

SOLUCIONES.

**Ejercicio 1.**

Sea  $\varphi$  la indicatriz de Euler y consideremos el conjunto  $A = \{m \in \mathbb{Z}^+ : \varphi(m) | m - 1\}$ .

- $A$  contiene al conjunto de los números primos (por el Teorema de Fermat).
- Por absurdo, supongamos que  $m \in A$  y que  $p^2 | m$  con  $p$  primo, tenemos que  $p | \varphi(m)$  (utilizar la fórmula para  $\varphi$ ), pero dado que  $m \in A$  también tendríamos que  $p | m - 1$ , lo cual es absurdo pues  $p | m$ .
- Si  $m = pq \in A$  entonces  $\varphi(m) = (p - 1)(q - 1) | pq - 1 = m - 1$ , por lo tanto  $q - 1 \equiv pq - 1 \equiv 0 \pmod{p - 1}$  y  $p - 1 \equiv pq - 1 \equiv 0 \pmod{q - 1}$  así que  $q - 1 = p - 1$  y por lo tanto  $p = q$  absurdo.

**Ejercicio 2.**

- Los factores primos de  $n$ ,  $p$  y  $q$  son muy cercanos y por lo tanto  $n$  puede factorizarse fácilmente utilizando el Método de Fermat.
- Debemos primero resolver  $ed \equiv 1 \pmod{\varphi(n)}$ , como  $24623 \cdot 6803 - 26892 \cdot 6229 = 1$  tenemos que  $24623 \cdot 6803 \equiv 1 \pmod{26892}$  así que  $d = 6803$ .  
Los valores de los bloques son  $THG = 20 \cdot 31^2 + 7 \cdot 31 + 6 = 19443$  y  $S!H = 19 \cdot 31^2 + 29 \cdot 31 + 7 = 19165$ . Para descryptar el primer bloque debemos calcular  $19443^{6803} \pmod{27221}$ .

$$\begin{cases} x \equiv 19443^{6803} \equiv 71^{6803} \equiv 71^{-3} \equiv (71^3)^{-1} \equiv 30^{-1} \pmod{167} \\ y \equiv 19443^{6803} \equiv 46^{6803} \equiv 46^{-1} \pmod{163} \end{cases}$$

donde se ha usado que  $6803 \equiv -3 \pmod{166}$ ,  $6803 \equiv -1 \pmod{162}$  y el Teorema de Fermat. Así que

$$\begin{cases} 30x \equiv 1 \pmod{167} \\ 46y \equiv 1 \pmod{163} \end{cases}$$

De las ecuaciones  $30 \cdot 39 - 7 \cdot 167 = 1$  y  $46 \cdot 39 - 11 \cdot 163 = 1$  tenemos que  $x = 39$  e  $y = 39$ . Luego  $X = 19443^{6803}$  verifica el sistema de congruencias

$$\begin{cases} X \equiv 39 \pmod{167} \\ X \equiv 39 \pmod{163} \end{cases}$$

Otra solución evidente es  $X = 39$  así que  $19443^{6803} \equiv 39 \pmod{27221}$ .  
Tenemos que  $39 = 1 \cdot 31 + 8 = BI$ .

Para descryptar el segundo bloque debemos calcular  $19165^{6803} \pmod{27221}$ .

$$\begin{cases} x \equiv 19165^{6803} \equiv 127^{6803} \equiv 127^{-3} \equiv (127^3)^{-1} \equiv 128^{-1} \pmod{167} \\ y \equiv 19165^{6803} \equiv 94^{6803} \equiv 94^{-1} \pmod{163} \end{cases}$$

donde se ha usado que  $6803 \equiv -3 \pmod{166}$ ,  $6803 \equiv -1 \pmod{162}$  y el Teorema de Fermat. Así que

$$\begin{cases} 128x \equiv 1 \pmod{167} \\ 94y \equiv 1 \pmod{163} \end{cases}$$

De las ecuaciones  $128 \cdot 137 - 105 \cdot 167 = 1$  y  $94 \cdot 137 - 79 \cdot 163 = 1$  tenemos que  $x = 137$  e  $y = 137$ . Luego  $X = 19165^{6803}$  verifica el sistema de congruencias

$$\begin{cases} X \equiv 137 \pmod{167} \\ X \equiv 137 \pmod{163} \end{cases}$$

Otra solución evidente es  $X = 137$  así que  $19443^{6803} \equiv 137 \pmod{27221}$ .  
Tenemos que  $137 = 4 \cdot 31 + 13 = EN$ .

Por lo tanto el mensaje original era BIEN.

### Ejercicio 3.

- a
  - i. Tenemos que  $\varphi(m) \in S$  por el Teorema de Fermat-Euler, así que  $S$  es no vacío.
  - ii. Sea  $n = sq + r$  con  $0 \leq r < s$  entonces  $a^n = (a^s)^q a^r \equiv a^r \pmod{p}$  pues  $s \in S$ , pero como  $n \in S$  tenemos que  $a^r \equiv a^n \equiv 1 \pmod{p}$ , luego por la minimalidad de  $s$  tenemos  $r = 0$ .
- b)
  - i. Sea  $s = \min\{n \in \mathbb{Z}^+ : a^n \equiv 1 \pmod{p}\}$ , por hipótesis y usando la parte anterior tenemos que  $s|q$  donde  $q$  es primo, así que  $s = 1$  ó  $s = q$ . Pero como  $a^1 \not\equiv 1 \pmod{p}$  se tiene que  $s \neq 1$  así que  $s = q$ .
  - ii. Por el Teorema de Fermat  $a^{p-1} \equiv 1 \pmod{p}$  (por hipótesis  $a$  no es múltiplo de  $p$ ), luego por las partes anteriores se tiene que  $q|p-1$ .
- c)
  - i. Vemos que  $a_1^8 = (a_1^2)^4 \equiv a_2^4 = (a_2^2)^2 \equiv a_3^2 \equiv a_1 \pmod{p}$ . Como  $a_1 \not\equiv 0 \pmod{p}$  con  $p$  primo, podemos dividir ambos lados de la congruencia por  $a_1$  obteniendo que  $a_1^7 \equiv 1 \pmod{p}$ , luego por la parte b) tenemos que  $7|p-1$  o equivalentemente  $p \equiv 1 \pmod{7}$ .
  - ii. Por la parte b), tenemos que  $p \equiv 1 \pmod{7}$  y como  $700 \leq p \leq 725$ , tenemos que  $p \in \{701, 708, 715, 722\}$ . Pero 708 y 722 son pares y  $5|715$  así que el único primo es  $p = 701$ . Haciendo la tablita de exponenciación rápida se observa que los números  $361^{2^n} \pmod{701}$  se repiten periódicamente con período 3, como  $361 \equiv 1 \pmod{3}$  resulta que  $361^{2^{361}} \equiv 361^{2^1} \equiv 636 \pmod{701}$ .