

EXAMEN - 24 DE JULIO DE 2014.

Ejercicio 1.

a. Ver teórico.

b. Por letra $\text{mcd}(a, b) = \text{mcd}(4, a)$ por lo que, $\text{mcd}(a, b) = 1, 2$ o 4 . Veamos caso por caso.

- Si $\text{mcd}(a, b) = 1$: se tiene que cumplir que $ab = 675 = 3^3 5^2$ y como son coprimos las posibilidades son:
 - $a = 1, b = 675$, que no cumple $a \equiv 4 \pmod{b}$.
 - $a = 25, b = 27$, que no cumple $a \equiv 4 \pmod{b}$.
 - $a = 27, b = 25$, que no cumple $a \equiv 4 \pmod{b}$.
 - $a = 675, b = 1$, que cumple las hipótesis.
- Si $\text{mcd}(a, b) = 2$: se cumple que $ab = 4 \times 675 = 2700 = 2^2 3^3 5^2$ y las posibilidades son:
 - $a = 2, b = 1350$, que no cumple $a \equiv 4 \pmod{b}$.
 - $a = 50, b = 54$, que no cumple $a \equiv 4 \pmod{b}$.
 - $a = 54, b = 50$, que cumple las hipótesis.
 - $a = 1350, b = 2$, que cumple las hipótesis.
- Si $\text{mcd}(a, b) = 4$: se cumple que $ab = 16 \times 675 = 10800 = 2^4 3^3 5^2$ y las posibilidades son:
 - $a = 4, b = 2700$, que cumple las hipótesis.
 - $a = 100, b = 108$, que no cumple $a \equiv 4 \pmod{b}$.
 - $a = 108, b = 100$, que no cumple $a \equiv 4 \pmod{b}$.
 - $a = 2700, b = 4$, que cumple las hipótesis.

En conclusión las soluciones son $a = 675, b = 1, a = 1350, b = 2, a = 4, b = 2700, a = 2700, b = 4$ y $a = 54, b = 50$.

Ejercicio 2.

a. La solución módulo $\text{mcm}(6, 11, 13) = 6 \cdot 11 \cdot 13 = 858$ es

$$\begin{aligned} x &= 4 \times (11 \cdot 13)^{-1} \pmod{6} \times (11 \cdot 13) + 0 \times (6 \cdot 13)^{-1} \pmod{11} \times (6 \cdot 13) \\ &\quad + 1 \times (6 \cdot 11)^{-1} \pmod{13} \times (6 \cdot 11) \\ &= 4 \times (11 \cdot 13)^{-1} \pmod{6} \times (11 \cdot 13) + 1 \times (6 \cdot 11)^{-1} \pmod{13} \times (6 \cdot 11). \end{aligned}$$

Hallemos los inversos involucrados,

$$\begin{aligned} (11 \cdot 13)^{-1} \pmod{6} &\equiv (-1)^{-1} \pmod{6} \equiv 5 \pmod{6}, \\ (6 \cdot 11)^{-1} \pmod{13} &\equiv 1^{-1} \pmod{13} \equiv 1 \pmod{13}. \end{aligned}$$

Por lo que $x = 2926 \equiv 352 \pmod{858}$.

b. Por el teorema chino del resto $x \equiv 22^{300} \pmod{4290}$ si y solo si

$$\left\{ \begin{array}{l} x \equiv 22^{300} \pmod{5} \\ x \equiv 22^{300} \pmod{6} \\ x \equiv 22^{300} \pmod{11} \\ x \equiv 22^{300} \pmod{13} \end{array} \right. \text{ si y solo si } \left\{ \begin{array}{l} x \equiv 2^0 \pmod{5} \\ x \equiv 4^{300} \pmod{6} \\ x \equiv 0^{300} \pmod{11} \\ x \equiv 9^0 \pmod{13} \end{array} \right. \text{ si y solo si } \left\{ \begin{array}{l} x \equiv 1 \pmod{5} \\ x \equiv 4 \pmod{6} \\ x \equiv 0 \pmod{11} \\ x \equiv 1 \pmod{13} \end{array} \right.$$

y utilizando la parte anterior, el sistema es equivalente a

$$\left\{ \begin{array}{l} x \equiv 1 \pmod{5} \\ x \equiv 352 \pmod{858} \end{array} \right.$$

Como $2 \times 858 - 343 \times 5 = 1$ entonces $x \equiv 352 \times (-343) \times 5 + 1 \times 2 \times 858 \pmod{4290} \equiv 2926 \pmod{4290}$

Ejercicio 3.

- a. Ver teórico.
- b. Ver teórico.
- c. Sabemos que $D_3 = \{\text{id}, s, sr, sr^2, r, r^2\}$ y $r^3 = \text{id}$, $s^2 = \text{id}$ y $rs = sr^2$. Por el teorema de Lagrange, sabemos que si H es un subgrupo de D_3 tiene que tener orden 1, 2, 3 o 6 ya que $|D_3| = 6$. Si un subgrupo tiene orden primo tiene que ser cíclico, por lo que los subgrupos de D_3 tienen que ser los generados por elementos del mismo y D_3 . Veamos cuales son los subgrupos:
- $\{\text{id}\}$.
 - $\langle s \rangle = \{\text{id}, s\}$.
 - $(sr)^2 = sr sr = s sr^2 r = s^2 r^3 = \text{id}$, por lo que $\langle sr \rangle = \{\text{id}, sr\}$.
 - $(sr^2)^2 = sr^2 sr^2 = r s sr^2 = r^3 = \text{id}$, por lo que $\langle sr^2 \rangle = \{\text{id}, sr^2\}$.
 - $\langle r \rangle = \{\text{id}, r, r^2\}$.
 - D_3 .
- d. i) Como p es un primo impar tenemos que $\text{mcd}(2, p) = 1$ y por lo tanto $\varphi(2p) = \varphi(p)$. Además, nuevamente como $\text{mcd}(2, p) = 1$ podemos utilizar el teo. chino del resto y tenemos que $y^a \equiv 1 \pmod{2p}$ si y sólo si

$$\begin{cases} y^a \equiv 1 \pmod{2} \\ y^a \equiv 1 \pmod{p} \end{cases}$$

Por lo tanto, si x es impar, tenemos que x^a es impar y por lo tanto $x^a \equiv 1 \pmod{2}$. Entonces, si x es impar tenemos que $x^a \equiv 1 \pmod{2p}$ si y sólo si $x^a \equiv 1 \pmod{p}$. Y entonces $x^a \not\equiv 1 \pmod{2p}$ si y sólo si $x^a \not\equiv 1 \pmod{p}$.

Por otro lado, si x es impar y coprimo con p tenemos que x es raíz primitiva módulo $2p$ si y sólo si $x^a \not\equiv 1 \pmod{2p}$ para todo a divisor de $\varphi(2p) = \varphi(p)$, y por lo visto recién, ésto sucede si y sólo si $x^a \not\equiv 1 \pmod{p}$ para todo a divisor de $\varphi(p)$; es decir, si y sólo si x es raíz primitiva módulo p .

- ii) Como 11 es impar, por la pate anterior, alcanza ver que es raíz primitiva módulo 41 ya que $82 = 2 \cdot 41$. Veamos eso: hay que probar que $11^{\frac{\varphi(41)}{p}} \not\equiv 1 \pmod{41}$ para $p = 2, 5$ ya que $\varphi(41) = 40 = 2^3 \cdot 5$. Usando exponenciación rápida:

n	$11^{2^n} \pmod{41}$
0	11
1	$121 \equiv -2$
2	4
3	16
4	$256 \equiv 10$

Ahora $\frac{\varphi(41)}{2} = 2^2 \cdot 5 = 20 = 2^3 + 2^1$ y $\frac{\varphi(41)}{5} = 8 = 2^3$, por lo que $11^{\frac{\varphi(41)}{2}} \equiv 10 \cdot (-2) \pmod{41} \equiv 21 \pmod{41}$, y $11^{\frac{\varphi(41)}{5}} \equiv 16 \pmod{41}$.

- iii) Si $f : U(82) \rightarrow D_3$ homomorfismo de grupos y $g \in U(82)$ entonces $g = 11^n$ por lo que $f(g) = f(11)^n$, y alcanza con dar el valor de $f(11) \in D_3$ para describir f .
Por las partes anteriores $|\text{Im}(f)|$ divide $\text{mcd}(|U(82)|, |D_3|) = \text{mcd}(40, 6) = 2$, y $|\text{Im}(f)| = 1$ o 2 .
Vemos entonces que $\text{o}(f(11)) = 1$ o 2 , y $f(11) = \text{id}, s, sr, sr^2$.

Ejercicio 4. Dados $n = 209$ y $e = 17$:

- a. Para cifrar x debemos calcular $x^{17} \pmod{209}$, utilizamos exponenciación rápida:

n	$5^{2^n} \pmod{209}$
0	5
1	25
2	$625 \equiv -2$
3	4
4	16

Como $17 = 2^4 + 2^0$ entonces $5^{17} \equiv 5 \cdot 16 \pmod{209} \equiv 80 \pmod{209}$.

b. Descomponemos n , $209 = 11 \cdot 19$ y $\varphi(n) = 10 \cdot 18 = 180$.

c. Para encontrar la función de descifrado debemos hallar d el inverso de 17 módulo 180. Utilizando el algoritmo de Euclides extendido vemos que $d = 53$ y la función de descifrado es $D(y) = y^{53} \pmod{209}$. Calculamos $D(10)$ usando exponenciación rápida:

n	$10^{2^n} \pmod{209}$
0	10
1	100
2	$10000 \equiv -32$
3	$1024 \equiv -21$
4	23
5	111

Ahora $53 = 2^5 + 2^4 + 2^2 + 2^0$ y $10^{53} \equiv 111 \cdot 23 \cdot (-32) \cdot 10 \pmod{209} \equiv 21 \pmod{209}$.

Hay otras formas de resolver esta parte, por ejemplo utilizando el teorema chino del resto. Tenemos que $x \equiv 10^{53} \pmod{209}$ si y sólo si

$$\begin{cases} x \equiv 10^{53} \pmod{11} \equiv (-1)^{53} \pmod{11} \equiv -1 \pmod{11} \\ x \equiv 10^{53} \pmod{19} \equiv 10^{3 \times 18 - 1} \pmod{19} \equiv 10^{-1} \pmod{19} \equiv 2 \pmod{19} \end{cases}$$

Y resolviendo el sistema anterior resulta $x \equiv 21 \pmod{209}$.