

EXAMEN - 13 DE FEBRERO DE 2015.

Ejercicio 1.

- a. Supongamos que $a > 11$ y $b > 11$, y como a y b son naturales $a \geq 12$, $b \geq 12$. Entonces

$$a \cdot b \geq 12 \cdot 12 = 144 > 130,$$

contradiendo la hipótesis.

- b. Por la parte anterior vemos que si $n \leq 130$ entonces sus divisores primos son menores o iguales a 11. Con lo anterior podemos utilizar la criba de Eratóstenes (ver teórico), eliminando los múltiplos de 2, 3, 5, 7, 11 y vemos que los primos menores que 130 son:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127.

- c. Tenemos que resolver la siguiente diofántica

$$3860 = 238x + 178y,$$

con x, y enteros no negativos. La diofántica anterior tiene solución ya que $\text{mcd}(238, 178) = 2 \mid 3860$. Aplicando el Algoritmo de Euclides Extendido vemos que

$$2 = 238 \cdot 3 + 178 \cdot (-4),$$

y multiplicando la ecuación por $\frac{3860}{2} = 1930$, obtenemos una solución particular de la diofántica

$$3860 = 238 \cdot (3 \cdot 1930) + 178 \cdot (-4 \cdot 1930) = 238 \cdot 5790 + 178 \cdot (-7720).$$

Con lo cual obtenemos la solución general de la diofántica

$$(x, y) = \left(5790 - \frac{178}{2} \cdot k, -7720 + \frac{238}{2} \cdot k \right) = (5790 - 89 \cdot k, -7720 + 119 \cdot k), \quad k \in \mathbb{Z}.$$

Como queremos que $x, y \geq 0$, se tiene que cumplir que $5790 \geq 89 \cdot k$ y $119 \cdot k \geq 7720$, con lo cual

$$65,056... \geq k \geq 64,873... .$$

Concluimos que $k = 65$ y $(x, y) = (5, 15)$.

Ejercicio 2.

- a. Primero calculamos $\varphi(81) = \varphi(3^4) = 2 \cdot 3^3 = 2 \cdot 27 = 54$. Como 79 y 81 son coprimos podemos utilizar el Teorema de Euler y obtenemos que

$$79^{221} \equiv (-2)^5 \pmod{81} \equiv -32 \pmod{81} \equiv 49 \pmod{81},$$

ya que $221 \equiv 5 \pmod{54}$.

- b. Factorizamos $595 = 5 \cdot 7 \cdot 17$ y aplicamos el Teorema Chino del Resto para obtener la siguiente equivalencia

$$x \equiv 11^{181} \pmod{595} \iff \begin{cases} x \equiv 11^{181} \pmod{5} \\ x \equiv 11^{181} \pmod{7} \\ x \equiv 11^{181} \pmod{17} \end{cases} \iff \begin{cases} x \equiv 1 \pmod{5} \\ x \equiv 4 \pmod{7} \\ x \equiv 10 \pmod{17} \end{cases} .$$

Aplicando el Teorema Chino del Resto obtenemos que $x \equiv 571 \pmod{595}$.

Ejercicio 3.

a. Primero calculamos $\varphi(86) = \varphi(2 \cdot 43) = 42 = 2 \cdot 3 \cdot 7$.

i) Para hallar el orden de 9 alcanza con probar las potencias de 9 que dividen a 42. O sea que hay que probar con los $d \in \{1, 2, 3, 6, 7, 14, 21, 42\}$. Veamos cual es la primer potencia que es 1,

$$9^2 \equiv 81 \pmod{86}$$

$$9^3 \equiv 41 \pmod{86}$$

$$9^6 \equiv 47 \pmod{86}$$

$$9^7 \equiv 79 \pmod{86}$$

$$9^{14} \equiv 49 \pmod{86}$$

$$9^{21} \equiv 1 \pmod{86}$$

ii) Como $9 = 3^2$ y $\text{o}(9) = 21$, $2 \nmid 21$ entonces $\text{o}(3) = 42$.

b. Para hallar la clave tenemos que calcular $994^{12} \pmod{997} \equiv (-3)^{12} \pmod{997} \equiv 81^3 \pmod{997}$. Para calcular la potencia anterior vemos que $81^2 = 6561 = 6 \cdot 1000 + 561 = 6 \cdot (997 + 3) + 561 \equiv 6 \cdot 3 + 561 \pmod{997} \equiv 579 \pmod{997}$. Por último $81^3 \equiv 579 \cdot 81 \pmod{997} \equiv 46899 \pmod{997} \equiv 46 \cdot 3 + 899 \pmod{997} \equiv 40 \pmod{997}$.

Ejercicio 4.

a. Ver teórico.

b. i) Ver teórico.

ii) Ver teórico.

iii) La afirmación es falsa. Sea $G = U(12)$, con $|G| = \varphi(12) = 4$. Se cumple que si $\overline{(-1)} \in G$, entonces $\overline{(-1)}^1 = \overline{(-1)}^3$, pero $1 \not\equiv 3 \pmod{|G|}$.