Divisibilidad y congruencias

Ana Rechtman Bulajich y Carlos Jacob Rubio Barrios

Revista Tzaloa, año 1, número 2

Empecemos por explicar el significado de la palabra divisibilidad. En este texto vamos a trabajar únicamente con los números enteros. Un número entero r es divisible entre un número entero s ($s \neq 0$), si el resultado de la división $\frac{r}{s}$ es un número entero. Por ejemplo, 9 es divisible entre 3, ya que $\frac{9}{3} = 3$, pero 11 no es divisible entre 3 porque $\frac{11}{3} = 3.66\ldots$ que no es un número entero. Dicho de otra forma, los números que son divisibles entre 3 son los múltiplos de 3.
Existen diferentes criterios de divisibilidad, es decir, métodos que nos permiten determinar si un número es o no divisible entre otro. En muchos casos, es más sencillo utilizar los criterios de divisibilidad que efectuar directamente la división. Por ejemplo, para el número 3 el criterio es: *un entero positivo es divisible entre 3 si y sólo si la suma de sus dígitos es divisible entre 3.*

¿Qué quiere decir esta frase? ¿Por qué es cierta esta afirmación?

Si y sólo si quiere decir que si un número es divisible entre 3 la suma de sus dígitos es divisible entre 3, y que si la suma de los dígitos de un número es divisible entre 3, el número también lo es. Podemos cambiar este criterio de divisibilidad entre 3 por: *un número no es divisible entre* 3 *si y sólo si la suma de sus dígitos no es divisible entre* 3.
Tratemos de dar una *demostración* matemática al criterio de divisibilidad entre 3. Consideremos un entero positivo n, y escribámoslo en notación decimal:

$$n = a_0 + 10a_1 + 10^2a_2 + \cdots + 10^ka_k,$$

donde los números $a_0, a_1, \ldots, a_k$ son los dígitos de n. Entonces la suma de los dígitos de n es igual a $a_0 + a_1 + \cdots + a_k$. Observemos que para todo entero positivo $l \geq 1$:

$$10^l - 1 = 9(\underbrace{11\ldots1}_{l \text{ veces}}).$$

Por ejemplo:

$$\begin{aligned} 10 - 1 &= 9 = 9(1) \\ 10^2 - 1 &= 99 = 9(11) \\ 10^3 - 1 &= 999 = 9(111), \end{aligned}$$

etcétera. Entonces tenemos que:

$$\begin{aligned} n - (a_0 + a_1 + \cdots + a_k) &= (10-1)a_1 + (10^2-1)a_2 + \cdots + (10^k-1)a_k \\ &= 9(a_1 + 11a_2 + \cdots + \underbrace{11\ldots1}_{k \text{ veces}}a_k). \end{aligned}$$

El lado derecho de la ecuación es divisible entre 9, en particular, es divisible entre 3. Así que si el número es divisible entre 3, $a_0 + a_1 + \cdots + a_k$ tiene que ser divisible entre 3. Análogamente

si $a_0 + a_1 + \cdots + a_k$ es divisible entre 3, el número n tiene que ser divisible entre 3. Es decir, hemos demostrado el criterio de divisibilidad entre 3. De hecho, también demostramos el criterio de divisibilidad entre 9.
Vamos a introducir una nueva notación. Consideremos un entero cualquiera x. Al dividir x entre 3, obtenemos un cociente b y un residuo c, donde c es igual a 0, 1 ó 2. Es decir, $x = 3b + c$. Ahora bien, vamos a decir que x *es congruente con* c *módulo* 3, denotado por $x \equiv c \pmod 3$, si c es el residuo que se obtiene al dividir x entre 3. Por ejemplo:

$$\begin{aligned} 100 = 3 \cdot 33 + 1 &\Rightarrow 100 \equiv 1 \pmod 3 \\ 242 = 3 \cdot 80 + 2 &\Rightarrow 242 \equiv 2 \pmod 3 \\ 48 = 3 \cdot 16 &\Rightarrow 48 \equiv 0 \pmod 3. \end{aligned}$$

Sin embargo podemos escribir también:

$$\begin{aligned} 242 &\equiv -1 \pmod 3 \\ 242 &\equiv 5 \pmod 3 \\ 242 &\equiv -4 \pmod 3. \end{aligned}$$

Es decir, $242 \equiv d \pmod 3$ si el número $242 - d$ es divisible entre 3. Por ejemplo, $242 \equiv -4 \pmod 3$ ya que $242 - (-4) = 246 = 3(82)$.
Con este nuevo concepto vamos a demostrar el criterio de divisibilidad entre 3. Como antes, consideramos un entero positivo $n = a_0 + 10a_1 + \cdots + 10^k a_k$, donde a_0, $a_1, \ldots, a_k$ son los dígitos de n. Tenemos que para todo entero $l \geq 1$, el número $10^l - 1$ es divisible entre 3, es decir $10^l \equiv 1 \pmod 3$. Vamos a demostrar entonces que:

1. $10^l a_l \equiv a_l \pmod 3$ para todo $1 \leq l \leq k$;
2. $n = a_0 + 10a_1 + \cdots + 10^k a_k \equiv a_0 + a_1 + \cdots + a_k \pmod 3$.

Para ver que el primer punto es cierto, vamos a demostrar que si $x \equiv c \pmod 3$, entonces $a \cdot x \equiv a \cdot c \pmod 3$ para todo entero positivo a. La demostración de este hecho es muy sencilla. Si escribimos $x = 3b + c$, para algún entero b, tenemos que $a \cdot x = 3(a \cdot b) + a \cdot c$ lo que prueba la afirmación anterior. Entonces como $10^l \equiv 1 \pmod 3$ obtenemos que $10^l a_l \equiv a_l \pmod 3$.
Enfoquémonos ahora en el segundo punto. Lo que queremos demostrar es que si tenemos dos enteros x_1 y x_2 tales que:

$$\begin{aligned} x_1 &\equiv c_1 \pmod 3, \\ x_2 &\equiv c_2 \pmod 3, \end{aligned}$$

entonces $x_1 + x_2 \equiv c_1 + c_2 \pmod 3$. Sabemos que existen números b_1 y b_2 tales que $x_1 = 3b_1 + c_1$ y $x_2 = 3b_2 + c_2$. Esto implica que $x_1 + x_2 = 3(b_1 + b_2) + (c_1 + c_2)$, o dicho de otra forma que $x_1 + x_2 \equiv c_1 + c_2 \pmod 3$.
Regresando a la demostración del criterio de divisibilidad entre 3, concluimos que:

$$n \equiv a_0 + a_1 + \cdots + a_k \pmod 3.$$

Dicho de otra forma, n es divisible entre 3 si y sólo si la suma de sus dígitos es divisible entre 3.
Hasta ahora hemos definido las congruencias módulo 3, pero podemos hacerlo para cualquier entero positivo m. Decimos entonces que un entero x es congruente con un entero c módulo m, si el número $x - c$ es divisible entre m y escribimos $x \equiv c \pmod m$.
Veamos algunos ejemplos para aclarar esta definición.

- $91 \equiv 1 \pmod{10}$ pues $91 - 1 = 90$ es múltiplo de 10;

- $2n + 1 \equiv 1 \pmod{n}$, ya que $2n + 1 - 1 = 2n$ es múltiplo de n;
- $8 \not\equiv 2 \pmod{5}$, pues $8 - 2 = 6$ no es múltiplo de 5.

Según la definición anterior, la notación $x \equiv c \pmod{m}$ significa que x lo podemos escribir como $c + mb$ para algún entero b. Si $c = 0$, entonces $x \equiv 0 \pmod{m}$ significa que x es múltiplo de m.
En la demostración del criterio de divisibilidad entre 3, demostramos dos propiedades que son válidas también cuando trabajamos módulo m. Es decir, tenemos que:

1. si $x \equiv c \pmod{m}$ entonces $a \cdot x \equiv a \cdot c \pmod{m}$ para todo entero positivo a;
2. si $x_1 \equiv c_1 \pmod{m}$ y $x_2 \equiv c_2 \pmod{m}$, entonces $x_1 + x_2 \equiv c_1 + c_2 \pmod{m}$.

A continuación demostraremos unas cuantas propiedades más, que nos serán útiles para resolver problemas más adelante.

Propiedades de la congruencia. Sea m un entero positivo y sean b, c, d, x, y enteros. Entonces:

1. $x \equiv x \pmod{m}$.
2. Si $x \equiv c \pmod{m}$, entonces $c \equiv x \pmod{m}$.
3. Si $x \equiv c \pmod{m}$ y $c \equiv d \pmod{m}$, entonces $x \equiv d \pmod{m}$.
4. Si $x \equiv c \pmod{m}$ y $y \equiv d \pmod{m}$, entonces $xy \equiv cd \pmod{m}$.
5. Si $x \equiv c \pmod{m}$, entonces $x^n \equiv c^n \pmod{m}$ para todo entero positivo n.
6. Si $xb \equiv bc \pmod{m}$, entonces $x \equiv c \pmod{\frac{m}{(b,m)}}$ donde (b, m) denota el máximo común divisor de b y m.

Demostración. Las propiedades 1 y 2 son inmediatas, pues $x - x = 0$ es múltiplo de m, y si $x - c = mb$ para algún entero b, entonces $c - x = m(-b)$.
Para demostrar la propiedad 3, supongamos que $x - c = mb_1$ y $c - d = mb_2$ para algunos enteros b_1 y b_2. Entonces $x - d = (x - c) + (c - d) = m(b_1 + b_2)$, de donde $x \equiv d \pmod{m}$.
Para demostrar la propiedad 4, supongamos que $x - c = mb_1$ y $y - d = mb_2$ para algunos enteros b_1 y b_2. Entonces:

$$xy - cd = (x - c)y + (y - d)c = m(b_1 y + b_2 c),$$

de donde $xy \equiv cd \pmod{m}$.
La demostración de la propiedad 5 la haremos por inducción en n (ver el Criterio **??** del apéndice). Si $n = 1$ no hay nada que demostrar, pues por hipótesis tenemos que $x \equiv c \pmod{m}$. Supongamos que la congruencia $x \equiv c \pmod{m}$ implica la congruencia $x^k \equiv c^k \pmod{m}$ para algún entero $k > 1$. Entonces, aplicando la propiedad 4 tenemos que:

$$x \cdot x^k \equiv c \cdot c^k \pmod{m},$$

es decir, $x^{k+1} \equiv c^{k+1} \pmod{m}$. Esto completa la inducción. (¿Cómo demostraría el lector la propiedad 5 sin usar inducción?).
Para demostrar la propiedad 6, supongamos que $xb - bc = mk$ para algún entero k. Si dividimos esta igualdad entre $g = (b, m)$, tenemos que $(x - c)\frac{b}{g} = \frac{m}{g}k$. Como $\frac{b}{g}$ y $\frac{m}{g}$ son primos relativos (¿por qué?) y $\frac{m}{g}$ divide a $(x - c)\frac{b}{g}$, tenemos que $\frac{m}{g}$ divide a $x - c$. Es decir, $x \equiv c \pmod{\frac{m}{g}}$.

Para entrenarnos en la utilización de los módulos, vamos a demostrar los siguientes criterios de divisibilidad.

1. Un entero positivo n es divisible entre 2 si y sólo si su dígito de las unidades es par.

2. Un entero positivo n es divisible entre 4 si y sólo si el número formado por sus dos últimos dígitos es divisible entre 4.

3. Un entero positivo n es divisible entre 8 si y sólo si el número formado por sus tres últimos dígitos es divisible entre 8.

4. Un entero positivo n es divisible entre 9 si y sólo si la suma de sus dígitos es divisible entre 9.

5. Un entero positivo n es divisible entre 11 si y sólo si la suma de los dígitos de n en posición par menos la suma de los dígitos de n en posición impar, es divisible entre 11.

Demostraciones. Usaremos congruencias para demostrar estos criterios, así como lo hicimos con el criterio de divisibilidad entre 3. Como antes, consideremos la notación decimal de n:

$$n = a_0 + 10a_1 + 10^2a_2 + \cdots + 10^k a_k.$$

1. Como $10 \equiv 0 \pmod 2$, tenemos que $10^l \equiv 0 \pmod 2$ para todo entero $l \geq 1$ y por lo tanto $n = a_0 + 10a_1 + 10^2a_2 + \cdots + 10^k a_k \equiv a_0 \pmod 2$. De aquí que n es divisible entre 2, o dicho de otra forma, $n \equiv 0 \pmod 2$ si y sólo si $a_0 \equiv 0 \pmod 2$ si y sólo si a_0 es par. Es decir, n es divisible entre 2 si y sólo si su dígito de las unidades es par.
2. Como $10 \equiv 2 \pmod 4$, tenemos que $10^2 \equiv 2^2 \equiv 0 \pmod 4$. De aquí que si $l \geq 2$, entonces:

$$10^l = 10^2 \cdot 10^{l-2} \equiv 0 \cdot 10^{l-2} = 0 \pmod 4.$$

Luego, $n \equiv a_0 + 10a_1 \pmod 4$. Por lo tanto, n es divisible entre 4, o equivalentemente $n \equiv 0 \pmod 4$, si y sólo si $a_0 + 10a_1 \equiv 0 \pmod 4$. Esto ocurre solamente cuando el número $a_0 + 10a_1$, formado por los dos últimos dígitos de n, es divisible entre 4.
3. Como $10 \equiv 2 \pmod 8$, tenemos que $10^3 \equiv 2^3 \equiv 0 \pmod 8$. Luego, para todo entero $l \geq 3$:

$$10^l = 10^3 \cdot 10^{l-3} \equiv 0 \cdot 10^{l-3} = 0 \pmod 8.$$

De aquí que $n \equiv a_0 + 10a_2 + 10^2a_2 \pmod 8$. Por lo tanto, n es divisible entre 8, o bien $n \equiv 0 \pmod 8$, si y sólo si $a_0 + 10a_1 + 10^2a_2 \equiv 0 \pmod 8$. Es decir, esto ocurre cuando el número $a_0 + 10a_1 + 10^2a_2$ formado por los tres últimos dígitos de n es divisible entre 8.
4. Como $10 \equiv 1 \pmod 9$, tenemos que $10^l \equiv 1 \pmod 9$ para todo entero $l \geq 1$. Luego, $n \equiv a_0 + a_1 + a_2 + \cdots + a_k \pmod 9$. Por lo tanto, n es divisible entre 9, o bien $n \equiv 0 \pmod 9$, si y sólo si $a_0 + a_1 + a_2 + \cdots + a_k \equiv 0 \pmod 9$. Entonces, n es divisible entre 9 si y sólo si la suma de sus dígitos es divisible entre 9.
5. Como $10 \equiv -1 \pmod{11}$, tenemos que $10^l \equiv \pm 1 \pmod{11}$ dependiendo si l es par o impar. Luego:

$$n \equiv a_0 - a_1 + a_2 - \cdots + (-1)^k a_k \pmod{11}.$$

Por lo tanto, n es divisible entre 11 si y sólo si $n \equiv 0 \pmod{11}$ si y sólo si:

$$a_0 - a_1 + a_2 - \cdots + (-1)^k a_k \equiv 0 \pmod{11}.$$

Por lo tanto, n es divisible entre 11 si y sólo si la suma de los dígitos de n en posición par menos la suma de los dígitos de n en posición impar es divisible entre 11.

Veamos ahora la utilidad de las congruencias en problemas de olimpiada.

Problema 1. Demuestre que ningún entero de la forma $4n+3$ se puede escribir como la suma de dos cuadrados de enteros.

Solución. Si a es un entero, entonces $a \equiv 0, 1, 2$ ó $3 \pmod 4$. Luego, $a^2 \equiv 0 \pmod 4$ ó $a^2 \equiv 1 \pmod 4$. De aquí que los residuos posibles al dividir entre 4 para la suma de dos cuadrados de enteros son $0+0=0$, $0+1=1$ ó $1+1=2$. Como un entero de la forma $4n+3$ es congruente con 3 módulo 4, tenemos que no es posible escribirlo como la suma de dos cuadrados de enteros.

Problema 2. Sean a y b enteros tales que $a+5b$ y $5a-b$ son ambos múltiplos de 2002. Demuestre que a^2+b^2 también es múltiplo de 2002.

Solución. Observemos primero que si un entero r es múltiplo de un entero s, entonces r^2 es múltiplo de s^2. Usando congruencias, esto lo podemos escribir como: $r \equiv 0 \pmod s$ implica que $r^2 \equiv 0 \pmod{s^2}$. Usaremos esta propiedad en la solución del problema.
Si $a+5b \equiv 0 \pmod{2002}$ y $5a-b \equiv 0 \pmod{2002}$, entonces:

$$(a+5b)^2 \equiv 0 \pmod{2002^2} \qquad \text{y} \qquad (5a-b)^2 \equiv 0 \pmod{2002^2}.$$

Luego, $(a+5b)^2+(5a-b)^2 \equiv 0 \pmod{2002^2}$. Simplificando tenemos que:

$$26(a^2+b^2) \equiv 0 \pmod{2002^2}.$$

Utilizando la propiedad número 6 de las congruencias, tenemos que:

$$a^2+b^2 \equiv 0 \pmod{77 \cdot 2002}.$$

Esto implica que a^2+b^2 es divisible entre $77(2002)$, en particular es divisible entre 2002. Por lo tanto, $a^2+b^2 \equiv 0 \pmod{2002}$.

Problema 3. Determine todas las parejas de enteros positivos (m,n) que satisfacen la ecuación $3^m+7=2^n$.

Solución. Observemos que $3^m+7 \equiv 0+1 \equiv 1 \pmod 3$, ya que $3 \equiv 0 \pmod 3$ y $7 \equiv 1 \pmod 3$. Luego, $2^n \equiv 1 \pmod 3$. Ahora, como $2 \equiv -1 \pmod 3$ tenemos que $2^n \equiv (-1)^n \pmod 3$. Por lo tanto, n es par. Supongamos que $n=2k$. Entonces, la ecuación original es equivalente a la ecuación $3^m+7=4^k$. Intentemos ahora con congruencias módulo 4. Tenemos que $4^k-7 \equiv 0-(-1)=1 \pmod 4$, ya que $4 \equiv 0 \pmod 4$ y $7 \equiv -1 \pmod 4$. Luego, 3^m debe ser congruente con 1 módulo 4. Como $3 \equiv -1 \pmod 4$, tenemos que $3^m \equiv (-1)^m \pmod 4$, de modo que m debe ser par. Supongamos que $m=2p$. Entonces la ecuación original es equivalente a la ecuación $3^{2p}+7=2^{2k}$. Es decir:

$$7 = 2^{2k}-3^{2p} = (2^k-3^p)(2^k+3^p).$$

Como 7 es número primo y $2^k-3^p < 2^k+3^p$, la única posibilidad es que $2^k-3^p=1$ y $2^k+3^p=7$. Resolviendo este sistema de ecuaciones, encontramos que $k=2$ y $p=1$. Es decir, $m=2$ y $n=4$.

Problema 4. Sea n un entero mayor que 6. Demuestre que si $n-1$ y $n+1$ son ambos números primos, entonces $n^2(n^2+16)$ es múltiplo de 720. ¿Es cierto el recíproco?

Solución. Notemos primero que si $n \equiv 1, 2, 3, 4$ ó $5 \pmod 6$, entonces alguno de $n-1$ ó $n+1$ no sería primo. Luego, $n \equiv 0 \pmod 6$. Sea $n=6m$ con m entero positivo. Tenemos que

$$n^2(n^2+16) = (6m)^2((6m)^2+16) = 144m^2(9m^2+4).$$

Si $m \equiv 0 \pmod 5$, entonces $n^2(n^2+16)$ es múltiplo de $144 \times 5 = 720$. Si m es congruente a ± 1 módulo 5, entonces n es de la forma $30a \pm 6$ y es fácil ver que alguno de $n-1$ ó $n+1$ es múltiplo de 5 y no sería primo. Por último si $m \equiv \pm 2 \pmod 5$, entonces $9m^2 + 4 \equiv 9(4) + 4 \equiv 0 \pmod 5$ y por lo tanto, $n^2(n^2+16)$ es múltiplo de $144 \times 5 = 720$.
Ahora veamos que el recíproco es falso. Para esto, basta encontrar un entero $n > 6$ tal que $n^2(n^2+16)$ es múltiplo de 720 y alguno de los números $n-1$ ó $n+1$ no es primo. Si $n = 720$, entonces es fácil ver que $n^2(n^2+16)$ es múltiplo de 720, pero $n+1 = 721 = 7 \times 103$ no es primo.

Concluimos esta sección con algunos ejercicios para el lector.

Ejercicios

1. Sean n y r enteros tales que $n \equiv r \pmod 7$. Demuestre que:

$$1000n \equiv 7 - r \pmod 7.$$

2. Demuestre que un entero n es divisible entre 5 si y sólo si su dígito de las unidades es divisible entre 5.

3. Sean p y q números primos distintos. Demuestre que un entero es divisible entre pq si y sólo si es divisible entre p y entre q. Deduzca los criterios de divisibilidad entre 6 y entre 10.

4. Determine todos los enteros positivos n tales que $\underbrace{111\ldots1}_{n \text{ veces}} \equiv 0 \pmod{101}$.

5. Sea p un primo y sean a y n enteros positivos. Demuestre que si $2^p + 3^p = a^n$, entonces $n = 1$.

6. Sea n un entero positivo y sean $a < b < c < d$ los cuatro divisores positivos más pequeños de n. Determine todos los enteros n tales que $n = a^2 + b^2 + c^2 + d^2$.

Bibliografía

1. D. Fomin, S. Genkin, I. Itenberg. *Mathematical Circles (Russian Experience)*. American Mathematical Society. 1996.

2. C.J. Rubio Barrios. *Problemas para la* 20^a *Olimpiada Mexicana de Matemáticas (Problemas Avanzados)*. 2006.

3. C.J. Rubio Barrios. *Problemas para la* 21^a *Olimpiada Mexicana de Matemáticas (Problemas Avanzados)*. 2007.