Recherche Opérationnelle 2

Exercices préparatoires à l'examen de juin 2014 (méthodes stochastiques et algorithmes randomisés)

Exercice 1 Il y a trois polynômes $P(x)$, $Q(x)$, $R(x)$, $\deg P = 80$, $\deg Q = 120$, $\deg R = 200$. On cherche à tester si $P \cdot Q = R$. Pour cela, on calcule les valeurs de $P \cdot Q$ et de R pour des valeurs de x tirées au hasard dans l'ensemble des entiers de 0 à 1000. On répète l'opération 10 fois, et chaque fois les valeurs sont égales. Quelle est la probabilité que les polynômes ne soient *pas* égaux ? Combien de fois faut-il répéter l'opération pour garantir que la probabilité d'une réponse erronée soit inférieure à 2^{-100} ?

Exercice 2 Soit l'ensemble de nombres $\{14, 2, 30, 61, 1, 7, 4\}$. Déterminer la médiane et la moyenne de cet ensemble.

Exercice 3 Appliquer le test de Fermat à $n = 33$, $x = 5$.

Exercice 4 Déterminer le PGCD d des nombres 12546 et 984, ainsi que deux entiers x et y tels que $12546x + 984y = d$. On détaillera les étapes du calcul.

Exercice 5 Déterminer l'inverse de 17 modulo 42. On détaillera les étapes du calcul.

Exercice 6 Une clé publique RSA a la valeur $(115, 27)$.

1. Quel est le résultat du codage de l'entier 2 ?
2. Déterminer la clé privée correspondant à la clé publique.

Exercice 7 On rappelle la méthode ρ de Pollard pour déterminer un facteur d'un entier n : la fonction $f : [0, n-1] \to [0, n-1]$ étant définie par $f(x) = x^2 + 1 \mod n$,

- on tire un entier x_0 dans $[0, n-1]$ et on pose $y_0 = x_0$;
- on calcule les termes successifs des suites x_i et y_i définies, pour $i \geq 1$, par les relations de récurrence $x_i = f(x_{i-1})$, $y_i = f(f(y_{i-1}))$;
- on s'arrête quand le PGCD d_i de $|x_i - y_i|$ et n est différent de 1 : si $d_i = 0$ l'algorithme échoue ; sinon, d_i est le facteur cherché.

Appliquer cet algorithme au cas $n = 77$ en choisissant pour x_0 la valeur 0. Appliquer l'algorithme au cas $n = 1001$ en prenant la valeur de x_0 à votre choix. On précisera à chaque fois le facteur retourné et le nombre d'itérations.

Exercice 8 Soit $\pi(N)$ dénote la quantité des nombres premiers $p \leq N$. Le *théorème des nombres premiers* affirme qu'une bonne approximation à cette fonction est donnée par la formule $N/\ln(N)$ où la notation "ln" signifie le logarithme sur la base e.

1. On choisit un entier entre 1 et 10^{13} au hasard. Quelle est la probabilité de tomber sur un nombre premier ?
2. On choisit des entiers uniquement parmis ceux qui sont égaux à 1 ou à 5 modulo 6 (expliquer pourquoi). Quelle est alors la probabilité de tomber sur un nombre premier ?

Exercice 9 Un entier s'appelle *palindrome* si la suite de ses chiffres décimaux est la même quand on la lit de droite à gauche ou de gauche à droite. Par exemple, 17255271 est un palindrome. Montrer que tout palindrome de longueur paire est divisible par 11.

Exercice 10 Soient trois ensembles disjoints X, Y, Z de tailles $|X| = m$, $|Y| = n$, $|Z| = k$. On considère l'union $V = X \cup Y \cup Z$ comme l'ensemble de sommets de graphes pour lesquels il est interdit de tracer des arêtes entre deux points d'un même ensemble. (Seules donc les arêtes entre X et Y, entre X et Z, et entre Y et Z, sont autorisées.) Quel est le nombre des graphes vérifiant cette propriété pour des valeurs données de paramètres m, n, k ?