Universidad de la República
Facultad de Ingeniería
Instituto de Matemática y Estadística

Matemática Discreta 2
Curso 2021

PRÁCTICO 6: Teorema Chino del Resto - Teoremas de Euler y Fermat

Ejercicio 1. Resolver los siguientes sistemas de módulos coprimos de dos formas: por substitución y utilizando la solución particular vista en teórico.

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. 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?

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

Ejercicio 4. Para $m \in \mathbb{Z}^+$ definimos $\mathrm{Cop}(m) := \{i : \mathrm{mcd}(i, m) = 1, 1 \leq i \leq m\}$. Podemos escribir $\mathrm{Cop}(m) = \{i_1, i_2, \ldots, i_{\varphi(m)}\}$ donde $\varphi(m) = \#\,\mathrm{Cop}(m)$. Sea $a \in \mathbb{Z}$ tal que $\mathrm{mcd}(a, m) = 1$.

a. Probar que los números $ai_1, ai_2, \ldots, ai_{\varphi(m)}$ dejan restos $i_1, i_2, \ldots, i_{\varphi(m)}$ (en algún orden) en la división por m.

b. Probar el Teorema de Fermat-Euler: si $\mathrm{mcd}(a, m) = 1$ entonces $a^{\varphi(m)} \equiv 1 \pmod m$.

Ejercicio 5. Cuando pedimos calcular $a \pmod m$ nos referimos a hallar el entero $0 \leq x < m$ tal que $a \equiv x \pmod m$, en particular $a^{-1} \pmod m$ denota al inverso de a módulo m. En los siguientes casos, calcular:

a. los últimos dos dígitos de 7^{42} y de 23^{41};

b. $2^{61} \pmod{77}$ y $13^{31} \pmod{77}$ (sug. en el último caso descomponer módulo 7 y módulo 11);

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

d. $123^{253} \pmod{490}$ (sug. descomponer módulo 2, 5 y 49).

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

Ejercicio 7. Probar que $\varphi(mn) = \frac{\varphi(m)\varphi(n)d}{\varphi(d)}$ donde $d = \mathrm{mcd}(m, n)$ y φ 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. 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 (*Sugerencia: hallar b^{561} dependiendo si b es coprimo o no con 561*).

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

- i) Probar que n es libre de cuadrados e impar.
- ii) Utilizando la parte anterior y el Teorema Chino del resto 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.

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