

Universidad de la República
Facultad de Ingeniería.

Examen de Matemática Discreta II
.... de diciembre de 2013

Número de Examen	Cédula	Nombre y Apellido

1. (aa puntos)

- a) Hallar todas las soluciones posibles con $a, b \in \mathbb{N}$ de
- $a + b = 1235$
 - $\text{mcm}(a, b) = 714 \text{ mcd}(a, b)$.
- b) ¿Qué restos puede dejar un cubo perfecto al dividir entre $(d - 10)$? (siendo $d = \text{mcd}(a, b)$ de la parte anterior).
- c) Mostrar que la ecuación $x^3 - 117y^3 = 5$ no tiene soluciones enteras.

2. (bb puntos)

- a) Sea $f : (G_1, *) \rightarrow (G_2, \star)$ un morfismo de grupos. Definir $\text{Ker}(f)$ y demostrar que $\text{Ker}(f)$ es un subgrupo normal de G_1 .
- b) Sea $R(x)$ el grupo de las funciones racionales con el producto.....
- c) Sea $f : (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$ un morfismo de grupos,
- i. Demostrar que $h : \mathbb{Z} \rightarrow R(x)$, tal que $h(n) = x^{f(n)}$ es un morfismo de grupos.
 - ii. Hallar el $\text{Ker}(h)$.
- d) Sabiendo que $h(-1) = \frac{1}{x^a}$ donde a es la menor raíz primitiva de $U(17)$, describir el morfismo f .

3. (cc puntos)

- a) Mostrar que 3 es raíz primitiva módulo 31.
- b) Calcular $\sum_{i=0}^{309} 3^i \pmod{31}$

4. (dd puntos)

- a) Describir el Criptosistema RSA.
- b) Definir la función dde descryptado y demostrar que descrypta.