Matemática Discreta I

Parcial 4: Junio 9, 2022
Tema 1 - Turno Tarde

Ejercicios:

(1) Probar utilizando congruencias que para todo $n \in \mathbb{N}$, $6^{2n+3} - 2^3 \cdot 7^{2n}$ es divisible por 13.

(2) Dada la ecuación $52\,x \equiv 8\,(88)$,
  (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 $[-40, 20]$.

(3) Calcular el resto de la división de $45 \cdot 74^{337}$ por 23.

Solución

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

(*) $$13 \mid \left(6^{2n+3} - 2^3 \cdot 7^{2n}\right) \quad \Leftrightarrow \quad 6^{2n+3} - 2^3 \cdot 7^{2n} \equiv 0 \pmod{13}.$$

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

(**) $$\begin{aligned} 36 = 13 \cdot 2 + 10 \quad &\Rightarrow \quad 36 \equiv 10 \pmod{13}. \\ 49 = 13 \cdot 3 + 10 \quad &\Rightarrow \quad 49 \equiv 10 \pmod{13}. \\ 60 = 13 \cdot 4 + 8 \quad &\Rightarrow \quad 6^3 \equiv 6 \cdot 10 \equiv 8 \pmod{13}. \end{aligned}$$

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:

$$\begin{aligned} 6^{2n+3} - 2^3 \cdot 7^{2n} &\equiv 6^3 \cdot 36^n - 8 \cdot 49^n \pmod{13} && \text{(por p.p.)} \\ &\equiv 8 \cdot 10^n - 8 \cdot 10^n \pmod{13} && \text{(por (**))} \\ &\equiv 0 \pmod{13} && \text{(aritmética)} \end{aligned}$$

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

(2) Como $4 \mid 8,\ 4 \mid 52,\ 4 \mid 88$, sabemos que: $52\,x \equiv 8 \pmod{88}$ admite solución si y sólo si $13\,x \equiv 2 \pmod{22}$ 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:

$$\begin{aligned}
22 &= 13 + 9 &&\Rightarrow\quad (22,13) = (13,9).\\
13 &= 9 + 4 &&\Rightarrow\quad (13,9) = (9,4).\\
9 &= 2\cdot 4 + 1 &&\Rightarrow\quad (9,4) = (4,1).\\
4 &= 4\cdot 1 + 0 &&\Rightarrow\quad (4,1) = (1,0).
\end{aligned}$$

De donde, $d := (22,13) = (1,0) = 1$. Como $1 \mid 2$, por *Teorema 4.2.1.* del Apunte, la ecuación en congruencia $13\,x \equiv 2 \pmod{22}$ 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) $$9 = 22 - 13$$

(2) $$4 = 13 - 9$$

Ahora, vamos reemplazando las ecuaciones hacia atrás:

$$\begin{aligned}
1 &= 9 + (-2)\cdot 4 \\
&= 9 + (-2)\cdot(13 - 9) && \text{(por (2))}\\
&= 3\cdot 9 + (-2)\cdot 13 && \text{(aritmética)}\\
&= 3\cdot(22 - 13) + (-2)\cdot 13 && \text{(por (1))}\\
&= 3\cdot 22 + (-5)\cdot 13 && \text{(aritmética)}
\end{aligned}$$

En resumen, $d = 1 = 3\cdot 22 + (-5)\cdot 13$. Luego,

$$1 \equiv 3\cdot 22 + (-5)\cdot 13 \equiv (-5)\cdot 13 \pmod{22} \quad\Rightarrow\quad 2 \equiv (-10)\cdot 13 \pmod{22},$$

lo cual es equivalente a tener $13\cdot 12 \equiv 2 \pmod{22}$, ya que $22 = 12 + 10$. Así, $x_0 := 12$ 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:

$$x = x_0 + k\cdot\frac{22}{d} = 12 + k\cdot\frac{22}{1} = 12 + k\cdot 22,$$

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

(2) (b) Como todas las soluciones son de la forma $x = 12 + k \cdot 22$, con $k \in \mathbb{Z}$, entonces

$$\begin{aligned} -40 \leq x \leq 20 \quad &\Leftrightarrow \quad -40 \leq 12 + k \cdot 22 \leq 20 \\ &\Leftrightarrow \quad -52 \leq k \cdot 22 \leq 8 \\ &\Leftrightarrow \quad -\frac{52}{22} \leq k \leq \frac{8}{22} \\ &\Leftrightarrow \quad -2.36 \leq k \leq 0.36 \end{aligned}$$

Debido a que k debe ser entero, se sigue que $k \in \{-2, -1, 0\}$. Así, las soluciones pedidas son:

$$\begin{aligned} &12 + (-2) \cdot 22 = 12 - 44 = -32, \\ &12 + (-1) \cdot 22 = 12 - 22 = -10, \\ &12 + 0 \cdot 22 = 12. \end{aligned}$$

(3) En este caso, por la Proposición 4.1.2, requerimos hallar $0 \leq r < 23$ tal que

$$45 \cdot 74^{337} \equiv r \pmod{23}.$$

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:

$$2 \cdot 23 = 46 = 45 + 1 \quad \Rightarrow \quad 45 \equiv -1 \pmod{23}.$$

$$74 = 3 \cdot 23 + 5 \quad \Rightarrow \quad 74 \equiv 5 \pmod{23} \quad \Rightarrow \quad 74^{337} \equiv 5^{337} \pmod{23}.$$

Como 23 es un número primo (por el criterio de la raíz ya que 23 no es divisible ni por 2, ni por 3), y $(5, 23) = 1$ (esto equivale a $23 \nmid 5$), podemos usar el *Teorema de Fermat*, y se cumple:

$$5^{22} \equiv 1 \pmod{23}.$$

Luego, dividimos la potencia 337 por 22 y nos quedamos con el resto:

$$337 = 22 \cdot 15 + 7 \quad \Rightarrow \quad 5^{337} \equiv \left(5^{22}\right)^{15} \cdot 5^7 \equiv 1^{15} \cdot 5^7 \equiv 5^7 \pmod{23}.$$

Así, reducimos el problema original a encontrar $0 \leq r < 23$ tal que

$$45 \cdot 74^{337} \equiv -5^7 \equiv r \pmod{23}.$$

En efecto, calculando directamente las potencias de 5 módulo 23:

$$\begin{aligned} &5^2 \equiv 25 \equiv 2 \pmod{23} && \text{(por } 25 = 23 + 2\text{)} \\ &5^6 \equiv (5^2)^3 \equiv 8 \pmod{23} \\ &5^7 \equiv 5^6 \cdot 5 \equiv 8 \cdot 5 \equiv 17 \pmod{23} && \text{(por } 40 = 23 + 17\text{)} \end{aligned}$$

Por lo tanto,

$$45 \cdot 74^{337} \equiv -5^7 \equiv -17 \equiv 6 \pmod{23},$$

ya que $23 = 17 + 6$. Como $0 \leq 6 < 37$, entonces concluimos que $r = 6$.