Universidad de la República **Matemática Discreta 2**
Facultad de Ingeniería **Curso 2018**
Instituto de Matemática y Estadística

PRÁCTICO 5: Teorema Chino del Resto- Teorema de Fermat-Euler

Ejercicio 1. Resolver los siguientes sistemas:

a. $\begin{cases} x \equiv 3 \pmod 7 \\ x \equiv 5 \pmod{13} \end{cases}$ **b.** $\begin{cases} x \equiv 3 \pmod{14} \\ 2x \equiv 3 \pmod{11} \end{cases}$ **c.** $\begin{cases} 3x \equiv 13 \pmod{22} \\ 5x \equiv -1 \pmod{31} \end{cases}$

Ejercicio 2. Sean m_1 y m_2 enteros coprimos.

a. Probar que existen b_1, $b_2 \in \mathbb{Z}$ tales que $b_1 m_2 \equiv 1 \pmod{m_1}$ y $b_2 m_1 \equiv 1 \pmod{m_2}$.

b. Probar que para b_1 y b_2 como en la parte anterior, para todo a_1, $a_2 \in \mathbb{Z}$, el entero $x = a_1 b_1 m_2 + a_2 b_2 m_1$ es solución del sistema

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

c. Utilizar lo anterior para hallar todas las soluciones del sistema

$$\begin{cases} x \equiv 5 \pmod{14} \\ x \equiv 3 \pmod{11} \end{cases}$$

Ejercicio 3. Resolver los siguientes sistemas:

a. $\begin{cases} x \equiv 16 \pmod{19} \\ x \equiv 9 \pmod{36} \\ x \equiv 7 \pmod{49} \end{cases}$ **b.** $\begin{cases} x \equiv 11 \pmod{23} \\ x \equiv 8 \pmod{42} \\ x \equiv 15 \pmod{25} \end{cases}$

Ejercicio 4. Sean $m_1, m_2, \cdots, m_k$ enteros coprimos 2 a 2.

a. Definimos

$$M_i = \frac{m_1 m_2 \cdots m_k}{m_i} = \prod_{j \neq i} m_j,$$

probar que existen b_1, $b_2, \cdots, b_k \in \mathbb{Z}$ tales que

$$b_i M_i \equiv 1 \pmod{m_i} \forall i = 1, \cdots, k.$$

b. Probar que para $b_1, b_2, \cdots, b_k$ como en la parte anterior, para todo a_1, $a_2, \cdots, a_k \in \mathbb{Z}$ el entero $x = a_1 b_1 M_1 + a_2 b_2 M_2 + \cdots + a_k b_k M_k$ es solución del sistema

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

c. Utilizar lo anterior para hallar todas las soluciones del sistema

$$\begin{cases} x \equiv 5 \pmod{11} \\ x \equiv 3 \pmod{7} \\ x \equiv 10 \pmod{12} \end{cases}$$

Ejercicio 5.

a. Hallar el menor natural que dividido 3 da resto 1, divido 4 da resto 3 y dividido 7 da resto 5.

b. Encontrar el menor natural n que dividido 2 da resto 1, dividido 3 da resto 2, dividido 4 da resto 3, dividido 5 da resto 4, dividido 6 da resto 5, dividido 7 da resto 6, dividido 8 da resto 7 y dividido 9 da resto 8. Sugerencia: considerar $n+1$.

c. Hallar el menor par $x > 199$ que cumpla $2x + 3 \equiv 4 \pmod{5}$ y $3x + 4 \equiv 3 \pmod{7}$.

d. Una banda de 13 piratas obtuvo un cofre pequeo con monedas de oro, que trataron de distribuir entre sí equitativamente, pero les sobraban 8 monedas. Imprevistamente dos de ellos fueron expulsados de la banda por intentar robarse todo el botín. Al volver a intentar el reparto, sobraban ahora 3 monedas. Posteriormente, tres de ellos se ahogaron y al intentar distribuir las monedas quedaban 5. ¿Cuántas monedas habían en el botín?

e. Un bibliotecario cuenta los libros de un armario. Si los agrupa de a 4 o de a 5 o de a 6 siempre sobra 1. Si los agrupa de a 7 no le sobra ninguno. Sabiendo que los libros son menos de 400 ¿cuántos libros tiene?

f. La producción diaria de huevos de una granja es inferior a 75 unidades. Cierto día el recolector informa que la cantidad de huevos recogida es tal que contando de a 3 le sobran 2, contando de a 5 sobran 4 y contando de a 7 sobran 5. El capataz, que estudia aritmética a escondidas, le dice que eso es imposible. ¿Quién tiene razón?

g. Un mago me pidió que pensara un número natural no mayor que 1000. Yo elegí x. Luego me pidió el resto de la división entre 7. Le dije que era 1. Inmediatamente después me dijo que dividiera el número pensado entre 11 y que también le diera el resto. Le dije que era 8. Y por último la misma operación dividiendo el número pensado entre 13. Le dije que el resto era 1. Entonces el mago dijo que utilizó la fórmula mágica de los restos y con los números 1, 8 y 1, que son los restos, dedujo que el número era x. ¡¡Acertó!! Hallar el valor de x justificando la respuesta.

Ejercicio 6. Investigar si los siguientes sistemas tienen solución, y en caso de que así sea, hallarlas todas (observar que cuando existen soluciones, son únicas modulo el mínimo común múltiplo de los módulos de cada ecuación).

a. $\begin{cases} x \equiv 1 \pmod{7} \\ x \equiv 6 \pmod{21} \\ x \equiv 11 \pmod{15} \end{cases}$ **b**. $\begin{cases} x \equiv 1 \pmod{7} \\ x \equiv 15 \pmod{21} \\ x \equiv 12 \pmod{15} \end{cases}$ **c**. $\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 6 \pmod{15} \\ x \equiv 7 \pmod{18} \end{cases}$ **d**. $\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 6 \pmod{15} \\ x \equiv 15 \pmod{18} \end{cases}$

Ejercicio 7. Cuando pedimos calcular $a \pmod{n}$ nos referimos a hallar el entero $0 \leq x < n$ tal que $a \equiv x \pmod{n}$. En los siguientes casos, calcular:

a. $560^{48} \pmod{1001}$. **b**. $22^{232} \pmod{36}$.

c. Hallar el último dígito de $2^{1000000}$ representado en base 13.

d. Investigar si 257 es primo y calcular $3^{9990} \pmod{257}$.

e. $132^{231} \pmod 7$.

f. $246^{218} \pmod{11}$.

g. $2^{69} \pmod{71}$.

h. $3^{279} \pmod{283}$.

i. $2^{71} \pmod{111}$.

j. $2^{156} \pmod{11}$.

k. $2^{30} \pmod 3$ y $2^{30} \pmod{37}$ y utilizarlos para calcular $2^{30} \pmod{111}$.

l. $347^{231} \pmod{35}$ (sugerencia: imitar lo hecho en la parte anterior).

m. $12^{22} \pmod{100}$.

n. $70^{151} \pmod{252}$.

ñ. Hallar el resto de dividir 123^{253} entre 490 (sugerencia: hallar los restos de dividir 123^{253} entre 2, 5 y 49).

o. Hallar el resto de dividir 24^{253} entre 490.

Ejercicio 8. Si p y q son primos distintos tales que $a^p \equiv a \pmod q$ y $a^q \equiv a \pmod p$, probar que $a^{pq} \equiv a \pmod{pq}$.

Ejercicio 9. Probar que $\varphi(mn) = \frac{\varphi(m)\varphi(n)d}{\varphi(d)}$ donde $d = \operatorname{mcd}(m, n)$ y φ la función de Euler.

Ejercicio 10. Se dice que un entero n es un *Pseudoprimo de Carmichael* si n es compuesto y $a^n \equiv a \pmod n$ para todo $a \in \mathbb{Z}$.

a. Sea b un número entero positivo y coprimo con 561.

  i) Demostrar que $b^2 \equiv 1 \pmod 3$, $b^{10} \equiv 1 \pmod{11}$ y $b^{16} \equiv 1 \pmod{17}$.

  ii) Hallar $b^{560} \pmod 3$, $b^{560} \pmod{11}$ y $b^{560} \pmod{17}$.

  iii) Probar que 561 es un Pseudoprimo de Carmichael (*Sug: hallar b^{561} dependiendo si b es coprimo o no con 561*).

b. Probar que si n es un entero compuesto tal que $\varphi(n)|n-1$ entonces n es un pseudoprimo de Carmichael.

c. Sea n compuesto y libre de cuadrados (no es divisible por ningún cuadrado), tal que todo divisor primo p de n cumple que $p-1|n-1$.

  i) Probar que n es un pseudoprimo de Carmichael.

  ii) Probar que n es impar.

  iii) Probar que n posee al menos tres factores primos distintos.