8INF433 Algorithmique

Devoir 4

(À remettre au plus tard: mardi le 24 avril 2018 avant 11h00.
Aucun retard ne sera accepté)

Justifiez toutes vos réponses

Vous serez évalué pour la rectitude et la qualité de vos réponses.

Vous pouvez travailler en équipe de deux ou trois étudiants (remettre une seule copie par équipe).

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 3.

2. On peut montrer que si n est un nombre premier, alors pour tout entier positif b on a
$$b^{(n-1)/2} \bmod n = J(b, n), \tag{1}$$
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 $\text{PGCD}(b, n) = 1$.

   (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.

3. Considérez deux algorithmes de Monte-Carlo A et B pour résoudre un même problème P. A est p-correct et vrai-biaisé tandis que B est q-correct et faux-biaisé. Le temps d'exécution de A est $T_A(n)$ et celui de B est $T_B(n)$.

   (a) Utilisez ces deux algoritmes pour construire un algorithme de Las Vegas pour résoudre le problème

   (b) Analysez le temps d'exécution de votre algorithme

   (c) Analyse la rectitude de votre algorithme. Pour quelle valeur maximale de r peut-t-on dire que votre algorihme est r-correct?

4. Trouvez les clefs publique et privée RSA avec les nombres premiers $p = 43$ et $q = 37$. Après avoir trouvé une valeur adéquate pour e, montrez toutes les étapes de l'algorithme d'Euclide étendu permettant de trouver d (j'utilise ici les même noms de variables qu'en classe). Donnez toutes les étapes de vos calculs. Vous devez me donner la séquence de tous les appels résursifs, les paramètres utilisés et les valeurs de retour.