Universidad de la República - Facultad de Ingeniería - IMERL: Matemática Discreta 2

SEGUNDO PARCIAL - 4 DE JULIO DE 2014

Segundo parcial - soluciones

Ejercicio 1.

a. Si a es el orden de $\overline{g}$ en $U(p^2)$, en particular tenemos que $g^a \equiv 1 \pmod{p^2}$. Entonces p^2 divide a $g^a - 1$ y entonces (por la transitiva de la divisibilidad) tenemos que p divide a $g^a - 1$. Por lo tanto tenemos que $g^a \equiv 1 \pmod{p}$. Y como b es el orden de $\overline{g}$ concluímos que $b \mid a$.

b. i) Para probar que 10 es raíz primiitiva módulo 19, basta con probar que para cada primo q divisor de $19 - 1 = 18$, $10^{18/q} \not\equiv 1 \pmod{19}$. Es decir (tomando $q = 2$ y $q = 3$), tenemos que probar que $10^9 \not\equiv 1 \pmod{19}$ y que $10^6 \not\equiv 1 \pmod{19}$.

Como $20 \equiv 1 \pmod{19}$, tenemos que $10^2 = 100 = 20 \times 5 \equiv 5 \pmod{19}$; luego $10^4 \equiv 5^2 \pmod{19} \equiv 6 \pmod{19}$. Por lo tanto $10^6 = 10^4 10^2 \equiv 6(5) \pmod{19} \equiv 11 \pmod{19}$.

Por otro lado $10^8 \equiv 36 \pmod{19} \equiv -2 \pmod{19}$, y por lo tanto $10^9 \equiv -20 \pmod{19} \equiv 18 \pmod{19}$.

ii) Por la parte i) el orden de $\overline{10}$ en $U(19)$ es 18 y por la parte a) tenemos que si b es el orden de $\overline{10}$ en $U(19^2)$, entonces $18 \mid b$.

Por otro lado, como $\varphi(19^2) = 19^2 - 19 = 19(18)$ y $b \mid \varphi(19^2)$ concluímos que $b = 18$ o $b = 19(18)$. Para probar que 10 es raíz primitiva módulo 19^2 tenemos que probar que $b = 19(18)$. Por lo tanto basta con probar que $b \neq 18$. Para ésto, basta con ver que $10^{18} \not\equiv 1 \pmod{19^2}$.

Por el dato brindado en la letra tenemos que $10^5 \equiv 3 \pmod{19^2}$; entonces $10^{10} \equiv 9 \pmod{19^2}$ y $10^{15} \equiv 27 \pmod{19^2}$. Utilizando el dato que y $3(19)^2 = 1083$, tenemos que $10^3 = 1000 \equiv (-83) \pmod{19^2}$.

Por lo tanto, $10^{18} = 10^{15}10^3 \equiv 27(-83) \pmod{19^2} \equiv -2241 \pmod{19^2} \equiv 2(-1083) - 75 \pmod{19^2} \equiv -75 \pmod{19^2}$. Como $19^2 = 361$, concluímos que $10^{18} \equiv -75 \pmod{361} \not\equiv 1 \pmod{19^2}$.

iii) Ya vimos que 10 es raíz primitiva módulo 19^2. Por lo visto en teórico tenemos que 10 es raíz primitiva módulo 19^k para todo k. Como 10 es par, por lo visto en teórico (y práctico), para cada k tenemos que $10 + 19^k$ es raíz primitiva módulo $2(19)^k$.

Ejercicio 2.

a. Ver teórico.

b. Por el Teorema de órdenes para homomorfismos, tenemos que si $f : S_4 \to \mathbb{Z}_{35}$ es un homomorfismo, entonces $4! = |S_4| = |\mathrm{Ker}(f)||\mathrm{Im}(f)|$. Por lo tanto, $|\mathrm{Im}(f)|$ divide a $4!$. Por otro lado, por el Teorema de Lagrange, como $\mathrm{Im}(f) < \mathbb{Z}_{35}$ tenemos que también $|\mathrm{Im}(f)|$ divide a 35. Como $\mathrm{mcd}(4!, 35) = 1$ concluímos que $|\mathrm{Im}(f)| = 1$ y por lo tanto $\mathrm{Im}(f) = \{\overline{0}\}$ y entonces el único homomorfismo es el trivial.

c. En este caso, si $f : \mathbb{Z}_{15} \to \mathbb{Z}_6$ es un homorfismo, como $\mathbb{Z}_{15} = \langle \overline{1} \rangle$ veamos las posibilidades para $f(\overline{1})$ (ya que sabiendo el valor de $f(\overline{1})$, si f es homomorfismo tendremos que para todo $m \in \{0, \cdots, 14\}$, $f(\overline{m}) = f(m\overline{1}) = f(\underbrace{\overline{1} + \cdots + \overline{1}}_{m \text{ veces}}) = \underbrace{f(\overline{1}) + \cdots + f(\overline{1})}_{m \text{ veces}} = mf(\overline{1})$. Como $o(f(\overline{1}))$ divide a $o(\overline{1}) = 15$, tenemos que las posibilidades para $o(f(\overline{1}))$ son $1, 3, 5$ y 15. Pero además, como $f(\overline{1}) \in K$, tenemos que $o(f(\overline{1}))$ también divide a $|K| = 6$. Por lo tanto, $o(f(\overline{1}))$ es 1 o 3.

- Si $o(f(\overline{1})) = 1$, entonces $f(\overline{1})$ es el neutro de K, es decir $f(\overline{1}) = \overline{0}$, y entonces $f(\overline{m}) = m\overline{0} = \overline{0}$ para todo $m \in \{0, \cdots, 14\}$.
- Si $o(f(\overline{1})) = 3$ entonces $f(\overline{1})$ es $\overline{2}$ o $\overline{4}$. Entonces tenemos dos posibilidades para f: $f(\overline{m}) = m\overline{2} = \overline{2m}$ para todo $m \in \{0, \cdots, 14\}$ y $f(\overline{m}) = m\overline{4} = \overline{4m}$ para todo $m \in \{0, \cdots, 14\}$.

Ejercicio 3. Ver teórico.

Ejercicio 4.

a. La clave es $c \equiv 1005^8 \pmod{1009} \equiv (-4)^8 \pmod{1009} \equiv 2^{16} \pmod{1009} = 2^{10}2^6 \pmod{1009} \equiv 1024(64) \pmod{1009} \equiv 15(64) \pmod{1009} \equiv 960 \pmod{1009}$. Por lo tanto $c = 960$.

b. Tenemos que $960 = (28)34 + 8$ y $34 = (28) + 6$, tenemos que $960 = 28^2 + 6(28) + 8$, y por lo tanto la clave es $k = (1, 6, 8)$ o pasado a letras es $k =$ `BGI`.

c. Para desencriptar el mensaje, primero lo convertimos a una sucesión de números según la tabla: `WUFAGHFCWÑKZBXHEÑ␣DXMUG` correponde a la sucesión

$$(23, 21, 5, 0, 6, 7, 5, 2, 23, 14, 10, 26, 1, 24, 7, 4, 14, 27, 3, 24, 12, 21, 6).$$

Restando (módulo 28) la sucesión

$$(1, 6, 8, 1, 6, 8, 1, 6, 8, 1, 6, 8, 1, 6, 8, 1, 6, 8, 1, 6, 8, 1, 6)$$

obtenemos

$$(22, 15, 25, 27, 0, 27, 4, 24, 15, 13, 4, 18, 0, 18, 27, 3, 8, 19, 2, 18, 4, 20, 0),$$

que corresponde al texto: `VOY␣A␣EXONERAR␣DISCRETA`.

Ejercicio 5. Ver teórico.