

SÓLUCION DEL EXAMEN DE MATEMÁTICA DISCRETA 2

Ejercicio 1.

- (a) De la primer ecuación obtenemos: $x \equiv 25 \pmod{49} \Rightarrow x \equiv 25 \pmod{7} \Rightarrow x \equiv 4 \pmod{7}$ y de la segunda obtenemos $x \equiv 13 \pmod{21} \Rightarrow x \equiv 13 \pmod{7} \Rightarrow x \equiv 6 \pmod{7}$ y por lo tanto el sistema no tiene solución.
- (b) La primer ecuación implica que $x \equiv 4 \pmod{7}$ y la tercera implica que $x \equiv 17 \pmod{3} \equiv 2 \pmod{3}$. Por el teorema chino del resto tenemos que la segunda ecuación es equivalente a

$$\begin{cases} x \equiv a \pmod{7} \\ x \equiv a \pmod{3} \end{cases}$$

Por lo tanto, para que el sistema tenga solución es necesario que

$$\begin{cases} a \equiv 4 \pmod{7} \\ a \equiv 2 \pmod{3} \end{cases}$$

La única solución $0 \leq a \leq 20$ es $a = 11$.

Luego, tomando $a = 11$ el sistema

$$\begin{cases} x \equiv 25 \pmod{49} \\ x \equiv 11 \pmod{21} \\ x \equiv 17 \pmod{27} \end{cases} \text{ es equivalente al sistema } \begin{cases} x \equiv 25 \pmod{49} \\ x \equiv 17 \pmod{27} \end{cases}$$

el cual, por el Teorema Chino del resto tiene solución, por ser $\text{mcd}(49, 27) = 1$.

- (c) Sea x el resto de dividir 5^{44} entre 1323. Entonces $x \equiv 5^{44} \pmod{1323}$. Como $1323 = 27 \cdot 49$ y 27 y 49 son coprimos, esto es equivalente a

$$\begin{cases} x \equiv 5^{44} \pmod{49} \\ x \equiv 5^{44} \pmod{27} \end{cases}$$

Como $\varphi(49) = \varphi(7^2) = 7^2 - 7 = 42$ y $\varphi(27) = \varphi(3^3) = 3^3 - 3^2 = 18$, y $\text{mcd}(5, 49) = \text{mcd}(5, 27) = 1$, aplicando el teorema de Euler para ambas ecuaciones obtenemos que este sistema es equivalente a

$$\begin{cases} x \equiv 5^2 \pmod{49} \\ x \equiv 5^8 \pmod{27} \end{cases} \Leftrightarrow \begin{cases} x \equiv 25 \pmod{49} \\ x \equiv 25^4 \pmod{27} \equiv (-2)^4 \pmod{27} \end{cases} \Leftrightarrow \begin{cases} x \equiv 25 \pmod{49} \\ x \equiv 16 \pmod{27} \end{cases}$$

Las soluciones a este sistema son de la forma $x = 25 \cdot A \cdot 27 + 16 \cdot B \cdot 49$, donde $27A \equiv 1 \pmod{49}$ y $49B \equiv 1 \pmod{27}$. Utilizando el Algoritmo de Euclides extendido obtenemos que $27 \cdot 20 - 49 \cdot 11 = 1$ y por lo tanto $A \equiv 20 \pmod{49}$ y $B \equiv -11 \pmod{27}$. Así que $x \equiv 25 \cdot 20 \cdot 27 - 16 \cdot 11 \cdot 49 \pmod{1323} \equiv 13500 - 8624 \pmod{1323} \equiv 270 - 8624 \pmod{1323} \equiv -8354 \pmod{1323} \equiv -416 \pmod{1323}$. Por lo tanto (pues $0 \leq x < 1323$) $x = 907$

Ejercicio 2.

- (a) Si G es un grupo finito y H es un subgrupo de G entonces $|H|$ divide a $|G|$.
- (b) Sea G un grupo de orden p y sea $g \in G$ con $e \neq g$. Tomamos $H = \langle g \rangle$; entonces por el teorema de Lagrange, $|H|$ divide a $|G| = p$. Pero como p es primo, las posibilidades son $|H| = 1$ o p ; pero como $e \neq g$ se tiene que $|H| > 1$ así que $|H| = p$. Por lo tanto $G = H = \langle g \rangle$ y entonces G es cíclico.

- (c) Sea $H = G_1 \cap G_2$. Como H es un subgrupo de G_1 , $|H|$ divide a $|G_1| = p$. Así que $|H| = 1$ o p . Supongamos que $|H| = p$, entonces $H = G_1$ y además como $H \subset G_2$, tendríamos que $G_1 \subset G_2$ y al tener los dos subgrupos el mismo orden, tendríamos que $G_1 = G_2$. Como por hipótesis $G_1 \neq G_2$ tenemos que $|H| = 1$ así que $H = \{e\}$
- (d) Como vimos en la parte b), si H es un subgrupo con orden p , entonces H es cíclico (y generado por un elemento de orden p). Veamos primero quienes son los elementos $g = (a, b) \in \mathbb{Z}_p \times \mathbb{Z}_p$ con orden p . Claramente $p(a, b) = (pa, pb) = (0, 0) = e$; así que el orden de todo elemento divide a p . Por lo tanto el único elemento que no tiene orden p es el neutro $e = (0, 0)$.

Por lo tanto hay $p^2 - 1$ elementos de orden p en $\mathbb{Z}_p \times \mathbb{Z}_p$. Cada uno de estos elementos, genera un subgrupo de $\mathbb{Z}_p \times \mathbb{Z}_p$ con orden p , pero hay repeticiones. Cada uno de estos subgrupos es generado por todos sus elementos $g \neq (0, 0)$; es decir, cada uno de estos subgrupos tiene $p - 1$ posibles generadores.

Por lo tanto, la cantidad de subgrupos de orden p es $\frac{p^2 - 1}{p - 1} = p + 1$.

Ejercicio 3. Sean p y q dos primos distintos y $n = pq$.

- (a) $\varphi(p) = \#\{a \in \mathbb{N} : 1 \leq a \leq p \text{ y } \text{mcd}(a, p) = 1\} = (\text{por ser } p \text{ primo}) = \#\{a \in \mathbb{N} : 1 \leq a \leq p \text{ y } p \nmid a\} = \#\{1, 2, \dots, p - 1\} = p - 1$.

$\varphi(n) = \#\{a \in \mathbb{N} : 1 \leq a \leq n \text{ y } \text{mcd}(a, n) = 1\} = (\text{por ser } n = pq \text{ con } p \text{ y } q \text{ coprimos})$
 $= \#\{a \in \mathbb{N} : 1 \leq a \leq n, \text{mcd}(a, p) = 1 \text{ y } \text{mcd}(a, q) = 1\} = (\text{por ser } p \text{ y } q \text{ primos})$
 $= \#\{a \in \mathbb{N} : 1 \leq a \leq n, p \nmid a \text{ y } q \nmid a\} = \#(\{1, 2, \dots, n\} \setminus \{a \in \{1, \dots, n\} : p|a \text{ o } q|a\}) =$
 $\#\{1, 2, \dots, n\} - \#\{p, 2p, \dots, qp\} - \#\{q, 2q, \dots, (p-1)q\} = n - q - (p-1) = pq - q - (p-1) =$
 $(p-1)q - (p-1) = (p-1)(q-1)$

- (b) Si $p = 13$ y $q = 53$,

$\#\{e : (689, e) \text{ es una clave válida}\} = \#\{e \in \{1, \dots, \varphi(n)\} : \text{mcd}(e, \varphi(n)) = 1\}$

y como $\varphi(n) = \varphi(13 \times 53) = 12 \times 52 = 624$ esto es

$\#\{e \in \{1, \dots, 624\} : \text{mcd}(e, 624) = 1\} = \varphi(624) = \varphi(2^4 \times 3 \times 13) = (2^4 - 2^3)2(12) = 8 \times 2 \times 12 = 192$.

- (c) Como $\varphi(13) = 12$, para ver que 2 es raíz primitiva módulo 13, hay que ver que el orden de 2 en $U(13)$ es 12. Como por Fermat tenemos que $2^{12} \equiv 1 \pmod{13}$, tenemos que el orden de 2 debe dividir a 12. Así que el orden es 12 si y solo si $2^a \not\equiv 1 \pmod{13}$, para todo a divisor propio de 12. En realidad basta con ver esto para $a = 6$ y $a = 4$. Y tenemos que $2^4 = 16 \equiv 3 \pmod{13}$ y $2^6 = 2^4 2^2 \equiv 3 \times 4 \pmod{13} \equiv 12 \pmod{13}$.

De forma análoga, para ver que 2 es raíz primitiva módulo 53, basta con ver que $2^a \not\equiv 1 \pmod{53}$, para todo a divisor propio de 52. Y como $52 = 4 \times 13$, basta con ver que esto vale para $a = 4$ y $a = 26$. Tenemos que $2^4 \equiv 16 \pmod{53}$; además $2^6 = 16 \times 4 = 64 \equiv 11 \pmod{53}$, $2^{12} \equiv 121 \pmod{53} \equiv 15 \pmod{53}$ y $2^{24} \equiv 225 \pmod{53} \equiv 13 \pmod{53}$. Por lo tanto $2^{26} \equiv 13 \times 4 \pmod{53} \equiv 52 \pmod{53}$.

- (d) Si $E(4) \equiv 105 \pmod{689}$ entonces $4^e \equiv 105 \pmod{689}$; y por el Teo.Chino del Resto, esto equivale a

$$\begin{cases} 4^e \equiv 105 \pmod{13} \\ 4^e \equiv 105 \pmod{53} \end{cases} \Leftrightarrow \begin{cases} 2^{2e} \equiv 1 \pmod{13} \\ 2^{2e} \equiv -1 \pmod{53} \end{cases}$$

Y como 2 es raíz primitiva módulo 13 y 53, esto es equivalente a que

$$\begin{cases} 2e \equiv 0 \pmod{12} \\ 2e \equiv 26 \pmod{52} \end{cases} \Leftrightarrow \begin{cases} e \equiv 0 \pmod{6} \\ e \equiv 13 \pmod{26} \end{cases}$$

Y como la primer ecuación implica que $e \equiv 0 \pmod{2}$ y la segunda implica que $e \equiv 13 \pmod{2} \equiv 1 \pmod{2}$, no existe ningún e .