Examen - 6 de diciembre de 2014. Duración: 3 horas y media.

N° de examen	Cédula	Apellido y nombre

Ejercicio 1.

a. Enunciar el Teorema Chino del Resto.

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?

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?

Ejercicio 2.

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

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

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

Ejercicio 3.

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

b. Sea el primo $p = 29$.

i) Hallar el orden de 13 módulo p.

ii) Probar que 10 es raíz primitiva módulo p.

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

Ejercicio 4.

a. Probar que la función de desencriptado D en el protocolo RSA desencripta correctamente.

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

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

ii) Descifrar $y = 11$.