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

1. [1.5 puntos] En esta pregunta usted debe demostrar el Lema de Schwartz-Zippel.

   Sea $p(x_1, \ldots, x_n)$ un polinomio en $\mathbb{Q}$ no nulo y de grado k, y sea A un subconjunto finito y no vacío de $\mathbb{Q}$. Demuestre que si $a_1, \ldots, a_n$ son elegidos de manera uniforme e independiente desde A, entonces

   $$\Pr(p(a_1, \ldots, a_n) = 0) \quad \leq \quad \frac{k}{|A|}.$$

2. [1.5 puntos] Dados dos polinomios $p(x_1, \ldots, x_n)$ y $q(x_1, \ldots, x_n)$ en $\mathbb{Q}$, recuerde que decimos que $p(x_1, \ldots, x_n)$ y $q(x_1, \ldots, x_n)$ son equivalentes si para toda secuencia $a_1, \ldots, a_n$ de números en $\mathbb{Q}$, se tiene que $p(a_1, \ldots, a_n) = q(a_1, \ldots, a_n)$.

   Dados dos polinomios $p(x_1, \ldots, x_n)$ y $q(x_1, \ldots, x_n)$ en $\mathbb{Q}$, decimos que $p(x_1, \ldots, x_n)$ y $q(x_1, \ldots, x_n)$ son linealmente-equivalentes si existe un polinomio $r(x_1, \ldots, x_n)$ tal que: (i) $r(x_1, \ldots, x_n)$ es nulo o es un polinomio de grado menor o igual a 1, y (ii) $p(x_1, \ldots, x_n)$ es equivalente a $q(x_1, \ldots, x_n) + r(x_1, \ldots, x_n)$. Por ejemplo, los polinomios $p(x, y) = x \cdot (x - 1) + 2 \cdot y$ y $q(x, y) = (x - 1) \cdot (x - 2) + y + 1$ son linealmente-equivalentes puesto que

   $$p(x, y) \quad = \quad q(x, y) + r(x, y),$$

   donde $r(x, y) = 2 \cdot x + y - 3$.

   De un algoritmo aleatorizado que resuelva el problema de determinar si dos polinomios $p(x_1, \ldots, x_n)$ y $q(x_1, \ldots, x_n)$ son linealmente-equivalentes. Su algoritmo debe funcionar en tiempo polinomial en el peor caso y su probabilidad de error debe ser menor o igual a $\frac{1}{2^{100}}$. Además, usted debe justificar claramente por qué su algoritmo es correcto, funciona en tiempo polinomial y tiene probabilidad de error acotada por $\frac{1}{2^{100}}$.

3. Fije un número natural $n \geq 2$. Recuerde que la función ϕ de Euler es definida como $\phi(n) = |\mathbb{Z}_n^*|$.

   Dado $a \in \mathbb{Z}_n^*$, el orden de a en $\mathbb{Z}_n^*$ se define como el menor número natural $k \geq 1$ tal que $a^k \equiv 1 \bmod n$. Por ejemplo, el orden de 1 en $\mathbb{Z}_8^*$ es 1 puesto que $1^1 \equiv 1 \bmod 8$, el orden de 3 en $\mathbb{Z}_8^*$ es 2 puesto que $3 \not\equiv 1 \bmod 8$ y $3^2 \equiv 1 \bmod 8$, y el orden de 3 en $\mathbb{Z}_{11}^*$ es 5.

   Sea $a \in \mathbb{Z}_n^*$. Demuestre lo siguiente:

   (a) [0.4 puntos] Existe un número $k \geq 1$ tal $a^k \equiv 1 \bmod n$, por lo que a tiene orden en $\mathbb{Z}_n^*$.

   (b) [0.8 puntos] Si k es el orden de a en $\mathbb{Z}_n^*$, entonces se tiene que k divide a $\phi(n)$.

   (c) [0.3 puntos] $a^{\phi(n)} \equiv 1 \bmod n$.

4. [1.5 puntos] Construya un algoritmo aleatorizado que reciba como entrada un número natural $n \geq 2$, y determine si n es la potencia de un número primo, vale decir, si $n = p^k$ donde p es un número primo y k es un número natural mayor o igual a 1. Su algoritmo debe funcionar en tiempo polinomial en el peor caso y su probabilidad de error debe ser menor o igual a $\frac{1}{2^{100}}$. Además, usted debe justificar claramente por qué su algoritmo es correcto, funciona en tiempo polinomial y tiene probabilidad de error acotada por $\frac{1}{2^{100}}$.

   Importante: Para resolver este problema puede utilizar los resultados demostrados en clases sobre los números primos y compuestos. Además, puede utilizar los procedimientos **MCD**(a, b) y **Exp**(a, b, n) vistos en clases. Si necesita de otros procedimientos debe implementarlos; en particular, **no** puede suponer como dado al procedimiento **TestPrimalidad**(n, k).