Pontificia Universidad Católica de Chile
Departamento de Ciencia de la Computación
IIC2283 - Diseño y Análisis de Algoritmos
Profesor: Nicolás Van Sint Jan
Ayudante: Dante Pinto

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:

$$p(b) \equiv 0 \mod n$$

Demuestre que $p(x)$ tiene a lo más k raíces en módulo n.
Solución: Esta demostración se encuentra en la clase 22.

Problema 2: Grupos y Biyecciones

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

1. f es $1-1$ si para cada $a, b \in A$, $a \neq b \to f(a) \neq f(b)$
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 $(g \circ f) : A \to C$ 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 $f : \{1, ..., n\} \to \{1, ..., n\}$. Demuestre que $(\mathcal{B}_n, \circ)$ es un grupo.

Solución: Para demostrar que $(\mathcal{B}_n, \circ)$ es un grupo debemos demostrar que cumple las siguientes condiciones:

- Asociatividad:

$$\begin{aligned}(g \circ f) \circ h &= g(f(x)) \circ h \\ &= g(f(h(x))) \\ &= g \circ f(h(x)) \\ &= g \circ (f \circ h)\end{aligned}$$

- Neutro: Es claro que el elemento neutro será $f(x) = x$, pues:

$$g \circ f = g(f(x)) = g(x)$$

$$f \circ g = f(g(x)) = g(x)$$

- Inverso: Sabemos que la función inversa de una función biyectiva siempre será biyectiva, pero esto se puede demostrar fácilmente pensando en que las biyecciones sobre estos conjuntos se comportarán como permutaciones o demostrando la inyectivividad y sobreyectividad de la función inversa de f.
- Cerrado: Nuevamente sabemos por matemáticas discretas que la composición de dos biyecciones será una biyección, pero podemos demostrar esto fácilmente definiendo $f(g(x))$ y usando que f y g son biyecciones para demostrar las dos propiedades que nos interesan.

Problema 3: Grupos conmutativos

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 $S = (g_1, ..., g_n)$ 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 $G = \langle g_1, ..., g_n \rangle$, definimos un subproducto aleatorio como:

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

   donde cada ε_i se elige de forma uniforme 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 $S = g_1, ..., g_n$ y una operación binaria $\circ$ determine si el grupo generado por S y $\circ$ es conmutativo.

Solución: La solución a esta pregunta se encuentra en el siguiente video.