Correction Examen 1ère session 2022-2023

Exercice 1.
(a). Avant d'appliquer l'algorithme d'Euclide, on doit se ramener au cas d'un rationnel positif en isolant la partie entière. On a $-1 < \frac{-4}{15} < 0$, donc la partie entière de $\frac{-4}{15}$ est -1, et on a

$$\frac{-4}{15} = -1 + \frac{11}{15} = \left[-1, \frac{15}{11}\right]$$

On calcule donc le développement en fraction continue de $\frac{15}{11}$ avec l'algorithme d'Euclide ;

$$\begin{aligned} 15 &= 11 \cdot 1 + 4 \\ 11 &= 4 \cdot 2 + 3 \\ 4 &= 3 \cdot 1 + 1 \\ 3 &= 1 \cdot 3 + 0 \end{aligned}$$

Donc $\frac{15}{11} = [1, 2, 1, 3]$ et $\frac{-4}{15} = [-1, 1, 2, 1, 3]$.
(b)(i). On a

$$\begin{aligned} \sqrt{a^2+b} = a + \frac{1}{x} &\Leftrightarrow x = \frac{1}{\sqrt{a^2+b} - a} \\ &\Leftrightarrow x = \frac{\sqrt{a^2+b}+a}{(\sqrt{a^2+b}-a)(\sqrt{a^2+b}+a)} \\ &\Leftrightarrow x = \frac{\sqrt{a^2+b}+a}{a^2+b-a^2} \\ &\Leftrightarrow x = \frac{\frac{1}{x}+2a}{b} \\ &\Leftrightarrow \frac{1}{x} = \frac{b}{2a+\frac{1}{x}} \end{aligned}$$

On a donc par une récurrence immédiate, on a alors

$$\sqrt{a^2+b} = a + \frac{b}{2a+\frac{1}{x}} = a + \frac{b}{2a+\frac{b}{2a+\frac{1}{x}}} = a + \cfrac{b}{2a+\cfrac{b}{2a+\cfrac{b}{\ddots}}}$$

(ii). Par hypothèse, on a un certain entier k tel que $bk = 2a$. On a donc

$$\frac{1}{x} = \frac{b}{bk+\frac{1}{x}} = \frac{1}{k+\frac{1}{bx}} \quad \text{et} \quad \frac{1}{bx} = \frac{b}{b(bk+\frac{1}{x})} = \frac{1}{bk+\frac{1}{x}}$$

D'où $x = [k, bx]$ et $bx = [bk, x]$. Ainsi

$$\sqrt{a^2+b} = a + \frac{1}{x} = [a, x] = [a, k, bx] = [a, k, bk, x] = [a, k, bk, k, bx] = \ldots = [a, \overline{k, bk}]$$

On note que la partie entière de $\sqrt{a^2+b}$ est a car $a^2 \leqslant a^2+b < a^2+2a+1$ ($0 \leqslant b < 2a+1$ par hypothèse).

Exercice 2. Le fait que le partage soit égal entre les pirates et que le reste soit donné au cuisinier indique qu'on fait la division de N par le nombre de pirates, et que le reste de cette division est donné au cuisinier. Dans un premier temps, il y a 17 pirates et

$$N = 17k + 3$$

Chaque pirate aura k pièces du trésor, et il reste 3 pièces pour le cuisinier. L'information importante est que $N \equiv 3[17]$.
Dans un second temps, 6 pirates sont tués et il en reste 11. On a alors $N \equiv 4[11]$. On sait donc que N est une solution du système de congruences suivant :

$$(S) \ : \ \begin{cases} N \equiv 3[17] \\ N \equiv 4[11] \end{cases}$$

Comme les entiers 11 et 17 sont premiers entre eux, on peut appliquer le théorème des restes chinois, qui nous indique que, si N_0 est une solution particulière de (S), on a $N \equiv N_0[11 \vee 17]$. On a $11 \vee 17 = 187$.

La fortune minimale que peut espérer le cuisinier s'il se débarasse des pirates est la plus petite solution positive du système (S). On cherche une solution particulière au système (S). Si N est solution, on a $N = 3+17p = 4+11q$ pour un certain couple d'entiers (p, q). On a en particulier $17p - 11q = 1$. Par l'algorithme d'Euclide étendu, on trouve $17 \cdot 2 - 11 \cdot 3 = 1$. Ainsi, $(p, q) = (2, 3)$ donne une solution particulière $N = 17 \cdot 2 + 3 = 37$. On a donc

$$(S) \Leftrightarrow N \equiv 37[187]$$

La plus petite solution positive de ce système est $N = 37$. Le cuisinier obtiendra donc au moins 37 pièces d'or si il empoisonne les pirates.

Exercice 3.
(a) On a $n = pq = 33$ et $\varphi(n) = (p-1)(q-1) = 20$.
(b) La valeur d de la clé privée est l'inverse de 3 modulo 20. On prend donc $d = 7$.
(c) On crypte le message m par $m^3 = 8^3 = 64 \cdot 8 \equiv -2 \cdot 8 \equiv -16[33]$. On décrypte le message en calculant $(-16)^7$ modulo 33. On a

$$(-16)^7 = (-1)^7 \cdot 2^{4 \cdot 7} = -2^{28} = -2^{25} \cdot 2^3 = -32^5 \cdot 8 \equiv -(-1)^5 \cdot 8 \equiv 8[33]$$

On retrouve bien le message m de base comme annoncé.

Exercice 4. On pose $A := (a_{i,j})_{i,j \in [\![1,n]\!]}$, $B := (b_{i,j})_{i,j \in [\![1,n]\!]}$, $C := (c_{i,j})_{i,j \in [\![1,n]\!]}$. Par définition du produit de matrices, on a

$$c_{i,j} = \sum_{k=1}^{n} a_{i,k} b_{k,j}$$

Le calcul de $c_{i,j}$ demande donc n produits d'entiers de taille au plus $L(m)$. Comme il y a n^2 coefficients $c_{i,j}$, on a un total de n^3 produits d'entiers de taille au plus $L(m)$ (prenant chacun $O(L(m)^2)$ opérations élémentaires). On doit également calculer, pour chaque $c_{i,j}$, n somme d'entiers de longueur $L(m)^2$ (prenant chacune $O(L(m)^2)$ opérations élémentaires). On a donc au total une complexité en $O(2n^3 L(m)^2)$.

$(c)(i)$ En considérant le produit par bloc des matrices A et B, on a $C_{i,j} = A_{i,1}B_{1,j} + A_{i,2}B_{2,j}$, d'où le résultat voulu.
(ii). L'algorithme "diviser pour régner" naïf consisterai à calculer les $C_{i,j}$ plutôt que C toute entière. Le calcul de $C_{i,j}$ se fait d'après la question précédente en $2T(\frac{n}{2}) + O(n^2)$ opérations (le $O(n^2)$ correspondant à la somme des deux matrices $A_{i,1}B_{1,j}$ et $A_{i,2}B_{2,j}$). Comme il faut calculer quatre blocs, on a $T(n) = 8T(\frac{n}{2}) + O(n^2)$. En

posant $a = 8, b = 2$ et $d = 2$, on a bien $d < 3 = \log_2(8)$, et donc $T(n) = O(n^3)$: nous n'avons rien gagné (ce qui n'est pas étonnant, vu la naïveté de l'algorithme).

$(d)(i)$ Le calcul des matrices intermédiaires demande une ou deux somme de matrices de taille $\frac{n}{2}$ (pour $O(\frac{n^2}{4})$ opérations) ainsi que le produit de deux matrices de taille $\frac{n}{2}$. Comme il y a 7 matrices intermédiaires, le calcul des M_i prend au total $7T(\frac{n}{2}) + O(n^2)$ opérations. Il faut ensuite ajouter/soustraire différentes matrices M_i pour obtenir les $C_{i,j}$, mais on reste en $O(n^2)$ opérations, d'où $T(n) = 7T(\frac{n}{2}) + O(n^2)$.

En posant $a = 7, b = 2$ et $d = 2$, on a bien $d < \log_2(7)$, donc $T(n) = O(n^{\log_2(7)})$.