Universidad de la República - Facultad de Ingeniería - IMERL: Matemática Discreta 2

Primer parcial - 27 de abril de 2017. Duración: 3 horas

N° de parcial	Cédula	Apellido y nombre	Horario muestra

Ejercicio 1. Encontrar todos los $a, b \in \mathbb{N}$ tales que $a + b = 407$ y $\text{mcm}(a, b) = 210\,\text{mcd}(a, b)$.

Ejercicio 2. Sean $a, b, c \in \mathbb{Z}$ con $(a, b) \neq (0, 0)$. Probar que la ecuación diofántica

$$ax + by = c$$

tiene solución si y solo si $\text{mcd}(a, b) \mid c$.

Ejercicio 3.

a. Hallar el menor x natural que verifica

$$\begin{cases} x & \equiv & 6 & (\text{mód } 13) \\ x & \equiv & 62 & (\text{mód } 103) \end{cases}$$

b. Si $(n, e) = (1339, 311)$ calcular $E(11)$, donde E es la función de cifrado del criptosistema RSA con clave pública (n, e).

c. Sabiendo que $1339 = 13 \cdot 103$ calcular la función de descifrado D del criptosistema RSA para la clave pública (n, e) de la parte anterior.

d. Sean $n = p \cdot q$, con p, q primos, y $0 < e < \varphi(n)$ con $\text{mcd}(e, \varphi(n)) = 1$. Dadas las funciones de cifrado E y descifrado D del criptosistema RSA para (n, e), probar que $D(E(x)) \equiv x$ (mód n) cuando $\text{mcd}(x, n) = 1$.

Ejercicio 4. Demostrar la siguiente versión del teorema chino del resto.
Sean m_1, m_2 enteros coprimos y a_1, $a_2 \in \mathbb{Z}$, entonces el sistema

$$\begin{cases} x & \equiv & a_1 & (\text{mód } m_1) \\ x & \equiv & a_2 & (\text{mód } m_2) \end{cases}, x \in \mathbb{Z},$$

tiene solución y es única módulo $m_1 m_2$.