**Université de Paris** **2019-2020**
**MI2**

# Devoir Maison du 25 juin 2020 - Session 2

Ce devoir maison permet de valider la deuxième session. Vous disposez de 24h pour l'effectuer à partir du 25 juin à 8h. Vous avez droit à tout le matériel à votre disposition chez vous. Toute production doit être individuelle. Les copies seront comparées entre elles. Contrairement à la session 1 où il a été décidé de ne pas sanctionner les productions ayant des similitudes, toutes copies présentant des similitudes mêmes ponctuelles pour 1 exercice ou même 1 seule question se verront affectée de 0. Vous déposerez votre production scannée ou photographiée sur le moodle dans la rubrique correspondante à ce devoir, avant le 26 juin 8h. Vous devrez déposer 1 seul fichier, sous format pdf. Tout autre format ou autre présentation ne sera pas acceptée. Si vous avez une question ou des soucis de tout ordre vous pouvez envoyer un mail à vandebro@univ-paris-diderot.fr avec comme sujet "Devoir maison L1 info MI2". Je répondrai aussi vite que possible

**Exercice 1.** Soit $M_0, M_1, M_2, M_3, M_4$ les 5 points du plan dont les affixes respectives $z_0, z_1, z_2, z_3, z_4$ sont les racines 5ième de l'unité.
1) Placer les points $M_0, M_1, M_2, M_3, M_4$ dans un repère orthonormé.
Soit $M$ un point dont l'affixe $z$ vérifie $|z| = 1$.
2) Démontrer que

$$\sum_{i=0}^{4} PM_i^2$$

est une constante indépendante de la position de $P$ sur le cercle unité. On détaillera les calculs.
Indications :
a) On utilisera que pour deux points $A$ et $B$ du plan $AB = |z_B - z_A|$ où $z_A$ et $z_B$ sont les affixes respectives de $A$ et $B$ ($AB$ désigne la distance $d(A, B)$).
b) On rappelle également que pour tout complexe $w$, on a $|w|^2 = w\overline{w}$.

**Exercice 2.** Soient $a$ et $b$ deux réels tels que $0 \leq a \leq b$. On définit deux suites réelles $(U_n)$ et $(V_n)$ par leurs premiers termes $U_0 = a$, $V_0 = b$, et les relations de récurrence :

$$U_{n+1} = \sqrt{U_n V_n} \quad \text{et} \qquad V_{n+1} = \frac{U_n + V_n}{2}.$$

1) Question préliminaire : Montrer que pour tous réels $x$ et $y$ tels que $0 \leq x \leq y$, on a $x \leq \sqrt{xy} \leq \dfrac{x+y}{2} \leq y$.
2) a) Montrer que pour tout entier $n$, on a $U_n \leq V_n$.
b) Montrer que $(U_n)$ est croissante et $(V_n)$ est décroissante.
3) a) Montrer que pour tout entier $n$, on a $0 \leq V_{n+1} - U_{n+1} \leq \dfrac{1}{2}(U_n - V_n)$.
b) En déduire que pour tout entier $n$, on a $0 \leq V_n - U_n \leq \dfrac{1}{2^n}(b - a)$.
c) En déduire que la limite quand $n$ tend vers l'infini de $(V_n - U_n)$ est nulle.
4) En déduire que les suites $(U_n)$ et $(V_n)$ convergent vers la même limite $l \in [a, b]$ appelée moyenne arithmético-géométrique de $a$ et $b$.
5) Déduire une approximation à $10^{-3}$ près de cette moyenne lorsque $a = 1$ et $b = 2$.

**Exercice 3.** Soit $j$ la racine troisième de l'unité $\exp(\frac{2i\pi}{3})$.

1) Démontrer que si $j$ est racine d'un polynôme $F \in \mathbb{R}[X]$, $j^2$ est aussi racine de ce polynôme $F$.

2) Calculer les racines complexes du polynôme $X^2 + X + 1$ et donner une factorisation de ce polynôme dans $\mathbb{C}[X]$. En déduire que $(1-j)(1-j^2) = 3$ puis que $j^2 = -(1+j)$.

Soit maintenant $P$ le polynôme $(X+1)^5 - X^5 - 1$.

3) Montrez que $P$ a deux racines rationnelles évidentes.

4) Montrez que $j$ est aussi racine de $P$. En déduire une décomposition de $P$ en produits de facteurs irréductibles dans $\mathbb{C}[X]$, puis dans $\mathbb{R}[X]$.

5) Donnez la forme développée de $P$.

**Exercice 4.** On effectue la division euclidienne d'un entier naturel $a$ par 38. On trouve un quotient $q$ et un reste égal à $4q^2 - 4$. Donner les valeurs possibles pour $a$ et expliciter les divisions euclidiennes correspondantes.

**Exercice 5.** Le but de cet exercice est d'envisager une méthode de cryptage à clé publique d'une information numérique, appelée système RSA, en l'honneur des mathématiciens Ronald Rivest, Adi Shamir et Leonard Adleman, qui ont inventé cette méthode de cryptage en 1977 et l'ont publiée en 1978. Les questions 1 et 2 sont des questions préparatoires, la question 3 aborde le cryptage, la question 4 le décryptage.

1. Le calcul d'un reste de division euclidienne
   a). Justifier que le reste de la division euclidienne de $32^8$ par 85 est 1. En déduire le reste de la division euclidienne de $32^{32}$ par 85.
   b). Justifier que le reste de la division euclidienne de $32^7$ par 85 est 8. En déduire que $32^{39}$ est congru à 8 modulo 85.

2. Dans cette question, on considère l'équation $(E) \quad 23x - 64y = 1$, dont les solutions sont des couples $(x; y)$ d'entiers relatifs.
   a). Justifier par un argument du cours le fait que l'équation $(E)$ admet au moins un couple solution. Donner un couple, solution particulière de l'équation $(E)$.
   b). Déterminer tous les couples d'entiers relatifs solutions de l'équation $(E)$.
   c). En déduire qu'il existe un unique entier $d$ vérifiant les conditions $0 \leq d < 64$ et $23d \equiv 1 \mod 64$.

3. Cryptage dans le système RSA
   Une personne A choisit deux nombres premiers $p$ et $q$, puis calcule les produits $N = pq$ et $n = (p-1)(q-1)$. Elle choisit également un entier naturel $c$ premier avec $n$. La personne A publie alors le couple $(N; c)$, qui est une clé publique permettant à quiconque de lui envoyer un nombre crypté. Les messages sont numérisés et transformés en une suite d'entiers compris entre 0 et $N-1$. Pour crypter un entier $a$ de cette suite, on procède ainsi : on calcule le reste $b$ dans la division euclidienne par $N$ du nombre $a^c$, et le nombre crypté est l'entier $b$.
   Dans la pratique, cette méthode est sûre si la personne A choisit des nombres premiers $p$ et $q$ très grands, s'écrivant avec plusieurs dizaines de chiffres. On va l'envisager ici avec des nombres plus simples : $p = 5$ et $q = 17$.
   La personne A choisit également $c = 39$.
   a). Calculer les nombres $N$ et $n$ pour ces choix de $p$ et $q$. Donner la clef publique.
   b). Vérifier et justifier que la valeur $c$ choisie par $A$ vérifie la condition voulue.
   Un émetteur B souhaite envoyer à la personne A le nombre $a = 32$ (par exemple en ayant codé le message AF).
   c). Déterminer la valeur du nombre (message) crypté $b$ à envoyer par l'emetteur B.

4. Décryptage dans le système RSA
   La personne A calcule dans un premier temps l'unique entier naturel $d$ vérifiant les conditions $0 \leq d < n$ et $cd \equiv 1 \mod n$. Elle garde secret ce nombre $d$ qui lui permet, et à elle seule, de décrypter les nombres qui lui ont été envoyés cryptés avec sa clé publique $(N; c)$. Le couple $(N; d)$ constitue la clef privée à ne pas diffuser.
   Pour décrypter un nombre crypté $b$, la personne A calcule le reste $a$ dans la division euclidienne par $N$ du nombre $b^d$, et le nombre en clair – c'est-à-dire le nombre avant cryptage – est le nombre $a$. On admet l'existence et l'unicité de l'entier $d$, et le fait que le décryptage fonctionne. Les nombres choisis par A sont encore $p = 5$, $q = 17$ et $c = 39$.
   a). Quelle est la valeur de $d$ ?
   b). Quel critère fondamental dans le codage RSA permet de justifier que $d$ est unique ?
   c). En appliquant la règle de décryptage, retrouver le nombre en clair lorsque le nombre crypté est $b = 8$ (attention il y a plusieurs calculs de puissances successives à faire). d). Justifier la règle de décryptage, c'est à dire que le reste de la division de $b^d$ par $N$ est nécessairement $a$ (attention il y a plusieurs étapes de calcul pour cette question, des recherches internet de votre part sur le codage RSA sur le net peuvent être nécessaires pour y répondre proprement. Ces recherches seront valorisées si tant est qu'elles sont comprises. On devra produire des preuves de tous les résultats intermédiaires utilisés, quitte à les reprendre d'internet mais en les rendant compréhensibles avec les outils du cours d'arithmétique).

**Exercice 6.** Soient $x, y, z \in \mathbb{C}$, calculer par deux méthodes différentes, le déterminant de la matrice de taille $3 \times 3$ :

$$V = \begin{pmatrix} 1 & x & x^2 \\ 1 & y & y^2 \\ 1 & z & z^2 \end{pmatrix}.$$

Généraliser aux matrices de taille $n \times n$.

**Exercice 7.** Soit la matrice $A = \begin{pmatrix} 0 & 1 & 0 \\ -4 & 4 & 0 \\ -2 & 1 & 2 \end{pmatrix}$.

1) Calculer $(A - 2I)^2$ (on désigne par $I$ la matrice identité de taille $3 \times 3$.
2) En déduire $A^{-1}$ - on développera le polynôme $(X - 2)^2$.
3) Retrouver $A^{-1}$ par calcul direct.