

Le crible d'Ératosthène

Soit $N \in \mathbb{N}$. On se donne une liste $s = [s_0, s_1, \dots, s_N]$ de longueur $N + 1$. Tous les éléments de s sont égaux à 1, sauf s_0 et s_1 . On initialise un entier p à 2. Tant que $p \leq \sqrt{N}$:

1. Pour tout $k \in \llbracket 2, \lfloor N/p \rfloor \rrbracket$, kp est composé. On met s_{kp} à 0. Le nombre d'opérations nécessaires pour effectuer cette opération est $O(N/p)$.
2. On incrémente p jusqu'au premier indice de s égal à 1 (s'il existe).

L'incrément de p de la ligne 2 nécessite un nombre cumulé d'opérations de l'ordre de $O(N)$.

Le nombre cumulé d'opérations effectuées à la ligne 1 est de l'ordre de

$$C_N = \sum_{p \leq \sqrt{N}} \frac{N}{p} = N \sum_{p \leq \sqrt{N}} \frac{1}{p}$$

où la somme ci-dessus est effectuée pour p premier. Un résultat non trivial nous dit que lorsque n tend vers l'infini,

$$\sum_{p \leq n} \frac{1}{p} \sim \ln \ln n$$

Ainsi,

$$C_N \sim N \ln \ln \sqrt{N} = N \ln \frac{1}{2} + N \ln \ln N \sim N \ln \ln N$$

On voit donc que le nombre d'opérations nécessaires à l'exécution de la ligne 2 est négligeable devant le nombre d'opérations nécessaires à l'exécution de la ligne 1. Finalement, la complexité de notre algorithme est $O(N \ln \ln N)$.