

## Solución del primer parcial de Mat. Discreta

**Ejercicio 1.**

**A.** Sea  $d = \text{mcd}(a, b)$  y  $a', b'$  tales que  $\text{mcd}(a', b') = 1$  y  $a = da', b = db'$ . Como  $\text{mcm}(a, b) = 26 \text{mcd}(a, b)$ , entonces  $da'b' = 26d$  y por lo tanto  $a'b' = 26$  y por lo tanto  $(a', b') = (1, 26)$  o  $(a', b') = (2, 13)$ . Entonces  $(a, b) = (d, 26d)$  o  $(a, b) = (2d, 13d)$ . En la primer posibilidad, el resto de dividir  $b$  entre  $a$  es 0. Así que  $(a, b) = (2d, 13d)$ . Además  $a = bq + 7$  entonces  $d|7$  y por lo tanto  $d = 1$  o  $d = 7$ . Si  $d = 1$ ,  $(a, b) = (2, 13)$  pero el resto de dividir  $b$  entre  $a$  es 1. Si  $d = 7$ , el par  $(a, b) = (14, 91)$  cumple las dos condiciones.

**B.**  $5^2 \equiv -1 \pmod{13} \Rightarrow 5^4 \equiv 1 \pmod{13} \Rightarrow 5^{4n+1} \equiv 5 \pmod{13}$ .

Por Fermat,  $4^6 = 2^{12} \equiv 1 \pmod{13}$ . Entonces  $2 \times 4^{6n+1} \equiv 8 \pmod{13}$ .

Entonces  $5^{4n+1} + 2 \times 4^{6n+1} \equiv 5 + 8 \pmod{13} \Rightarrow 5^{4n+1} + 2 \times 4^{6n+1} \equiv 0 \pmod{13}$ .

También se podía probar por inducción en  $n$ . El caso  $n = 0$  queda  $5 + 8 = 13$ . Paso inductivo: si sabemos que  $5^{4n+1} + 2 \times 4^{6n+1}$  es múltiplo de 13, entonces  $5^{4(n+1)+1} + 2 \times 4^{6(n+1)+1} = 5^{4n+1}5^5 + 2 \times 4^{6n+1} \times 4^6 = 5^{4n+1}625 + 2 \times 4^{6n+1} \times 4096 = 5^{4n+1}625 + 2 \times 4^{6n+1} \times (625 + 3471) = 625(5^{4n+1} + 2 \times 4^{6n+1}) + 4^{6n+1}3471$ . El primer sumando es múltiplo de 13 por hipótesis inductiva, y el segundo sumando también ya que  $3471 = 13 \times 267$ .

**Ejercicio 2.**

**A.** Por el teorema chino del resto,

$$x \equiv a28 + b21 + c12 \pmod{84} \text{ con } \begin{cases} a28 \equiv 1 \pmod{3} \Rightarrow a \equiv 1 \pmod{3} \\ b21 \equiv 0 \pmod{4} \Rightarrow b \equiv 0 \pmod{4} \\ c12 \equiv 6 \pmod{7} \Rightarrow c5 \equiv 6 \pmod{7} \Rightarrow c \equiv 4 \pmod{7} \end{cases}$$

Entonces  $x \equiv 28 + (4)12 \pmod{84} \Rightarrow x \equiv 76 \pmod{84}$ , entonces  $x = 76$ .

**B.** Como no podemos usar Euler, usamos el método de exponenciación que utiliza el Teorema chino del resto.

$$\begin{cases} 34^{1234} \equiv 1^{1234} \pmod{3} = 1 \pmod{3} \\ 34^{1234} = 2^{1234}17^{1234} \equiv 0 \pmod{4} \\ 34^{1234} \equiv 6^{1234} \pmod{7} \equiv 6^{1234} \pmod{7} \equiv 1 \pmod{7} \end{cases}$$

El Teorema Chino del Resto nos asegura que si  $x$  es solución de  $\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 0 \pmod{4} \\ x \equiv 1 \pmod{7} \end{cases}$  entonces

$$34^{1234} \equiv x \pmod{84}.$$

Resolvemos el sistema (análogo a la parte A)

$$x \equiv a28 + b21 + c12 \pmod{84} \text{ con } \begin{cases} a28 \equiv 1 \pmod{3} \Rightarrow a \equiv 1 \pmod{3} \\ b21 \equiv 0 \pmod{4} \Rightarrow b \equiv 0 \pmod{4} \\ c12 \equiv 1 \pmod{7} \Rightarrow c5 \equiv 1 \pmod{7} \Rightarrow c \equiv 3 \pmod{7} \end{cases}$$

Entonces  $x \equiv 28 + (3)12 \pmod{84} \Rightarrow x \equiv 64 \pmod{84}$ , entonces  $x = 64$ .

### Ejercicio 3.

- A. El teorema de Bezout dice que si  $\text{mcd}(a, n) = d$  entonces existen  $x, y \in \mathbb{Z}$  tales que  $ax + ny = d$ . Entonces si  $\text{mcd}(a, n) = 1$ , existen  $x, y \in \mathbb{Z}$  tales que  $ax + ny = 1$  y por lo tanto  $ax = 1 - ny$ , entonces  $ax \equiv 1 \pmod{n}$ .
- B. Directo: Si  $p$  es primo y  $a \in \{1, \dots, p-1\}$  entonces  $\text{mcd}(p, a) = 1$ . Por la parte anterior, existe  $x \in \mathbb{Z}$  tal que  $ax \equiv 1 \pmod{p}$ . Tomando  $x'$  el resto de dividir  $x$  entre  $p$  ( $x' \in \{0, \dots, p-1\}$ ), tenemos que  $ax' \equiv 1 \pmod{p}$  y por lo tanto  $x' \neq 0$ , es decir  $x' \in \{1, \dots, p-1\}$ .

Recíproco: Probaremos que si  $p$  no es primo, entonces existe  $a \in \{1, \dots, p-1\}$  tal que para todo  $x \in \mathbb{Z}$ ,  $ax \not\equiv 1 \pmod{p}$ .

Si  $p$  no es primo, entonces  $p = ab$  con  $a, b \in \{1, \dots, p-1\}$ . Si existiera  $x \in \mathbb{Z}$  tal que  $ax \equiv 1 \pmod{p}$ , entonces multiplicando por  $b$  a ambos lados, tenemos que  $bax \equiv b \pmod{p}$  y por lo tanto  $0 \equiv b \pmod{p}$  lo cual es absurdo ya que  $b \in \{1, \dots, p-1\}$ .

- C.  $55x \equiv 1 \pmod{127}$  si y sólo si existe  $y \in \mathbb{Z}$  tal que  $55x = 1 + 127y$  es decir  $55x - 127y = 1$ .  
Aplicando el algoritmo de Euclides extendido, obtenemos que  $55(-30) - 127(-12) = 1$  y por lo tanto  $x = -30 + 127 = 97$ .

### Ejercicio 4.

- A. Ver teórico (es parte de la demostración del teorema de Euler).
- B. Teorema de Euler: Sean  $a, n$  enteros coprimos, entonces  $a^{\varphi(n)} \equiv 1 \pmod{n}$ . La demostración se dio en el teórico.
- C. Como  $\text{mcd}(33, 35) = 1$ , por el teorema de Euler tenemos que  $33^{\varphi(35)} \equiv 1 \pmod{35}$ . Como  $35 = 5 \times 7$  y  $\varphi$  es multiplicativa para coprimos, tenemos que  $\phi(35) = \varphi(5)\varphi(7) = 4 \times 6 = 24$ . Entonces

$$33^{482} = 33^{(24)(200)+2} = (33^{24})^{200} 33^2 \equiv 1^{200} 33^2 \pmod{35} \equiv 33^2 \pmod{35} \equiv (-2)^2 \pmod{35} \equiv 4 \pmod{35}.$$

Por lo tanto, el resto de dividir  $33^{482}$  entre 35 es 4.