Cálculo de Potencias. Criterios de Divisibilidad.

Alan Reyes-Figueroa
Teoría de Números (Aula 08) 05.agosto.2021

Bases

Aplicación: Cálculo de potencias grandes módulo n.

Con frecuencia deseamos calcular el valor de una potencia $a^k \pmod{n}$, cuando k es grande. ¿Existe una forma eficiente de obtener este cálculo?

Uno de esos procedimientos, es llamado el **algoritmo exponencial binario**, y se basa en elevar al cuadrado de forma sucesiva, módulo n.
Más específicamente, el exponente k se escribe en forma binaria, como

$$k = (a_m a_{m-1} \cdots a_2 a_1 a_0)_2 = \sum_{k=0}^{m} a_k d^k,$$

y los valores $a^{2^j} \pmod{n}$ se calculan para las potencias de 2, que corresponden a los 1's en la representación binaria de k. Estos resultados parciales luego se multiplican para dar la respuesta final.

Bases

Ejemplo: Calcular $5^{110} \pmod{131}$.

Primero, expresamos el exonente 110 en base 2 como

$$110 = 64 + 32 + 8 + 4 + 2 = 2^6 + 2^5 + 2^3 + 2^2 + 2^1 = (1101110)_2.$$

Obtenemos ahora las potencias de $5^{2^j} \pmod{131}$, correspondientes a los 1's en la representación anterior:

$$\begin{aligned}
5^2 &\equiv 25 \pmod{131}, \\
5^4 &\equiv 25^2 \equiv 625 \equiv 101 \pmod{131}, \\
5^8 &\equiv 101^2 \equiv 10201 \equiv 114 \pmod{131}, \\
5^{16} &\equiv 114^2 \equiv 12996 \equiv 27 \pmod{131}, \\
5^{32} &\equiv 27^2 \equiv 729 \equiv 74 \pmod{131}, \\
5^{64} &\equiv 74^2 \equiv 5476 \equiv 105 \pmod{131}.
\end{aligned}$$

Bases

Multiplicamos ahora los resultados parciales, correspondientes a los 1's en la expansión binaria del exponente

$$5^{110} = 5^{64} \cdot 5^{32} \cdot 5^{8} \cdot 5^{4} \cdot 5^{2} \equiv 105 \cdot 74 \cdot 114 \cdot 101 \cdot 25 \equiv 60 \pmod{131}.$$

Como una variación del procedimiento anterior, se podrían calcular módulo 131, las potencias $5^2, 5^3, 5^6, 5^{12}, 5^{24}, 5^{48}, 5^{96}$ para llegar al resultado

$$5^{110} = 5^{96} \cdot 5^{12} \cdot 5^{2} \equiv 41 \cdot 117 \cdot 25 \equiv 60 \pmod{131},$$

lo que requeriría menos multiplicaciones.

Teorema

Sea $P(x) = \sum_{k=0}^{m} c_k x^k$ una función polinomial de x, con coeficientes enteros $c_k \in \mathbb{Z}$. Si $a \equiv b \pmod{n}$, entonces $P(a) \equiv P(b) \pmod{n}$.

Prueba: Como $a \equiv b \pmod{n}$, de las propiedades de congruencias, tenemos que $a^k \equiv b^k \pmod{n}$, para todo $k = 0, 1, 2, \ldots, m$. Luego, $c_k a^k \equiv c_k b^k \pmod{m}$, para todo $k = 0, 1, 2, \ldots, n$. Sumando todas estas congruencias, se obtiene

$$P(a) = \sum_{k=0}^{m} c_k a^k \equiv \sum_{k=0}^{m} c_k b^k = P(b) \pmod{n}.$$

Corolario

Si a es una solución de $P(x) \equiv 0 \pmod{n}$ y $a \equiv b \pmod{n}$, entonces b también es una solución.

Prueba: Del teorema, $a \equiv \pmod{n}$ implica que $P(a) \equiv P(b) \pmod{n}$. Por tanto, si a es una solución de $P(x) \equiv 0 \pmod{n}$, entonces $P(b) \equiv P(a) \equiv 0 \pmod{n}$, y b una solución.

Mostramos ahora algunos de los criterios de divisibilidad que comúnmente usamos. Para ello, consideramos la representación de un número entero n en base 10:

$$n = (a_d \ldots a_2 a_1 a_0)_{10} = \sum_{k=0}^{d} a_k 10^k.$$

Criterio del 2: Como $10 \equiv 0 \pmod 2$, entonces

$$n = \sum_{k=0}^{d} a_k 10^k \equiv \underbrace{\sum_{k=1}^{d} a_k 10^k}_{\equiv 0} + a_0 \equiv a_0 \pmod 2.$$

Así, $n \equiv 0 \pmod 2 \;\Leftrightarrow\; a_0 \equiv 0 \pmod 2$.
Luego, $2 \mid n \;\Leftrightarrow\; 2 \mid a_0$, esto es, **un número es par, si y sólo si su último dígito es par**.

Criterio del 5: De igual forma, como $10 \equiv 0 \pmod 5$, entonces

$$n = \sum_{k=0}^{d} a_k 10^k \equiv \sum_{k=1}^{d} a_k 10^k + a_0 \equiv a_0 \pmod 5.$$

Así, $n \equiv 0 \pmod 5 \iff a_0 \equiv 0 \pmod 5$. Luego, $5 \mid n \iff 5 \mid a_0$, esto es, **un número es divisible entre 5, si y sólo si su último dígito es 0 ó 5**.

Criterio del 10: De nuevo, como $10 \equiv 0 \pmod{10}$, entonces

$$n = \sum_{k=0}^{d} a_k 10^k \equiv \sum_{k=1}^{d} a_k 10^k + a_0 \equiv a_0 \pmod{10}.$$

Así, $n \equiv 0 \pmod{10} \iff a_0 \equiv 0 \pmod{10}$. Luego, $10 \mid n \iff 10 \mid a_0$, esto es, **un número es divisible entre 10, si y sólo si su último dígito es 0**.

Criterios de Divisibilidad

Criterio del 4: Observe que $10 \equiv 2 \pmod 4$, y $10^k \equiv 0 \pmod 4$, para $k \geq 2$. Entonces

$$n = \sum_{k=0}^{d} a_k 10^k \equiv \sum_{k=2}^{d} a_k 1^k + a_1 10 + a_0 \equiv 10a_1 + a_0 \pmod 4.$$

Así, $n \equiv 0 \pmod 4 \;\Leftrightarrow\; (a_1a_0)_{10} = 10a_1 + a_0 \equiv 0 \pmod 4$. Luego, $4 \mid n \;\Leftrightarrow\; 4 \mid (a_1a_0)_{10}$, esto es, **un número es divisible entre 4, si y el número formado por sus últimos dos dígitos es múltiplo de 4**.

Criterio del 8: Observe que $10^k \equiv 0 \pmod 8$, para $k \geq 3$. Entonces

$$n = \sum_{k=0}^{d} a_k 10^k \equiv \sum_{k=3}^{d} a_k 1^k + a_2 10^2 + a_1 10 + a_0 \equiv 100a_2 + 10a_1 + a_0 \pmod 8.$$

Así, $n \equiv 0 \pmod 8 \;\Leftrightarrow\; (a_2a_1a_0)_{10} = 100a_2 + 10a_1 + a_0 \equiv 0 \pmod 8$. Luego, $8 \mid n \;\Leftrightarrow\; 8 \mid (a_2a_1a_0)_{10}$, esto es, **un número es divisible entre 8, si y el número formado por sus últimos tres dígitos es múltiplo de 8**.

Criterios de Divisibilidad

Criterio del 3: Observe que $10 \equiv 1 \pmod 3$, entonces

$$n = \sum_{k=0}^{d} a_k 10^k \equiv \sum_{k=0}^{d} a_k 1^k \equiv \sum_{k=0}^{d} a_k \pmod 3.$$

Así, $n \equiv 0 \pmod 3 \;\Leftrightarrow\; \sum_{k=0}^{d} a_k \equiv 0 \pmod 3$. Luego, $3 \mid n \;\Leftrightarrow\; 3 \mid \sum_{k=0}^{d} a_k$, esto es, **un número es divisible entre 3, si y sólo si la suma de sus dígitos es múltiplo de 3.**

Criterio del 9: Observe que $10 \equiv 1 \pmod 9$, entonces

$$n = \sum_{k=0}^{d} a_k 10^k \equiv \sum_{k=0}^{d} a_k 1^k \equiv \sum_{k=0}^{d} a_k \pmod 9.$$

Así, $n \equiv 0 \pmod 9 \;\Leftrightarrow\; \sum_{k=0}^{d} a_k \equiv 0 \pmod 9$. Luego, $9 \mid n \;\Leftrightarrow\; 9 \mid \sum_{k=0}^{d} a_k$, esto es, **un número es divisible entre 9, si y sólo si la suma de sus dígitos es múltiplo de 9.**

Criterio del 11: Observe que $10 \equiv -1 \pmod{11}$, entonces

$$n = \sum_{k=0}^{d} a_k 10^k \equiv \sum_{k=0}^{d} a_k (-1)^k \pmod{11}.$$

Así, $n \equiv 0 \pmod{11} \;\Leftrightarrow\; \sum_{k=0}^{d}(-1)^k a_k \equiv 0 \pmod{11}$. Luego, $11 \mid n \;\Leftrightarrow\; 11 \mid \sum_{k=0}^{d}(-1)^k a_k$, esto es, **un número es divisible entre 11, si y sólo si la suma alterna de sus dígitos es múltiplo de 11**.

Existen otros criteros que son combinación de los anterioes. Por ejemplo:

- n es divisible entre 6 si, y sólo si, es divisible entre 2 y es divisible entre 3.
- n es divisible entre 15 si, y sólo si, es divisible entre 3 y es divisible entre 5.

Estamos interesados en generar criterios para números primos, por lo general, números terminados en 1, 3, 7 ó 9.

Criterios de Divisibilidad

Criterio del 7: Dado $n = (a_d \dots a_2 a_1 a_0)_{10}$, consideramos los números que se obtienen de separar la última cifra de n, esto es

$$a_d \dots a_2 a_1 \mid a_0 \quad \longrightarrow \quad (a_d \dots a_2 a_1)_{10} \text{ y } a_0.$$

En particular, el número $q = (a_d \dots a_2 a_1)_{10}$ corresponde a $\frac{n-a_0}{10}$, y tenemos que $n = 10q + a_0$.

Consideramos ahora el número $F(n) = q - 2a_0 = \frac{n-a_0}{10} - 2a_0$. Observe ahora que en módulo 7

$$\begin{aligned} F(n) = q - 2a_0 \equiv 0 \pmod 7 \quad &\iff \quad q \equiv 2a_0 \pmod 7 \iff 10q \equiv 20a_0 \pmod 7 \\ &\iff \quad n = 10q + a_0 \equiv 21a_0 \equiv 0 \pmod 7. \end{aligned}$$

Luego, $7 \mid n \;\Leftrightarrow\; 7 \mid F(n) = q - 2a_0$. Este tipo de criterios radica en reducir la divisibilidad módulo k de n, a un número mucho menor ($F(n)$ es aproximadamente la décima parte de n).

Ejemplo: ¿Es 441 divisible entre 7? ¿Y 1846?

Aplicamos el criterio anterior de forma sucesiva:

$$441 \equiv 44 - 2(1) = 42 \equiv 4 - 2(2) \equiv 0 \pmod 7.$$

Como $7 \mid 0$, esto muestra que $7 \mid 441$.

En el otro caso, de nuevo aplicamos el criterio

$$1846 \equiv 184 - 2(6) = 172 \equiv 17 - 2(2) = 13 \equiv 6 \pmod 7.$$

Como $7 \nmid 13$, esto muestra que $7 \nmid 1846$.

Criterios de Divisibilidad

Mostramos un criterio de divisibilidad general para números terminados en 1,3, 7, ó 9.

Al igual que en el caso del 7, si $n = (a_d \dots a_2 a_1 a_0)_{10}$, consideramos los números que se obtienen de separar la última cifra de n: $q = (a_d \dots a_2 a_1)_{10} = \frac{n - a_0}{10}$ y a_0, de modo que $n = 10q + a_0$.

Definimos el número $F(n)$ en función de la terminación del módulo m en el cual queremos dividir:

$$F(n) = q + ta_0, \; \text{donde } t = \begin{cases} \dfrac{9m+1}{10} = 9k+1, & \text{si } m = 10k+1; \\ \dfrac{3m+1}{10} = 3k+1, & \text{si } m = 10k+3; \\ \dfrac{7m+1}{10} = 7k+5, & \text{si } m = 10k+7; \\ \dfrac{m+1}{10} = k+1, & \text{si } m = 10k+9. \end{cases}$$

Veremos que la divisibilidad de un número módulo m, se reduce a mostrar la divisibilidad de $F(n)$ módulo m. Para ello, dividimos la prueba en casos:

Criterios de Divisibilidad

- $\underline{m = 10k+1}$:
  $F(n) = q + ta_0 = q + (9k+1)a_0 \equiv q + (10k+1)a_0 - ka_0 \equiv q - ka_0 \pmod{m}$. Luego $F(n) \equiv 0 \pmod{m} \;\Rightarrow\; q \equiv ka_0 \pmod{m}$ y
  $$\begin{aligned} n = 10q + a_0 &\equiv 10(ka_0) + a_0 \equiv (10k+1)a_0 \pmod{m} \\ &\equiv 0 \pmod{m}. \end{aligned}$$
  Entonces $F(n) \equiv 0 \pmod{m} \;\Rightarrow\; n \equiv 0 \pmod{m}$.

- $\underline{m = 10k+3}$:
  $F(n) = q + ta_0 = q + (3k+1)a_0 \equiv q + (10k+3)a_0 - 7ka_0 - 2a_0 \equiv q - 7ka_0 - 2a_0 \pmod{m}$. Luego $F(n) \equiv 0 \pmod{m} \;\Rightarrow\; q \equiv 7ka_0 + 2a_0 \pmod{m}$ y
  $$\begin{aligned} n = 10q + a_0 &\equiv 10(7ka_0 + 2a_0) + a_0 \equiv 7(10k+3)a_0 \pmod{m} \\ &\equiv 0 \pmod{m}. \end{aligned}$$
  Entonces $F(n) \equiv 0 \pmod{m} \;\Rightarrow\; n \equiv 0 \pmod{m}$.

Criterios de Divisibilidad

- $\underline{m = 10k + 7}$:
  $F(n) = q + ta_0 = q + (7k+5)a_0 \equiv q + (10k+7)a_0 - 3ka_0 - 2a_0 \equiv q - 5ka_0 - 2a_0 \pmod{m}$. Luego $F(n) \equiv 0 \pmod{m} \Rightarrow q \equiv 3ka_0 + 2a_0 \pmod{m}$ y

$$\begin{aligned} n = 10q + a_0 &\equiv 10(3ka_0 + 2a_0) + a_0 \equiv 3(10k+7)a_0 \pmod{m} \\ &\equiv 0 \pmod{m}. \end{aligned}$$

  Entonces $F(n) \equiv 0 \pmod{m} \Rightarrow n \equiv 0 \pmod{m}$.

- $\underline{m = 10k + 9}$:
  $F(n) = q + ta_0 = q + (k+1)a_0 \equiv q + (10k+9)a_0 - 9ka_0 - 8a_0 \equiv q - 9ka_0 - 8a_0 \pmod{m}$. Luego $F(n) \equiv 0 \pmod{m} \Rightarrow q \equiv 9ka_0 + 8a_0 \pmod{m}$ y

$$\begin{aligned} n = 10q + a_0 &\equiv 10(9ka_0 + 8a_0) + a_0 \equiv 9(10k+9)a_0 \pmod{m} \\ &\equiv 0 \pmod{m}. \end{aligned}$$

  Entonces $F(n) \equiv 0 \pmod{m} \Rightarrow n \equiv 0 \pmod{m}$.

Criterios de Divisibilidad

Ejemplo: Criterio de divisibilidad entre 7.

$m = 7$ es de la forma $10(0) + 7$, de modo que $F(n) = q + (7k+5)a_0 \equiv q + 5a_0 \equiv q - 2a_0 \pmod 7$.
Por ejemplo, si quisiéramos saber si $7 \mid 1810$. Hacemos

$$1810 \equiv 181 - 2(0) \equiv 181 \equiv 18 - 2(1) \equiv 16 \equiv 2 \pmod 7.$$

Como $7 \nmid 16$, esto muestra que $7 \nmid 1810$.

Ejemplo: Criterio de divisibilidad entre 93.

$m = 93$ es de la forma $10(9) + 3$, de modo que $F(n) = q + (3k+1)a_0 \equiv q + 28a_0 \pmod{93}$.
Por ejemplo, si quisiéramos saber si $93 \mid 174189$. Hacemos

$$\begin{aligned} 174189 &\equiv 17418 + 28(9) \equiv 17670 \equiv 1767 + 28(0) \equiv 1767 \equiv 176 + 28(7) \equiv 372 \equiv 37 + 28(2) \\ &\equiv 93 \equiv 0 \pmod{93}. \end{aligned}$$

Como $93 \mid 93$, esto muestra que $93 \mid 174189$.

Ejemplo: Criterio de divisibilidad entre 47.

$m = 47$ es de la forma $10(4) + 7$, de modo que
$F(n) = q + (7k + 5)a_0 \equiv q + 33a_0 \equiv q - 14a_0 \pmod{47}$.
Por ejemplo, si quisiéramos saber si $47 \mid 2021$. Hacemos

$$2021 \equiv 202 - 14(1) \equiv 188 \equiv 18 - 14(8) \equiv -94 \equiv 0 \pmod{47}.$$

Como $47 \mid -94$, esto muestra que $47 \mid 2021$.

Ejemplo: Criterio de divisibilidad entre 95.

$95 = 5 \cdot 19$. Basta estudiar el criterio del 19. $m = 19$ es de la forma $10(1) + 9$, de modo que $F(n) = q + (k + 1)a_0 \equiv q + 2a_0 \pmod{19}$.
Por ejemplo, si quisiéramos saber si $19 \mid 11325$. Hacemos

$$11305 \equiv 1130 + 2(5) \equiv 1140 \equiv 114 + 2(0) \equiv 114 \equiv 11 + 2(4) \equiv 19 \equiv 0 \pmod{19}.$$

Como $19 \mid 19$, esto muestra que $19 \mid 11305$. Además, $5 \mid 11305$, de modo que $95 \mid 11305$.