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

Diseño y Análisis de Algoritmos - IIC2283
Interrogación 3
Tiempo: 2.5 horas

0. Dé una estimación e de la nota de su prueba. Si la nota real r de su prueba satisface que $|e - r| \leq 0.5$, entonces usted recibirá 0.2 puntos en su nota final. Por favor dé esta estimación en la misma hoja de respuesta que la pregunta 1.

1. [1.5 puntos] Demuestre el Teorema de Lagrange. Vale decir, demuestre que si $(G, \circ)$ es un grupo finito y $(H, \circ)$ es un subgrupo de $(G, \circ)$, entonces $|H|$ divide a $|G|$.

2. [1.5 puntos] Dado $n \in \mathbb{N}$ tal que $n \geq 2$, recuerde que **EsPotencia**(n) es un procedimiento que verifica si $n = m^k$ para $m, k \in \mathbb{N}$ tal que $k \geq 2$. Además, dados $a, b \in \mathbb{N}$ tales que $a, b \geq 1$, recuerde que **MCD**(a, n) calcula el máximo común divisor entre a y n, mientras que **EXP**(a, b, n) calcula $a^b \bmod n$. Dados estos procedimientos, considere el siguiente algoritmo que recibe como entrada números $n, k \in \mathbb{N}$ tales que $n = 4 \cdot \ell + 3$ y $k \geq 1$:

```
TestPrimalidad(n, k)
    if EsPotencia(n) then return COMPUESTO
    else
        sea a_1, ..., a_k una secuencia de números elegidos de
                                manera uniforme e independiente desde {1, ..., n-1}
        for i := 1 to k do
            if MCD(a_i, n) > 1 then return COMPUESTO
            else b_i := EXP(a_i, (n-1)/2, n)
        for i := 1 to k do
            if b_i ≢ 1 mod n and b_i ≢ -1 mod n then return COMPUESTO
        return PRIMO
```

Demuestre que **TestPrimalidad**(n, k) verifica si n es un número primo con una probabilidad de error menor o igual a $(\frac{1}{2})^k$.

3. Responda las siguientes preguntas.

   (a) [0.7 puntos] Demuestre que todo número natural que es un palíndromo y tiene largo par es divisible por 11.

(b) [0.8 puntos] Tres número primos p, q, r son llamados trillizos si $q = p + 2$ y $r = p + 4$. Por ejemplo, los números 3, 5, 7 son primos trillizos. Demuestre que el único trio de números trillizos es el 3, 5, 7.

4. [1.5 puntos] Dados $a, b \in \mathbb{N}$ con $b \geq 1$, recuerde que **EXP**(a, b) calcula a^b.

   Sea **EsPotenciaRango**(ℓ, n) un procedimiento que, dados $\ell, n \in \mathbb{N}$ tales que $\ell, n \geq 2$, verifica si existen $a, b \in \{2, \ldots, n\}$ tales que $\ell = a^b$. En esta pregunta usted debe desarrollar un algoritmo que implemente **EsPotenciaRango**(ℓ, n) y realice a lo más $c \cdot n$ llamadas a la función **EXP**, donde c es una constante fija. Debe además justificar por qué su algoritmo realiza este número de llamadas.

   Importante: El algoritmo que va a desarrollar en esta pregunta sólo puede utilizar las operaciones de comparación $=$, $>$ y $<$, y las funciones $+$ y $-$.