Matemática Discreta I

Parcial 4: Junio 9, 2022
Tema 2 - Turno Mañana

Ejercicios:

(1) Probar utilizando congruencias que para todo $n \in \mathbb{N}$, $3^{4n+2} + 2^{6n+3}$ es múltiplo de 17.

(2) Dada la ecuación $42\,x \equiv 6\,(76)$,
   (a) calcular todas las soluciones enteras posibles de la ecuación,
   (b) determinar cuáles son las soluciones enteras de la ecuación que se encuentran en el intervalo $(-30, 50]$.

(3) Calcular el resto de la división de $111^{34} - 43^{2021}$ por 37.

Solución

(1) Sea $n \in \mathbb{N}$. Por la definición de *congruencia*, se cumple que:

$$(*) \qquad 17 \mid \left(3^{4n+2} + 2^{6n+3}\right) \quad \Leftrightarrow \quad 3^{4n+2} + 2^{6n+3} \equiv 0 \pmod{17}.$$

Así que basta con demostrar dicha congruencia. En efecto, por la *Proposición* 4.1.2., tenemos que:

$$(**) \qquad 64 = 17 \cdot 3 + 13 \quad \Rightarrow \quad 64 \equiv 13 \pmod{17}.$$
$$81 = 17 \cdot 4 + 13 \quad \Rightarrow \quad 81 \equiv 13 \pmod{17}.$$

Ahora bien, por el *Teorema* 4.1.5. (las congruencias son compatibles con la suma, producto, y potencias positivas), y las propiedades de las potencias (abreviatura: **p.p.**), desarrollamos el lado izquierdo de la congruencia en (*), esto es:

$$\begin{aligned} 3^{4n+2} + 2^{6n+3} &\equiv 9 \cdot 81^n + 8 \cdot 64^n \pmod{17} && \text{(por p.p.)} \\ &\equiv 9 \cdot 13^n + 8 \cdot 13^n \pmod{17} && \text{(por (**))} \\ &\equiv (9+8) \cdot 13^n \pmod{17} && \text{(aritmética)} \\ &\equiv 17 \cdot 13^n \equiv 0 \pmod{17} && \text{(por } km \equiv 0 \pmod{m}\text{)} \end{aligned}$$

Así, por la transitividad de las congruencias, concluimos que ambas expresiones en (*) son válidas para todo $n \in \mathbb{N}$.

(2) Como $2 \mid 6,\ 2 \mid 42,\ 2 \mid 76$, sabemos que: $42\,x \equiv 6 \pmod{76}$ admite solución si y sólo si $21\,x \equiv 3 \pmod{38}$ admite solución. Más aún, ambas ecuaciones lineales en congruencias tienen las mismas soluciones. Así, basta con resolver la ecuación lineal en congruencia más reducida.

(2) (a) Vamos a resolver este ejercicio en tres pasos.

Primer paso: Verificamos que la ecuación en congruencia admite solución. En efecto, por el *Algoritmo de la División* y el *Algoritmo de Euclides*, obtenemos:

$$\begin{aligned} 38 &= 21 + 17 \quad \Rightarrow \quad (38, 21) = (21, 17). \\ 21 &= 17 + 4 \quad \Rightarrow \quad (21, 17) = (17, 4). \\ 17 &= 4 \cdot 4 + 1 \quad \Rightarrow \quad (17, 4) = (4, 1). \\ 4 &= 4 \cdot 1 + 0 \quad \Rightarrow \quad (4, 1) = (1, 0). \end{aligned}$$

De donde, $d := (38, 21) = (1, 0) = 1$. Como $1 \mid 3$, por *Teorema 4.2.1.* del Apunte, la ecuación en congruencia $21\,x \equiv 3 \pmod{38}$ admite solución.

Segundo paso: Encontramos una solución particular x_0 de la ecuación en congruencia. De las ecuaciones que obtuvimos anteriormente, despejamos los restos, así:

(1) $$17 = 38 - 21$$

(2) $$4 = 21 - 17$$

Ahora, vamos reemplazando las ecuaciones hacia atrás:

$$\begin{aligned} 1 &= 17 + (-4) \cdot 4 \\ &= 17 + (-4) \cdot (21 - 17) && \text{(por (2))} \\ &= 5 \cdot 17 + (-4) \cdot 21 && \text{(aritmética)} \\ &= 5 \cdot (38 - 21) + (-4) \cdot 21 && \text{(por (1))} \\ &= 5 \cdot 38 + (-9) \cdot 21 && \text{(aritmética)} \end{aligned}$$

En resumen, $d = 1 = 5 \cdot 38 + (-9) \cdot 21$. Luego,

$$1 \equiv 5 \cdot 38 + (-9) \cdot 21 \equiv (-9) \cdot 21 \pmod{38} \quad \Rightarrow \quad 3 \equiv (-27) \cdot 21 \pmod{38},$$

lo cual es equivalente a tener $21 \cdot 11 \equiv 3 \pmod{38}$, ya que $38 = 27 + 11$. Así, $x_0 := 11$ es una solución particular de la ecuación en congruencia.

Tercer paso: Escribimos todas las soluciones de la ecuación en congruencia. Nuevamente, por *Teorema 4.2.1.*, todas las soluciones x de la ecuación en congruencia son de la forma:

$$x = x_0 + k \cdot \frac{38}{d} = 11 + k \cdot \frac{38}{1} = 11 + k \cdot 38,$$

con $k \in \mathbb{Z}$.

(2) (b) Como todas las soluciones son de la forma $x = 11 + k \cdot 38$, con $k \in \mathbb{Z}$, entonces

$$\begin{aligned} -30 < x \leq 50 \quad &\Leftrightarrow \quad -30 < 11 + k \cdot 38 \leq 50 \\ &\Leftrightarrow \quad -41 < k \cdot 38 \leq 39 \\ &\Leftrightarrow \quad -\frac{41}{38} < k \leq \frac{39}{38} \\ &\Leftrightarrow \quad -1.8 < k \leq 1.02 \end{aligned}$$

Debido a que k debe ser entero, se sigue que $k \in \{-1, 0, 1\}$. Así, las soluciones pedidas son:

$$\begin{aligned} &11 + (-1) \cdot 38 = 11 - 38 = -27, \\ &11 + 0 \cdot 38 = 11, \\ &11 + 1 \cdot 38 = 11 + 38 = 49. \end{aligned}$$

(3) En este caso, por la Proposición 4.1.2, requerimos hallar $0 \leq r < 37$ tal que

$$111^{34} - 43^{2021} \equiv r \pmod{37}.$$

Por comodidad en las cuentas, lo primero que hacemos es reducir las bases de ambas potencias requeridas a un número más chico, esto es, por el algoritmo de la división:

$$111 = 3 \cdot 37 + 0 \quad \Rightarrow \quad 111 \equiv 0 \pmod{37} \quad \Rightarrow \quad 111^{34} \equiv 0 \pmod{37}.$$

$$43 = 1 \cdot 37 + 6 \quad \Rightarrow \quad 43 \equiv 6 \pmod{37} \quad \Rightarrow \quad 43^{2021} \equiv 6^{2021} \pmod{37}.$$

Como 37 es un número primo (por el criterio de la raíz ya que 37 no es divisible ni por 2, ni por 3, y tampoco por 5), y $(6, 37) = 1$ (esto equivale a $37 \nmid 6$), podemos usar el *Teorema de Fermat*, y se cumple:

$$6^{36} \equiv 1 \pmod{37}.$$

Luego, dividimos la potencia 2021 por 36 y nos quedamos con el resto:

$$2021 = 36 \cdot 56 + 5 \quad \Rightarrow \quad 6^{2021} \equiv \left(6^{36}\right)^{56} \cdot 6^5 \equiv 1^{56} \cdot 6^5 \equiv 6^5 \pmod{37}.$$

Así, reducimos el problema original a encontrar $0 \leq r < 37$ tal que

$$111^{34} - 43^{2021} \equiv -6^5 \equiv r \pmod{37}.$$

En efecto, calculando directamente las potencias de 6 módulo 37:

$$\begin{aligned} &6^2 \equiv 36 \equiv -1 \pmod{37} && \text{(por } 37 = 36 + 1\text{)} \\ &6^4 \equiv (6^2)^2 \equiv 1 \pmod{37} \\ &6^5 \equiv 6^4 \cdot 6 \equiv 6 \pmod{37} \end{aligned}$$

Por lo tanto,

$$111^{34} - 43^{2021} \equiv -6^5 \equiv -6 \equiv 31 \pmod{37},$$

ya que $37 = 31 + 6$. Como $0 \leq 31 < 37$, entonces concluimos que $r = 31$.