

EXAMEN - 6 DE DICIEMBRE DE 2014.

Ejercicio 1.

- a. Enunciar el Teorema Chino del Resto.

Ver notas de teórico.

- b. Una señora va a la feria con una cesta con huevos. En un momento deposita la cesta en el piso y un joven en bicicleta se los rompe. El joven le ofrece pagarselos y le pregunta cuantos tenía. La señora no se acuerda, pero cuando los tomó de a 5 le sobraban 4, cuando los tomó de a 7 le sobraban 6, cuando los tomó de a 11 le sobraban 10 y cuando los tomó de a 13 no le sobro ninguno. ¿Cuál es la cantidad mínima de huevos que tenía la señora?

El sistema a resolver es:

$$\begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 6 \pmod{7} \\ x \equiv 10 \pmod{11} \\ x \equiv 0 \pmod{13} \end{cases} \quad ,$$

que tiene solución porque los módulos son todos primos. El sistema es equivalente a

$$\begin{cases} x \equiv -1 \pmod{5 \cdot 7 \cdot 11} \\ x \equiv 0 \pmod{13} \end{cases} \quad .$$

La solución módulo $\text{mcm}(13, 385) = 5005$ es $x = -1 + (5 \cdot 7 \cdot 11) \times ((5 \cdot 7 \cdot 11)^{-1} \pmod{13})$. Calculemos el inverso anterior:

$$(5 \cdot 7 \cdot 11)^{-1} \pmod{13} \equiv 8^{-1} \pmod{13} \equiv 5 \pmod{13}.$$

Entonces $x \equiv 385 \cdot 5 - 1 \pmod{5005} \equiv 1924 \pmod{5005}$.

- c. Luego del incidente anterior, el mismo joven volvió a pisarle la cesta con huevos a otra señora, por lo cual el joven se compromete nuevamente a recompensarla. La señora conociendo la historia anterior le dice que cuando los tomó de a 10 le sobraron 5, cuando los tomó de a 12 le sobraron 7 y cuando los tomó de a 14 le sobro 2. Luego de meditarlo un momento, el joven increpa a la señora y le dice que eso no puede ser así. ¿Cuál de las dos partes tiene la razón?

El sistema a resolver es:

$$\begin{cases} x \equiv 5 \pmod{10} \\ x \equiv 7 \pmod{12} \\ x \equiv 2 \pmod{14} \end{cases} \quad .$$

Observar que si x es solución del sistema, entonces $x \equiv 7 \pmod{12}$ y por lo tanto $x \equiv 7 \pmod{2} \equiv 1 \pmod{2}$; es decir, x es impar. Por otro lado, $x \equiv 2 \pmod{14}$ entonces $x \equiv 2 \pmod{2} \equiv 0 \pmod{2}$ y por lo tanto x es par. Concluimos entonces que el sistema no tiene solución por lo que el joven tiene razón.

Ejercicio 2.

- a. Sea la función φ de Euler y dos enteros m, n tales $\text{mcd}(m, n) = 1$, probar que

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Ver notas de teórico.

- b. Reducir $2^{1511} \pmod{1323}$.

Primero calculamos $\varphi(1323) = \varphi(3^3 \cdot 7^2) = 2 \cdot 3^2 \cdot 6 \cdot 7 = 756$. También vemos que $1511 \equiv 755 \pmod{756} \equiv -1 \pmod{756}$. Y por el teorema de Euler,

$$2^{1511} \equiv 2^{-1} \pmod{1323}.$$

Ahora, $1323 = 2 \cdot 662 - 1$ y $2^{-1} \equiv 662 \pmod{1323}$.

Ejercicio 3.

- a. Sea un grupo finito G y $g \in G$, probar que si $k \in \mathbb{Z}^+$, entonces $o(g^k) = \frac{o(g)}{\text{mcd}(o(g), k)}$.

Ver notas de teórico.

- b. Sea el primo $p = 29$.

- i) Hallar el orden de 13 módulo p .

Por el teorema de Lagrange, $o(13) \mid \varphi(29) = 28 = 2^2 \cdot 7$, por lo que $o(13) \in \{1, 2, 4, 7, 14, 28\}$. Calculamos algunas potencias, $13^2 = 169 \equiv 24 \pmod{29} \equiv -5 \pmod{29}$, por lo que $o(13) \neq 2$. $13^4 \equiv (-5)^2 \pmod{29} \equiv 25 \pmod{29} \equiv -4 \pmod{29}$ y $o(13) \neq 4$. $13^7 \equiv 13^{1+2+4} \pmod{29} \equiv 13 \cdot (-5) \cdot (-4) \pmod{29} \equiv 260 \pmod{29} \equiv -1 \pmod{29}$, por lo que $o(13) \neq 7$. Por último, $13^{14} \equiv (-1)^2 \pmod{29} \equiv 1 \pmod{29}$, y $o(13) = 14$.

- ii) Probar que 10 es raíz primitiva módulo p .

Observar que $10^2 \equiv 100 \pmod{29} \equiv 13 \pmod{29}$. Utilizando la formula de la primer parte del ejercicio, con $g = 10$ y $k = 2$, vemos que

$$o(13) \text{mcd}(o(10), 2) = o(10).$$

Como antes, $o(10) \in \{1, 2, 4, 7, 14, 28\}$. Si $o(10) = 7$, entonces $14 = o(13) = o(13) \text{mcd}(o(10), 2) = o(10) = 7$ lo cual es absurdo. Todas las otras posibilidades para el orden, que no sean 1, nos da que $\text{mcd}(o(10), 2) = 2$ y vemos que $o(10) = 28$, por lo cual es raíz primitiva.

- iii) Hallar todos los $k \in \mathbb{Z}$ tales que $10^k \equiv 20 \pmod{29}$.

Por las partes anteriores, $20 = (-5) \cdot (-4) \equiv 13^2 13^4 \pmod{29} \equiv 10^4 10^8 \pmod{29} \equiv 10^{12} \pmod{29}$. Por lo tanto $k_0 = 12$ es solución. Ahora $10^k \equiv 20 \pmod{29}$ si y sólo si $10^k \equiv 10^{12} \pmod{29}$; si y sólo si $10^{k-12} \equiv 1 \pmod{29}$. Y como 10 es raíz primitiva módulo 29, esto sucede si y sólo si $28 \mid k - 12$. Es decir, si y sólo si $k \equiv 12 \pmod{28}$.

Ejercicio 4.

- a. Probar que la función de descifrado D en el protocolo RSA descifra correctamente.

Ver notas de teórico.

- b. Sean $n = 91$ y $e = 5$.

- i) Hallar la función de descifrado D para el protocolo RSA.

Calculemos $\varphi(91) = \varphi(7 \cdot 13) = 6 \cdot 12 = 72$ y $5^{-1} \equiv 29 \pmod{72}$. Por lo cual $D(y) = y^{29} \pmod{91}$.

- ii) Descifrar $y = 11$.

$$11^{29} \equiv 72 \pmod{91}$$