Question 1

Donnez toutes les étapes de l'algorithme de Miller-Rabin pour tester si 97 est premier. Vous devez supposer que le générateur pseudo aléatoire retourne le nombre 5.

Ce que nous savons du problème:

$$n = 97$$
$$n - 1 = 96 = 2^5 * 3$$
$$b = 5$$

On peut alors exécuter l'algorithme de Miller-Robin pour déterminer si 97 est possiblement un nombre premier:

$$b^t = 5^3 = 125 \equiv 28 (mod\, 97)$$
$$b^{2t} = 28^2 = 784 \equiv 8 (mod\, 97)$$
$$b^{2^2 t} = 8^2 = 64 \equiv 64 (mod\, 97)$$
$$b^{2^3 t} = 64^2 = 4096 \equiv 22 (mod\, 97)$$
$$b^{2^4 t} = 22^2 = 484 \equiv 96 (mod\, 97) \equiv -1 (mod\, 97)$$

Puisque nous avons une valeur de -1 à la dernière itération montrée, nous pouvons donc dire que 97 est probablement premier sur une base 5.