PONTIFICIA UNIVERSIDAD CATOLICA DE CHILE
ESCUELA DE INGENIERIA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACION

Diseño y Análisis de Algoritmos - IIC2283
Interrogación 2

1. En esta pregunta usted va a analizar un algoritmo para transformar una moneda cargada en una moneda no cargada. De manera más precisa, sea **Moneda**( ) un procedimiento que retorna 0 con probabilidad p y 1 con probabilidad $1-p$, donde $0 < p < 1$, y defina **Lanzar**( ) como el siguiente algoritmo:

   Lanzar( )
   a_1 := **Moneda**( )
   a_2 := **Moneda**( )
   if $a_1 \neq a_2$ **then return** a_1
   else return sin_resultado

   (a) [0.7 puntos] Calcule Pr(**Lanzar**( ) retorne sin_resultado).

   (b) [0.7 puntos] Demuestre que Pr(**Lanzar**( ) retorne 0) = Pr(**Lanzar**( ) retorne 1), vale decir, **Lanzar**( ) se puede considerar como una moneda no cargada.

   (c) [0.6 puntos] Considere la siguiente versión modificada del algoritmo **Lanzar**( ):

   RepLanzar( )
   a_1 := **Moneda**( )
   a_2 := **Moneda**( )
   while $a_1 = a_2$
   a_1 := **Moneda**( )
   a_2 := **Moneda**( )
   return a_1

   Indique cuál es el número esperado de veces que se debe llamar al procedimiento **Moneda**( ) hasta que **RepLanzar**( ) entregue un resultado. Nótese que este número esperado es una función de p, y recuerde que p es la probabilidad de que **Moneda**( ) retorne 0.

2. [1.6 puntos] Dada una función $f : A \to B$, recuerde que: (i) f es 1-1 si para cada $a, b \in A$ tal que $a \neq b$, se tiene que $f(a) \neq f(b)$; (ii) f es sobre si para cada $b \in B$, existe $a \in A$ tal que $f(a) = b$; (iii) f es biyectiva si f es 1-1 y sobre. Además, dada una función $g : B \to C$, recuerde que la composición $(g \circ f) : A \to C$ es una función definida 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 $f : \{1, \ldots, n\} \to \{1, \ldots, n\}$. Demuestre que $(\mathcal{B}_n, \circ)$ es un grupo, donde $\circ$ es la composición de funciones.

3. Sea p un número primo.

   (a) [1.2 puntos] Demuestre que un polinomio $r(x)$ de grado k tiene a lo más k raíces en módulo p, vale decir, existen a lo más k elementos $a \in \{0, \ldots, p-1\}$ tales que $r(a) \equiv 0 \bmod p$.

   (b) [1.2 puntos] Suponiendo que p es impar, sean

$$\begin{aligned} S_p^+ &= \{a \in \mathbb{Z}_p^* \mid a^{\frac{p-1}{2}} \equiv 1 \bmod p\}, \\ S_p^- &= \{a \in \mathbb{Z}_p^* \mid a^{\frac{p-1}{2}} \equiv -1 \bmod p\}. \end{aligned}$$

   Demuestre que $|S_p^+| = |S_p^-| = \frac{p-1}{2}$.