Pontificia Universidad Católica de Chile
Departamento de Ciencia de la Computación
IIC2283 - Diseño y Análisis de Algoritmos

Ayudantía 10 - Teoría de números

18 de noviembre de 2021

Profesor Marcelo Arenas

Bernardo Barías

Pregunta 1 - Lema del capítulo

Sea n un número primo y

$$p(X) \;=\; \sum_{i=0}^{k} a_i x^i,$$

donde $k \geq 0$, $a_k \in \{1, ..., n\}$ y cada $a_j \in \{0, ..., n\}$. Demuestre que $p(X)$ tiene a lo más k raíces en módulo n (lema de la diapositiva 60/89 del siguiente link).

Pregunta 2 - Utilizando el lema

Usando la pregunta 1, demuestre que $(p-1)! \equiv -1 \mod p$.

Pregunta 3 - Bonus

Sea $(G, \cdot)$ un grupo. Se define el orden multiplicativo de un elemento $a \in G$ como el menor $k \in \mathbb{N}$ tal que $a^k = 1$. Lo denotamos por $O_G(a)$. Por ejemplo, si $G = \mathbb{Z}_3^*$, el orden multiplicativo de 1 es 1 y el del elemento 2 es 2 ($2^2 \equiv 4 \equiv 1 \mod 3$). Además, definimos el conjunto generado por un elemento $a \in G$ como

$$\langle a \rangle \;:=\; \{a^i \mid i \in \mathbb{Z}\},$$

donde a^{-i} es el inverso de a^i en G y a^0 es el elemento neutro de G.

a) Demuestre que $O_G(a) = |\langle a \rangle|$

b) Demuestre que para todo $a \in G$, se cumple que $O_G(a)$ divide a $|G|$

c) Demuestre el teorema de Euler: si a y n son primos relativos, entonces

$$a^{\varphi(n)} \equiv 1 \mod n,$$

donde $\varphi(n)$ es la función de Euler: la cantidad de números enteros menores o igual a n que son coprimos con este.

d) ¿Cómo se relacionan el teorema de Euler con el pequeño teorema de Fermat?