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

**Diseño y Análisis de Algoritmos - IIC2283**
**Tarea 2**
**Entrega: Viernes 17 de noviembre**

Dados números naturales $a$, $b$, $n$ con $n > 0$, decimos que $b$ es una raíz cuadrada de $a$ en modulo $n$ si $b^2 \equiv a \mod n$. Por ejemplo, 2 y 9 son raíces cuadradas de 4 en modulo 11 puesto que $2^2 \equiv 4 \mod 11$ y $9^2 \equiv 4 \mod 11$. Dado un número primo impar $p$ y un número $a \in \{1, \ldots, p-1\}$, en clases demostramos que $a$ tiene raíz cuadrada en módulo $p$ si y sólo si

$$a^{\frac{p-1}{2}} \equiv 1 \mod p$$

Por ejemplo, tenemos que $4^5 = 1024$ y $1024 \equiv 1 \mod 11$, por lo que 4 tiene raíz cuadrada en módulo 11. Por el contrario, $2^5 = 32$ y $32 \equiv -1 \mod 11$, por lo que 2 no tiene raíz cuadrada en módulo 11.

En esta tarea usted va a desarrollar e implementar un algoritmo para calcular raíces cuadradas en módulo un número primo impar $p$. La idea del algoritmo esta basado en los siguientes pasos, los cuales usted tiene que generalizar y demostrar que son correctos.

Sea $a \in \{1, \ldots, p-1\}$ tal que $a^{\frac{p-1}{2}} \equiv 1 \mod p$, lo cual nos asegura que $a$ tiene raíz cuadrada en módulo $p$. Dado que $p$ es impar, tenemos que $p - 1 = 2^t \cdot s$, donde $t \geq 1$ y $s$ es un número impar. Además, dado que $a$ tiene raíz cuadrada en módulo $p$ concluimos que:

$$a^{2^{t-1} \cdot s} \equiv 1 \mod p$$

Si $t = 1$, entonces tenemos que:

$$a^s \equiv 1 \mod p$$

En este caso tenemos los ingredientes necesarios para calcular una raíz cuadrada de $a$:

$$\begin{aligned} a^s \equiv 1 \mod p \quad &\Rightarrow \quad a^{s+1} \equiv a \mod p \\ &\Rightarrow \quad (a^{\frac{s+1}{2}})^2 \equiv a \mod p \end{aligned}$$

Tenemos que $a^{\frac{s+1}{2}}$ es una raíz cuadrada de $a$ en módulo $p$, la cual está bien definida puesto que $\frac{s+1}{2}$ es un número natural ya que $s$ es impar.

Nos queda considerar el caso en que $t > 1$. Suponemos en este caso que tenemos un número natural $\gamma$ tal que:

$$\gamma^{\frac{p-1}{2}} \equiv -1 \mod p$$

Vale decir, $\gamma$ no tiene raíz cuadrada en módulo $p$. En este caso es posible demostrar que existe $k_1 \in \{0, 1\}$ tal que:

$$(a^s)^{2^{t-2}} \cdot (\gamma^s)^{2^{t-1} \cdot k_1} \equiv 1 \mod p$$

Si $t = 2$, nuevamente tenemos una forma de calcular una raíz cuadrada de $a$:

$$\begin{aligned}
(a^s)^{2^{t-2}} \cdot (\gamma^s)^{2^{t-1} \cdot k_1} \equiv 1 \bmod p \quad &\Rightarrow \quad (a^s) \cdot (\gamma^s)^{2 \cdot k_1} \equiv 1 \bmod p \\
&\Rightarrow \quad (a^{s+1}) \cdot (\gamma^s)^{2 \cdot k_1} \equiv a \bmod p \\
&\Rightarrow \quad (a^{\frac{s+1}{2}})^2 \cdot (\gamma^s)^{2 \cdot k_1} \equiv a \bmod p \\
&\Rightarrow \quad (a^{\frac{s+1}{2}})^2 \cdot (\gamma^{s \cdot k_1})^2 \equiv a \bmod p \\
&\Rightarrow \quad (a^{\frac{s+1}{2}} \cdot \gamma^{s \cdot k_1})^2 \equiv a \bmod p
\end{aligned}$$

Así, $a^{\frac{s+1}{2}} \cdot \gamma^{s \cdot k_1}$ es una raíz cuadrada de $a$ en módulo $p$ que está bien definida porque $s$ es un número impar.

Pero nuevamente nos puede pasar que no se cumpla la condición y que $t > 2$. En este caso es posible demostrar que existe $k_2 \in \{0, 1\}$ tal que:

$$(a^s)^{2^{t-3}} \cdot (\gamma^s)^{2^{t-2} \cdot k_1} \cdot (\gamma^s)^{2^{t-1} \cdot k_2} \equiv 1 \bmod p$$

Nótese que aquí estamos considerando el mismo valor $\gamma$ utilizado en la iteración anterior. Si $t = 3$, nuevamente tenemos una forma de calcular una raíz cuadrada de $a$:

$$\begin{aligned}
(a^s)^{2^{t-3}} \cdot (\gamma^s)^{2^{t-2} \cdot k_1} \cdot (\gamma^s)^{2^{t-1} \cdot k_2} \equiv 1 \bmod p \quad &\Rightarrow \quad (a^s) \cdot (\gamma^s)^{2 \cdot k_1} \cdot (\gamma^s)^{4 \cdot k_2} \equiv 1 \bmod p \\
&\Rightarrow \quad (a^{s+1}) \cdot (\gamma^s)^{2 \cdot k_1} \cdot (\gamma^s)^{4 \cdot k_2} \equiv a \bmod p \\
&\Rightarrow \quad (a^{\frac{s+1}{2}})^2 \cdot (\gamma^s)^{2 \cdot k_1} \cdot (\gamma^s)^{4 \cdot k_2} \equiv a \bmod p \\
&\Rightarrow \quad (a^{\frac{s+1}{2}})^2 \cdot (\gamma^{s \cdot k_1})^2 \cdot (\gamma^s)^{4 \cdot k_2} \equiv a \bmod p \\
&\Rightarrow \quad (a^{\frac{s+1}{2}})^2 \cdot (\gamma^{s \cdot k_1})^2 \cdot (\gamma^{2 \cdot s \cdot k_2})^2 \equiv a \bmod p \\
&\Rightarrow \quad (a^{\frac{s+1}{2}} \cdot \gamma^{s \cdot k_1} \cdot \gamma^{2 \cdot s \cdot k_2})^2 \equiv a \bmod p
\end{aligned}$$

Nuevamente, $a^{\frac{s+1}{2}} \cdot \gamma^{s \cdot k_1} \cdot \gamma^{2 \cdot s \cdot k_2}$ es una raíz cuadrada de $a$ en módulo $p$ que está bien definida porque $s$ es un número impar. Finalmente, si la condición no se cumple y tenemos que $t > 3$, el proceso puede continuar de la misma forma hasta que el primer término de la multiplicación sea $a^s$.

En esta tarea usted debe responder las siguientes preguntas.

(1) [2 puntos] Formalice la idea mostrada anteriormente como un algoritmo aleatorizado de Las Vegas. En particular, utilizando la notación desarrollada en clases de un pseudocódigo para una función **RaízCuadrada**($p$, $a$, $k$), la cual recibe cómo parámetros un número primo impar $p$, un número natural $a \in \{1, \ldots, p-1\}$ y un número natural $k \geq 1$, y retorna uno de los siguientes valores: si $a$ no tiene raíz cuadrada de módulo $p$ entrega *sin_raíz_cuadrada*, y si $a$ tiene raíz cuadrada en módulo $p$, entonces con probabilidad $(1 - \frac{1}{2^k})$ entrega un número $b \in \{1, \ldots, p-1\}$ tal que $b^2 \equiv a \bmod p$, y con probabilidad $\frac{1}{2^k}$ entrega *sin_resultado*.

(2) [1 puntos] Formalice y demuestre las propiedades necesarias para establecer que el algoritmo dado en (1) es correcto, vale decir, las propiedades que muestran que si el algoritmo entrega un valor distinto de *sin_resultado*, entonces este valor es correcto.

(3) [1 puntos] Analice la complejidad del algoritmo considerando como operaciones básicas a contar la suma, resta, multiplicación, división y cálculo del resto para números enteros. Además, demuestre que la probabilidad de que el algoritmo entregue *sin_resultado* es $\frac{1}{2^k}$.

(4) [2 puntos] Implemente el procedimiento **RaízCuadrada**. Para mostrar que su programa funciona correctamente se deberá proveer de una interfaz que de dos opciones al usuario:

   (a) Leer desde pantalla un número primo impar $p$, un número natural $a \in \{1, \ldots, p-1\}$ y un número natural $k \geq 1$, y retornar en pantalla el valor de la llamada **RaízCuadrada**($p$, $a$, $k$).

   (b) Salir de la ejecución del programa.

   En la implementación de la interfaz puede suponer que las entradas vienen en el formato correcto.