Question 2

On peut montrer que si n est un nombre premier, alors pour tout entier positif b on a :

$$b^{(n-1)/2} mod\, n = J(b,n) \tag{1}$$

où $J(b,n)$ est une fonction appelée symbole de Jacobi (Il n'est pas nécessaire de connaître la définition exacte de $J(b,n)$ pour répondre à cette question).

D'autre part, si n est composé, alors la relation (1) est fausse pour au moins 50% de tous les entiers b pour lesquels $PGCD(b,n) = 1$.

a) En utilisant ces deux observations, trouvez un algorithme de Monte Carlo 50%-correct qui détermine si un entier positif n est premier. Vous pouvez supposer qu'il est possible de tester efficacement si la relation (1) est vraie.

b) Votre algorithme est-il biaisé? Si oui, est-il vrai-biaisé ou faux biaisé? Expliquez.

c) Montrez comment vous pouvez modifier votre algorithme pour en obtenir un qui soit 99.999%-correct.