Álgebra (Ingeniería Informática) **Curso 2007-2008**

Práctica 3-1: Aritmética modular

EJERCICIOS BÁSICOS

1. Obtener un criterio de divisibilidad de números enteros entre 4.

2. Resolver las siguientes congruencias:

$$\text{(a) } 3x \equiv 6 \pmod 9, \quad \text{(b) } 11x \equiv 16 \pmod{23}, \quad \text{(c) } 150x \equiv 444 \pmod{999}$$

3. Calcular los siguientes inversos:

$$\text{(a) } 6^{-1} \pmod{13}, \quad \text{(b) } 8^{-1} \pmod{17}, \quad \text{(c) } 238^{-1} \pmod{999}.$$

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

$$\text{(a)} \begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 0 \pmod 3 \\ x \equiv 4 \pmod 5 \\ x \equiv 5 \pmod 7 \end{cases} \qquad \text{(b)} \begin{cases} x \equiv 1 \pmod 3 \\ x \equiv -1 \pmod 4 \\ x \equiv -2 \pmod 5 \\ x \equiv 12 \pmod{11} \end{cases} \qquad \text{(c)} \begin{cases} x \equiv 5 \pmod 3 \\ x \equiv 1 \pmod 5 \\ x \equiv 3 \pmod 7 \\ x \equiv 4 \pmod{11} \\ x \equiv 2 \pmod{13} \end{cases}$$

5. Encontrar todas las soluciones de los siguientes sistemas de congruencias:

$$\text{(a)} \quad \begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 4 \\ x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 8 \end{cases} \qquad \text{(b)} \quad \begin{cases} x \equiv 2 \pmod 6 \\ x \equiv 4 \pmod 8 \\ x \equiv 2 \pmod{14} \\ x \equiv 14 \pmod{15} \end{cases}$$

6. Un viejo problema chino pregunta por el menor número de monedas de oro que podía tener un grupo de 17 piratas. Se sabe que se las repartieron por igual y que sobraron 3, y que después de pelear por esas 3, uno de ellos fue asesinado. Al repartir de nuevo el total de las monedas, sobraban 10, y de nuevo lucharon por ellas y uno de ellos resulto muerto. Después de eso, pudieron repartirse las monedas por igual. Resuelve el problema.

EJERCICIOS DE REFUERZO

1. Obtener criterios de divisibilidad de números enteros: a) Entre 7, b) Entre 8.

2. Resolver las siguientes congruencias:

$$\text{(a) } 19x \equiv 30 \pmod{40}, \quad \text{(b) } 10x \equiv 15 \pmod{25}, \quad \text{(c) } 387x \equiv 6 \pmod{453}.$$

3. Calcular los siguientes inversos:

$$\text{(a) } 2^{-1} \pmod{17}, \quad \text{(b) } 11^{-1} \pmod{25}, \quad \text{(c) } 387^{-1} \pmod{454}.$$

4. Demostrar que si a y m son coprimos, entonces existe un único inverso de a módulo m.

5. Encontrar todas las soluciones de los siguientes sistemas de congruencias:

(a) $\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{4} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$ (b) $\begin{cases} x \equiv 0 \pmod{2} \\ x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{4} \\ x \equiv 6 \pmod{7} \end{cases}$ (c) $\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv -2 \pmod{4} \\ x \equiv 3 \pmod{5} \\ x \equiv -4 \pmod{17} \end{cases}$ (d) $\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases}$

6. Resolver el siguiente acertijo indio: 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?

EJERCICIOS DE PROFUNDIZACIÓN

1. Demostrar 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 $a_1 \equiv a_2(\text{mod}(\text{mcd}(m_1, m_2)))$. (Indicación: escribe el conjunto de soluciones de la primera ecuación e introdúcelo en la segunda).

2. Investigar cómo se utilizan congruencias para calcular, dada una fecha, qué día de la semana fue. (**Indicación:** puedes comenzar la búsqueda por el algoritmo de Zeller).