Universidad de la República
Facultad de Ingeniería
Instituto de Matemática y Estadística

Matemática Discreta 2
Curso 2021

2do Parcial - 1 de julio de 2021.

Ejercicio 1.

(a) Demostrar que si p es primo y $d|(p-1)$ entonces la ecuación $x^d \equiv 1 \pmod{p}$ tiene exactamente d soluciones distintas y todas pertenecen a $U(p)$.

(b) Demostrar que si r es raíz primitiva de n, entonces $r^a \equiv r^b \mod n \iff a \equiv b \mod \phi(n)$.

(c) Demostrar que 2 es una raíz primitiva módulo 11.

(d) Hallar la cantidad de soluciones de la ecuación $x^5 \equiv -1 \pmod{p}$. *Sugerencia:* hacer el cambio de variable $x = 2y$.

(e) Hallar las soluciones de la ecuación $x^5 \equiv -1 \pmod{p}$.

Ejercicio 2.

(a) Demostrar el Teorema de Lagrange para grupos, a saber, que si un grupo es finito entonces el orden de cualquier subgrupo es un divisor del orden del grupo.

(b) Sea G un grupo y $x, y \in G$ elementos de orden finito. Probar que si $xy = yx$ y $\text{mcd}(o(x), o(y)) = 1$, entonces $o(xy) = o(x)o(y)$.

(c) Mostrar con dos ejemplos que cada hipótesis de la parte anterior es necesaria.

(d) Deducir a partir del teorema de Lagrange probado en la parte (a) el siguiente teorema de Euler:

Si $a, n \in \mathbb{Z}$ son coprimos entonces

$$a^{\varphi(n)} \equiv 1 \qquad \text{(mód n)}\,.$$

Ejercicio 3.

(a) Hallar el menor x no negativo que verifica $x \equiv 91$ (mód 101) y $x \equiv 10$ (mód 13).

(b) Si E es la función de cifrado con el método RSA con clave (n, e), describir D la función de descifrado y demostrar que descifra.

(c) Si $(n, e) = (1313, 271)$ calcular $E(10)$.

Escala de puntos:

1) 22 puntos : *(a) 5 (b) 5 (c) 4 (d) 4 (e) 4*
2) 24 puntos : *(a) 6 (b) 6 (c) 6 (d) 6*
3) 14 puntos: *(a) 4 (b) 6 (c) 4*