

Primer parcial de Matemática Discreta II
8 de mayo del 2007

Número de Parcial	Cédula	Nombre y Apellido

Ejercicio 1. (7 puntos)

Hallar todos los $a, b \in \mathbb{Z}^+$ tales que:
$$\begin{cases} a \equiv 12 \pmod{b} \\ b \text{ es impar} \\ ab = 12636 \end{cases}$$

Ejercicio 2. (8 puntos)

- (a) Determinar todos los valores de n , entero positivo, para que $2^n - 1$ sea divisible por 7.
- (b) Sea a el menor entero positivo par tal que $2^a - 1 \equiv 0 \pmod{7}$.
- Resolver:
$$\begin{cases} 7x \equiv 3 \pmod{17} \\ ax \equiv 7 \pmod{11} \end{cases}$$

Ejercicio 3. (12 puntos)

- Sea p primo, $p \geq 7$. Se considera $n = p^4 - 1$.
- (El objetivo del ejercicio es probar que n es divisible por 240.)
- (a) Probar que $p \equiv 1 \pmod{3}$ o $p \equiv -1 \pmod{3}$.
Deducir que 3 divide a n .
- (b) Mostrar que $p^2 - 1$ puede escribirse de la forma $4k(k+1)$ con $k \in \mathbb{N}$.
Deducir que n es divisible por 16.
- (c) Demostrar que 5 divide a n .
- (d) 1. Sean $a, b, c \in \mathbb{Z}^+$. Probar que si $a \mid c$, $b \mid c$ y $\text{mcd}(a, b) = 1$ entonces $ab \mid c$.
2. Deducir que 240 divide a n .
- (e) Discutir si existen 9 números primos $p_1, p_2, \dots, p_9 \geq 7$ tales que $A = p_1^4 + p_2^4 + \dots + p_9^4$ sea primo.

Ejercicio 4. (13 puntos)

- (a) Describir el método para generar una clave pública (n, e) en el RSA.
- (b) Definir las funciones E y D (encriptado y desencriptado) y probar que son inversas.
- (c) Quebrar la clave pública $(n, e) = (320347, 635)$ (o sea factorizar n).