

SOLUCIONES EXAMEN DE MATEMÁTICA DISCRETA 2

Ejercicio 1.

- A. (i) Tenemos que $(g^m)^k = g^{mk} = g^n = e$, la última igualdad usando que $o(g) = n$. Por otro lado, si $(g^m)^a = e \Rightarrow g^{ma} = e$, y como $o(g) = n$ tenemos que $n | ma \Rightarrow mk | ma \Rightarrow k | a$. Por lo tanto $o(g^m) = k$.
- (ii) Sea $r = o(g)$ y $s = o(h)$. Como $gh = hg$, para todo $m \in \mathbb{Z}$ se tiene que $(gh)^m = g^m h^m$. Así que $(gh)^{rs} = g^{rs} h^{rs} = (g^r)^s (h^s)^r = e^s e^r = e$. Resta probar que si $(gh)^m = e \Rightarrow rs | m$.
Si $(gh)^m = e \Rightarrow g^m h^m = e \Rightarrow (g^m h^m)^r = e \Rightarrow (g^m)^r (h^m)^r = e \Rightarrow (g^r)^m h^{mr} = e \Rightarrow h^{mr} = e$; y como $o(h) = s$ tenemos que $s | mr$, y al ser r y s coprimos, por el Lema de Euclides concluimos que $s | m$. Análogamente (elevando $(gh)^m$ a la s), se prueba que $r | m$. Como s y r son coprimos y ambos dividen a m concluimos que $rs | m$.
- (iii) Lo anterior en general es falso si $gh \neq hg$, Por ejemplo en S_3 si tomamos $h = (1\ 2)$ y $g = (1\ 2\ 3)$ tenemos que $gh \neq hg$, $o(g) = 2$ y $o(h) = 3$ y $o(hg) \neq 6$ (en S_3 no hay elementos de orden 6).
- B. (i) Como $b^{280} \equiv 400 \pmod{401} \equiv -1 \pmod{401} \Rightarrow b^{560} \equiv 1 \pmod{401}$ y por Fermat (como 401 es primo y $401 \nmid b$ pues $b \not\equiv 0 \pmod{401}$) sabemos que $b^{400} \equiv 1 \pmod{401}$. Así que $o(\bar{b})$ divide a 400 y a 560. Por lo tanto $o(\bar{b}) | \text{mcd}(400, 560)$ y entonces $o(\bar{b}) | 80$. Además, como $b^{280} \equiv -1 \pmod{401}$ tenemos que $o(\bar{b})$ no divide a 280. Por lo tanto $o(\bar{b}) = 80$ o 16, y como $b^{16} \equiv 39 \pmod{401} \not\equiv 1 \pmod{401}$, tenemos que $o(\bar{b}) = 80$.
- (iii) Para que $2^x b^y$ sea raíz primitiva módulo 401, necesitamos que $o(\overline{2^x b^y}) = 400 = 25 \times 16$. Por la parte A (i) tenemos que $o(\overline{2^8}) = 200/8 = 25$ y $o(\overline{b^5}) = 80/5 = 16$, y como $U(401)$ es abeliano, y $\text{mcd}(16, 25) = 1$, por la parte A (ii) tenemos que $o(\overline{2^8 b^5}) = 25 \times 16 = 400$, así que $2^8 b^5$ es raíz primitiva módulo 401.

Ejercicio 2.

- A. Sea $d = \text{mcd}(a, b)$, $b = db'$ y $a = da'$. Así que $\text{mcd}(a', b') = 1$.
Como $ab = 21 \text{mcd}(a, b) \Rightarrow a'b'd^2 = 21d$ así que $a'b'd = 21$. Además como $a \equiv d \pmod{b}$, tenemos que $a' \equiv 1 \pmod{b'}$.
Si $d = 1$ entonces $a'b' = 21$ y los que cumplen que $a' \equiv 1 \pmod{b'}$ son $(a, b) = (a', b') = (7, 3)$ y $(a, b) = (a', b') = (1, 21)$ y $(a, b) = (a', b') = (21, 1)$.
Si $d = 3$ entonces $a'b' = 7$ y los que cumplen que $a' \equiv 1 \pmod{b'}$ son $(a', b') = (1, 7)$ y $(a', b') = (7, 1)$ así que $(a, b) = (3, 21)$ y $(a, b) = (21, 3)$.
Si $d = 7$ entonces $a'b' = 3$ y los que cumplen que $a' \equiv 1 \pmod{b'}$ son $(a', b') = (1, 3)$ y $(a', b') = (3, 1)$ así que $(a, b) = (7, 21)$ y $(a, b) = (21, 7)$.
Si $d = 21$ entonces $a'b' = 1$ y la solución es $(a', b') = (1, 1)$ así que $(a, b) = (21, 21)$.
- B. (i) La ecuación $x \equiv 34 \pmod{49}$ implica que $x \equiv 34 \pmod{7}$, es decir $x \equiv 6 \pmod{7}$. La ecuación $x \equiv 11 \pmod{21}$ implica que $x \equiv 11 \pmod{7}$, es decir $x \equiv 4 \pmod{7}$. Y como $6 \not\equiv 4 \pmod{7}$ resulta que el sistema es incompatible.
- (ii) La ecuación $x \equiv 20 \pmod{49}$ implica $x \equiv 20 \pmod{7}$, es decir $x \equiv 6 \pmod{7}$. La ecuación $x \equiv 7 \pmod{9}$ implica $x \equiv 7 \pmod{3}$, es decir $x \equiv 1 \pmod{3}$.
Por el Teo chino del resto la ecuación $x \equiv 13 \pmod{21}$ es equivalente al sistema

$$\begin{cases} x \equiv 13 \pmod{7} \\ x \equiv 13 \pmod{3} \end{cases} \Leftrightarrow \begin{cases} x \equiv 6 \pmod{7} \\ x \equiv 1 \pmod{3} \end{cases}$$

Pero estas dos ecuaciones ya son consecuencia de las otras dos del sistema original. Así que el sistema original es equivalente al sistema

$$\begin{cases} x \equiv 20 \pmod{49} \\ x \equiv 7 \pmod{9} \end{cases}$$

y este sistema, por el Teorema Chino del Resto, al ser 49 y 9 coprimos, tiene solución única módulo $49 \times 9 = 441$. Una forma de hallar una solución es tomar $x = 20 \times A \times 9 + 7 \times B \times 49$ de forma tal que $A \times 9 \equiv 1 \pmod{49}$ y $B \times 49 \equiv 1 \pmod{9}$; es decir $A9 \equiv 1 \pmod{49}$ y $B4 \equiv 1 \pmod{9}$. Entonces basta con tomar $A = 11$ y $B = -2$ y por lo tanto $x = 20 \times 11 \times 9 + 7(-2)49 = 1980 - 686 = 1294 \equiv 412 \pmod{441}$.

Es decir, que todas las soluciones son $x = 412 + 441k$, con $k \in \mathbb{Z}$.

Ejercicio 3.

A. Ver teórico (hay que probar que para todo $x \in \mathbb{Z}$, $x^{de} \equiv x \pmod{n}$ y esto se prueba discutiendo según si $\text{mcd}(x, n) = 1$, o si alguno de los primos p y q (o ambos), divide a x).

B. Sean $p = 41$ y $q = 47$ y $n = pq$.

(i) $\varphi(n) = \varphi(41 \times 47) = 40 \times 46 = 1840$. Utilizando el algoritmo de Euclides se obtiene que $115 \times 1840 - 461 \times 459 = 1$ así que $\text{mcd}(1840, 459) = 1$ y además $459(-461) \equiv 1 \pmod{1840}$, así que $d \equiv (-461) \pmod{1840} \equiv 1840 - 461 \pmod{1840} \equiv 1379 \pmod{1840}$. Entonces la función de descryptado es $D : \mathbb{Z}_{1927} \rightarrow \mathbb{Z}_{1927}$ dada por $D(y) = y^{1379} \pmod{1927}$ (pues $n = 41 \times 47 = 1927$).

(ii) Tenemos que $494 \equiv 2 \pmod{41}$ y por Fermat $2^{40} \equiv 1 \pmod{41}$. Como $459 = 40 \times 11 + 19$ tenemos que $E(494) = 494^{459} \pmod{41} \equiv 2^{459} \pmod{41} \equiv 2^{19} \pmod{41}$. Y las potencias de 2 módulo 41 son 2, 4, 8, 16, 32, 64=23, 46=5, 10, $2^9 \equiv 20$, $2^{10} \equiv 40 \equiv -1$; así que $2^{19} \equiv -20 \pmod{41} \equiv 21 \pmod{41}$. Entonces el resto de dividir 494^{459} entre 41 es 21.

Tenemos que $494 \equiv 24 \pmod{47}$ y por Fermat $24^{46} \equiv 1 \pmod{47}$. Como $459 = 46 \times 10 - 1$ tenemos que $E(494) = 494^{459} \pmod{47} \equiv 24^{459} \pmod{47} \equiv 24^{-1} \pmod{47}$. Y como $24 \times 2 = 48 \equiv 1 \pmod{47}$ tenemos que el inverso de 24 módulo 47 es 2, y por lo tanto $494^{259} \equiv 2 \pmod{47}$; así que el resto de dividir 494^{259} entre 47 es 2.

(iii) Para hallar $E(494)$ hay que calcular $494^{259} \pmod{1927}$, por la parte anterior (y el Teo Chino del Resto) basta con encontrar $x \in \{0, 1, 2, \dots, 1926\}$ tal que

$$\begin{cases} x \equiv 21 \pmod{41} \\ x \equiv 2 \pmod{47} \end{cases}$$

Entonces tenemos que $x \equiv 21 \times A \times 47 + 2 \times B \times 41 \pmod{1927}$ con A y B tales que $47A \equiv 1 \pmod{41}$ y $41B \equiv 1 \pmod{47}$; por el dato de la letra tenemos que $A = 7$ y $B = -8$ y por lo tanto $x \equiv 21 \times 7 \times 47 + 2 \times (-8) \times 41 \pmod{1927} \equiv 6253 \pmod{1927} \equiv 472 \pmod{1927}$.