

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

PRUEBA PRESENCIAL - 14 DE JULIO 2020

N° de prueba	Apellido y Nombre	Cédula	Modalidad

Instrucciones:

- Si eligieron la opción de prueba de 70 puntos, tienen que hacer los ejercicios 1, 2 y el 3 o el 4.
- Si eligieron la opción de prueba de 100 puntos, tienen que hacer los 4 ejercicios.

Ejercicio 1.

Enunciar y probar el Teorema de Lagrange para grupos finitos

Ejercicio 2.

Alicia y Beatriz quieren acordar una clave común utilizando el protocolo Diffie-Hellman. Para ello acuerdan públicamente el uso de $p = 103$ y $g = 99$ como raíz primitiva. Alicia elige en secreto un número n y le envía $g^n \equiv 11 \pmod{103}$ a Beatriz. Beatriz elige en secreto $m = 31$ y le envía $g^m \equiv 12 \pmod{103}$ a Alicia.

¿Cuál es la clave común k acordada?

Ejercicio 3.

Sea p entero tal que $p \geq 2$. Probar que p es primo si y solo si para todo $a \in \{1, 2, \dots, p-1\}$ existe $x \in \mathbb{Z}$ tal que $ax \equiv 1 \pmod{p}$.

Ejercicio 4.

Hallar el entero $0 \leq x < 81$ tal que $50x \equiv 1 \pmod{81}$.