$.

Una vez visto este concepto, podemos introducir las propiedades más básicas que más adelante nos facilitaran el trabajo. Aunque no se indique explícitamente, todas las congruencias son bajo un mismo módulo cualquiera.

Propiedad *Si $a \equiv b$ entonces para todo k se tiene que*

- $a + k \equiv b + k$,
- $k \cdot a \equiv k \cdot b$,
- $a^k \equiv b^k$ *si* $k \in \mathbb{N}$.

Propiedad *Si $a \equiv b$ y $c \equiv d$ entonces*

- $a + c = b + d$,
- $a \cdot c \equiv b \cdot d$.

Probar estas propiedades no resulta difícil y puede ser un interesante ejercicio que queda para el lector. Si bien, alguna de las pruebas como la de las potencias requiere de inducción.

Otra propiedad que nos puede resultar útil nos la da el siguiente lema:

Lema 6.12
Sea $p|m$, es decir, sea p un divisor de m entonces si $n \equiv k \pmod m$ se tiene que $n \equiv k \pmod p$.

Sin embargo, el recíproco no es cierto y es fácil verlo con un contraejemplo. En módulo 4 tenemos que $6 \cong 2$, pero en módulo 8, un múltiplo de 4, esta congruencia no se da.

Con esto, ya estamos listos para resolver las dos preguntas propuestas al final del apartado anterior:

Ejemplo 6.4 ¿Es $7^n - 1$ múltiplo de 6? Como en módulo 6, $7 \equiv 1$, entonces $7^n \equiv 1^n$. Así

$$7^n - 1 \equiv 1^n - 1 = 0 \pmod 6.$$

Ejemplo 6.5 ¿Es $25^{3123} + 15$ divisible por 8? En módulo 8, $25 \equiv 1$, luego $25^{3123} = 1^{3123}$, de nuevo 1. Y además $15 \equiv 7$. Así $25^{3123} + 15 = 1^{3123} + 7 \equiv 1 + 7 \equiv 0 \pmod 8$.

Por otro lado, habrá ocasiones en las que usar números negativos nos puede ayudar y mucho, como en el próximo ejemplo:

Ejemplo 6.6 Determina todos los enteros positivos n para los cuales $2^n + 1$ es divisible por 3. Aquí queremos ver para qué valores de n se cumple que

$$2^n + 1 \equiv 0 \pmod 3$$

Pero esto es lo mismo que decir que

$$(-1)^n + 1 \equiv 0 \pmod 3$$

Luego esto solo es cierto para valores impares de n.

Podemos practicar con alguna congruencia como la de los ejercicios propuestos 4., 5. y 6..

6.4 Inversos modulares

Si observamos con cuidado las propiedades anteriores vemos que una nos dice que las congruencias se llevan bien con el producto, es decir, que si $a \equiv b$ entonces $k \cdot a \equiv k \cdot b$. Esto nos puede llevar a pensar que ocurre algo similar con la división, es decir, que podemos simplificar la k. Pero no siempre es cierto. Un contraejemplo de esto es:

$$2 \cdot 3 \equiv 2 \cdot 10 \pmod{14} \qquad \not\Rightarrow \qquad 3 \equiv 10 \pmod{14}.$$

En realidad esto se debe a que dividir es multiplicar por el inverso. Y aquí el dos no tiene inverso. Pero, ¿qué es esto del inverso?

Definición 6.3 (Inverso)

Dado un número a, si existe b tal que $a \cdot b = 1$, decimos que b es su inverso y lo denotamos como a^{-1}. En este caso a se llama invertible o inversible.

En los racionales nos sonará que

$$\frac{a}{b} = a \cdot \frac{1}{b} = a \cdot b^{-1}.$$

Pero aquí las cosas funcionan diferentes. Sin entrar en mucho detalle al trabajar en aritmética modular estamos aplicando un cociente en $\mathbb{Z}$ llegando a una estructura equivalente a $\mathbb{Z}_n$. No hace falta que entendamos del todo para este capítulo que significa esto, pero sí cuándo existe el inverso y cómo se puede calcular.

Definición 6.4 (Coprimo)

Decimos que dos números a y b son coprimos cuando no tienen factores en común, es decir, $mcd(a, b) = 1$.

Proposición 6.2

Dado un entero a módulo m, existe a^{-1} si y solo si $mcd(a, m) = 1$, es decir, son coprimos.

Así, cuando m es un número primo todo entero no nulo tiene inverso. Gracias a esta proposición sabemos cuando podemos simplificar la ecuación

$$k \cdot a \equiv k \cdot b \pmod{m},$$

puesto que tomando k^{-1}, si existiese, tendríamos

$$k^{-1} \cdot k \cdot a \equiv k^{-1} \cdot k \cdot b,$$

y como $k^{-1} \cdot k \equiv 1$ llegamos a que $a \equiv b$, justo lo que buscábamos.

En caso de que k no tuviese inverso, podríamos tomar un divisor de m coprimo con k como nos indica el Lema 6.12 y después simplificar al ser ya k invertible.

Ejemplo 6.7 Queremos como antes simplificar $2 \cdot 3 \equiv 2 \cdot 10 \pmod{14}$. Como $\text{mcd}(2, 14) = 2 \neq 1$ no podemos tomar el inverso de 2 para simplificarlo de ambos lados de la ecuación en congruencias. Sin embargo, como 7 es divisor de 14 sabemos que

$$2 \cdot 3 \equiv 2 \cdot 10 \pmod{14} \implies 2 \cdot 3 \equiv 2 \cdot 10 \pmod{7} \implies 3 \equiv 10 \pmod{7},$$

donde en el último paso ya hemos podido tomar el inverso al ser 7 un número primo.

De hecho en general tenemos el siguiente resultado.

Proposición 6.3

Dada la relación $k \cdot a \equiv k \cdot b \pmod{m}$ entonces $a \equiv b \pmod{n}$, donde

$$n = \frac{m}{mcd(k, m)}.$$

Para simplificar no necesitamos calcular el inverso, únicamente saber dónde existe y, por tanto, si podemos hacerlo. Sin embargo, habrá ejercicios donde conocerlo pueda resultar interesante o pueda darnos la solución directamente. ¿Cómo podemos encontrarlo?

Encontrar el inverso de a módulo m equivale a resolver la ecuación en congruencias

$$a \cdot b \equiv 1 \pmod{m}.$$

Pero esto es lo mismo que decir que $a \cdot b - 1$ es múltiplo de m. Es decir, que existe $n \in \mathbb{Z}$ tal que

$$a \cdot b - 1 = m \cdot n.$$

Reordenando tenemos que

$$a \cdot b - m \cdot n = 1,$$

donde a y m son conocidos, b y n son enteros a encontrar y b será el inverso. Este tipo de ecuaciones se llaman ecuaciones diofánticas y muchos ejercicios de congruencias se pueden trasladas a este tipo de ecuaciones. No obstante, estas ecuaciones quedan fuera del contenido del capítulo. Sin embargo, esto es también la expresión directa de la Identidad de Bezout o Lema de Bezout.

Lema 6.13 (Identidad de Bezout)

Sean a y m enteros existen b y n enteros tal que

$$a \cdot b + m \cdot n \equiv mcd(a, m).$$

La parte interesante es cómo encontrar dicho b y n y esto se hace mediante el algoritmo de Euclides. Este sirve también para calcular cual es el máximo común divisor de dos números.

El algoritmo consta de los siguientes pasos:

1. Se divide el número mayor entre el menor.
2. Se comprueba el resto de la división:
   - Si es cero (la división es exacta), el divisor es el mcd.
   - Si no es cero, repetimos el primer paso con el divisor y el resto.

Veamos un ejemplo para que queda todo más claro.

Ejemplo 6.8 Queremos calcular el mcd de 42 y 15. Para empezar hacemos

$$\begin{array}{r|l} 42 & 15 \\ \hline 12 & 2 \end{array}$$

Como la división no es exacta repetimos hasta obtener una exacta:

$$\begin{array}{r|l} 15 & 12 \\ \hline 3 & 1 \end{array} \quad \Longrightarrow \quad \begin{array}{r|l} 12 & 3 \\ \hline 0 & 4 \end{array}$$

Luego el mcd(42,15) = 3. ¿Cómo encontramos ahora b y n tal que $42b + 15n = 3$? Para ellos utilizaremos que el dividendo menos el divisor por el cociente da el resto. Así, de la segunda división sabemos que

$$15 - 12 \cdot 1 = 3.$$

Como la primera nos dice que $12 = 42 - 15 \cdot 2$ sustituimos el valor de 12. Así obtenemos

$$15 - (42 - 15 \cdot 2) \cdot 1 = 3 \quad \Longrightarrow \quad 15 - 42 + 15 \cdot 2 = 3 \quad \Longrightarrow \quad 42 \cdot (-1) + 15 \cdot 3 = 3.$$

Luego $b = -1$ y $n = 3$, aunque esta solución no es único y podemos encontrar más por otros procedimientos.

6.5 Algunas congruencias importantes y la propiedad cíclica

A parte de resolver los típicos ejercicios de congruencias, existen algunas que, sin ser preguntadas de forma explícita, su uso resulta muy conveniente.

Por ejemplo, gracias a las congruencias podemos conocer las últimas cifras de un número de forma sencilla. Por supuesto, esto solo es útil cuando el número es muy grande y no tenemos su expresión numérica completa para mirarlas.

Ejemplo 6.9 ¿En qué cifra termina $((2^3)^4)^5$? Pues haciendo congruencias módulo 10 tenemos que

$$((2^3)^4)^5 = (8^4)^5 = ((8^2)^2)^5 = (64^2)^5 \equiv (4^2)^5 \equiv 6^5 = 6^2 \cdot 6^2 \cdot 6 \equiv 6 \cdot 6 \cdot 6 = 36 \cdot 6 \equiv 36 \equiv 6$$

Al hacer congruencias módulo 10 obtenemos el resto de dividir entre 10 que es precisamente la última cifra. Pero en general podemos ir más allá:

Lema 6.14

Las últimas k cifras de un número n son $a_1a_2 \dots a_k$ si y solo si $n \equiv a_1a_2 \dots a_k \pmod{10^k}$.

Nota: *En el hipotético caso de que no estemos trabajando en base decimal deberemos cambiar el 10 por la base correspondiente.*

Otra congruencia que tiene cierto valor especial es la del 9, como nos indica el próximo lema.

Lema 6.15

Si las cifras de un número n suman k entonces

$$n \equiv k \pmod 9$$

Demostración La forma de ver que es cierto consiste en darse cuenta que si un número n tiene cifras $a_k a_{k-1} \dots a_1 a_0$ entonces, al estar estas cifras en base 10, tenemos que

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10 + a_0.$$

Aplicando módulo 9, como $10 \equiv 1$, nos queda

$$n \equiv a_k + a_{k-1} + \dots + a_1 + a_0 \pmod 9.$$

■

Esto sirve para probar los criterios de divisibilidad del 3 y del 9. Aunque procedimientos similares de descomponer el número en base 10 sirve para otros criterios (2, 4, 5, 8, 11,. . .). Podría ser interesante tratar de probarlos o incluso encontrar algún otro.

Por último, una propiedad que puede resultarnos útil es saber que los restos tienen un comportamiento cíclico al aplicar sucesivas potencias.

Lema 6.16

Los restos de dividir m^n entre k se repiten en un ciclo de longitud $l = |n_1 - n_2| \leq k$ donde n_1 y n_2 son los menores naturales distintos tal que $m^{n_1} \equiv m^{n_2} \pmod k$.

Una idea intuitiva de porque este hecho es cierto es que dichos restos son números que van desde 0 hasta $k-1$. Es decir, solo pueden tomar unos pocos valores. Pero el exponente n no tiene límite. Así, tras k aumentos de n, si no antes, no quedarán restos libres para elegir y se tendrá que repetir. Así, en un ciclo de longitud l tendremos que los restos potenciales se repiten cada l unidades, es decir, para $n_3 \in \mathbb{N}$ se tiene que

$$m^n \equiv m^{n+n_3 \times l} \pmod k.$$

Ejemplo 6.10 En módulo 7 tenemos que $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 1$, $2^4 \equiv 2$, $2^5 \equiv 4$, $2^6 \equiv 1 \dots$ Luego

$$2^k \equiv \begin{cases} 1 \pmod 7 & \text{si } k \equiv 0 \pmod 3, \\ 2 \pmod 7 & \text{si } k \equiv 1 \pmod 3, \\ 4 \pmod 7 & \text{si } k \equiv 2 \pmod 3, \end{cases} \iff 2^k \equiv \begin{cases} 1 \pmod 7 & \text{si } k = 3n \text{ (múltiplo de 3)}, \\ 2 \pmod 7 & \text{si } k = 3n+1, \\ 4 \pmod 7 & \text{si } k = 3n+2. \end{cases}$$

Así de forma directa podemos saber que como $2021 \equiv 2 \pmod 3$, entonces $2^{2021} \equiv 4 \pmod 7$.

6.6 Principales teoremas

Aunque la ciclicidad de es útil, hay ocasiones donde estos ciclos son muy grandes y no resultan nada prácticos. Es por eso que para estos casos podremos hacer uso de herramientas más poderosas como la que nos enuncia el siguiente teorema propuesto por Pierre de Fermat en 1636.

Teorema 6.1 (Pequeño teorema de Fermat)

Si p es un número primo y a es entero, entonces

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

Este mismo teorema, cuando $p \nmid a$ podemos escribirlo como

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

En este caso, $a \cdot a^{p-2} \equiv 1$, luego $a^{-1} \equiv a^{p-2}$. Si bien este tal vez no es el inverso más pequeño que podemos encontrar, sí que es una forma de calcular al menos uno sin necesidad de aplicar el algoritmo de Euclides.

Con estos resultados seremos capaces de resolver algunos de los problemas anteriormente propuestos con mayor agilidad, pero también podremos resolver nuevos como en el siguiente ejemplo.

Ejemplo 6.11 Ahora sin aplicar ciclos podemos llegar a saber que

$$2^{2021} = 2^{(6\cdot 336+5)} = (2^6)^{336} \cdot 2^5 \equiv 1^{336} \cdot 2^5 \equiv 2^5 \equiv 32 \equiv 4 \pmod{7}.$$

Por otro lado, otro famoso teorema que podemos aplicar cuando la base es prima es el siguiente:

Teorema 6.2 (Teorema de Wilson)

Si p es un número primo, entonces

$$(p-1)! \equiv p-1 \equiv -1 \pmod{p}$$

Finalmente, aunque no vayamos a hacer uso de él en este capítulo, conviene enunciar el que probablemente sea el teorema más importante de la aritmética modular.

Teorema 6.3 (Teorema de Euler-Fermat)

Si el mcd$(a, m) = 1$, entonces $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Aquí tenemos un resultado mucho más potente que el enunciado por el Pequeño Teorema de Fermat. Este se puede aplicar no solo en módulos primos, sino en cualquiera. Aunque requiere conocer la función φ («phi») de Euler. Aunque no es objetivo ya de este capítulo, $\varphi(m)$ es el número de naturales menores que m coprimos con él. Aunque para ahorrarnos cuenta presenta tres propiedades interesantes:

1. $\varphi(m \cdot n) = \varphi(m)\varphi(n)$ si mcd$(m, n) = 1$.
2. $\varphi(p) = p - 1$ si p es primo, obteniéndose así el Pequeño Teorema de Fermat.
3. $\varphi(p^k) = (p-1)p^{k-1}$ si p es primo.

6.7 Sistemas de congruencias

Hasta ahora hemos resuelto congruencias sencillas con una sola ecuación. Por ejemplo $n \cong 3 \pmod{6}$ tiene por soluciones: 3, 9, 15, -3, -9. . . En general todas las soluciones son de la forma $\pm 6k+3$. Sin embargo estas son ecuaciones muy simples y es frecuente encontrarse con situaciones donde se juntan varias condiciones que restringen el número de soluciones. Así que vamos a ver algunas formas de resolver sistemas de congruencias:

Proposición 6.4

$$\begin{cases} n \equiv k \pmod{a_1} \\ n \equiv k \pmod{a_2} \\ \vdots \\ n \equiv k \pmod{a_k} \end{cases} \Rightarrow n \equiv k \pmod{mcm(a_1, a_2, \ldots, a_k)}$$

Aunque esta primera propiedad es sencilla ya nos permite resolver problemas como el siguiente:

Problema 6.1 En una escalera, si bajamos los peldaños de 2 en 2 nos sobra 1, si los bajamos de 3 en 3 nos sobran 2, si los bajamos de 4 en 4 nos sobran 3, si los bajamos de 5 en 5 nos sobran 4, si los bajamos de 6 en 6 nos sobran 5 y de 7 en 7 no sobra ninguno. ¿Cuántos peldaños tiene como mínimo la escalera?

Solución *El primer paso es darse cuenta que en realidad casi todas las n son congruentes al mismo valor. Así:*

$$\begin{cases} n \equiv 1 \pmod 2 \\ n \equiv 2 \pmod 3 \\ n \equiv 3 \pmod 4 \\ n \equiv 4 \pmod 5 \\ n \equiv 5 \pmod 6 \\ n \equiv 0 \pmod 7 \end{cases} \Rightarrow \begin{cases} n \equiv -1 \pmod 2 \\ n \equiv -1 \pmod 3 \\ n \equiv -1 \pmod 4 \\ n \equiv -1 \pmod 5 \\ n \equiv -1 \pmod 6 \\ n \equiv 0 \pmod 7 \end{cases}$$

Aplicando ahora la Proposición 6.4 llegamos a que $n \equiv -1$ módulo 60. Es decir, $n + 1$ es múltiplo de 60. Los posibles n son por tanto $59, 119, 179 \ldots$ Pero como además debe ser múltiplo de 7, debe tener 119 peldaños.

Teorema 6.4 (Teorema chino del resto)

Sean $p_1, p_2, \ldots, p_k$ enteros coprimos entre sí dos a dos, entonces

$$\begin{cases} x \equiv a_1 \pmod{p_1} \\ x \equiv a_2 \pmod{p_2} \\ \vdots \\ x \equiv a_k \pmod{p_k} \end{cases}$$

tiene una única solución módulo $p_1 \cdot p_2 \cdots p_k$.

Y dicha solución es

$$x = \sum_{i=i}^{k} a_i s_i N_i$$

donde s_i se obtiene de la identidad de Bezout tal que

$$r_i p_i + s_i N_i = 1 \qquad \text{y} \qquad N_i = \frac{p_1 \cdot p_2 \cdots p_k}{p_i}.$$

Aunque es algo farragoso, lo normal será tener unas pocas ecuaciones en el sistema, 2 o 3 como mucho. De esta forma, no suele llevar muchos pasos. Un ejemplo de aplicación de este teorema se esconde detrás del siguiente enunciado:

Ejemplo 6.12 Proponle a un amigo que piense un número entero positivo menor que 1000 y que, tras dividirlo por 7, por 11 y por 13, te diga los respectivos restos a, b y c. Entonces tú les dirás que su número es el resto de dividir por 1001 el número

$$715a + 364b + 924c.$$

¿De dónde salen estos tres números? Pues salen de aplicar el Teorema chino del resto.

6.8 Problemas de olimpiadas matemáticas

A continuación vamos a mostrar y resolver un par de problemas de olimpiada donde vamos a juntar todo lo visto a lo largo de este capítulo.

Problema 6.2 (Olimpiada Matemática Española, Fase Nacional, Ciudad Real 2004). ¿Existe alguna potencia de 2 que al escribirla en el sistema decimal tenga todos sus dígitos distintos de cero y sea posible reordenar los mismos para formar con ellos otra potencia de 2? Justificar la respuesta.

Solución *En un primer momento puede parecernos que poco tiene que ver con la aritmética modular. Sin embargo eso de las cifras puede recordarnos a algunaa congruencia que hemos visto.*

Para empezar vamos a suponer que existen esas dos potencias con las mismas cifras. Llamémoslas 2^n *y* 2^m *con* $n < m$*. Como tienen las mismas cifras entonces*

$$2^n \equiv 2^m \pmod 9,$$

es decir

$$2^n - 2^m = 2^n(1 - 2^{m-n}) \equiv 0 \pmod 9.$$

Como $2^n(1 - 2^{m-n})$ *es múltiplo de 9 y* 2^n *no lo es*[1]*, entonces*

$$1 \equiv 2^{m-n} \pmod 9.$$

Veamos ahora si es posible que $2^{m-n} \equiv 1 \pmod 9$*. Antes de nada, como son números distintos y tienen el mismo número de cifras sabemos que*

$$1 < \frac{2^m}{2^n} < 10 \quad \Longrightarrow \quad 0 < m - n < \log_2 10 \approx 3,3219$$

Luego $m - n$ *puede valer* 1, 2 *o* 3*. Sin embargo, tanto* 2^1*, como* 2^2 *y* 2^3 *no son congruentes con 1 módulo 9. Por lo tanto, no existe tal potencia.*

Problema 6.3 (Olimpiada Matemática Española, Fase Nacional, 1994). Una oficina de turismo realiza una encuesta sobre el tiempo en seis regiones a lo largo de un año, obteniendo como resultado el Cuadro 6.3.

Región	Soleados o lluviosos	Inclasificables
A	336	29
B	321	44
C	335	30
D	343	22
E	329	36
F	330	35

Cuadro 6.3: Registro metereológico por regiones.

[1]El número no tiene más que al 2 como factor n veces y a ningún 3.

La persona encargada de la encuesta tiene esos datos más detallados aunque no los haya compartido. Se da cuenta de que, prescindiendo de una de las regiones, el número de días lluviosos pasa a ser la tercera parte del de días soleados. ¿Cuál es la región que omite para obtener dicho resultado?

Solución *Fijémonos solo en los datos de días soleados o lluviosos, omitiendo los inclasificables que no juegan ningún papel en este problema más allá de justificar el resto de días hasta 365. El enunciado nos dice que los soleados son el triple que los lluviosos. Luego si llamamos n a los lluviosos, los soleados son $3n$ y soleados o lluviosos hacer un total de $4n$, múltiplo de 4.*

Así, módulo 4 tenemos

$$336 \equiv 0 \qquad 335 \equiv 3 \qquad 329 \equiv 1$$
$$321 \equiv 1 \qquad 343 \equiv 3 \qquad 330 \equiv 2$$

Si sumamos todas las regiones obtenemos

$$336 + 321 + 335 + 343 + 329 + 330 \equiv 0 + 3 + 1 + 1 + 3 + 2 \equiv 10 \equiv 2 \pmod 4.$$

Luego para que la suma quede múltiplo de cuatro, es decir congruente con cero, la única posibilidad omitiendo una única región sería prescindir de la región F.

Ejercicios Propuestos

1. ¿Es 53 228 916 divisible por 156?

2. ¿Es 5 089 050 divisible por 220?

3. ¿Cuánto vale la cifra α para que $48\,\alpha 83\,332$ sea divisible por 26?

4. ¿Para qué valores de n el número $3^{6n} + 5^{6n}$ es divisible por 13?

5. Prueba que 3^{100} es la suma de 9 enteros consecutivos.

6. Prueba que $p^2 \equiv 1 \pmod{24}$ si p es un primo mayor que 3.

7. Hallar el resto de dividir por 7 el número $5555^{2222} + 2222^{5555}$.

8. ¿Son divisibles por 5 las expresiones $n^5 - n$, $n^5 - 1$ y $n^4 - 1$?

9. Resuelve el sistema de ecuaciones en congruencias
$$\begin{cases} 2x + 3 \equiv 1 \pmod{11}, \\ 3x \equiv 5 \pmod{8}. \end{cases}$$

10. Resuelve el sistema de ecuaciones en congruencias
$$\begin{cases} x \equiv 3 \pmod{19}, \\ x \equiv 7 \pmod{13}. \end{cases}$$

Bibliografía Adicional

1. Engel, A. (1998). Number Theory. *Problem-Solving Strategies*. Editorial Springer, 117-160.

2. Guitérrez Jiménez, J. M. & Lanchares Barrasa, V. (2010). *Elementos de matemática discreta*. Servicio de Publicaciones de la Universidad de La Rioja. https://dialnet.unirioja.es/servlet/libro?codigo=424510