Universidad de la República **Matemática Discreta 2**
Facultad de Ingeniería **Primer semestre 2024**
Instituto de Matemática y Estadística

PRÁCTICO 6: TEOREMA CHINO DEL RESTO Y TEOREMA DE FERMAT-EULER

Ejercicio 1. Hallar todas las soluciones de los siguientes sistemas lineales de congruencias:

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

Ejercicio 2.

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

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

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

d. 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 $n + 1$.

Ejercicio 3.

a. Probar que los siguientes sistemas son equivalentes. Sugerencia: usar TCR en cada ecuación.

i) $\begin{cases} x \equiv 15 \pmod{21} \\ x \equiv 12 \pmod{15} \\ x \equiv 1 \pmod{7} \end{cases}$ ii) $\begin{cases} x \equiv 1 \pmod{7} \\ x \equiv 0 \pmod{3} \\ x \equiv 2 \pmod{5} \end{cases}$

b. Investigar si el sistema tiene solución, y en caso de que así sea, hallarlas todas.

Ejercicio 4. Investigar si los siguientes sistemas tienen solución, y en caso de que así sea, hallarlas todas (observar que cuando existen soluciones, son únicas módulo el m.c.m. 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**. $\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 6 \pmod{15} \\ x \equiv 7 \pmod{18} \end{cases}$ **c**. $\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 6 \pmod{15} \\ x \equiv 15 \pmod{18} \end{cases}$

Ejercicio 5. En este ejercicio usamos la siguiente notación:

- $a \pmod{m}$, con $m > 0$, denota el resto de dividir a entre m.
- $a^{-1} \pmod{m}$ denota el inverso de a módulo m.

En los siguientes casos, calcular:

a. Los últimos dos dígitos de 7^{42} y de 23^{41}. Sugerencia: considerar la división entre 100.

b. $2^{61} \pmod{77}$ y $13^{31} \pmod{77}$. Sugerencia: en el último caso descomponer módulo 7 y módulo 11.

c. $2^{-1} \pmod{55}$ y $2^{38} \pmod{55}$.

d. $123^{253} \pmod{490}$. Sugerencia: descomponer módulo 5 y 2×49.

Ejercicios complementarios

Ejercicio 6. Sean p y q primos distintos tales que: $a^p \equiv a \pmod{q}$ y $a^q \equiv a \pmod{p}$. Probar que se cumple:

a. $a^{pq} \equiv a \pmod{q}$ y $a^{pq} \equiv a \pmod{p}$. Sugerencia: usar Fermat.

b. $a^{pq} \equiv a \pmod{pq}$.

Ejercicio 7. Probar que $\varphi(mn) = \frac{\varphi(m)\varphi(n)d}{\varphi(d)}$; donde $d = \mathrm{mcd}(m, n)$ y φ es la función de Euler. Sugerencia: escribir m, n y d en su descomposición en factores primos, diferenciando en m y n los que son comunes con d.

Ejercicio 8. Un entero n es un *Pseudoprimo de Carmichael* si n es compuesto y cumple: $a^n \equiv a \pmod{n}$, para todo $a \in \mathbb{Z}$. (Notar que si n fuese primo, la congruencia se cumple siempre, por Fermat).

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. Sugerencia: hallar b^{561} dependiendo si b es coprimo o no con 561.

b. Sea n es un entero compuesto tal que $\varphi(n) | (n-1)$.

i) Probar que n es impar y libre de cuadrados (no es divisible por ningún cuadrado).

ii) Utilizando la parte anterior, y el TCR, probar que n es un pseudoprimo de Carmichael.

c. Sea n compuesto y libre de cuadrados, 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.

Se puede probar que un número n compuesto es pseudoprimo de Carmichael, si y solo si n es libre de cuadrados y $(p-1)|(n-1)$, para todo primo p tal que $p|n$. Se prueba utilizando raíces primitivas, tema que se dará más adelante en el curso.