Examen du jeudi 5 janvier 2023 - Durée 2h00

L'usage de tout document ou appareil électronique (y compris calculatrice) est prohibé. Les réponses aux questions doivent être justifiées faute de quoi elles ne rapporteront aucun point, même si elles sont justes.

Exercice 1.

(a) Donner le développement en fraction continue du nombre $-4/15$.

(b) On considère deux entiers $a \in \mathbb{N}^*$ et $b \in \mathbb{N}^*$ tels que $b < 2a + 1$.

(i) En posant $\sqrt{a^2+b} = a + \dfrac{1}{x}$, montrer que $\dfrac{1}{x} = \dfrac{b}{2a + \dfrac{1}{x}}$ et en déduire que

$$\sqrt{a^2+b} = a + \cfrac{b}{2a + \cfrac{b}{2a + \cfrac{b}{2a + \ddots}}}$$

(ii) En supposant que b divise $2a$, donner la forme générale du développement en fraction continue de $\sqrt{a^2+b}$.

Exercice 2. Une bande de 17 pirates dispose d'un butin composé de N pièces d'or d'égale valeur. Ils décident de se le partager également et de donner le reste au cuisinier (non pirate). Celui ci reçoit 3 pièces. Mais une rixe éclate et 6 pirates sont tués. Tout le butin est reconstitué et partagé entre les survivants comme précédemment; le cuisinier reçoit alors 4 pièces.
Quelle est la fortune minimale que peut espérer le cuisinier lorsqu'il décide d'empoisonner le reste des pirates ?

Exercice 3. On considère le cryptage RSA associé aux valeurs $p = 11$, $q = 3$ et $e = 3$.

(a) Calculer la valeur publique associée n ainsi que $\varphi(n)$ (où φ est l'indicatrice d'Euler).

(b) Calculer la valeur d de la clé privée.

(c) On considère le message $m = 8$. Crypter ce message avec la clé publique (n, e) et vérifier le cryptage en redécodant.

Tourner la page

Pas de panique ! Ce dernier exercice a l'air long, mais il ne l'est pas.

Exercice 4. Soient A et B deux matrices carrées de taille $n \times n$, dont les coefficients entiers sont bornés en valeurs absolues par m.

(a) Méthode brute. Montrer que le calcul du produit $C = AB$ nécessite $O(n^3)$ multiplications d'entiers de taille $L(m)$. En déduire la complexité en fonction de n et m.

Dans les algorithmes "diviser pour régner", la complexité vérifie souvent une récurrence de la forme

$$T(n) = a\, T\left(\frac{n}{b}\right) + O(n^d).$$

On admettra que lorsque $d < \log_b a$, on a $T(n) = O(n^{\log_b a})$.

Dans la suite, on ne s'occupe que du nombre d'opérations (multiplication ou addition) sur les entiers sans mentionner leur taille.

(b) Algorithme diviser pour régner naïf. On suppose n divisible par 2.

(i) Les trois matrices A, B et C sont divisées en matrices par blocs de taille $n/2 \times n/2$:

$$A = \begin{pmatrix} A_{1,1} & A_{1,2} \\ A_{2,1} & A_{2,2} \end{pmatrix}, \quad B = \begin{pmatrix} B_{1,1} & B_{1,2} \\ B_{2,1} & B_{2,2} \end{pmatrix} \text{ et } C = \begin{pmatrix} C_{1,1} & C_{1,2} \\ C_{2,1} & C_{2,2} \end{pmatrix}.$$

Montrer que le calcul de $C_{i,j}$ nécessite deux multiplications de matrices de taille $n/2 \times n/2$ et une addition de telles matrices.

(ii) En déduire qu'on peut trouver un algorithme « diviser pour régner » dont la complexité est donnée par la récurrence : $T(n) = 8T(n/2) + O(n^2)$, et que par conséquent nous n'avons rien gagné par rapport à la méthode brute.

(c) Algorithme de Strassen

(i) Cet algorithme utilise des matrices M_i intermédiaires qui vont servir à exprimer les $C_{i,j}$.

$$\begin{aligned} M_1 &= (A_{1,1} + A_{2,2})(B_{1,1} + B_{2,2}) \\ M_2 &= (A_{2,1} + A_{2,2})B_{1,1} \\ M_3 &= A_{1,1}(B_{1,2} - B_{2,2}) \\ M_4 &= A_{2,2}(B_{2,1} - B_{1,1}) \\ M_5 &= (A_{1,1} + A_{1,2})B_{2,2} \\ M_6 &= (A_{2,1} - A_{1,1})(B_{1,1} + B_{1,2}) \\ M_7 &= (A_{1,2} - A_{2,2})(B_{2,1} + B_{2,2}) \end{aligned}$$

On a alors

$$C_{1,1} = M_1 + M_4 - M_5 + M_7, \quad C_{1,2} = M_3 + M_5, \quad C_{2,1} = M_2 + M_4, \quad C_{2,2} = M_1 - M_2 + M_3 + M_6.$$

Montrer que la complexité de cet algorithme est donnée par la récurrence $T(n) = 7T(n/2) + O(n^2)$.

(ii) En déduire que la complexité de cet algorithme est $T(n) = O(n^{\log_2 7})$.

Question hors barème : Montrer l'assertion admise avant la question (b) à propos des complexités.