Université Larbi Ben Mhidi

Département MI

Niveau : 1ère année Master AD

Module : Méthodes algorithmiques

Année : 2024-2025

Série de TD 4 : Les méthodes probabiliste

Exercice 01 :

Sachant que le théorème de **Fermat** est donne par

Si p est un nombre premier et a un entier qui n'est pas divisible par p (c'est-à-dire $\gcd(a, p) = 1$), alors :

$$a^{p-1} \equiv 1 \pmod{p}$$

Autrement dit, $a^{p-1} - 1$ est divisible par p.

Exemple :

Si $p = 7$ et $a = 3$, alors :

$$3^{7-1} = 3^6 = 729$$

$$729 \mod 7 = 1$$

1. Quelle approche probabiliste convient pour ce théorème : Monte Carlo ou Las Vegas ? Justifiez votre choix.
2. Écrivez l'algorithme correspondant pour tester la primalité d'un nombre en utilisant le Petit théorème de Fermat

Exercice 02 :

On vous donne un tableau A[1…n] contenant des entiers, mais vous ne savez pas s'ils sont triés ou non. Vous voulez vérifier si x est présent dans A, mais pour réduire le coût, vous ne voulez pas parcourir tous les éléments.

1. Proposez **une méthode probabiliste** qui sélectionne un sous-ensemble d'indices de A et vérifie si X est présent.

Exercice 03 :

Utiliser l'algorithme de **Monte Carlo** pour estimer l'aire d'un cercle inscrit dans un carré. Sachant que :

1. Considérez un cercle de rayon R inscrit dans un carré de côté 2R.
2. Générer N points aléatoires dans le carré et déterminer combien de ces points tombent à l'intérieur du cercle.
3. L'aire du cercle est estimée en utilisant la proportion des points dans le cercle, selon la formule suivante :

$$\text{Aire estimée du cercle} = \left(\frac{\text{nombre de points dans le cercle}}{\text{nombre total de points}} \right) \times 4R^2$$

TD Les méthodes probabiliste