Elementos de Matemáticas y Aplicaciones - Entrega 1

Victoria Eugenia Torroja Rubio

9 de diciembre de 2024

Ejercicio 1. Establece criterios de divisibilidad entre 2, 3, 4, 5, 6, 7 y 8 de un número en función de los dígitos de su expresión en base 8.
Por ejemplo, un número es múltiplo de 2 cuando la última cifra de su expresión en base 8 es 0, 2, 4 o 6.

Solución 1. Criterio del 2. El criterio de divisibilidad del 2 en base 8 nos viene dado en el enunciado, por tanto, solo tenemos que demostrarlo. Sea $n \in \mathbb{N}$ y sea

$$n = a_k 8^k + \cdots + a_1 8 + a_0 = \sum_{i=0}^{k} a_i 8^i$$

su expresión en base 8. Si $a_0 \in \{0,2,4,6\}$, $a_0 \equiv 0 \mod 2$. Como $8 \equiv 0 \mod 2$,

$$n \equiv a_k 8^k + \cdots + a_1 8 + a_0 \equiv a_k \cdot 0 + \cdots + a_1 \cdot 0 + a_0 \equiv 0 \mod 2.$$

Recíprocamente, si $a_0 \notin \{0,2,4,6\}$ no sería divisible entre 2, pues el resto de elementos de $\mathbb{Z}_8$ son impares y, por ello, indivisibles entre 2.

Criterio del 3. Tenemos que $8 \equiv 2 \mod 3$, $8^2 \equiv 1 \mod 3$ y, en general

$$8^{2k} \equiv \left(8^2\right)^k \equiv 1 \mod 3 \quad \text{y} \quad 8^{2k+1} \equiv 8^{2k} \cdot 8 \equiv 2 \mod 3, \text{ con } k \in \mathbb{N}.$$

Entonces, el criterio de divisibilidad del 3 consiste en que el doble de las cifras de posición par más la suma de las cifras de posición impar [1] debe ser múltiplo de 3 (las cifras están en base 8). Es decir, asumiendo, sin pérdida de generalidad, que $n = a_{2k}8^{2k} + \cdots + a_1 8^1 + a_0$ es necesario y suficiente que,

$$n \equiv a_{2k}8^{2k} + \cdots + a_1 8^1 + a_0 \equiv \sum_{i=0}^{k} a_{2i} 8^{2i} + \sum_{i=1}^{k} a_{2i-1} 8^{2i-1} \equiv \sum_{i=0}^{k} a_{2i} + 2\sum_{i=1}^{k} a_{2i-1} \equiv 0 \mod 3$$

Criterio del 4. Tenemos que $8 \equiv 0 \mod 4$. Por tanto, para que un número n sea divisible entre 4, su última cifra en base 8 tiene que ser 0 o 4. En efecto,si $a_0 \in \{0,4\}$,

$$n \equiv a_k 8^k + \cdots + a_1 8 + a_0 \equiv a_k \cdot 0 + \cdots + a_1 \cdot 0 + a_0 \equiv 0 \mod 4.$$

Si $a_0 \notin \{0,4\}$, entonces no sería divisible entre 4, pues en $\mathbb{Z}_8$ los únicos elementos divisibles entre 4 son 0 y 4.

[1] En todos los casos, los coeficientes de n en base 8 son elementos de $\mathbb{Z}_8$. Además, las cifras de posición impar son aquellas con subíndice par y las cifras de posición par son aquellas de subíndice impar.

Criterio del 5. Tenemos que $8 \equiv 3 \mod 5$, $8^2 \equiv 4 \mod 5$, $8^3 \equiv 2 \mod 5$ y $8^4 \equiv 1 \mod 5$. En general, tenemos que si $k \in \mathbb{N}$,

$$\begin{aligned} 8^{4k+1} &\equiv 8^{4k} \cdot 8 \equiv 3 \mod 5 \\ 8^{4k+2} &\equiv 8^{4k} \cdot 8^2 \equiv 4 \mod 5 \\ 8^{4k+3} &\equiv 8^{4k} \cdot 8^3 \equiv 2 \mod 5 \\ 8^{4k+4} &\equiv 8^{4k} \cdot 8^4 \equiv 1 \mod 5. \end{aligned}$$

Así, podemos deducir que el criterio de divisibilidad del 5 en base 8 consiste en que la suma de sus cifras que vayan con un exponente de 8 divisible entre 4, más el triple de la suma de las cifras que vayan acompañadas con 8^k tal que $k \equiv 1 \mod 4$, más cuatro veces la suma de las cifras acompañadas con un 8^k con $k \equiv 2 \mod 4$, más el doble de la suma de las cifras acompañadas con un 8^k donde $k \equiv 3 \mod 4$, sea múltiplo de 5. Asumamos, sin pérdida de generalidad, que $n = a_{4k}8^{4k} + \cdots + a_1 8 + a_0$, entonces debe cumplirse que

$$\begin{aligned} n \equiv & a_{4k}8^{4k} + \cdots + a_1 8 + a_0 \equiv \sum_{i=0}^{k} a_{4i}8^{4i} + \sum_{i=1}^{k} a_{4i-3}8^{4i-3} + \sum_{i=1}^{k} a_{4i-2}8^{4i-2} + \sum_{i=1}^{k} a_{4i-1}8^{4i-1} \\ & \equiv \sum_{i=0}^{k} a_{4i} + 3\sum_{i=1}^{k} a_{4i-3} + 4\sum_{i=1}^{k} a_{4i-2} + 2\sum_{i=1}^{k} a_{4i-1} \equiv 0 \mod 5. \end{aligned}$$

Criterio del 6. El criterio de divisibilidad del 6 consiste en que 4 veces la suma de las cifras de posición impar más dos veces la suma de las cifras de posición par sumen múltiplo de 6. Para demostrar esto vamos a demostrar en primer lugar que $8^{2k} \equiv 4 \mod 6$, donde $k \in \mathbb{N}$. Usamos el método de inducción. Tenemos que $8^2 \equiv 64 \equiv 4 \mod 6$. Asumimos que $8^{2k} \equiv 4 \mod 6$. En el caso $2(k+1)$:

$$8^{2(k+1)} \equiv 8^{2k} \cdot 8^2 \equiv 4 \cdot 4 \equiv 4 \mod 6.$$

Así, $\forall k \in \mathbb{N}$, $8^{2k} \equiv 4 \mod 6$. A partir de este resultado es fácil deducir que

$$8^{2k+1} \equiv 8^{2k} \cdot 8 \equiv 4 \cdot 8 \equiv 2 \mod 6, \ \forall k \in \mathbb{N}.$$

Es decir, asumamos sin pérdida de generalidad que la mayor potencia de 8 de n sea par:

$$n \equiv a_{2k}8^{2k} + \cdots + a_1 8 + a_0 \equiv \sum_{i=0}^{k} a_{2i}8^{2i} + \sum_{i=1}^{k} a_{2i-1}8^{2i-1} \equiv 4\sum_{i=0}^{k} a_{2i} + 2\sum_{i=1}^{k} a_{2i-1} \mod 6.$$

Criterio del 7. Dado que $8 \equiv 1 \mod 7$, para que n sea divisible entre 7 basta que la suma de sus cifras en base 8 sea múltiplo de 7. En efecto,

$$n \equiv a_k 8^k + \cdots + a_1 8 + a_0 \equiv a_k + \cdots + a_1 + a_0 \equiv 0 \mod 7.$$

Criterio del 8. Para que un número n sea divisible entre 8, su última cifra en base 8 debe ser 0 (no puede ser 8 pues las cifras son elementos de $\mathbb{Z}_8$). En efecto, si $a_0 = 0$,

$$n \equiv a_k 8^k + \cdots + a_1 8 + a_0 \equiv a_k \cdot 0 + \cdots + a_1 \cdot 0 + a_0 \equiv 0 \mod 8.$$

Si $a_0 \neq 0$, como $a_0 \in \mathbb{Z}_8$ y ningún otro elemento de $\mathbb{Z}_8$ es divisible entre 8, tenemos que $n \not\equiv 0 \mod 8$.

Ejercicio 2. El ISBN es un código numérico que identifica cada libro.

(a) Utilizando la aritmética modular, describe el algoritmo utilizado para calcular el dígito de control del ISBN de 13 dígitos.

(b) Aplicar el algoritmo anterior para calcular el dígito de control de un libro en el que se ha borrado. El resto del ISBN se ve correctamente: 978-84-131-8779-*.

Solución 2. **(a)** El algoritmo que se utiliza para calcular el dígito de control del ISBN de 13 dígitos consiste en multiplicar las cifras con posición impar por 1 y las cifras con posición par por 3 (las posiciones se cuentan de izquierda a derecha), sumar todos estos productos (a este valor lo denotaremos s), y encontrar el primer número $n \in \mathbb{N}$ que cumple $s + n \equiv 0 \mod 10$. Es decir el número n que buscamos cumple que

$$s + n \equiv 0 \mod 10 \iff n \equiv -s \mod 10.$$

Fuente: `https://www.grupoalquerque.es/mate_cerca/paneles_2012/168_ISBN2.pdf`

(b) En este caso, el valor de s será:

$$s = 9 + 3 \cdot 7 + 8 + 3 \cdot 8 + 4 + 3 \cdot 1 + 3 + 3 \cdot 1 + 8 + 3 \cdot 7 + 7 + 3 \cdot 9 = 138.$$

Así, $n \equiv -s \equiv -138 \equiv 2 \mod 10$. Por tanto, el dígito que buscamos es 2.

Ejercicio 3. **(a)** Encriptar el mensaje: 'CARA', según el algoritmo RSA con clave pública $(n, k) = (65, 5)$.

(b) Comprobar que se recupera el mensaje original, desencriptando el resultado obtenido en **(a)**.

Solución 3. **(a)** En primer lugar, debemos codificar el mensaje (en este caso vamos a usar la tabla que no contiene a la 'ñ'). Entonces, tenemos que el mensaje 'CARA' se traduce a

$$12 \ \ 10 \ \ 27 \ \ 10.$$

A continuación, encriptamos la codificación elevando cada número a 5 y reduciéndolo módulo 65.

$$\begin{aligned}
12^5 &\equiv \left(12^2\right)^2 \cdot 12 \equiv 144^2 \cdot 12 \equiv 14^2 \cdot 12 \equiv 12 \mod 65 \\
10^5 &\equiv \left(10^2\right)^2 \cdot 10 \equiv 100^2 \cdot 10 \equiv 35^2 \cdot 10 \equiv 30 \mod 65 \\
27^5 &\equiv \left(27^2\right)^2 \cdot 27 \equiv 729^2 \cdot 27 \equiv 14^2 \cdot 27 \equiv 27 \mod 65.
\end{aligned}$$

De esta manera, el texto cifrado que obtenemos es el siguiente:

$$12 \ \ 30 \ \ 27 \ \ 30.$$

(b) Para recuperar el mensaje transmitido, debemos encontrar el inverso de 5 módulo $\varphi(65)$ y elevar cada uno de los elementos del cifrado a este número y reducirlo módulo 65. En primer lugar, calculamos la función de Euler para 65. Dado que $65 = 13 \cdot 5$:

$$\varphi(65) = 65 \left(1 - \frac{1}{13}\right)\left(1 - \frac{1}{5}\right) = 12 \cdot 4 = 48.$$

Como $\operatorname{mcd}(5,48)=1$, tenemos que existe $5^{-1} \mod 48$. El número x que buscamos cumple que

$$5x \equiv 1 \mod 48.$$

Para resolver la congruencia comenzamos con encontrar una identidad de Bézout para 5 y 48:

$$1 = 2\cdot 48 + (-19)\cdot 5 \iff (-19)\,5 - 1 = (-2)\,48 \iff (-19)\,5 \equiv 1 \mod 48.$$

Entonces, $x \equiv 5^{-1} \equiv -19 \equiv 29 \mod 48$. Ahora, elevamos cada uno de los elementos del cifrado a 29 y lo reducimos módulo 65.

$$\begin{aligned}
12^{29} \equiv& 12^{16}\cdot 12^{8}\cdot 12^{4}\cdot 12 \equiv 14^{8}\cdot 14^{4}\cdot 14^{2}\cdot 12 \equiv 1^{4}\cdot 1^{2}\cdot 12 \equiv 12 \mod 65\\
30^{29} \equiv& 30^{16}\cdot 30^{8}\cdot 30^{4}\cdot 30 \equiv 55^{8}\cdot 55^{4}\cdot 55^{2}\cdot 30 \equiv 35^{4}\cdot 35^{2}\cdot 35\cdot 30 \equiv 55^{2}\cdot 55\cdot 35\cdot 30\\
\equiv& \underbrace{35^{2}\cdot 55}_{55^2\equiv 35 \mod 65} \cdot 30 \equiv 35\cdot 30 \equiv 10 \mod 65\\
27^{29} \equiv& 27^{16}\cdot 27^{8}\cdot 27^{4}\cdot 27 \equiv 14^{8}\cdot 14^{4}\cdot 14^{2}\cdot 27 \equiv 1^{4}\cdot 1^{2}\cdot 1\cdot 27 \equiv 27 \mod 65.
\end{aligned}$$

Así, recuperamos el mensaje dado por el enunciado, pues 12 10 27 10 $\rightarrow$ 'CARA'.