Segundo Parcial - Matemática Discreta II

Jueves 10 de diciembre de 2020

Número de lista	APELLIDO, Nombre	Cédula de identidad

Cada ejercicio de desarrollo correcto vale 15 puntos.
El parcial se realiza sin materiales de consulta, ni calculadora.
La duración del parcial es de tres horas y media.

Ejercicio 1

(a) Enunciar el Teorema de Lagrange para grupos finitos.
(b) Enunciar y demostrar el Teorema de Euler relativo a congruencias en módulo n.
Puede hacerlo asumiendo el Teorema de Lagrange.

Ejercicio 2

(a) Hallar la cantidad de raíces primitivas de $U(19)$. Probar que 3 es raíz primitiva en el grupo $U(19)$. Fundamentar.
(b) Describir el método de intercambio de claves de Diffie-Helmann.
(c) Roberto Carlos, que tiene un millón de amigos, quiere acordar una clave compartida con su favorito, Carlos Roberto. Roberto Carlos elige $m = 7$ y Carlos Roberto $n = 11$. Si acuerdan el método de Diffie-Helmann en $U(19)$ considerando la raíz primitiva $g = 3$, determinar la clave común k.

Ejercicio 3

(a) Definir subgrupo.
(b) Sea G un grupo y H un subconjunto de G que satisface las dos condiciones siguientes:
(i) H es no vacío.
(ii) Si $h_1, h_2 \in H$ entonces $h_1 h_2^{-1} \in H$.
Probar que H es un subgrupo de G.

Ejercicio 4

Determinar si existen homomorfismos no triviales $f : G \to K$ para cada grupo G y K.
En caso afirmativo dar un ejemplo, justificando que es un homomorfismo.

(a) $G = \mathbb{Z}_p$ con p primo y $K = S_{p-1}$.
(b) $G = U(p)$ con $p > 2$ primo, y $K = S_{p-2}$.
(c) $G = U(12)$ y $K = \mathbb{Z}_4$.

Importante: justificar detalladamente los razonamientos, citando los teoremas utilizados.