Seminario de problemas. Curso 2017–18

Estrategias matemáticas: congruencias

Sea m un entero positivo. Decimos que dos enteros a y b son congruentes módulo m si tienen el mismo resto al dividir por m, y se expresa

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

(Cuidado: Aunque el entero sea negativo, al dividir por m hay que quedarse con un resto positivo, y ese resto al hacer la división será un número entre 0 y $m-1$). Por ejemplo,

$$22 = 2 \cdot 9 + 4, \quad 94 = 10 \cdot 9 + 4, \quad 4 = 0 \cdot 9 + 4, \quad -23 = -3 \cdot 9 + 4,$$

así que

$$22 \equiv 94 \equiv 4 \equiv -23 \pmod{9}.$$

También podemos decir que dos enteros a y b son congruentes módulo m si m divide a $a-b$. Esto es equivalente a la definición que hemos dado al principio pues, si tomamos

$$a = a_1 m + r, \quad b = b_1 m + s,$$

tendremos $a - b = (a_1 - b_1)m + (r - s)$, luego resulta evidente que m divide a $a-b$ si y sólo si los dos restos r y s coinciden.

Usar congruencias es muy útil en muchos problemas aritméticos, sobre todo cuando aparecen cuestiones de divisibilidad. Según como sea el problema, a veces resulta más natural pensar en la primera definición que hemos dado (coincidencia de resto al dividir por m), y otras veces en la segunda (m divide a la resta).

Al efectuar congruencias módulo m, los únicos números importantes son $0, 1, 2, \ldots, m-1$, pues cualquier otro número entero es equivalente a uno de esos. Por ejemplo, módulo 5 tenemos

$$\begin{aligned}
\cdots \equiv -15 \equiv -10 \equiv -5 \equiv 0 \equiv 5 \equiv 10 \equiv 15 \equiv 20 \equiv \cdots \pmod{5},\\
\cdots \equiv -14 \equiv -9 \equiv -4 \equiv 1 \equiv 6 \equiv 11 \equiv 16 \equiv 21 \equiv \cdots \pmod{5},\\
\cdots \equiv -13 \equiv -8 \equiv -3 \equiv 2 \equiv 7 \equiv 12 \equiv 17 \equiv 22 \equiv \cdots \pmod{5},\\
\cdots \equiv -12 \equiv -7 \equiv -2 \equiv 3 \equiv 8 \equiv 13 \equiv 18 \equiv 23 \equiv \cdots \pmod{5},\\
\cdots \equiv -11 \equiv -6 \equiv -1 \equiv 4 \equiv 9 \equiv 14 \equiv 19 \equiv 24 \equiv \cdots \pmod{5}.
\end{aligned}$$

Todos los números de la misma línea son, esencialmente, el mismo, así que los consideramos agrupados y basta quedarse con un representante de todos ellos; normalmente, los representantes elegidos son $0, 1, 2, 3, 4$, pero daría igual si fuesen otros (a veces, estas agrupaciones se denotan $\widehat{0}, \widehat{1}, \widehat{2}, \widehat{3}, \widehat{4}$, pero no hace falta que lo hagamos). En general, al quedarnos con el representante módulo m (y considerar a todos sus congruentes agrupados con él), los enteros $\mathbb{Z}$ se agrupan en paquetitos (que se denominan clases de equivalencia), y esto se denota así:

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}.$$

Las congruencias se comportan muy bien con sumas y productos, ya que

$$a \equiv b \pmod{m},\ c \equiv d \pmod{m} \ \Rightarrow\ a+c \equiv b+d \pmod{m},\ a \cdot c \equiv b \cdot d \pmod{m}.$$

Vamos a comprobarlo para el producto (con la suma es similar): tenemos $a = a_1 m + r$, $b = b_1 m + r$, $c = c_1 m + s$, $d = d_1 m + s$, con lo cual

$$\begin{aligned} a \cdot c &= (a_1 m + r)(c_1 m + s) = (a_1 c_1 m + r c_1 + s a_1) m + rs \equiv rs \pmod{m}, \\ b \cdot d &= (b_1 m + r)(d_1 m + s) = (b_1 d_1 m + r d_1 + s b_1) m + rs \equiv rs \pmod{m}; \end{aligned}$$

luego, efectivamente, $a \cdot c \equiv b \cdot d \pmod{m}$. Este buen comportamiento es crucial, pues permite definir las operaciones suma y producto en $\mathbb{Z}_m$, ya que lo que sale al operar no depende del representante elegido.

Con congruencias se puede restar, pero no siempre se pude dividir. Sí que se puede dividir (por un número no nulo) cuando el módulo es un número primo. En general, también puede ocurrir que el producto de dos números no nulos sea nulo módulo m, por ejemplo, $2 \cdot 3 \equiv 0 \pmod{6}$. Eso tampoco sucede cuando el módulo es un primo. De hecho, cuando el módulo es primo, hay muchas más propiedades que se podrían mostrar. En particular, una muy importante es la siguiente:

Teorema pequeño de Fermat. *Sea p un primo y a un entero que no es divisible por p. Entonces,*

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

A menudo, este resultado se escribe en su forma equivalente $a^p \equiv a \pmod{p}$ que es válida incluso aunque p divida a a (pues la hipótesis $p \nmid a$ sólo añade el caso trivial $a^p \equiv 0 \equiv a \pmod{p}$). Ambos enunciados son equivalentes puesto que, si p divide a $a^p - a = (a^{p-1} - 1)a$ y a no es múltiplo de p (un primo), entonces p debe dividir a $a^{p-1} - 1$.

Demostración del teorema pequeño de Fermat. Probemos que $a^p - a$ es múltiplo de p por inducción sobre a. Para $a = 0$ o $a = 1$ es trivial. Ahora, supuesto que a lo cumple, para $a + 1$, desarrollando por el binomio de Newton, podemos escribir

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k = 1 + \sum_{k=1}^{p-1} \binom{p}{k} a^k + a^p;$$

entonces, teniendo en cuenta que

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!}, \qquad 1 \le k \le p-1,$$

es múltiplo de p (por ser primo, el p del numerador no se puede cancelar con ninguno de los factores del denominador), y que, por hipótesis de inducción, $a^p - a$ también es múltiplo de p, se sigue que

$$(a+1)^p - (a+1) = \sum_{k=1}^{p-1} \binom{p}{k} a^k + (a^p - a)$$

es múltiplo de p. Esto probaría el enunciado para los enteros positivos. Para los negativos, cuando $p = 2$ el resultado es trivial; y, en otro caso, al cambiar a por $-a$ obtenemos $(-a)^p - (-a) = -(a^p - a)$, luego podemos remitirnos a lo visto para los positivos. □

Aunque no lo vamos a usar (y tampoco lo vamos a demostrar), cuando m es producto de dos primos distintos hay un resultado similar (también hay un teorema, denominado teorema de Euler-Fermat, que muestra qué ocurre para m un entero positivo cualquiera, pero necesitaríamos explicar bastantes más cosas para dar la expresión correspondiente):

Teorema de la media de Fermat. *Sean p y q dos primos distintos y a un entero que no es divisible por p ni por q. Entonces,*

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

Puede resultar increíble, ¡pero esos dos teoremas son la base de toda la criptografía moderna! Eso es muy interesante, pero nos estamos apartando de nuestro objetivo, que es ver cómo aplicar las congruencias a la resolución de problemas.

Comencemos mostrando cómo las congruencias son la base de algunos criterios de divisibilidad:

Criterio (Divisibilidad por 9)**.** Un número es divisible por 9 si y sólo si la suma de sus dígitos es divisible por 9.

Demostración. Sea n el número, y escribámoslo (en base 10) como

$$n = a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0, \quad a_j \in \{0, 1, 2, \ldots, 8, 9\}.$$

Como $10 \equiv 1 \pmod 9$, tenemos

$$\begin{aligned} n &= a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0 \\ &\equiv a_k 1^k + a_{k-1}1^{k-1} + \cdots + a_2 1^2 + a_1 1 + a_0 \\ &\equiv a_k + a_{k-1} + \cdots + a_2 + a_1 + a_0 \pmod 9, \end{aligned}$$

luego 9 divide a n si y sólo si divide a $a_k + a_{k-1} + \cdots + a_2 + a_1 + a_0$. □

Como también $10 \equiv 1 \pmod 3$, de la misma forma se demuestra lo siguiente:

Criterio (Divisibilidad por 3)**.** Un número es divisible por 3 si y sólo si la suma de sus dígitos es divisible por 3.

Criterio (Divisibilidad por 11)**.** Para ver si un número n es divisible por 11, sea P la suma de sus cifras de lugar par, e I la suma de sus cifras de lugar impar. Entonces, n es divisible por 11 si y sólo si si $P - I$ es divisible por 11.

Demostración. Como $10 \equiv -1 \pmod{11}$, tenemos

$$\begin{aligned} n &= a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0 \\ &\equiv a_k (-1)^k + a_{k-1}(-1)^{k-1} + \cdots + a_2 (-1)^2 + a_1 (-1) + a_0 \\ &\equiv P - I \pmod{11}, \end{aligned}$$

luego 11 divide a n si y sólo si divide a $P - I$. □

Criterio (Divisibilidad por 7)**.** Para ver si un número n es divisible por 7, agrupemos sus dígitos de tres en tres, y sea P la suma de los grupos de lugar par, e I la suma de los grupos de lugar impar. Entonces, n es divisible por 7 si y sólo si $P - I$ es divisible por 7.

Demostración. Si n el número, escribirlo agrupando sus dígitos de tres en tres es poner

$$n = a_k 1000^k + a_{k-1}1000^{k-1} + \cdots + a_2 1000^2 + a_1 1000 + a_0, \quad a_j \in \{0, 1, 2, \ldots, 998, 999\}.$$

Como $1001 = 7 \cdot 11 \cdot 13$, 7 divide a $1000 + 1$, o $1000 \equiv -1 \pmod 7$. Entonces,

$$\begin{aligned} n &= a_k 1000^k + a_{k-1}1000^{k-1} + \cdots + a_2 1000^2 + a_1 1000 + a_0 \\ &\equiv a_k(-1)^k + a_{k-1}(-1)^{k-1} + \cdots + a_2(-1)^2 + a_1(-1) + a_0 \\ &\equiv P - I \pmod 7, \end{aligned}$$

luego 7 divide a n si y sólo si divide a $P - I$. □

Por la misma razón (13 divide a 1001) también se cumple lo siguiente:

Criterio (Divisibilidad por 13)**.** Para ver si un número n es divisible por 13, agrupemos sus dígitos de tres en tres, y sea P la suma de los grupos de lugar par, e I la suma de los grupos de lugar impar. Entonces, n es divisible por 13 si y sólo si $P - I$ es divisible por 13.

Finalmente, veamos algunos problemas que se resuelven usando congruencias:

Problema 1. Comprueba que $7^n - 1$ es divisible por 6 para cualquier $n \geq 1$.

Solución. Obsérvese que decir «m divide a a» equivale a «$a \equiv 0 \pmod m$». En nuestro caso, $7^n - 1 \equiv 1^n - 1 \equiv 1 - 1 \equiv 0 \pmod 6$, ¡y ya está! □

Problema 2. ¿Qué cifra falta en la igualdad 14! = 87178_91200?

Solución. Apliquemos lo que sabemos de las congruencias módulo 9. Observemos que 14! es múltiplo de 9, así que 87178_91200 debe ser múltiplo de 9 y, en consecuencia, la suma de sus cifras debe ser múltiplo de 9. De ahí sale de manera inmediata que la cifra que falta es un 2. □

Problema 3. Sean m y n enteros tales que $m^2 + n^2$ es múltiplo de 3. Probar que tanto m como n son múltiplos de 3.

Solución. Módulo 3, tendremos $n \equiv 0 \pmod 3$ o $n \equiv \pm 1 \pmod 3$, y su cuadrado es, respectivamente, $n^2 \equiv 0 \pmod 3$ o $n^2 \equiv 1 \pmod 3$. Lo mismo ocurre con m. De aquí queda claro que $m^2 + n^2 \equiv 0 \pmod 3$ si y solo si $n \equiv 0 \pmod 3$ y $m \equiv 0 \pmod 3$. □

Problema 4. Calcular el resto al dividir 2^{2017} entre 7.

Solución. Como $2^3 = 8 \equiv 1 \pmod 7$, tenemos

$$2^{2017} = 2^{3 \cdot 672 + 1} = (2^3)^{672} \cdot 2 \equiv 1^{672} \cdot 2 \equiv 2 \pmod 7,$$

así que el resto es 2. (También podíamos haber usado que, por el teorema pequeño de Fermat, $2^6 \equiv 1 \pmod 7$, pero no ha hecho falta.) □

Problema 5. Demostrar que si $n + 2$ es primo, $n > 1$, entonces $n2^n + 1$ no es primo.

Solución. Por el teorema pequeño de Fermat, $2^{n+1} \equiv 1 \pmod{n+2}$. Entonces,

$$2(n2^n + 1) = n2^{n+1} + 2 \equiv n + 2 \equiv 0 \pmod{n+2},$$

luego $n+2$ divide a $2(n2^n+1)$. Pero $n+2$ es primo e impar, así que $n+2$ divide a $n2^n+1$ y este número no puede ser primo. □