ÉNS de Lyon Option C
2018-2019

Algorithmes élémentaires

Exercice 1 — (Algorithme de Karatsuba) Soit $n \in \mathbb{N}^*$. Soient $a, b \in [\![0, 2^n - 1]\!]$ et $m = \lceil \frac{n}{2} \rceil$.

1. Montrer qu'on peut écrire $a = 2^m\alpha + \tilde{\alpha}$ et $b = 2^m\beta + \tilde{\beta}$, où $\alpha, \tilde{\alpha}, \beta, \tilde{\beta} \in [\![0, 2^m - 1]\!]$.

Soit $C(n)$ le temps en calcul pour calculer xy pour tous x, y de taille n

2. Montrer que $ab = 2^{2m}\alpha\beta + 2^m\big(\alpha\beta + \tilde{\alpha}\tilde{\beta} - (\alpha - \tilde{\alpha})(\beta - \tilde{\beta})\big) + \tilde{\alpha}\tilde{\beta}$. En déduire que $C(n) \leq 3C(m) + kn$, où $k \in \mathbb{N}$.

3. En déduire que $C(n) = O(n^{\log_2(3)})$.

4. Implémenter cet algorithme ainsi que l'algorithme de multiplication usuelle. Comparer le temps de calcul pour différentes valeurs de n.

Exercice 2 — (Coût de l'exponentiation rapide)
Soit $a \in \mathbb{N}^*$.

1. Soit $C(n)$ le coût du calcul de a^n par la « méthode » $a^n = a.a^{n-1}$. Majorer $C(n)$ en fonction de $C(n-1)$.

Soit $D(n)$ le coût du calcul de a^n par la « méthode » $a^n = (a^{n/2})^2$ si n est pair et $a^n = a.a^{(n-1)/2}$ si n est impair. Soit $f : \mathbb{N} \to \mathbb{N}$ définie par $f(n) = \lfloor \frac{n}{2} \rfloor$.

le u annoncé n'est pas bon

2. Soit $n \in \mathbb{N}^*$. Montrer que $D(n) \leq D(f(n)) + uf(n)^2$, où $u = \frac{\log(a)^3}{4}$.

l'introduction de la fonction g est inutile en calculant $D(2^\ell)$

3. Soit $g : \mathbb{N} \to \mathbb{N}$ définie par $g(n) = \sum_{k=0}^{+\infty}(f^{\circ k}(n))^2$. En utilisant le fait que g est croissante, montrer que pour tout $n \in \mathbb{N}$, $g(n) \leq \frac{4n^2-1}{3}$. En déduire une majoration de D. Est-ce très différent de C ?

4. Que se passe-t-il si on choisit $a \in \mathbb{Z}/N\mathbb{Z}$?