

## SOLUCIÓN

1. Sea  $g: \mathbb{Z}^3 \rightarrow \mathbb{Z}^2$  la función  $g(a, b, c) = (2187a - 9690b, 7c)$ .
- a) Mostrar que  $g$  es un morfismo de grupos, si tomamos  $\mathbb{Z}$  con la operación suma.
  - b) Probar que  $(12, 14) \in \text{Im}(g)$  y encontrar todos los  $\alpha \in \mathbb{Z}^3$  que verifican  $g(\alpha) = (12, 14)$ .
  - c) Hallar la imagen de  $g$ .
  - d) Encontrar  $H < \mathbb{Z}^3$  de forma que  $\hat{g}: \mathbb{Z}^3/H \rightarrow \mathbb{Z}^2$  definida por  $\hat{g}([\alpha]) = g(\alpha)$  sea un monomorfismo. Investigar si  $\hat{g}$  es isomorfismo.

### Solución:

- a) Es fácil verificar que  $g(a, b, c) + g(a', b', c') = g(a + a', b + b', c + c')$ .
- b) Comenzamos verificando que  $14 = 7 \times 2$ , o sea tomamos  $c = 2$ . Por otro lado necesitamos que existan  $a, b$  tal que  $12 = 2187a - 9690b$ . El  $\text{mcd}(2187, 9690) = 3$ , que divide a 12, por lo que la ecuación diofántica admite solución.

Para hallar todas las soluciones buscaremos primero una solución particular. Utilizando el Algoritmo de Euclides se puede probar que  $3 = 2187 \times (-1471) - 9690 \times (-332)$ . Entonces  $12 = 2187 \times (-5884) - 9690 \times (-1328)$ . Luego  $(a, b) = (-5884, -1328)$  es una solución particular. Luego todas las soluciones son de la forma:  $a = -5884 + 3230k$ ;  $b = -1328 + 729k$ , con  $k \in \mathbb{Z}$ .

- c) Por lo visto en el punto anterior, la ecuación diofántica  $2187a - 9690b = x$  tiene solución si y solo si  $3 = \text{mcd}(2187, 9690)$  divide a  $x$ . Luego  $\text{Im}(g) = (x, y) \in \mathbb{Z}^2$  tal que  $x$  es múltiplo de 3 e  $y$  es múltiplo de 7.
- d) La función  $\hat{g}$  nunca puede ser un isomorfismo pues  $\text{Im}(\hat{g}) \subseteq \text{Im}(g) \subset \mathbb{Z}^2$ . Por otro lado para obtener un monomorfismo necesitamos que  $H$  sea un subgrupo normal de  $\mathbb{Z}^3$  que contenga a  $N(g)$  (Núcleo de  $g$ ). Como  $\mathbb{Z}^3$  es abeliano todo subgrupo es normal. Así podemos considerar  $H = N(g) = \{ (a, b, c) \in \mathbb{Z}^3 / c = 0 \wedge a = 3230 \times t \wedge b = 729 \times t, t \in \mathbb{Z} \}$  o bien  $H = \mathbb{Z}^3$  (hay más opciones).

2. a) Probar que si  $n$  es un número compuesto, entonces  $(n-1)! + 1$  no es múltiplo de  $n$ .
- b) Sea  $p$  un número primo.
- i) Probar que en  $(\mathbb{Z}_p^*, \cdot)$  todos los elementos tienen inverso.
  - ii) Probar que 1 y  $p-1$  son inversos de si mismos (y son los únicos con esa propiedad).
  - iii) Demostrar que  $(p-1)! + 1$  es múltiplo de  $p$ .

### Solución:

- a) Si  $n$  es compuesto entonces existe  $d$  divisor de  $n$  con  $1 < d < n$ . Como  $(n-1)! \equiv 0 \pmod{d}$ , entonces  $(n-1)! + 1 \equiv 1 \pmod{d}$ . Por lo tanto  $(n-1)! + 1$  no es múltiplo de  $n$ .
- b) i) Si  $a$  no es cero (módulo  $p$ ), entonces  $\text{mcd}(a, p) = 1$ . Luego (por el Lema de Bezout) existen  $\alpha, \beta \in \mathbb{Z}$  tal que  $\alpha \times a + \beta \times p = 1$ . Entonces  $\alpha \times a \equiv 1 \pmod{p}$ , es decir  $\alpha$  es el inverso de  $a$  en  $\mathbb{Z}_p^*$ .

- ii) Planteamos la ecuación  $x^2 \equiv 1 \pmod{p}$ . Se resuelve si y solo si  $(x-1)(x+1)$  es múltiplo de  $p$ , o sea si  $x = \pm 1 \pmod{p}$ . O sea  $x \equiv 1 \pmod{p}$  o  $x \equiv -1 \pmod{p} \equiv p-1 \pmod{p}$ .
  - iii) En el producto  $2 \times 3 \times \dots \times (p-3) \times (p-2)$ , cada factor tiene un inverso, módulo  $p$ , en la productoria (y es único, como es conocido). Luego  $2 \times 3 \times \dots \times (p-3) \times (p-2) \equiv 1 \pmod{p}$ , y multiplicando por  $(p-1)$  de ambos lados obtenemos  $(p-1)! \equiv -1 \pmod{p}$ . Esto implica que  $(p-1)! + 1 \equiv 0 \pmod{p}$ , como queríamos probar.
3. Sea  $n$  un número que no es fácil de factorizar y que es producto de dos números primos grandes. Supongamos que Juan utiliza el criptosistema RSA y que eligió como su clave pública  $(n, e_1)$ . Juan pensó que sería más seguro utilizar además otra clave, pero con el mismo  $n$ . Digamos que la otra clave que eligió es  $(n, e_2)$ , donde  $\text{mcd}(e_1, e_2) = 3$ .

Sea  $c_1 = m^{e_1} \pmod{n}$  el mensaje enviado con la primera clave y  $c_2 = m^{e_2} \pmod{n}$  el mensaje enviado con la segunda clave.

- a) Mostrar cómo se puede recuperar  $m^3$  a partir de  $c_1$  y  $c_2$  si  $\text{mcd}(m, n) = 1$ .  
*Sugerencia:* Utilizar el Algoritmo de Euclides Extendido para encontrar una relación entre  $e_1$  y  $e_2$ .
- b) Juan decide enviar el mismo mensaje utilizando una tercer clave pública:  $(n, e_3)$ , con  $e_3 = 100$ . Probar que, a partir de lo anterior, es posible decodificar el mensaje.

### Solución:

- a) Suponemos  $\text{mcd}(m, n) = 1$ . Como  $\text{mcd}(e_1, e_2) = 3$ , aplicando el AEE, podemos hallar en forma eficiente  $\alpha, \beta \in \mathbb{Z}$  tal que  $\alpha \times e_1 + \beta \times e_2 = 3$ . Luego  $c_1^\alpha c_2^\beta \equiv m^{\alpha \times e_1 + \beta \times e_2} = m^3 \pmod{n}$ .
- b) El tercer mensaje enviado por Juan es  $c_3 \equiv m^{100} \pmod{n}$ . A través del algoritmo de Euclides hallamos  $\gamma$  tal que  $\gamma m^3 \equiv 1 \pmod{n}$  (o sea  $\gamma = m^{-3} \pmod{n}$ ). Entonces  $\gamma^{33} \times c_3 \equiv m^{100} \times (m^{-3})^{33} \equiv m \pmod{n}$ . De esta manera hemos recuperado el mensaje  $m$ .