TD8

Exercice 1. *Nombres premiers*

Soit n et N deux entiers, $n < N$. On tire un nombre premier p aléatoire, inférieur ou égal à n.

1. Quelle est est la probabilité que p divise N ?
2. Comment prendre n pour que cette probabilité soit au plus $1/2$.

Exercice 2. *Algorithme de Rabin-Karp*

Dans l'algorithme de Rabin-Karp, un nombre premier p est tiré aléatoirement. Or on ne sait faire cette opération que de manière probabiliste : il existe une probabilité ϵ que l'entier renvoyé soit composé.

1. Soit $n < N$ deux entiers, et p un nombre tiré aléatoirement inférieur ou égal à n, qui est premier avec probabilité $1 - \epsilon$ et composé avec probabilité ϵ. Borner la probabilité que p divise N, en fonction de n, N et ϵ. *On ne cherchera pas à estimer la probabilité qu'un nombre composé divise N.*
2. En prenant en compte la probabilité que l'entier choisi ne soit pas premier, borner l'espérance du nombre de faux positifs dans l'algorithme de Rabin-Karp, dans le cas où le motif n'apparaît pas. *Rappel. L'algorithme cherche un motif de taille m dans un texte de taille N, et tire pour cela un nombre premier aléatoire $\leq m^2 \ln m$.*
3. En déduire l'espérance du temps de calcul de l'algorithme, en tenant compte de la probabilité que l'entier choisi ne soit pas premier.

L'algorithme de primalité de Miller-Rabin a une probabilité de succès $\geq 1/2$. *On admet*[1] *que si on tire aléatoirement un nombre aléatoire $\leq N$ et qu'on teste sa primalité avec t applications de l'algorithme de Miller-Rabin, la probabilité que l'entier soit composé est $\leq \ln N / 2^t$. Autrement dit, avec t applications de l'algorithme de Miller-Rabin, on obtient $\epsilon = \ln(N)/2^t$ dans les questions précédentes.*

4. Quelle valeur de t faut-il choisir pour que l'algorithme de Rabin-Karp fonctionne en temps $O(m+N)$?

Exercice 3. *Plusieurs motifs*

On souhaite trouver l'emplacement d'un ensemble $\mathscr{M}$ de k motifs dans un texte.

1. Donner un algorithme évident pour ce problème, et sa complexité.
2. On suppose que $\mathscr{M}$ ne contient que des motifs de même taille. Décrire un algorithme de complexité $O(n+km)$.
3. Résoudre le cas général.

1. Voir les notes de cours pour la démonstration.