# Devoir surveillé n° 4

**samedi 14 décembre 2024**

*La durée de l'épreuve est de 4 heures et aucune sortie définitive avant la fin n'est autorisée. Il est possible d'obtenir la note maximale sans avoir traité l'intégralité du sujet.*

*Avant de commencer, lisez l'intégralité du sujet.*

*Aucun document n'est autorisé. Les calculatrices et téléphones portables sont interdits.*

*Rédigez sur une copie double* ***lisiblement et proprement****. Laissez une marge à gauche et de la place au début de la copie pour mes appréciations. Écrivez à l'encre bleue ou noire. N'utilisez pas de blanc correcteur.* ***Encadrez ou soulignez les résultats principaux.***

*Veuillez apporter un soin particulier à la rédaction, à la rigueur et aux raisonnements.* ***Tout résultat doit être justifié****. Ces éléments seront pris en compte dans la notation. N'oubliez pas d'introduire toutes les variables que vous utilisez, lorsqu'il le faut. Évitez les symboles $\forall$, $\exists$, $\Rightarrow$ et $\Leftrightarrow$ sauf si vous savez les utiliser correctement.*

## Exercice 1 : Questions en vrac

***Cet exercice devra être traité sur une copie séparée. Il ne pourra être traité que lors des 80 premières minutes de ce devoir. Les copies seront ensuite ramassées et les 160 dernières minutes devront être consacrées exclusivement aux exercices 2, 3 et 4. Il est tout à fait possible de commencer à traiter les exercices 2, 3 et 4 avant la fin des 80 premières minutes.***

***Temps maximum conseillé pour les questions de cet exercice : 20 min, 10 min, 10 min, 20 min, 20 min***

1) Résoudre $54x + 75y = 6$ d'inconnue $(x, y) \in \mathbb{Z}^2$.

2) Calculer
$$\lim_{n \to +\infty} \frac{(-1)^{n^7} - 7n^7 + \sqrt[7]{n}(\ln(n))^{77}}{n^7 + n^{7!}(\pi/7)^n + \sqrt{7}\cos(e^{n!})}.$$

3) Montrer que l'ensemble
$$A = \left\{ \frac{mn}{(m+n)^2} \,\middle|\, m \in \mathbb{N}^*,\ n \in \mathbb{N}^*,\ m \neq n \right\}$$
admet $\dfrac{1}{4}$ pour borne supérieure et déterminer aussi sa borne inférieure. Est-ce que ce sont les maximum et minimum respectivement ?

4) Résoudre le problème de Cauchy
$$(1 + x^2)y' + x\,y = \frac{x^2}{\sqrt{1 + x^2}}, \qquad y(0) = 1$$
d'inconnue $y$ dérivable sur $\mathbb{R}$.

5) Résoudre l'équation différentielle $y'' + 6y' + 5y = 4\,\mathrm{sh}(x)$, d'inconnue $y$ deux fois dérivable sur $\mathbb{R}$.

Dans tout cet exercice, on se donne $n \in \mathbb{N}\backslash\{0;1\}$, $a \in \mathbb{N}^*$ et $b \in \mathbb{N}^*$.

### Partie A : Préliminaires

1) On suppose qu'il existe $k \in \mathbb{N}^*$ tel que $a^k \equiv 1\,[n]$. Justifier que $a \wedge n = 1$.

2) Supposons que $a$ est premier avec $n$.
   a) Justifier qu'il existe $k_1$ et $k_2$ des entiers naturels distincts tels que $a^{k_2} \equiv a^{k_1}\,[n]$.
   b) Quitte à échanger leurs noms, supposons que $k_2 > k_1$. En déduire qu'il existe $k \in \mathbb{N}^*$ tel que $a^k \equiv 1\,[n]$.

3) a) En utilisant le petit théorème de Fermat, montrer que $4^{12} \equiv 1\,[195]$.
   b) Vérifier (à la main) que $4^6 \equiv 1\,[195]$ et que, pour tout $k \in [\![1\,;5]\!]$, $4^k \not\equiv 1\,[195]$.

   Ainsi $6$ est la plus petite puissance (sans compter $4^0$) de $4$ qui est congrue à $1$ modulo $195$.

L'exemple précédent illustre le fait que le petit théorème de Fermat est très utile pour trouver une puissance d'un entier congrue à $1$ modulo $n$ (du moins lorsque $n$ n'admet pas de facteur premier carré) mais qu'il ne donne pas a priori la plus petite puissance congrue à $1$.

### Partie B : Notion d'ordre d'un entier modulo $n$

1) a) On suppose que $a \wedge n = 1$. Justifier que $\{k \in \mathbb{N}^* \,|a^k \equiv 1\,[n]\}$ admet un plus petit élément. On le note $\omega_n(a)$ et on l'appelle l'ordre de $a$ modulo $n$. Autrement dit $a^{\omega_n(a)}$ est la plus petite puissance de $a$ (sans compte $a^0$) qui est congrue à $1$ modulo $n$.
   b) Est-ce que $\omega_n(a)$ a un sens lorsque $a \wedge n \neq 1$.

Dans la suite, supposons que $a \wedge n = 1$

2) Soit $k \in \mathbb{N}^*$. Montrer que $a^k \equiv 1\,[n]$ si et seulement si $\omega_n(a)|k$.
   *Pour le sens direct, on pourra commencer par écrire la division euclidienne de $k$ par $\omega_n(a)$.*

3) Justifier que, lorsque $n$ est premier, $\omega_n(a)|n-1$.

### Partie C : Quelques propriétés de l'ordre

On suppose dans toute cette partie que $a \wedge n = 1$ et $b \wedge n = 1$. On pensera à bien à utiliser le critère de la question B2.

1) Montrer que $\omega_n(ab)|\omega_n(a) \vee \omega_n(b)$.

2) Soit $d \in \mathbb{N}^*$.
   a) Justifier que $\omega_n(a^d) \,\Big|\, \dfrac{\omega_n(a)}{d \wedge \omega_n(a)}$.
   b) Justifier que $d \vee \omega_n(a) \,\big|\, d\,\omega_n(a^d)$.
   c) En déduire que $\omega_n(a^d) = \dfrac{\omega_n(a)}{d \wedge \omega_n(a)}$.

3) Supposons que $b$ est un inverse de $a$ modulo $n$ (c'est-à-dire $ab \equiv 1\,[n]$). Montrer que $\omega_n(a) = \omega_n(b)$.

4) On suppose que $\omega_n(a) \wedge \omega_n(b) = 1$.
   a) Notons $m = \omega_n(ab)$. Déduire des questions précédentes que
   $$\frac{\omega_n(a)}{m \wedge \omega_n(a)} = \frac{\omega_n(b)}{m \wedge \omega_n(b)}.$$
   b) Conclure que $\omega_n(a) \vee \omega_n(b)|m$ puis que $\omega_n(ab) = \omega_n(a) \vee \omega_n(b)$.

### Partie D : Application : résolution d'une équation diophantienne

On considère l'équation $(E)$ : $3^m - 2^n = 1$ d'inconnue $(m,n) \in \mathbb{N}^2$.

1) Déterminer toutes les solutions de l'équation pour lesquelles $n \leqslant 3$.

2) Donnons-nous un couple $(m,n)$ solution de $(E)$ avec $n \geqslant 4$.
   a) Calculer $\omega_{16}(3)$. Qu'en déduit-on sur $m$ ?
   b) Conclure en raisonnant modulo $5$.

### Partie E : Application : infinité des nombres premiers congrus à $1$ modulo $p^n$

On se donne un nombre premier $p$. Pour tout $n \in \mathbb{N}$, posons $x_n = 2^{p^n} - 1$.

1) Montrer que, pour tout $n \in \mathbb{N}$, $x_n \equiv 1\,[p]$.

2) Soit $n \in \mathbb{N}$.
   a) Montrer que $x_n | x_{n+1}$ et donner une expression de $y_n = \dfrac{x_{n+1}}{x_n}$ sous la forme d'une somme.
   b) Vérifier que $y_n \neq 1$ et que $y_n \equiv p\,[x_n]$.

3) En déduire que, pour tout $(i,j) \in \mathbb{N}^2$ tel que $i \leqslant j$, $x_i \wedge y_j = 1$.

4) Soit $n \in \mathbb{N}$. On se donne alors $q$ un diviseur premier de $y_n$.
   a) En utilisant la question précédente, montrer que $\omega_q(2) = p^{n+1}$.
   b) En déduire que $q \equiv 1\,[p^n]$.

5) Montrer que, pour tout $n \in \mathbb{N}^*$, il existe une infinité de nombres premiers congrus à $1$ modulo $p^n$.

## Exercice 3 : Approximation d'une racine carrée

Dans tout cet exercice on se donne $a$ un entier naturel qui n'est pas un carré parfait.

1) Montrer que $\sqrt{a}$ est irrationnel.

On souhaite construire une suite de rationnel qui converge vers $\sqrt{a}$.

2) a) Pour tout $n \in \mathbb{N}$, posons $u_n(a) = \dfrac{\lfloor 10^n \sqrt{a} \rfloor}{10^n}$. Montrer que $(u_n(a))_{n\in\mathbb{N}}$ converge vers $\sqrt{a}$.
   b) Expliquer pourquoi cette suite ne peut pas raisonnablement être utilisée pour calculer une valeur approchée $\sqrt{a}$.

3) On supposons qu'il existe $(p_n)_{n\in\mathbb{N}}$ et $(q_n)_{n\in\mathbb{N}}$ deux suites dont les termes sont des entiers naturels non nuls et telles que $\dfrac{p_n}{q_n} \xrightarrow[n\to+\infty]{} \sqrt{a}$.
   a) Montrer qu'une suite d'entiers qui converge est stationnaire.
   b) Supposons que $(q_n)_{n\in\mathbb{N}}$ ne tende pas vers $+\infty$. Construire soigneusement une sous-suite de $(q_n)_{n\in\mathbb{N}}$ qui est bornée.
   c) En déduire que $(q_n)_{n\in\mathbb{N}}$ admet une sous-suite constante.
   d) Aboutir à une contradiction puis conclure que $q_n \xrightarrow[n\to+\infty]{} +\infty$ puis $p_n \xrightarrow[n\to+\infty]{} +\infty$.

   Cela constitue donc une condition nécessaire pour que $\dfrac{p_n}{q_n} \xrightarrow[n\to+\infty]{} \sqrt{a}$.

Proposons, pour le reste de cet exercice, d'étudier les suites $(p_n)_{n\in\mathbb{N}}$ et $(q_n)_{n\in\mathbb{N}}$ définies par $p_0 = q_0 = 1$ et

$$\forall n \in \mathbb{N}, \qquad p_{n+1} = p_n + a q_n \qquad \text{et} \qquad q_{n+1} = p_n + q_n.$$

Une récurrence immédiate (que l'on ne demande pas de rédiger) montre que, pour tout $n \in \mathbb{N}$, $p_n$ et $q_n$ sont des entiers non nuls.

4) Montrer que $(p_n)_{n\in\mathbb{N}}$ et $(q_n)_{n\in\mathbb{N}}$ tendent vers $+\infty$.

Ces deux suites vérifient donc bien la condition nécessaire de la question 3. Pour tout $n \in \mathbb{N}$, posons $r_n = \dfrac{p_n}{q_n}$. Dans la suite, nous allons montrer que $r_n \xrightarrow[n\to+\infty]{} \sqrt{a}$ de deux façons (indépendantes) différentes.

5) **Méthode 1.** On définit la fonction $f : x \longmapsto \dfrac{x+a}{x+1}$ sur $\mathbb{R}_+$.

   a) Montrer que le segment $\left[1\,;\frac{1+a}{2}\right]$ est stable par $f$.

   b) Déterminer les variations des suites $(r_{2n})_{n\in\mathbb{N}}$ et $(r_{2n+1})_{n\in\mathbb{N}}$.
   *Il est attendu que tout soit redémontré à cette question. On précisera le sens de variation (au sens large) de chacune de ces deux suites.*

   c) En déduire $r_n \xrightarrow[n\to+\infty]{} \sqrt{a}$.

6) **Méthode 2.**

   a) Vérifier que, pour tout $n \in \mathbb{N}$, $q_{n+2} = 2q_{n+1} + (a-1)q_n$.
   Ainsi $(q_n)_{n\in\mathbb{N}}$ est une suite récurrence linéaire d'ordre $2$ à coefficients constants.

   b) En déduire une expression de $q_n$ en fonction de $a$ et de $n$ pour tout $n \in \mathbb{N}$.

   c) En déduire une expression de $r_n$ en fonction de $n$ pour tout $n \in \mathbb{N}$.
   *On rappelle que, pour tout* $n \in \mathbb{N}$, $q_{n+1} = p_n + q_n$.

   d) Montrer enfin que $r_n \xrightarrow[n\to+\infty]{} \sqrt{a}$.

## Exercice 4 : Étude d'une suite à valeurs complexes

On se donne $z$ et $a$ des complexes quelconques. On considère la suite $(u_n)_{n\in\mathbb{N}}$ définie par $u_0 = z$, $u_1 = a$ et

$$\forall n \in \mathbb{N}, \qquad u_{n+2} = u_{n+1} + \frac{u_n}{2^n}.$$

Pour tout $n \in \mathbb{N}$, on note

$$m_n = \max\{|u_n|\,;|u_{n+1}|\} \qquad \text{et} \qquad v_n = \prod_{k=0}^{n}\left(1+\frac{1}{2^k}\right).$$

1) a) Montrer que, pour tout $n \in \mathbb{N}$, $v_n \leqslant \mathrm{e}^2$.
   *On pourra utiliser une inégalité de convexité sur la fonction* $\ln$.

   b) Justifier que, pour tout $n \in \mathbb{N}$,
   $$m_{n+1} \leqslant \left(1+\frac{1}{2^n}\right) m_n.$$

   c) Montrer alors que, pour tout $n \in \mathbb{N}$, $m_n \leqslant \mathrm{e}^2 m_0$. En déduire que $(u_n)_{n\in\mathbb{N}}$ est une suite bornée.

2) Montrer que, si $z$ et $a$ sont des réels positifs, alors $(u_n)_{n\in\mathbb{N}}$ admet une limite finie.

3) On revient au cas général ($z$ et $a$ sont des complexes quelconques).

   a) Montrer que, pour tout $(n,p) \in (\mathbb{N}^*)^2$ tel que $p > n$, on a $|u_p - u_n| \leqslant \dfrac{\mathrm{e}^2 m_0}{2^{n-2}}$.

   b) Soit $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ strictement croissante. Montrer que $u_{\varphi(n)} - u_n \xrightarrow[n\to+\infty]{} 0$.

   c) Conclure que $(u_n)_{n\in\mathbb{N}}$ admet une limite $\ell$ (que l'on ne cherchera pas à expliciter).

   d) Soit $\varepsilon > 0$. Déterminer un entier $n_0$ (en fonction de $m_0$ et $\varepsilon$) tel que, pour tout $n \geqslant n_0$, $|\ell - u_n| \leqslant \varepsilon$.