

Examen de Matemática Discreta II
23 de diciembre de 2008

Número de Examen	Cédula	Nombre y Apellido

1. (35 puntos)

Sea $g : \mathbb{Z}^3 \rightarrow \mathbb{Z}^2$ la función $g(a, b, c) = (2187a - 9690b, 7c)$.

- Mostrar que g es un morfismo de grupos, si tomamos \mathbb{Z} con la operación suma.
- Probar que $(12, 14) \in \text{Im}(g)$ y encontrar todos los $\alpha \in \mathbb{Z}^3$ que verifican $g(\alpha) = (12, 14)$.
- Hallar la imagen de g .
- 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.

2. (35 puntos)

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

3. (30 puntos)

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

- 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 .
- 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.