Práctica 4
EJERCICIOS BÁSICOS

1. Recuerda que en $\mathbb{Z}_n$ el *inverso* a^{-1} de a es la solución de la ecuación $ax \equiv 1 \pmod{n}$. Calcula:
$$\text{(a) } 2^{-1} \pmod{17}, \quad \text{(b) } 7^{-1} \pmod{18}, \quad \text{(c) } 25^{-1} \pmod{54}.$$

2. Encuentra todas las soluciones de los siguientes sistemas de congruencias:
$$\text{(a)} \left\{ \begin{array}{l} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{array} \right\} \quad \text{(b)} \left\{ \begin{array}{l} x \equiv 0 \pmod{2} \\ x \equiv 1 \pmod{3} \\ x \equiv -2 \pmod{4} \\ x \equiv 6 \pmod{7} \end{array} \right\}$$

3. Cuando un general hizo que sus soldados se colocaran en filas de 7, quedaron 2 soldados sin fila. Cuando los colocó en filas de 12, quedaron 3 soldados sin fila. Por último, los colocó en filas de 14 y quedaron sin fila 9 soldados. ¿Cuál es el menor número de soldados que podía tener el general? ¿Cuántos soldados tenía si sabemos que eran entre 400 y 500?

4. Usa el Pequeño Teorema de Fermat para calcular:
$$\text{(a) } 7^{2156} \pmod{11} \qquad \text{(b) } 14^{27354} \pmod{19}.$$

`SAGE` 1. Comprueba con `solve_mod` tus soluciones del ejercicio 1.

`SAGE` 2. Estudia el uso de los comandos `CRT` y `CRT_list` para resolver sistemas como los del Teorema Chino de los Restos. Comprueba tus soluciones de los ejercicios 2 y 3.

`SAGE` 3. Utiliza el comando `Mod` para comprobar tus soluciones del ejercicio 4.

- Los ejercicios básicos son obligatorios y determinarán la calificación de las actividades semanales.
- Los ejercicios de refuerzo se proponen para adquirir mayor destreza.
- Los ejercicios de profundización se proponen para quienes tengan curiosidad.

EJERCICIOS DE REFUERZO

1. Utiliza congruencias para demostrar que un número es múltiplo de 3 si, y solo si, la suma de sus dígitos es múltiplo de 3.

2. Resuelve las siguientes congruencias:

$$\text{(a) } 2x \equiv 5 \pmod 7, \quad \text{(b) } 387x \equiv 6 \pmod{453}.$$

3. Calcula los siguientes inversos:

$$\text{(a) } 11^{-1} \pmod{25}, \quad \text{(b) } 8^{-1} \pmod{19}, \quad \text{(c) } 387^{-1} \pmod{454}$$

4. Encuentra todas las soluciones de los siguientes sistemas de congruencias:

$$\text{(a)} \left\{ \begin{array}{l} x \equiv 1 \pmod 3 \\ x \equiv -2 \pmod 4 \\ x \equiv 3 \pmod 5 \\ x \equiv -4 \pmod{17} \end{array} \right\} \quad \text{(b)} \left\{ \begin{array}{l} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 4 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{array} \right\} \quad \text{(c)} \left\{ \begin{array}{l} x \equiv 1 \pmod 3 \\ x \equiv 3 \pmod 4 \\ x \equiv 3 \pmod 5 \\ x \equiv 12 \pmod{11} \end{array} \right\}$$

5. Decides crear un cluster con tus cuatro ordenadores para poder ejecutar un bucle en paralelo. El compilador asignó el mismo número de iteraciones a cada uno de los ordenadores y sabes que: El primero las organizó en paquetes de 3, y le sobraron 2 iteraciones. El segundo las organizó en paquetes de 4, y le sobraron 3 iteraciones. El tercero las organizó en paquetes de 6, y le sobraron 5 iteraciones. El cuarto las organizó en paquetes de 7, y le sobraron también 5 iteraciones. ¿Cuántas iteraciones se asignaron en total?

6. Un grupo de 19 gamers acordaron repartirse entre ellos cierta cantidad de votos para el premio *Gamer del año*. Tras un empalagoso cruce de halagos en un directo de Twitch, decidieron repartírselos por igual y comprobaron que al final les sobraban 3. Al día siguiente, uno de ellos se retiró de la competición y mudarse al pueblo a cultivar tomates ecológicos, así que los que quedaban hicieron otro directo para repartirse de nuevo el total de votos, comprobando que ahora les sobraban 2. Dos días más tarde, una de las gamers fue nombrada ministra de educación y quedó fuera de la competición, así que los que quedaban hicieron un tercer directo y, esta vez sí, consiguieron repartirse por igual el total de votos. ¿Cuál era esa cantidad total de votos?

7. Resuelve el siguiente acertijo: si los huevos de una cesta se retiran de 2 en 2, de 3 en 3, de 4 en 4, de 5 en 5 o de 6 en 6, quedan, respectivamente, 1, 2, 3, 4 y 5 huevos. Sin embargo, si se retiran de 7 en 7 no queda ninguno. ¿Cuál es la menor cantidad de huevos que debe haber en la cesta?

8. En el primer ejercicio de una oposición van colocando a los candidatos en un aula con 8 puestos por fila y queda una fila sin llenar, con solo 5 puestos cubiertos. El aula del segundo ejercicio tiene 11 puestos en cada fila y queda una fila sin llenar, con 3 puestos cubiertos. En el tercer y último ejercicio, el aula tiene 12 puestos por fila y la que queda sin llenar tiene cubiertos 9 de ellos. ¿Cuál es el menor número de opositores que pueden estar haciendo el examen? ¿Cuál es el número de opositores si sabemos que eran entre 400 y 600?

9. Usa el Pequeño Teorema de Fermat para calcular:

$$\text{(a) } 5^{2003} \pmod 7 \qquad \text{(b) } 15^{35743} \pmod{19}.$$

`SAGE` 1. Implementa un método que, dada una posible solución de un sistema de congruencias, compruebe si es realmente una solución, es decir, si cumple todas las ecuaciones del sistema.

`SAGE` 2. Implementa un método que, dado un $n \in \mathbb{N}$, determine qué elementos de $\mathbb{Z}_n$ tienen inverso.

EJERCICIOS DE PROFUNDIZACIÓN

1. Demuestra que si n es compuesto y $n \neq 4$, entonces $(n-1)! \equiv 0 \bmod n$.

2. Utiliza congruencias para obtener un criterio de divisibilidad de números enteros entre 8.

3. Demuestra que el sistema de congruencias

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

tiene solución si y sólo si $a_1 \equiv a_2 \pmod{\text{mcd}(m_1, m_2)}$. (**Indicación:** escribe el conjunto de soluciones de la primera ecuación e introdúcelo en la segunda).

4. Encuentra todas las soluciones de la ecuación $x^2 \equiv 16 \pmod{77}$. (**Indicación:** Resuelve la congruencia módulo 7 y módulo 11 y utiliza el teorema chino del resto).

`SAGE` 1. Implementa un método para resolver sistemas de congruencias del tipo

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

cuando tienen solución, es decir, cuando $a_1 \equiv a_2 \pmod{\text{mcd}(m_1, m_2)}$.