Matemática Discreta I - 2021/1

Tarea 9

Ejercicios

1. (i) Encontrar todas las soluciones de la ecuación en congruencia

$$30\,x \equiv 2 \pmod{67}$$

usando el método visto en clase.

(ii) Dar todas las soluciones x de la ecuación anterior tales que $0 < x < 300$.

2. Encontrar los últimos dos dígitos de 2^{338}. (Se cumple que $2^{22} \equiv 4 \pmod{100}$).

Solución

1. (i) Vamos a resolver este ejercicio en tres pasos.

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

$$\begin{aligned}
67 &= 2 \cdot 30 + 7 &\Rightarrow&\quad (67, 30) = (30, 7).\\
30 &= 4 \cdot 7 + 2 &\Rightarrow&\quad (30, 7) = (7, 2).\\
7 &= 3 \cdot 2 + 1 &\Rightarrow&\quad (7, 2) = (2, 1).\\
2 &= 2 \cdot 1 + 0 &\Rightarrow&\quad (2, 1) = (1, 0).
\end{aligned}$$

De donde, $d := (67, 30) = (1, 0) = 1$. Como $1 \mid 2$, por *Teorema 4.2.1.*, la ecuación en congruencia $30\,x \equiv 2 \pmod{67}$ 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:

$$7 = 67 - 2 \cdot 30 = 67 + (-2) \cdot 30 \tag{1}$$

$$2 = 30 - 4 \cdot 7 = 30 + (-4) \cdot 7 \tag{2}$$

Ahora, vamos reemplazando las ecuaciones hacia atrás:

$$\begin{aligned}
1 &= 7 + (-3) \cdot 2 & \\
&= 7 + (-3) \cdot (30 + (-4) \cdot 7) & \text{(por (2))}\\
&= 13 \cdot 7 + (-3) \cdot 30 & \text{(aritmética)}\\
&= 13 \cdot (67 + (-2) \cdot 30) + (-3) \cdot 30 & \text{(por (1))}\\
&= 13 \cdot 67 + (-29) \cdot 30 & \text{(aritmética)}
\end{aligned}$$

En resumen, $d = 1 = 13 \cdot 67 + (-29) \cdot 30$. Luego,

$$1 \equiv 13 \cdot 67 + (-29) \cdot 30 \equiv (-29) \cdot 30 \pmod{67} \quad \Rightarrow \quad 2 \equiv (-58) \cdot 30 \pmod{67},$$

lo cual es equivalente a tener $30 \cdot 9 \equiv 2 \pmod{67}$, ya que $67 = 58 + 9$. Así, $x_0 := 9$ 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:

$$x = x_0 + k\,\frac{67}{d} = 9 + k\,\frac{67}{1} = 9 + k\;67,$$

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

1. (ii) Como todas las soluciones son de la forma $x = 9 + k\;67$, con $k \in \mathbb{Z}$, entonces

$$\begin{aligned} 0 < x < 300 \quad &\Leftrightarrow \quad 0 < 9 + k\;67 < 300 \\ &\Leftrightarrow \quad -9 < k\;67 < 291 \\ &\Leftrightarrow \quad -\frac{9}{67} < k < \frac{291}{67} \\ &\Leftrightarrow \quad -0.13 < k < 4.34 \end{aligned}$$

Debido a que k debe ser entero, se sigue que $k \in \{0, 1, 2, 3, 4\}$. Así, las soluciones pedidas son:

$$\begin{aligned} &9 + 0 \cdot 67 = 9, \\ &9 + 1 \cdot 67 = 9 + 67 = 76, \\ &9 + 2 \cdot 67 = 9 + 134 = 143, \\ &9 + 3 \cdot 67 = 9 + 201 = 210, \\ &9 + 4 \cdot 67 = 9 + 268 = 277. \end{aligned}$$

2. Tenemos que para todo natural $j \geq 2$, $10^j \equiv 0 \pmod{100}$. Luego, para cualquier $n \in \mathbb{N}$ escrito en la base 10, se satisface que:

$$n \equiv \sum_{j=2}^{k} a_j 0^j + 10a_1 + a_0 \equiv 10a_1 + a_0 \pmod{100}. \qquad (*)$$

Por lo tanto, para encontrar los últimos dos dígitos de 2^{338}, basta con hallar $0 \leq r < 100$ tal que

$$2^{338} \equiv r \pmod{100}.$$

Ahora bien, para usar la hipótesis de que $2^{22} \equiv 4 \pmod{100}$, dividimos 338 por 22, esto es:

$$338 = 22 \cdot 15 + 8 \quad \Rightarrow \quad 2^{338} = \left(2^{22}\right)^{15} \cdot 2^8 \equiv 4^{15} \cdot 2^8 \pmod{100}.$$

Por las propiedades de las potencias, obtenemos $4^{15} = (2^2)^{15} = 2^{30} = 2^{22} \cdot 2^8$, de donde

$$4^{15} \cdot 2^8 \equiv 2^{22} \cdot 2^{16} \equiv 4 \cdot 2^{16} \equiv 2^{18} \pmod{100}.$$

De otro lado, la primer potencia de 2 mayor que 100 es 2^7, por lo cual:

$$\begin{aligned}
2^7 &\equiv 128 \equiv 28 \pmod{100} && \text{(por (*))}\\
2^8 &\equiv 2^7 \cdot 2 \equiv 28 \cdot 2 \equiv 56 \pmod{100} &&\\
2^9 &\equiv 112 \equiv 12 \pmod{100} && \text{(por (*))}\\
2^{18} &\equiv 12^2 \equiv 144 \equiv 44 \pmod{100} && \text{(por (*))}
\end{aligned}$$

De todo lo anterior, los últimos dos dígitos de 2^{338} son $r := 44$.