Matemática Discreta I - 2021/1

Tarea 8

Ejercicios

1. Encontrar el resto de dividir 323^{5843} por 13.
2. Probar **usando congruencias** que todo número de la forma $4^{2n} - 7^n$ es divisible por 9, para todo $n \in \mathbb{N}$.

Antes de resolver los ejercicios, recordemos una propiedad muy útil que cumple las *congruencias*. Si k, m son enteros, con $m \geq 2$, entonces por la definición de congruencia se cumple que: $km \equiv 0 \pmod{m}$, ya que $m \mid km$. De donde, si $a = b \cdot q + r$, con $a, q \in \mathbb{Z}$, $b \geq 2$ y $0 \leq r < b$, por las propiedades de las congruencias (*Teorema 4.1.3 del Apunte*) y teniendo en mente que "$\equiv$" es una *relación de equivalencia*, obtenemos

(*) $$a \equiv b \cdot q + r \equiv 0 + r \equiv r \pmod{b}.$$

De otro lado, si existen números naturales c, d tales que $b = c + d$ (esto implica que $c < b$ y $d < b$), entonces

(**) $$c + d \equiv b \equiv 0 \pmod{b} \quad \Leftrightarrow \quad c \equiv -d \pmod{b} \quad \Leftrightarrow \quad d \equiv -c \pmod{b}.$$

En lo que sigue, aplicaremos (*) y (**), indicando cual de las igualdades se cumple: $a = b \cdot q + r$ o $b = c + d$, al trabajar módulo b.

Solución

1. En este caso, por la propiedad descrita anteriormente, requerimos hallar $0 \leq r < 13$ tal que

$$323^{5843} \equiv r \pmod{13}.$$

Por comodidad en las cuentas, lo primero que hacemos es reducir la base de la potencia requerida a un número más chico, esto es: por el algoritmo de la división,

$$323 = 13 \cdot 24 + 11 \quad \Rightarrow \quad 323 \equiv 11 \pmod{13} \quad \Rightarrow \quad 323^{5843} \equiv 11^{5843} \pmod{13}.$$

Debido a que resulta muy laborioso calcular a mano la potencia 11^{5843}, el objetivo es buscar una potencia de 11 que sea congruente a 1 ó a -1 módulo 13. La forma más rápida y precisa de hacerlo es determinar si podemos usar el *Corolario* del *Teorema de Fermat*. Como 13 es un número primo y $(11, 13) = 1$ (esto equivale a $13 \nmid 11$), si lo podemos usar, y se cumple:

$$11^{12} \equiv 1 \pmod{13}.$$

Luego, dividimos la potencia 5843 por 12 y nos quedamos con el resto:

$$5843 = 12 \cdot 486 + 11 \quad \Rightarrow \quad 11^{5843} \equiv \left(11^{12}\right)^{486} \cdot 11^{11} \equiv 1^{486} \cdot 11^{11} \equiv 11^{11} \pmod{13}.$$

Así, reducimos el problema original a encontrar $0 \leq r < 13$ tal que

$$11^{11} \equiv r \pmod{13}.$$

En efecto, tenemos que:

$$\begin{aligned} 13 = 11 + 2 \quad &\Rightarrow \quad 11 \equiv -2 \pmod{13} \\ &\Rightarrow \quad 11^{11} \equiv (-2)^{11} \equiv (-2)^4 \cdot (-2)^4 \cdot (-2)^3 \pmod{13}. \end{aligned}$$

Pero,

$$\begin{aligned} &(-2)^4 \equiv 16 \equiv 3 \pmod{13} && \text{(por } 16 = 13 + 3) \\ &(-2)^3 \equiv -8 \equiv 5 \pmod{13} && \text{(por } 13 = 8 + 5) \end{aligned}$$

De donde,

$$11^{11} \equiv 3^2 \cdot 5 \equiv 45 \equiv 6 \pmod{13} \qquad \text{(por } 45 = 13 \cdot 3 + 6)$$

Como $0 \leq 6 < 13$, concluimos que 6 es el resto de dividir 323^{5843} por 13.

Observación

(i) Otra forma de hallar r tal que $11^{11} \equiv r \pmod{13}$ es calculando directamente las potencias de 11 módulo 13:

$$\begin{aligned} &11^2 \equiv 121 \equiv 4 \pmod{13} && \text{(por } 121 = 13 \cdot 9 + 4) \\ &11^3 \equiv 4 \cdot 11 \equiv 44 \equiv 5 \pmod{13} && \text{(por } 44 = 13 \cdot 3 + 5) \\ &11^4 \equiv 4^2 \equiv 3 \pmod{13} \end{aligned}$$

Por lo tanto,

$$11^{11} \equiv 11^4 \cdot 11^4 \cdot 11^3 \equiv 3^2 \cdot 5 \equiv 6 \pmod{13}. \quad \checkmark$$

(ii) Una tercera forma, aunque menos directa, es notar que basta con calcular el inverso multiplicativo de 11 módulo 13 (el cual existe pues $(11, 13) = 1$). Es decir, si existe $t \in \mathbb{Z}$ tal que $t \cdot 11 \equiv 1 \pmod{13}$, podemos proceder como sigue:

$$\begin{aligned} 11^{12} \equiv 1 \pmod{13} \quad &\Rightarrow \quad (t \cdot 11) \cdot 11^{11} \equiv t \pmod{13} \\ &\Rightarrow \quad 11^{11} \equiv t \pmod{13}. \end{aligned}$$

Ahora bien, una manera de hallar t es usando el algoritmo de Euclides:

$$\begin{aligned} &13 = 11 + 2 \quad \Rightarrow \quad 2 = 13 - 11 \\ &11 = 5 \cdot 2 + 1 \end{aligned}$$

Luego,

$$1 = 11 - 5 \cdot 2 = 11 - 5(13 - 11) = 6 \cdot 11 - 5 \cdot 13 \quad \Rightarrow \quad 1 \equiv 6 \cdot 11 \pmod{13}.$$

Así, $t = 6$. ✓

2. Para todo $n \in \mathbb{N}$, tenemos que:

$$9 \mid \left(4^{2n} - 7^n\right) \quad \Leftrightarrow \quad 4^{2n} - 7^n \equiv 0 \pmod 9 \quad \Leftrightarrow \quad 4^{2n} \equiv 7^n \pmod 9.$$

De donde, basta con probar que $4^{2n} \equiv 7^n \pmod 9$. En efecto,

$$\begin{aligned}
&16 \equiv 7 \pmod 9 && \text{(por } 16 = 9 + 7\text{)}\\
&\Rightarrow 16^n \equiv 7^n \pmod 9 && \text{(por Teorema 4.1.3.)}\\
&\Rightarrow \left(4^2\right)^n \equiv 7^n \pmod 9\\
&\Rightarrow 4^{2n} \equiv 7^n \pmod 9.
\end{aligned}$$