



## Ayudantía 12

Teoría de Números 2: Electric boogalooo

### Problema 1: Raíces de polinomios

Sea  $p(x)$  un polinomio:

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

Donde  $0 \leq a_i \leq n-1$  para todo  $i$ ,  $a_k \neq 0$  y  $k \geq 1$ . Decimos que  $b$  es una raíz de  $p(x)$  en módulo  $n$  si:

$$p(b) \equiv 0 \pmod{n}$$

Demuestre que  $p(x)$  tiene a lo más  $k$  raíces en módulo  $n$ .

### Problema 2: Grupos y Biyecciones

Dadas funciones  $f : A \rightarrow B$  y  $g : B \rightarrow C$  decimos que:

1.  $f$  es 1-1 si para cada  $a, b \in A$ ,  $a \neq b \rightarrow f(a) \neq f(b)$
2.  $f$  es sobre si para cada  $b \in B$ , existe  $a \in A$  tal que  $f(a) = b$
3.  $f$  es biyectiva si es 1-1 y sobre.
4. La composición de  $(g \circ f) : A \rightarrow C$  se define como  $(g \circ f)(x) = g(f(x))$

Sea  $n \geq 1$  un número natural y sea  $\mathcal{B}_n$  el conjunto de todas las biyecciones  $f : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ . Demuestre que  $(\mathcal{B}_n, \circ)$  es un grupo.

### Problema 3

Un grupo  $(G, \circ)$  se dice conmutativo si para todos  $x, y \in G$  se cumple que  $x \circ y = y \circ x$ . Como notación, definimos  $[a, b] = a^{-1} \circ b^{-1} \circ a \circ b$ .

1. Demuestre que  $a \circ b = b \circ a$  si y solo si  $[a, b] = 1$ .
2. Decimos que un grupo es generado por  $S \subseteq G$  si todo elemento  $g \in G$  se puede expresar como producto de elementos e inversos de elementos en  $S$ .  
Desarrolle y analice un algoritmo que dado un conjunto finito  $S = (g_1, \dots, g_n)$  y una operación binaria  $\circ$ , determine si el grupo generado  $S$  y  $\circ$  es conmutativo.
3. Definimos el centro de un grupo  $G$  como:

$$Z(G) = \{x \in G \mid \text{para todo } g \in G. [x, g] = 1\}$$

Además para cada  $g \in G$ , definimos el centralizador de  $g$  como:

$$C(g) = \{x \in G \mid [x, g] = 1\}$$

Demuestre que  $Z(G)$  es un subgrupo de  $G$  y que para todo  $g \in G$ ,  $C(g)$  es un subgrupo de  $G$ .

4. Dado un grupo  $G = (g_1, \dots, g_n)$ , definimos un subproducto aleatorio como:

$$r = g_1^{\varepsilon_1} \circ \dots \circ g_n^{\varepsilon_n} \in G$$

donde cada  $\varepsilon_i$  se elige de forma uniuiforme e independiente del conjunto  $\{0, 1\}$ .

Demuestre que si  $H$  es un subgrupo propio de  $G$ , entonces:

$$Pr[r \notin H] \geq \frac{1}{2}$$

5. Desarrolle y analice un algoritmo aleatorizado que dados generadores  $S = g_1, \dots, g_n$  y una operación binaria  $\circ$  determine si el grupo generado por  $S$  y  $\circ$  es conmutativo.