Devoir surveillé n°6

Sujet donné le samedi 11 février 2023, 4h. **L'usage de la calculatrice n'est pas autorisé.**
La notation tiendra particulièrement compte de **la qualité de la rédaction, la précision des raisonnements et l'énoncé des formules utilisées. Les réponses aux questions seront numérotées et séparées par un trait horizontal. Les résultats essentiels devront être encadrés ou soulignés.**

BON TRAVAIL

Congruences sur les rationnels et applications arithmétiques

Dans tout le problème, p **désigne un nombre premier supérieur ou égal à** 3 et, pour $(a,b) \in \mathbb{Z}^2$, $a \equiv b\ [p]$ désigne la relation de congruence modulo p sur les entiers relatifs.

L'objet de ce problème est de définir une relation de congruence sur les nombres rationnels puis d'établir des règles de manipulation de cette relation de congruence afin de l'utiliser pour prouver des résultats arithmétiques.

I Préliminaires

Les deux questions suivantes sont indépendantes et les résultats qu'elles proposent d'établir pourront être admis pour traiter la partie II.

I.1. (a) Soit $x \in \mathbb{Q}$. Montrer qu'il existe un unique couple $(N,D) \in \mathbb{Z} \times \mathbb{N}^*$ tel que

$$x = \frac{N}{D} \quad \text{et} \quad N \wedge D = 1\ .$$

Dans la suite du problème, on notera $N(x)$ et $D(x)$ l'unique couple solution du problème ci-dessus.
La fraction $\dfrac{N(x)}{D(x)}$ est appelée **le représentant irréductible de** x**.**

(b) Soient $x = \dfrac{N(x)}{D(x)}$ et $y = \dfrac{N(y)}{D(y)}$ les représentants irréductibles des deux rationnels x et y.
Montrer que, si $d \in \mathbb{N}$ est un diviseur commun à $N(x)$ et $N(y)$, alors d et $D(x)D(y)$ sont premiers entre eux et d divise $N(x+y)$.

I.2. (a) Soit $k \in [\![1, p-1]\!]$.

i. En utilisant une relation de Bezout, montrer qu'il existe un entier relatif u tel que $uk \equiv 1\ [p]$.

ii. Notons alors r le reste de la division euclidienne de u par p. Montrer que $rk \equiv 1[p]$ et que r est l'unique $h \in \mathbb{Z}$ tel que $hk \equiv 1\ [p]$ et $h \in [\![1, p-1]\!]$.

(b) Les justifications précédentes permettent donc de définir $\mathcal{I}_p \left| \begin{array}{ccc} [\![1,p-1]\!] & \to & [\![1,p-1]\!] \\ k & \mapsto & r \end{array} \right.$.

i. Expliciter $\mathcal{I}_5$.

ii. Montrer que l'application $\mathcal{I}_p$ est une permutation de $[\![1, p-1]\!]$ (c'est-à-dire une bijection de $[\![1, p-1]\!]$ dans $[\![1, p-1]\!]$).

iii. Formuler, dans le cadre de l'anneau $\mathbb{Z}/p\mathbb{Z}$, le résultat qui vient d'être établi concernant ses éléments inversibles.

II Congruences sur les rationnels

Soient k **un entier naturel non nul et** p **un nombre premier fixés**.

On considère sur $\mathbb{Q}$ la relation binaire $\mathcal{R}$ suivante : $x \in \mathbb{Q}$ est en relation avec $y \in \mathbb{Q}$ si p^k divise $N(x-y)$ (le numérateur du représentant irréductible de $x-y$).

II.1. Montrer que $\mathcal{R}$ est une relation d'équivalence sur $\mathbb{Q}$.

On notera désormais $x \equiv_{\mathbb{Q}} y\ [p^k]$ l'assertion $x\mathcal{R}y$.

II.2. Caractériser (ce qui signifie donner un énoncé équivalent) à l'aide de la relation de divisibilité habituelle sur $\mathbb{Z}$, les assertions
— $a \equiv_{\mathbb{Q}} b\ [p^k]$ lorsque $(a,b) \in \mathbb{Z}^2$,
— $x \equiv_{\mathbb{Q}} 0\ [p^k]$ lorsque $x \in \mathbb{Q}$.

II.3. Soient $(x,y,x',y') \in \mathbb{Q}^4$ tels que $x \equiv_{\mathbb{Q}} y\ [p^k]$ et $x' \equiv_{\mathbb{Q}} y'\ [p^k]$.
Montrer que $x+x' \equiv_{\mathbb{Q}} y+y'\ [p^k]$.

II.4. Soient $(x,y) \in \mathbb{Q}^2$ tels que $x \equiv_{\mathbb{Q}} y\ [p^k]$ et $z \in \mathbb{Q}$.
A-t-on nécessairement $xz \equiv_{\mathbb{Q}} yz\ [p^k]$?
Donner une condition portant sur $D(z)$ et montrer qu'elle suffit pour établir $xz \equiv_{\mathbb{Q}} yz\ [p^k]$.

III Applications arithmétiques

On note S_{p-1} le nombre rationnel

$$S_{p-1} = \sum_{k=1}^{p-1} \frac{1}{k} = \frac{A_p}{B_p}$$

où l'on a posé $A_p = N(S_{p-1})$ et $B_p = D(S_{p-1})$.

III.1. Donner les représentants irréductibles de S_{p-1} pour $p=3$, $p=5$ et dans chaque cas donner la valeur de la plus grande puissance de p divisant A_p.

III.2. (a) Justifier que $S_{p-1} = \displaystyle\sum_{k=1}^{p-1} \frac{1}{p-k}$ puis montrer qu'il existe $V \in \mathbb{N}$ tel que $2S_{p-1} = \dfrac{pV}{(p-1)!}$.

(b) En déduire que p divise A_p et $p \wedge B_p = 1$ (résultat dû à Waring (1782)).

III.3. Montrer que, pour tout $s \in [\![1, p-1]\!]$,

$$\frac{1}{1-\frac{p}{s}} \equiv_{\mathbb{Q}} \left(1+\frac{p}{s}\right)\ [p^2]$$

et en déduire que

$$S_{p-1} \equiv_{\mathbb{Q}} -\sum_{s=1}^{p-1} \frac{1}{s}\left(1+\frac{p}{s}\right)\ [p^2]$$

puis

$$2S_{p-1} \equiv_{\mathbb{Q}} -p\sum_{s=1}^{p-1} \frac{1}{s^2}\ [p^2]$$

III.4. Soit $k \in [\![1, p-1]\!]$ et $h = \mathcal{I}(k)$ où $\mathcal{I}$ est l'application définie dans la partie I (préliminaires).
Montrer que $\dfrac{1}{k} \equiv_{\mathbb{Q}} h\ [p]$ et $\dfrac{1}{k^2} \equiv_{\mathbb{Q}} h^2\ [p]$.

III.5. Conclure en établissant que, si p est un nombre premier supérieur ou égal à 5, alors p^2 divise A_p. Ce résultat est connu sous le nom du théorème de Wolstenholme.

Anneau $\mathbb{Z}_\alpha$

Dans tout le problème, on considère le polynôme $P = X^2 + bX + c$, unitaire, à coefficients entiers (c'est-à-dire $(b, c) \in \mathbb{Z}^2$) et de discriminant $\Delta = b^2 - 4c < 0$.

I Structure d'anneau sur $\mathbb{Z}_\alpha$

I.1. On note α et β les racines de P sur $\mathbb{C}$.

(a) Montrer que $\alpha + \beta$ et $\alpha \times \beta$ sont des nombres entiers dont on donnera les valeurs.

(b) Prouver que $\beta = \overline{\alpha}$ et exprimer la valeur de $|\alpha|$ en fonction de c. (Pourquoi c est-il nécessairement positif ?)

On note $\mathbb{Z}_\alpha$ l'ensemble $\{p + \alpha q \mid (p, q) \in \mathbb{Z}^2\}$.

I.2. (a) Montrer que $(\mathbb{Z}_\alpha, +, \times)$ est un anneau commutatif.

(b) Montrer que pour tout $(p, q, p', q') \in \mathbb{Z}^4$, on a l'équivalence :
$$p + \alpha q = p' + \alpha q' \iff [p = p' \text{ et } q = q']$$

(c) On note $G_\alpha = \{z \in \mathbb{Z}_\alpha \mid \exists\ z' \in \mathbb{Z}_\alpha, \text{ tel que } z \times z' = 1\}$. Pourquoi G_α est-il un groupe (on précisera vis-à-vis de quelle loi) ?

II Suite récurrente

On considère dans cette partie la matrice $N = \begin{pmatrix} 0 & 1 \\ -c & -b \end{pmatrix}$.

II.1. Montrer que $P(N) = 0$.

II.2. Soit $m \in \mathbb{N}$. On note respectivement Q_m et R_m le quotient et le reste de la division euclidienne de X^m par P dans $\mathbb{C}[X]$.

(a) Montrer que $R_m = \dfrac{\alpha^m - \overline{\alpha}^m}{\alpha - \overline{\alpha}} X + \dfrac{\alpha\overline{\alpha}^m - \overline{\alpha}\alpha^m}{\alpha - \overline{\alpha}}$.

(b) En déduire une expression de N^m en fonction de N, I_2, α, $\overline{\alpha}$ et m.

II.3. L'expression précédente est-elle vraie pour $m \in \mathbb{Z}$?

On considère la suite u définie par $(u_0, u_1) \in \mathbb{Z}^2$ et, pour tout $n \in \mathbb{N}$,
$$u_{n+2} = -bu_{n+1} - cu_n$$

On pose, pour tout $n \in \mathbb{N}$, $X_n = \begin{pmatrix} u_n \\ u_{n+1} \end{pmatrix}$.

II.4. (a) Montrer que, pour tout $n \in \mathbb{N}$, $X_n = N^n X_0$.

(b) En déduire, pour tout $n \in \mathbb{N}$, une expression explicite de u_n en fonction de α, $\overline{\alpha}$, u_0, u_1 et n.

II.5. Étude d'une suite particulière. Nous considérons désormais la suite u définie par
$$u_0 = 0\ ,\ u_1 = 1\ ,\ \forall n \in \mathbb{N}\ ,\ u_{n+2} = -2u_{n+1} - 3u_n$$
ce qui correspond au cas particulier de l'étude précédente pour $b = 2$ et $c = 3$.

(a) Montrer que, pour tout $n \in \mathbb{N}$, $u_n = \dfrac{1}{\sqrt{2}} \mathrm{Im}\left((-1 + i\sqrt{2})^n\right)$.

(b) En déduire que, pour tout $n \in \mathbb{N}$, $u_n = \displaystyle\sum_{\substack{k=1 \\ k \equiv 1\ [2]}}^{n} \binom{n}{k} (-1)^{n-k} (-1)^{\frac{k-1}{2}} \sqrt{2}^{k-1}$.

(c) Étude des termes d'indices un nombre premier. Soit p un nombre premier supérieur ou égal à 3.

i. Établir que $u_p \equiv (-2)^{\frac{p-1}{2}}\ [p]$. On justifiera soigneusement tout résultat utilisé.

ii. Montrer que $\overline{u_p}$ est une racine de $X^2 - 1$ dans $\mathbb{Z}/p\mathbb{Z}$. Quelle est la forme factorisée de $X^2 - 1$ dans le corps $\mathbb{Z}/p\mathbb{Z}$? Que peut-on en déduire concernant la congruence de u_p modulo p ?

(d) Étude des termes d'indices une puissance de 2. Notons v la suite définie par
$$v_0 = 1\ ,\ v_1 = -1\ ,\ \forall n \in \mathbb{N}\ ,\ v_{n+2} = -2v_{n+1} - 3v_n$$
ce qui correspond, comme pour la suite u, au cas particulier de l'étude précédente pour $b = 2$ et $c = 3$.

i. Montrer que $\forall n \in \mathbb{N}$, $v_n = \dfrac{\alpha^n + \overline{\alpha}^n}{2}$ où α est une racine du trinôme $X^2 + 2X + 3$.

ii. En reconnaissant une identité remarquable, déterminer, pour tout $n \in \mathbb{N}$, une relation simple entre $u_{2^{n+1}}$, u_{2^n} et v_{2^n}.

iii. En déduire, par récurrence, que $u_{2^n} \equiv 0\ [2^n]$ pour tout $n \in \mathbb{N}$.

III Corps $\mathbb{Q}[N]$

Cette partie est consacrée à l'étude de l'ensemble $\mathbb{Q}[N] = \{Q(N) \mid Q \in \mathbb{Q}[X]\}$ où N est la matrice introduite dans la partie II.

III.1. Montrer que $\mathbb{Q}[N] = \{sN + tI_2 \mid (s,t) \in \mathbb{Q}^2\}$.
Pour l'inclusion directe, on pourra utiliser le résultat de la question II.2.

III.2. En déduire que $\mathbb{Q}[N]$ est un sous-anneau commutatif de $\mathcal{M}_2(\mathbb{Q})$.

III.3. Cette question propose l'étude d'un exemple qui sera généralisée dans la question suivante.

(a) Effectuer explicitement la division euclidienne de $P = X^2 + bX + c$ par $X + 2$.

(b) En évaluant en -2, justifier que le reste est non nul.

(c) En déduire que $N + 2I_2$ est une matrice inversible dans $\mathbb{Q}[N]$ et préciser son inverse.

III.4. (a) Soient $(s,t) \in \mathbb{Q}^2$ tels que $s \neq 0$. Posons $M = sN + tI_2$.
Prouver l'existence de $M' \in \mathbb{Q}[N]$ telle que $MM' = M'M = I_2$.

(b) À l'aide de la question précédente, montrer que $\mathbb{Q}[N]$ est un corps.

Correction

Congruences sur les rationnels et applications arithmétiques

Dans tout le problème, p **désigne un nombre premier supérieur ou égal à** 3 et, pour $(a,b) \in \mathbb{Z}^2$, $a \equiv b\ [p]$ désigne la relation de congruence modulo p sur les entiers relatifs.

L'objet de ce problème est de définir une relation de congruence sur les nombres rationnels puis d'établir des règles de manipulation de cette relation de congruence afin de l'utiliser pour prouver des résultats arithmétiques.

I Préliminaires

Les deux questions suivantes sont indépendantes et les résultats qu'elles proposent d'établir pourront être admis pour traiter la partie II.

I.1. (a) Soit $x \in \mathbb{Q}$. Montrer qu'il existe un unique couple $(N,D) \in \mathbb{Z} \times \mathbb{N}^*$ tel que

$$x = \frac{N}{D} \quad \text{et} \quad N \wedge D = 1\ .$$

Dans la suite du problème, on notera $N(x)$ et $D(x)$ l'unique couple solution du problème ci-dessus.
La fraction $\dfrac{N(x)}{D(x)}$ est appelée **le représentant irréductible de x.**

Par définition de $\mathbb{Q}$, il existe $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$ tel que $x = \dfrac{a}{b}$.
Notons $\delta = a \wedge b$,
alors il existe $a', b' \in \mathbb{Z} \times \mathbb{Z}^*$ tel que $a = \delta a'$ et $b = \delta b'$ avec $a' \wedge b' = 1$.
Prenons alors $D = b'$ et $N = a'$ si $b > 0$ ou $D = -b'$ et $N = -a'$ si $b < 0$.
On a alors $x = \dfrac{N}{D}$ avec $N \wedge D = 1$ et $D \in \mathbb{N}^*$.
Reste à montrer l'unicité.
Si $x = \dfrac{N_1}{D_1} = \dfrac{N_2}{D_2}$ avec $N_1 \wedge D_1 = N_2 \wedge D_2 = 1$ et $D_1, D_2 \in \mathbb{N}^*$,
alors $D_2 N_1 = D_1 N_2$, donc D_1 divise $D_2 N_1$. Or $N_1 \wedge D_1 = 1$, donc d'après le lemme de Gauss $D_1 | D_2$.
pour des raisons symétriques : $D_2 | D_1$. Ainsi D_1 et D_2 sont associés dans $\mathbb{Z}$.
Autrement écrit : il existe $\lambda \in \{-1, 1\}$ tel que $D_1 = \lambda D_2$.
Mais $D_1, D_2 \in \mathbb{N}$, donc $\lambda = 1$ et $D_1 = D_2$ et par suite $N_1 = N_2$.

> Pour tout $x \in \mathbb{Q}$, il existe un unique couple $(N,D) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $x = \dfrac{N}{D}$ et $N \wedge D = 1$.

(b) Soient $x = \dfrac{N(x)}{D(x)}$ et $y = \dfrac{N(y)}{D(y)}$ les représentants irréductibles des deux rationnels x et y.
Montrer que, si $d \in \mathbb{N}$ est un diviseur commun à $N(x)$ et $N(y)$, alors d et $D(x)D(y)$ sont premiers entre eux et d divise $N(x+y)$.

Supposons que $d \wedge D(x)D(y) \neq 1$. Soit p un diviseur premier de $d \wedge D(x)D(y)$ (il existe bien !).
Comme p est premier, p divise $D(x)$ ou p divise $D(y)$.
Sans perte de généralité (SPDG), on peut supposer p divise $D(y)$ (respectivement $D(x)$).
Alors, par transitivité de la divisibilité, p divise d donc $N(x)$ et $N(y)$.
Ainsi, p divise $D(y)$ et p divise $N(y)$ (resp. $D(x)$ et $N(x)$).
Ainsi $p | D(y) \wedge N(y) = 1$ (resp. $p | D(x \wedge N(x) = 1$).
Ceci est impossible pour un nombre premier. Donc

$$\boxed{d \wedge D(x)D(y) = 1}$$

Puis $x + y = \dfrac{D(y)N(x) + D(x)N(y)}{D(x)D(y)}$.
On a vu que $N(x+y)$ est la fraction irréductible qui définit $x+y$, donc tout numérateur de $x+y$ est un multiple de $N(x+y)$.
Ainsi avec $\delta = [D(y)N(x) + D(x)N(y)] \wedge [D(x)D(y)] \in \mathbb{Z}$ on a : $\delta \times N(x+y) = D(y)N(x) + D(x)N(y)$.

Puis d divise $N(x)$ et $N(y)$ donc toute combinaison linéaire de ces nombres,
ainsi d divise $D(y)N(x) + D(x)N(y)$ et donc d divise $\delta \times N(x+y)$.
Or si on note $t = \delta \wedge d$, t divise δ donc $D(x)D(y)$ (puisque PGCD),
donc t divise $d \wedge D(x)D(y) = 1$, donc $t = 1$.
On applique alors le lemme de Gauss :

$$\boxed{d \text{ divise } N(x+y).}$$

I.2. (a) Soit $k \in [\![1, p-1]\!]$.

i. En utilisant une relation de Bezout, montrer qu'il existe un entier relatif u tel que $uk \equiv 1\ [p]$.

---

p est un nombre premier, il est donc en particulier avec tous les nombres qu'il ne divise pas,
c'est le cas de tous les nombres de $[\![1, p-1]\!]$. Ainsi $p \wedge k = 1$.
On peut appliquer une relation de Bézout : $\exists\ u, v \in \mathbb{Z}$ tel que $uk + vp = 1$.
Si l'on passe cette relation modulo p, on trouve :

$$\boxed{\exists\ u \in \mathbb{Z} \text{ tel que } uk \equiv 1[p]}$$

---

ii. Notons alors r le reste de la division euclidienne de u par p. Montrer que $rk \equiv 1[p]$ et que r est l'unique $h \in \mathbb{Z}$ tel que $hk \equiv 1\ [p]$ et $h \in [\![1, p-1]\!]$.

Il existe donc $q \in \mathbb{Z}$ tel que $u = pq + r$, donc $u \equiv r[p]$.
On a donc, par stabilité des produits modulo p :

$$\boxed{1 \equiv uk \equiv rk \quad [p]}$$

Soit $h \in [\![1, p-1]\!]$ tel que $hk \equiv 1[p]$, alors $hk \equiv rk[p]$. Donc $p | hk - rk = (h-r)k$
Or $p \wedge k = 1$ (déjà vu), donc $p | h - r$.
Or $1 - (p-1) \leqslant h - r \leqslant (p-1) - 1$, donc $h - r \in [\![-p+2, p-2]\!] \cap p\mathbb{Z} = \{0\}$.

$$\boxed{\text{Ainsi } h = r.\ r \text{ est unique dans } [\![1, p-1]\!].}$$

(b) Les justifications précédentes permettent donc de définir $\mathcal{I}_p \left| \begin{array}{ccc} [\![1,p-1]\!] & \to & [\![1,p-1]\!] \\ k & \mapsto & r \end{array} \right.$.

i. Expliciter $\mathcal{I}_5$.

$1 \times 1 \equiv 1[5]$, $2 \times 3 = 6 \equiv 1[5]$ et $4 \times 4 = 16 \equiv 1[5]$. Donc

$$\boxed{\mathcal{I}_5 : \begin{cases} 1 & \mapsto & 1 \\ 2 & \mapsto & 3 \\ 3 & \mapsto & 2 \\ 4 & \mapsto & 4 \end{cases}}$$

---

ii. Montrer que l'application $\mathcal{I}_p$ est une permutation de $[\![1, p-1]\!]$ (c'est-à-dire une bijection de $[\![1, p-1]\!]$ dans $[\![1, p-1]\!]$).

Notons que $\mathcal{I}_p$ est une application définie d'un ensemble E dans lui-même, de cardinal fini. Donc, il suffirait de montrer que $\mathcal{I}_p$ est injective ou $\mathcal{I}_p$ est surjective pour pouvoir affirmer directement que $\mathcal{I}_p$ est bijective.
Néanmoins, nous allons montrer ici que $\mathcal{I}_p$ est surjective puis injective donc bijective.
Soit $r \in [\![1, p-1]\!]$. Soit $k = \mathcal{I}_p(r)$. On a donc $k \in [\![1, p-1]\!]$,
et $r \times k = r \times \mathcal{I}_p(r) \equiv 1[p]$, donc $I_p(k) = r$. Et $\mathcal{I}_p$ est surjective de $[\![1, p-1]\!]$ sur $[\![1, p-1]\!]$.
Soient k_1, k_2 de $[\![1, p-1]\!]$ tels que $\mathcal{I}_p(k_1) = \mathcal{I}_p(k_2) := r$.

alors $k_1 r \equiv k_2 r \equiv 1[p]$, donc $p|(k_1 - k_2)r$ donc $p|k_1 - k_2$ car $p \wedge r = 1$ ($r \in [\![1, p-1]\!]$).
Et comme précédemment : $k_1 - k_2 \in [\![-p+2, p-2]\!] \cap p\mathbb{Z} = \{0\}$, donc $k_1 = k_2$, et $\mathcal{I}_p$ est injective.

$\boxed{\mathcal{I}_p \text{ est une permutation de } [\![1, p-1]\!].}$

---

iii. Formuler, dans le cadre de l'anneau $\mathbb{Z}/p\mathbb{Z}$, le résultat qui vient d'être établi concernant ses éléments inversibles.

On note $\overline{u}$, la classe de u pour la relation d'équivalence de la congruence modulo p.
On a vu dans le cours que pour tout $r, k \in \mathbb{Z}$, $\overline{r \times k} = \overline{r} \overline{\times} \overline{k}$.
Et, le neutre de l'anneau $(\mathbb{Z}/p\mathbb{Z}, \overline{+}, \overline{\times})$ est $\overline{1}$.
On a donc avec les questions précédentes :

$$\forall\, o \in \mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}, \exists\, u, r \in [\![1, p-1]\!] \text{ tels que } o = \overline{u} \text{ et } o \overline{\times} \overline{r} = \overline{ur} = \overline{1} = \overline{r} \overline{\times} o$$

Ainsi, on vient de montrer que

$$\boxed{(\mathbb{Z}/p\mathbb{Z})^\times := \{\text{Les éléments inversibles de } \mathbb{Z}/p\mathbb{Z}\} = \mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}.}$$

De plus, l'application $\mathcal{I}$ correspond, sur $(\mathbb{Z}/p\mathbb{Z})^\times$, à l'application qui à tout élément associe son symétrique multiplicatif donc

$$\boxed{\text{l'inversion est une permutation du groupe}((\mathbb{Z}/p\mathbb{Z})^\times, \times).}$$

II Congruences sur les rationnels

Soient k **un entier naturel non nul et** p **un nombre premier fixés**.

On considère sur $\mathbb{Q}$ la relation binaire $\mathcal{R}$ suivante : $x \in \mathbb{Q}$ est en relation avec $y \in \mathbb{Q}$ si p^k divise $N(x-y)$ (le numérateur du représentant irréductible de $x - y$).

II.1. Montrer que $\mathcal{R}$ est une relation d'équivalence sur $\mathbb{Q}$.

• Pour tout $x \in \mathbb{Q}$, $N(x-x) = 0$ et $p^k|0$. Donc $x\mathcal{R}x$.
Ainsi $\mathcal{R}$ est réflexif.

• Soient $x, y \in \mathbb{Q}$ tel que $x\mathcal{R}y$. Alors $p^k|\mathbb{N}(x-y)$.
Puis $y - x = -(x-y) = \dfrac{-N(x-y)}{D(x-y)}$. Or dans cet écriture, $D \in \mathbb{N}$ et $-N \wedge D = 1$,
il s'agit donc de l'écriture unique de la première partie.
On peut identifier : $N(y-x) = -N(y-x)$ et donc $p^k|N(y-x)$.
Ainsi $y\mathcal{R}x$.
On a démontré que $\mathcal{R}$ est symétrique.

• Soient $x, y, z \in \mathbb{Q}$ tel que $x\mathcal{R}y$ et $y\mathcal{R}z$. Alors $p^k|\mathbb{N}(x-y)$ et $p^k|N(y-z)$.
Puis $x - z = (x-y) + (y-z)$. On peut appliquer la réponse à la question 1.(b). avec $d \leftarrow p^k$, $x \leftarrow x - y$ et $y \leftarrow y - z$.
alors $p^k|N(x-z)$. Ainsi $x\mathcal{R}z$.
On a démontré que $\mathcal{R}$ est transitif.

$\boxed{\mathcal{R} \text{ est une relation d'équivalence sur } \mathbb{Q}.}$

On notera désormais $x \equiv_{\mathbb{Q}} y\ [p^k]$ l'assertion $x\mathcal{R}y$.

II.2. Caractériser (ce qui signifie donner un énoncé équivalent) à l'aide de la relation de divisibilité habituelle sur $\mathbb{Z}$, les assertions
— $a \equiv_{\mathbb{Q}} b\ [p^k]$ lorsque $(a,b) \in \mathbb{Z}^2$,
— $x \equiv_{\mathbb{Q}} 0\ [p^k]$ lorsque $x \in \mathbb{Q}$.

Dans le cas où $a, b \in \mathbb{Z}$, alors l'écriture irréductible de $a-b$ est $a-b = \dfrac{a-b}{1}$.
Donc $N(a-b) = a-b$. Ainsi

$$\boxed{a \equiv_{\mathbb{Q}} b\ [p^k] \text{ lorsque } (a,b) \in \mathbb{Z}^2 \iff p^k | a-b.}$$

Si $x \in Q$, alors $N(x-0) = N(x)$ (et $D(x-0) = D(x)$), et donc

$$\boxed{x \equiv_{\mathbb{Q}} 0\ [p^k] \text{ lorsque } x \in \mathbb{Q} \iff p^k | N(x).}$$

II.3. Soient $(x, y, x', y') \in \mathbb{Q}^4$ tels que $x \equiv_{\mathbb{Q}} y\ [p^k]$ et $x' \equiv_{\mathbb{Q}} y'\ [p^k]$.
Montrer que $x + x' \equiv_{\mathbb{Q}} y + y'\ [p^k]$.

On peut le faire en deux temps : $x + x' \equiv_{\mathbb{Q}} y + x' \equiv_{\mathbb{Q}} y + y'\ [p^k]$. On peut aussi le faire directement...
Supposons donc que $x \equiv_{\mathbb{Q}} y\ [p^k]$ et $x' \equiv_{\mathbb{Q}} y'\ [p^k]$,
Donc $p^k | N(x-y)$ et $p^k | N(x'-y')$.
On peut encore appliquer la réponse à la question 1.(b). avec $d \leftarrow p^k$, $x \leftarrow x-y$ et $y \leftarrow x'-y'$.
On a alors $p^k | N((x-y)+(x'-y')) = N((x+x')-(y+y'))$.

$$\boxed{\text{Ainsi } x + x' \equiv_{\mathbb{Q}} y + y' [p^k].}$$

II.4. Soient $(x, y) \in \mathbb{Q}^2$ tels que $x \equiv_{\mathbb{Q}} y\ [p^k]$ et $z \in \mathbb{Q}$.
A-t-on nécessairement $xz \equiv_{\mathbb{Q}} yz\ [p^k]$?
Donner une condition portant sur $D(z)$ et montrer qu'elle suffit pour établir $xz \equiv_{\mathbb{Q}} yz\ [p^k]$.

Si $y = p^k + x$ (avec $x, y \in \mathbb{Q}$), alors $x \equiv_Q y [p^k]$.
Puis si $z = \dfrac{1}{p}$, alors $xz - yz = xz - p^k z - xz = p^{k-1}$ et donc $xz \not\equiv_{\mathbb{Q}} yz [p^k]$.

$$\boxed{\text{Ainsi, on n'a pas nécessairement } xz \equiv_{\mathbb{Q}} yz\ [p^k].}$$

Il faut visiblement que $p \wedge D(z) = 1$ (même si on n'a pas démontrer que cette condition est nécessaire).
Montrons que cette condition est suffisante. Supposons donc que $p \wedge D(z) = 1$
Notons que $xz - yz = (x-y)z = \dfrac{N(x-y)N(z)}{D(x-y)D(z)}$.
Cette écriture n'est a priori par la forme irréductible.
Notons $\lambda = [N(x-y)N(z)] \wedge [D(x-y)D(z)]$.
Alors, en simplifiant par λ, on obtient la forme irréductible donc $N(x-y)N(z) = \lambda \times N(xz-yz)$ et $D(x-y)D(z) = \lambda \times D(xz-yz)$.
Si $p | \lambda$, alors $p | D(x-y)D(z)$ (car c'est un PGCD).
Or d'après notre condition : $p \wedge D(z) = 1$, on a donc (Lemme de Gauss) : $p | D(x-y)$.
mais $p^k | N(x-y)$ et donc on a $p | N(x-y)$ et $p | D(x-y)$ et donc $\dfrac{N(x-y)}{D(x-y)}$ non irréductible.
Ceci est impossible donc p ne divise pas λ. p étant premier : $p \wedge \lambda = 1$.
On enfin $p^k \wedge \lambda = 1$. Or $p^k | N(x-y)N(z) = \lambda N(xz-yz)$,
donc d'après le lemme de Gauss : $p^k | N(xz-yz)$ et donc $xz \equiv_{\mathbb{Q}} yz [p^k]$.

$$\boxed{\text{Soient } (x,y) \in \mathbb{Q}^2 \text{ tels que } x \equiv_{\mathbb{Q}} y\ [p^k] \text{ et } z \in \mathbb{Q}. \text{ Si } p \wedge D(z) = 1, \text{ alors } xz \equiv_{\mathbb{Q}} yz [p^k].}$$

III Applications arithmétiques

On note S_{p-1} le nombre rationnel

$$S_{p-1} = \sum_{k=1}^{p-1} \frac{1}{k} = \frac{A_p}{B_p}$$

où l'on a posé $A_p = N(S_{p-1})$ et $B_p = D(S_{p-1})$.

III.1. Donner les représentants irréductibles de S_{p-1} pour $p = 3$, $p = 5$ et dans chaque cas donner la valeur de la plus grande puissance de p divisant A_p.

Pour $p = 3$, il faut faire le calcul jusqu'à $k = 2$:

$$\boxed{S_2 = 1 + \frac{1}{2} = \frac{3}{2} \qquad \text{donc} \qquad A_3 = N(S_2) = 3 \text{ et } B_3 = N(S_2) = 2}$$

car la fraction obtenue est irréductible. Pour $p = 5$, il faut faire le calcul jusqu'à $k = 4$:

$$\boxed{S_2 = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} = \frac{12 + 6 + 4 + 3}{12} = \frac{25}{12} \qquad \text{donc} \qquad A_5 = N(S_5) = 25 \text{ et } B_5 = N(S_5) = 12}$$

car la fraction obtenue est irréductible.

$$\boxed{\text{La plus grande puissance de 3 qui divise } A_3 \text{ est 3. La plus grande puissance de 5 qui divise } A_5 \text{ est } 5^2.}$$

III.2. (a) Justifier que $S_{p-1} = \displaystyle\sum_{k=1}^{p-1} \frac{1}{p-k}$ puis montrer qu'il existe $V \in \mathbb{N}$ tel que $2S_{p-1} = \dfrac{pV}{(p-1)!}$.

Il s'agit de faire un changement de variable $h = p-k \Leftrightarrow p-h$. On a $k = 1 \iff h = p-1$ et $k = p-1 \iff h = 1$

$$\boxed{S_{p-1} = \sum_{k=1}^{p-1} \frac{1}{k} = \sum_{h=1}^{p-1} \frac{1}{p-h}}$$

Et donc, en additionnant deux fois cette même somme (avec deux écritures différentes) :

$$2S_{p-1} = \sum_{k=1}^{p-1} \frac{1}{k} + \sum_{k=1}^{p-1} \frac{1}{p-k} = \sum_{k=1}^{p-1} \frac{(p-k)+k}{k(p-k)} = p \sum_{k=1}^{p-1} \frac{1}{k(p-k)}$$

Puis, comme pour tout $k \in [\![1, p-1]\!]$, k et $p-k$ sont dans le produit qui définit $(p-1)!$, il existe $a_p \in \mathbb{N}$ tel que $(p-1)! = a_p \times k(p-k)$.

$$2S_{p-1} = p \sum_{k=1}^{p-1} \frac{a_p}{(p-1)!} = \frac{p}{(p-1)!} \underbrace{\sum_{k=1}^{p-1} a_k}_{=V}$$

$$\boxed{\text{Il existe } V \in \mathbb{N} \text{ tel que } 2S_{p-1} = \frac{pV}{(p-1)!}.}$$

(b) En déduire que p divise A_p et $p \wedge B_p = 1$ (résultat dû à Waring (1782)).

Ainsi $pV = 2S_{p-1}(p-1)!$ donc $pB_pV = 2A_p(p-1)!$.
Donc $p | 2A_p(p-1)!$ Or $p \wedge k = 1$, pour tout $k \in [\![1, p-1]\!]$. Donc d'après un corollaire du lemme de Gauss : $p \wedge 2(p-1)! = 1$.
Puis d'après le lemme de Gauss :

$$\boxed{p \wedge A_p = 1 \text{ et donc } p \wedge B_p = 1}$$

sinon la fraction $\dfrac{A_p}{B_p}$ ne serait pas irréductible.

III.3. Montrer que, pour tout $s \in [\![1, p-1]\!]$,

$$\frac{1}{1-\frac{p}{s}} \equiv_{\mathbb{Q}} \left(1+\frac{p}{s}\right) \ [p^2]$$

et en déduire que

$$S_{p-1} \equiv_{\mathbb{Q}} -\sum_{s=1}^{p-1} \frac{1}{s}\left(1+\frac{p}{s}\right) \ [p^2]$$

puis

$$2S_{p-1} \equiv_{\mathbb{Q}} -p\sum_{s=1}^{p-1} \frac{1}{s^2} \ [p^2]$$

Soit $s \in [\![1, p-1]\!]$.

$$\frac{1}{1-\frac{p}{s}} - \left(1+\frac{p}{s}\right) = \frac{s}{s-p} - \frac{s+p}{s} = \frac{s^2-(s^2-p^2)}{s(s-p)} = \frac{p^2}{s(s-p)}$$

Or on obtient ici la fraction irréductible car si $\delta = p^2 \wedge s(s-p)$,
alors $\delta | p^2$ donc $\delta | p$ et donc $\delta = 1$ ou $\delta = p$;
cette dernière hypothèse est impossible car $p | s(s-p)$ calors que s et $s-p \in [\![1, p-1]\!]$ et p premier.

Donc $p^2 = N\left(\frac{1}{1-\frac{p}{s}} - \left(1+\frac{p}{s}\right)\right)$ et donc

$$\boxed{\frac{1}{1-\frac{p}{s}} \equiv_{\mathbb{Q}} \left(1+\frac{p}{s}\right) \ [p^2]}$$

Puis :

$$S_{p-1} = \sum_{s=1}^{p-1} \frac{1}{p-s} = \sum_{s=1}^{p-1} \frac{1}{s\left(\frac{p}{s}-1\right)} = \sum_{s=1}^{p-1} \frac{-1}{s} \frac{1}{1-\frac{p}{s}}$$

Puis par addition des congruences et la question précédente :

$$\boxed{S_{p-1} \equiv_{\mathbb{Q}} \sum_{s=1}^{p-1} \frac{-1}{s}\left(1+\frac{p}{s}\right) \quad [p^2]}$$

On additionne alors $S_{p-1} = \sum_{s=1}^{p-1} \frac{1}{s}$:

$$2S_{p-1} \equiv_{\mathbb{Q}} \frac{1}{s}\left(1-\left(1+\frac{p}{s}\right)\right) \equiv_{\mathbb{Q}} -p\sum_{s=1}^{p-1} \frac{1}{s^2} \quad [p^2]$$

III.4. Soit $k \in [\![1, p-1]\!]$ et $h = \mathcal{I}(k)$ où $\mathcal{I}$ est l'application définie dans la partie I (préliminaires).
Montrer que $\frac{1}{k} \equiv_{\mathbb{Q}} h \ [p]$ et $\frac{1}{k^2} \equiv_{\mathbb{Q}} h^2 \ [p]$.

On a vu que $h \times k \equiv 1 [p]$, donc $\frac{1}{k} - h = \frac{1-kh}{k}$.
Même si cette fraction n'est peut-être pas la fraction irréductible, on a $p \wedge k = 1$ ($k \in [\![1, p-1]\!]$), et $p | 1-kh$.
Donc en simplifiant numérateur et dénominateur de cette fraction par $\lambda = (1-kh) \wedge k$, on a toujours $p | N(\frac{1}{k} - h)$.

$$\boxed{\text{Ainsi } \frac{1}{k} \equiv_{\mathbb{Q}} h [p].}$$

De même $\frac{1}{k^2} - h^2 = \frac{1-k^2h^2}{k} = \frac{(1-kh)(1+kh)}{k}$.
Même si cette fraction n'est pas la fraction irréductible, on a $p \wedge k = 1$ ($k \in [\![1, p-1]\!]$), et $p | 1-kh$.
Donc en simplifiant cette fraction par $\lambda = (1-k^2h^2) \wedge k$, on a toujours $p | N(\frac{1}{k^2} - h^2)$.

$$\boxed{\text{Ainsi } \frac{1}{k^2} \equiv_{\mathbb{Q}} h^2 [p].}$$

III.5. Conclure en établissant que, si p est un nombre premier supérieur ou égal à 5, alors p^2 divise A_p. Ce résultat est connu sous le nom du théorème de Wolstenholme.

Supposons que p soit un nombre premier supérieur ou égal à 5.
D'après la question précédente, pour tout $s \in [\![1, p-1]\!]$, $\dfrac{1}{s^2} \equiv_{\mathbb{Q}} (\mathcal{I}(s))^2 [p]$.

Puis par bijectivité de $\mathcal{I}$ de $[\![1, p-1]\!]$ sur $[\![1, p-1]\!]$, $\displaystyle\sum_{s \in [\![1,p-1]\!]} \mathcal{I}(s)^2 = \sum_{k \in [\![1,p-1]\!]} k^2 = \frac{(p-1)p(2p-1)}{6}$.

Donc $\displaystyle\sum_{s=1}^{p-1} \frac{1}{s^2} \equiv_{\mathbb{Q}} 0[p]$ car $6 \wedge p = 1$ (à ne pas oublier !!) puisque $p \geqslant 5$.

Ainsi $p \displaystyle\sum_{s=1}^{p-1} \frac{1}{s^2} \equiv_{\mathbb{Q}} 0[p^2]$. Donc $2S_{p-1} \equiv_{\mathbb{Q}} 0[p^2]$. Donc :

$$\boxed{p^2 | A_p}$$

Anneau $\mathbb{Z}_\alpha$

Dans tout le problème, on considère le polynôme $P = X^2 + bX + c$, unitaire, à coefficients entiers (c'est-à-dire $(b, c) \in \mathbb{Z}^2$) et de discriminant $\Delta = b^2 - 4c < 0$.

I Structure d'anneau sur $\mathbb{Z}_\alpha$

I.1. P étant de degré 2, il est scindé dans $\mathbb{C}$ et admet donc deux racines (non nécessairement distinctes a priori) que l'on note α et β.

(a) Montrer que $\alpha + \beta$ et $\alpha \times \beta$ sont des nombres entiers dont on donnera les valeurs.

P est unitaire de degré 2 dans $\mathbb{C}[X]$ et scindé de racines α et β donc sa forme factorisée est

$$P = \underbrace{1}_{P \text{ unitaire}} \times (X - \alpha)(X - \beta) = X^2 - (\alpha + \beta)X + \alpha\beta$$

or $P = X^2 + bX + c$ et deux polynômes sont égaux si et seulement si ils ont les mêmes coefficients donc

$$\boxed{\alpha + \beta = -b \in \mathbb{Z} \text{ et } \alpha\beta = c \in \mathbb{Z}.}$$

(b) Prouver que $\beta = \overline{\alpha}$ et exprimer la valeur de $|\alpha|$ en fonction de c. (Pourquoi c est-il nécessairement positif ?)

P est à coefficients réels donc

$$\overline{P(\alpha)} = \overline{\alpha^2 + b\alpha + c} = \overline{\alpha^2} + \overline{b\alpha} + \overline{c} = \overline{\alpha}^2 + \overline{b}\overline{\alpha} + \overline{c} \underbrace{=}_{(b,c) \in \mathbb{R}^2} \overline{\alpha}^2 + b\overline{\alpha} + c = P(\overline{\alpha})$$

or α est racine de P donc $P(\overline{\alpha}) = \overline{P(\alpha)} = \overline{0} = 0$ donc $\overline{\alpha}$ est aussi racine de P.
De plus, le discriminant de P est strictement négatif donc P n'a aucune racine réelle,
donc $\alpha \neq \overline{\alpha}$, or P a deux racines qui sont α et β

$$\boxed{\text{donc } \beta = \overline{\alpha}.}$$

On en déduit, d'après la question précédente que $c = \alpha\beta = \alpha\overline{\alpha} = |\alpha|^2$

$$\boxed{\text{donc } c \geqslant 0,}$$

puis en prenant la racine carrée, puisque $|\alpha| \geqslant 0$,

$$\boxed{|\alpha| = \sqrt{c}.}$$

Rmq : on a vu que $c \geqslant 0$, si $c = 0$, alors $\Delta = b^2 - 4c = b^2 \geqslant 0$ ce qui est une contradiction donc $\boxed{c > 0.}$

On note $\mathbb{Z}_\alpha$ l'ensemble $\{p+\alpha q \mid (p,q)\in\mathbb{Z}^2\}$.

I.2. (a) Montrer que $(\mathbb{Z}_\alpha,+,\times)$ est un anneau commutatif.

⋆ $\mathbb{Z}_\alpha\subset\mathbb{C}$ et $(\mathbb{C},+,\times)$ est un anneau de référence (c'est même un corps !).

⋆ $1=\underbrace{1}_{\in\mathbb{Z}}+\underbrace{0}_{\in\mathbb{Z}}\times\alpha$ donc $\mathbb{Z}_\alpha\neq\emptyset$ et contient le neutre multiplicatif de l'anneau $\mathbb{C}$.

⋆ Soient $(z,z')\in\mathbb{Z}_\alpha^2$ fixés quelconques.
Il existe $(p,q,p',q')\in\mathbb{Z}^4$ tels que $z=p+\alpha q$ et $z=p'+\alpha q'$.
D'une part,

$$z-z'=\underbrace{(p-p')}_{\in\mathbb{Z}}+\alpha\underbrace{(q-q')}_{\in\mathbb{Z}}\quad\text{donc } z-z'\in\mathbb{Z}_\alpha.$$

D'autre part, en utilisant que α est racine de P (donc $\alpha^2+b\alpha+c=0\iff\alpha^2=-b\alpha-c$),

$$zz'=pp'+\alpha qp'+\alpha pq'+\alpha^2qq'=\underbrace{(pp'-cqq')}_{\substack{\in\mathbb{Z}\\ \text{car } c\in\mathbb{Z}}}+\alpha\underbrace{(qp'+pq'-bqq')}_{\substack{\in\mathbb{Z}\\ \text{car } b\in\mathbb{Z}}}\quad\text{donc } zz'\in\mathbb{Z}_\alpha.$$

Ainsi, $\mathbb{Z}_\alpha$ est un sous-anneau de l'anneau commutatif $(\mathbb{C},+,\times)$, donc un anneau commutatif pour les lois induites.

(b) Montrer que pour tout $(p,q,p',q')\in\mathbb{Z}^4$, on a l'équivalence : $\quad p+\alpha q=p'+\alpha q'\iff[p=p'\text{ et }q=q']$

⋆ Le sens réciproque de l'équivalence est immédiat : si $p=p'$ et $q=q'$, alors $p+\alpha q=p'+\alpha q'$.

⋆ Supposons que $p+\alpha q=p'+\alpha q'$.
En prenant la partie réelle et la partie imaginaire, on obtient, puisque $(p,q)\in\mathbb{R}^2$,

$$p+q\mathrm{Re}(\alpha)=p'+q'\mathrm{Re}(\alpha)\quad(*)\qquad\text{et}\qquad q\mathrm{Im}(\alpha)=q'\mathrm{Im}(\alpha)\quad(**)$$

La théorie du discriminant qui permet de calculer les racines complexes d'un trinôme du second degré à coefficients réels donne comme racines de P :

$$-\frac{b}{2}-i\frac{\sqrt{|\Delta|}}{2}\quad\text{et}\quad-\frac{b}{2}-i\frac{\sqrt{|\Delta|}}{2}$$

où $\Delta=b^2-4c<0$ donc $\sqrt{|\Delta|}\neq0$.

Puisque α est l'une de ces deux racines, $|\mathrm{Im}(\alpha)|=\dfrac{\sqrt{|\Delta|}}{2}$,
donc $\mathrm{Im}(\alpha)\neq0$ si bien que l'égalité $(**)$ donne $q=q'$ puis en reportant dans $(*)$ on obtient $p=p'$.

Ainsi, $p+\alpha q=p'+\alpha q'\iff[p=p'\text{ et }q=q'.$

(c) On note $G_\alpha=\{z\in\mathbb{Z}_\alpha\mid\exists\,z'\in\mathbb{Z}_\alpha,\text{ tel que }z\times z'=1\}$. Pourquoi G_α est-il un groupe (on précisera vis-à-vis de quelle loi) ?

L'anneau $\mathbb{Z}_\alpha$ étant commutatif, la définition de l'ensemble G_α montre qu'il s'agit des éléments de cet anneau symétrisables pour la loi multiplicative de l'anneau (aussi appelés éléments inversibles de l'anneau), or nous savons que les éléments inversibles d'un anneau constituent, pour la loi multiplicative, un groupe.

Ainsi, $(G_\alpha,\times)$ est un groupe.

II Suite récurrente

On considère dans cette partie la matrice $N=\begin{pmatrix}0&1\\-c&-b\end{pmatrix}$.

II.1. Montrer que $P(N)=0$.

Le calcul donne $N^2=\begin{pmatrix}-c&-b\\bc&-c+b^2\end{pmatrix}$ donc

$$P(N)=N^2+bN+cI_2=\begin{pmatrix}-c&-b\\bc&-c+b^2\end{pmatrix}+\begin{pmatrix}0&b\\-bc&-b^2\end{pmatrix}+\begin{pmatrix}c&0\\0&c\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$$

$\boxed{\text{Ainsi, } P(N) = 0.}$

II.2. Soit $m \in \mathbb{N}$. On note respectivement Q_m et R_m le quotient et le reste de la division euclidienne de X^m par P dans $\mathbb{C}[X]$.

(a) Montrer que $R_m = \dfrac{\alpha^m - \overline{\alpha}^m}{\alpha - \overline{\alpha}} X + \dfrac{\alpha\overline{\alpha}^m - \overline{\alpha}\alpha^m}{\alpha - \overline{\alpha}}$.

Compte tenu de la définition de Q_m et R_m :

$$X^m = PQ_m + R_m \quad \text{et} \quad \deg R_m < \deg P = 2$$

Par conséquent, R_m est de degré inférieur ou égal à 1 si bien que

$$\exists (a_m, b_m) \in \mathbb{C}^2 \ : \ R_m = a_m X + b_m$$

d'où

$$X^m = PQ_m + a_m X + b_m$$

Prenons l'image de la relation ci-dessus par les morphismes d'évaluation en α et en $\overline{\alpha}$ pour obtenir

$$\left\{ \begin{array}{rcl} \alpha^m & = & P(\alpha)Q_m(\alpha) + a_m\alpha + b_m \\ \overline{\alpha}^m & = & P(\overline{\alpha})Q_m(\overline{\alpha}) + a_m\overline{\alpha} + b_m \end{array} \right. \underbrace{\iff}_{\alpha \text{ et } \overline{\alpha} \text{ sont racines de } P} \left\{ \begin{array}{rcl} \alpha^m & = & a_m\alpha + b_m \quad (1) \\ \overline{\alpha}^m & = & a_m\overline{\alpha} + b_m \quad (2) \end{array} \right.$$

En effectuant la différence $(1) - (2)$ des deux équations, on obtient

$$(\alpha - \overline{\alpha})a_m = \alpha^m - \overline{\alpha}^m$$

or $\alpha \neq \overline{\alpha}$ (car α est complexe non réelle) donc $a_m = \dfrac{\alpha^m - \overline{\alpha}^m}{\alpha - \overline{\alpha}}$. En effectuant la combinaison $\overline{\alpha}(1) - \alpha(2)$ des deux équations, on obtient

$$\overline{\alpha}\alpha^m - \alpha\overline{\alpha}^m = (\overline{\alpha} - \alpha)b_m$$

d'où $b_m = \dfrac{\alpha\overline{\alpha}^m - \overline{\alpha}\alpha^m}{\alpha - \overline{\alpha}}$.

$$\boxed{\text{Ainsi, } R_m = \frac{\alpha^m - \overline{\alpha}^m}{\alpha - \overline{\alpha}} X + \frac{\alpha\overline{\alpha}^m - \overline{\alpha}\alpha^m}{\alpha - \overline{\alpha}}.}$$

(b) En déduire une expression de N^m en fonction de N, I_2, α, $\overline{\alpha}$ et m.

Prenons l'image de la relation polynomiale dans $\mathbb{C}[X]$:

$$X^m = PQ_m + a_m X + b_m$$

par le morphisme d'évaluation en N (morphisme d'anneaux de l'anneau $\mathbb{C}[X]$ dans l'anneau $\mathcal{M}_2(\mathbb{C})$) :

$$N^m = \underbrace{P(N)}_{= 0 \text{ quest. II.1}} Q_m(N) + a_m N + b_m I_2$$

$$\boxed{\text{Ainsi, } N^m = \frac{\alpha^m - \overline{\alpha}^m}{\alpha - \overline{\alpha}} N + \frac{\alpha\overline{\alpha}^m - \overline{\alpha}\alpha^m}{\alpha - \overline{\alpha}} I_2.}$$

II.3. L'expression précédente est-elle vraie pour $m \in \mathbb{Z}$?

- La relation $P(N) = 0$, qui est $N^2 + bN + cI_2 = 0$ donne $N(N + bI_2) = -cI_2$ d'où, puisque $c \neq 0$ (car $c > 0$),

$$N\left(-\frac{1}{c}N - \frac{b}{c}I_2\right) = I_2$$

or les matrices N et $\left(-\dfrac{1}{c}N - \dfrac{b}{c}I_2\right)$ commutent donc

$$\boxed{N \text{ est inversible et } N^{-1} = -\frac{1}{c}N - \frac{b}{c}I_2.}$$

- Prouvons le résultat par récurrence en considérant la propriété $\mathcal{P}(\cdot)$ définie pour tout $n \in \mathbb{N}$ par

$$\mathcal{P}(n) \ : \ \text{« } N^{-n} = \frac{\alpha^{-n} - \overline{\alpha}^{-n}}{\alpha - \overline{\alpha}} N + \frac{\alpha\overline{\alpha}^{-n} - \overline{\alpha}\alpha^{-n}}{\alpha - \overline{\alpha}} I_2 \text{ ».}$$

⋆ Pour $n = 0$, la formule établie dans la question précédente est valide donc $\mathcal{P}(0)$ est vraie.

⋆ Pour $n = 1$, d'une part $N^{-1} = -\dfrac{1}{c}N - \dfrac{b}{c}I_2$,
et d'autre part

$$\frac{\alpha^{-1} - \overline{\alpha}^{-1}}{\alpha - \overline{\alpha}} = \frac{-1}{\alpha\overline{\alpha}} \frac{\alpha^1 - \overline{\alpha}^1}{\alpha - \overline{\alpha}} = -\frac{1}{\alpha\overline{\alpha}} = -\frac{1}{c} \quad \text{et} \quad \frac{\alpha\overline{\alpha}^{-1} - \overline{\alpha}\alpha^{-1}}{\alpha - \overline{\alpha}} = \frac{1}{\alpha\overline{\alpha}} \frac{\alpha^2 - \overline{\alpha}^2}{\alpha - \overline{\alpha}} = \frac{1}{c}(\alpha + \overline{\alpha}) = -\frac{b}{c}$$

si bien que

$$\frac{\alpha^{-1} - \overline{\alpha}^{-1}}{\alpha - \overline{\alpha}} N + \frac{\alpha\overline{\alpha}^{-1} - \overline{\alpha}\alpha^{-1}}{\alpha - \overline{\alpha}} I_2 = -\frac{1}{c}N - \frac{b}{c}I_2 = N^{-1}$$

donc $\mathcal{P}(1)$ est vraie.

⋆ Soit $n \in \mathbb{N}$ fixé quelconque tel que $\mathcal{P}(n)$ est vraie.
Posons $\lambda = \dfrac{\alpha^{-n} - \overline{\alpha}^{-n}}{\alpha - \overline{\alpha}}$ et $\mu = \dfrac{\alpha\overline{\alpha}^{-n} - \overline{\alpha}\alpha^{-n}}{\alpha - \overline{\alpha}}$ de sorte que la véracité de $\mathcal{P}(n)$ donne $N^{-n} = \lambda N + \mu I_2$.
Alors, sachant que $N^{-1} = -\dfrac{1}{c}N - \dfrac{b}{c}I_2$,

$$N^{-(n+1)} = N^{-1} \times N^{-n} = \left(-\frac{1}{c}N - \frac{b}{c}I_2\right)(\lambda N + \mu I_2) = -\frac{\lambda}{c}N^2 + \left(-\frac{\mu}{c} - \frac{\lambda b}{c}\right)N - \frac{b}{c}\mu I_2$$

or $N^2 = -bN - cI_2$ donc

$$N^{-(n+1)} = \left(-\frac{\mu}{c} - \frac{\lambda b}{c} + \frac{\lambda b}{c}\right)N + \left(-\frac{b}{c}\mu + \lambda\right)I_2 = -\frac{\mu}{c}N + \left(\lambda - \frac{b\mu}{c}\right)I_2$$

D'une part, puisque $c = \alpha\overline{\alpha}$,

$$-\frac{\mu}{c} = -\frac{1}{\alpha\overline{\alpha}} \frac{\alpha\overline{\alpha}^{-n} - \overline{\alpha}\alpha^{-n}}{\alpha - \overline{\alpha}} = -\frac{\overline{\alpha}^{-n-1} - \alpha^{-n-1}}{\alpha - \overline{\alpha}} = \frac{\alpha^{-(n+1)} - \overline{\alpha}^{-(n+1)}}{\alpha - \overline{\alpha}}$$

et d'autre part, puisque $-b = \alpha + \overline{\alpha}$,

$$\lambda - \frac{b\mu}{c} = \frac{\alpha^{-n} - \overline{\alpha}^{-n}}{\alpha - \overline{\alpha}} + \frac{\frac{\alpha+\overline{\alpha}}{\alpha\overline{\alpha}}(\alpha\overline{\alpha}^{-n} - \overline{\alpha}\alpha^{-n})}{\alpha - \overline{\alpha}} = \frac{\alpha^{-n} - \overline{\alpha}^{-n} + (\alpha + \overline{\alpha})(\overline{\alpha}^{-n-1} - \alpha^{-n-1})}{\alpha - \overline{\alpha}} = \frac{\alpha\overline{\alpha}^{-n-1} - \overline{\alpha}\alpha^{-n-1}}{\alpha - \overline{\alpha}}$$

donc

$$N^{-(n+1)} = -\frac{\mu}{c}N + \left(\lambda - \frac{b\mu}{c}\right)I_2 = \frac{\alpha^{-(n+1)} - \overline{\alpha}^{-(n+1)}}{\alpha - \overline{\alpha}} N + \frac{\alpha\overline{\alpha}^{-(n+1)} - \overline{\alpha}\alpha^{-(n+1)}}{\alpha - \overline{\alpha}} I_2$$

ce qui établit $\mathcal{P}(n+1)$.

Ainsi, l'expression précédente est vraie pour $m \in \mathbb{Z}$.

On considère la suite u définie par $(u_0, u_1) \in \mathbb{Z}^2$ et, pour tout $n \in \mathbb{N}$,

$$u_{n+2} = -bu_{n+1} - cu_n$$

On pose, pour tout $n \in \mathbb{N}$, $X_n = \begin{pmatrix} u_n \\ u_{n+1} \end{pmatrix}$.

II.4. (a) Montrer que, pour tout $n \in \mathbb{N}$, $X_n = N^n X_0$.

Considérons la propriété $\mathcal{P}(\cdot)$ définie pour tout $n \in \mathbb{N}$ par

$$\mathcal{P}(n) \ : \ \text{« } X_n = N^n X_0 \text{ ».}$$

⋆ Par définition, $N^0 = I_2$ donc $N^0 X_0 = X_0$ si bien que $\mathcal{P}(0)$ est vraie.

⋆ Soit $n \in \mathbb{N}$ fixé quelconque tel que $\mathcal{P}(n)$ est vraie.
Par associativité du produit matriciel,

$$N^{n+1}X_0 = \underbrace{N(N^nX_0) = NX_n}_{\mathcal{P}(n) \text{ vraie}} = \begin{pmatrix} 0 & 1 \\ -c & -b \end{pmatrix} \begin{pmatrix} u_n \\ u_{n+1} \end{pmatrix} = \begin{pmatrix} 0 \times u_n + 1 \times u_{n+1} \\ -c \times u_n - b \times u_{n+1} \end{pmatrix} = \begin{pmatrix} u_{n+1} \\ u_{n+2} \end{pmatrix} = X_{n+1}$$

donc $\mathcal{P}(n+1)$ est vraie.

$$\boxed{\text{Ainsi, pour tout } n \in \mathbb{N},\ X_n = N^n X_0.}$$

(b) En déduire, pour tout $n \in \mathbb{N}$, une expression explicite de u_n en fonction de α, $\overline{\alpha}$, u_0, u_1 et n.

Soit $n \in \mathbb{N}$ fixé quelconque.
Détaillons l'expression de N^n qui se déduit de la formule établie dans la question II.2(b) :

$$N^n = \frac{\alpha^n - \overline{\alpha}^n}{\alpha - \overline{\alpha}} \begin{pmatrix} 0 & 1 \\ -c & -b \end{pmatrix} + \frac{\alpha\overline{\alpha}^n - \overline{\alpha}\alpha^n}{\alpha - \overline{\alpha}} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \dfrac{\alpha\overline{\alpha}^n - \overline{\alpha}\alpha^n}{\alpha - \overline{\alpha}} & \dfrac{\alpha^n - \overline{\alpha}^n}{\alpha - \overline{\alpha}} \\ -c\dfrac{\alpha^n - \overline{\alpha}^n}{\alpha - \overline{\alpha}} & \dfrac{\alpha\overline{\alpha}^n - \overline{\alpha}\alpha^n}{\alpha - \overline{\alpha}} - b\dfrac{\alpha^n - \overline{\alpha}^n}{\alpha - \overline{\alpha}} \end{pmatrix}$$

donc

$$\begin{pmatrix} u_n \\ u_{n+1} \end{pmatrix} = X_n = N^n X_0 = \begin{pmatrix} \dfrac{\alpha\overline{\alpha}^n - \overline{\alpha}\alpha^n}{\alpha - \overline{\alpha}} & \dfrac{\alpha^n - \overline{\alpha}^n}{\alpha - \overline{\alpha}} \\ -c\dfrac{\alpha^n - \overline{\alpha}^n}{\alpha - \overline{\alpha}} & \dfrac{\alpha\overline{\alpha}^n - \overline{\alpha}\alpha^n}{\alpha - \overline{\alpha}} - b\dfrac{\alpha^n - \overline{\alpha}^n}{\alpha - \overline{\alpha}} \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \end{pmatrix} = \begin{pmatrix} \dfrac{\alpha\overline{\alpha}^n - \overline{\alpha}\alpha^n}{\alpha - \overline{\alpha}} u_0 + \dfrac{\alpha^n - \overline{\alpha}^n}{\alpha - \overline{\alpha}} u_1 \\ \cdots \end{pmatrix}$$

$$\boxed{\text{Ainsi, } \forall n \in \mathbb{N},\ u_n = \frac{\alpha\overline{\alpha}^n - \overline{\alpha}\alpha^n}{\alpha - \overline{\alpha}} u_0 + \frac{\alpha^n - \overline{\alpha}^n}{\alpha - \overline{\alpha}} u_1.}$$

II.5. Étude d'une suite particulière. Nous considérons désormais la suite u définie par

$$u_0 = 0\ ,\ u_1 = 1\ ,\ \forall n \in \mathbb{N}\ ,\ u_{n+2} = -2u_{n+1} - 3u_n$$

ce qui correspond au cas particulier de l'étude précédente pour $b = 2$ et $c = 3$.

(a) Montrer que, pour tout $n \in \mathbb{N}$, $u_n = \dfrac{1}{\sqrt{2}} \mathrm{Im}\left((-1 + i\sqrt{2})^n\right)$.

Appliquons la formule établie dans la question II.4(b) pour

$$\alpha = -1 + i\sqrt{2}\ ,\ u_0 = 0\ ,\ u_1 = 1$$

ce qui est possible car le discriminant de $P = X^2 + 2X + 3$ est $\Delta = -8 = (2i\sqrt{2})^2$ si bien que $-1 + i\sqrt{2}$ en est une racine d'où

$$\forall n \in \mathbb{N}\ ,\ u_n = \frac{\overbrace{\alpha^m - \overline{\alpha}^m}^{= 2i\mathrm{Im}(\alpha^m)}}{(-1 + i\sqrt{2}) - (-1 - i\sqrt{2})} = \frac{2i\mathrm{Im}(\alpha^m)}{2i\sqrt{2}} = \frac{1}{\sqrt{2}} \mathrm{Im}\left((-1 + i\sqrt{2})^n\right)$$

$$\boxed{\text{Ainsi, } \forall n \in \mathbb{N},\ u_n = \frac{1}{\sqrt{2}} \mathrm{Im}\left((-1 + i\sqrt{2})^n\right).}$$

(b) En déduire que, pour tout $n \in \mathbb{N}$, $u_n = \displaystyle\sum_{\substack{k=1 \\ k \equiv 1\ [2]}}^{n} \binom{n}{k} (-1)^{n-k} (-1)^{\frac{k-1}{2}} \sqrt{2}^{k-1}$.

En développant avec la formule du binôme de Newton,

$$\begin{aligned}
(-1 + i\sqrt{2})^n &= \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} i^k \sqrt{2}^k \\
&= \sum_{\substack{k=0 \\ k \equiv 0\ [2]}}^{n} \binom{n}{k} (-1)^{n-k} i^k \sqrt{2}^k + \underbrace{\sum_{\substack{k=0 \\ k \equiv 1\ [2]}}^{n} \binom{n}{k} (-1)^{n-k} i^k \sqrt{2}^k}_{= \displaystyle\sum_{\substack{k=1 \\ k \equiv 1\ [2]}}^{n} \binom{n}{k} (-1)^{n-k} i\sqrt{2} \times i^{k-1} \sqrt{2}^{k-1} \text{ car } k=0 \text{ est pair donc exclu}} \\
&= \underbrace{\sum_{\substack{k=0 \\ k \equiv 0\ [2]}}^{n} \binom{n}{k} (-1)^{n-k} (i^2)^{\frac{k}{2}} \sqrt{2}^{k-1}}_{\in \mathbb{R} \text{ car } i^2 = -1} + i\sqrt{2} \underbrace{\sum_{\substack{k=1 \\ k \equiv 1\ [2]}}^{n} \binom{n}{k} (-1)^{n-k} (i^2)^{\frac{k-1}{2}} (\sqrt{2})^{k-1}}_{\text{ce qui a un sens car } k \equiv 1[2] \Rightarrow \frac{k-1}{2} \in \mathbb{Z}}
\end{aligned}$$

donc, d'après la question précédente,

$$\begin{aligned} u_n &= \frac{1}{\sqrt{2}}\mathrm{Im}\left((-1+i\sqrt{2})^n\right) \\ &= \frac{1}{\sqrt{2}} \times \sqrt{2} \sum_{\substack{k=1 \\ k\equiv 1\ [2]}}^{n} \binom{n}{k} (-1)^{n-k}(-1)^{\frac{k-1}{2}}\sqrt{2}^{k-1} \end{aligned}$$

$$\boxed{\text{Ainsi, } \forall n \in \mathbb{N},\ u_n = \sum_{\substack{k=1 \\ k\equiv 1\ [2]}}^{n} \binom{n}{k} (-1)^{n-k}(-1)^{\frac{k-1}{2}}\sqrt{2}^{k-1}.}$$

(c) Étude des termes d'indices un nombre premier. Soit p un nombre premier supérieur ou égal à 3.

i. Établir que $u_p \equiv (-2)^{\frac{p-1}{2}}\ [p]$. On justifiera soigneusement tout résultat utilisé.

D'après l'expression obtenue dans la question précédente appliquée pour $n \leftarrow p$,

$$\begin{aligned} u_p &= \sum_{\substack{k=1 \\ k\equiv 1\ [2]}}^{p} \binom{p}{k} (-1)^{p-k}(-1)^{\frac{k-1}{2}}2^{\frac{k-1}{2}} \quad \text{car } \sqrt{2}^{k-1} = 2^{\frac{k-1}{2}} \\ &= \binom{p}{p}(-1)^{p-p}(-1)^{\frac{p-1}{2}}2^{\frac{p-1}{2}} + \sum_{\substack{k=1 \\ k\equiv 1\ [2]}}^{p-1} \binom{p}{k} (-1)^{p-k}(-1)^{\frac{k-1}{2}}2^{\frac{k-1}{2}} \quad \text{car } p \text{ premier} \geqslant 3 \text{ donc } p \equiv 1\ [2] \\ &= (-2)^{\frac{p-1}{2}} + \sum_{\substack{k=1 \\ k\equiv 1\ [2]}}^{p-1} \underbrace{\binom{p}{k}}_{\equiv 0\ [p]} \underbrace{(-1)^{p-k}(-1)^{\frac{k-1}{2}}2^{\frac{k-1}{2}}}_{\in \mathbb{Z}} \end{aligned}$$

En effet, pour tout $i \in [\![1, p-1]\!]$, $p \mid \binom{p}{i}$ car

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} = \frac{p}{i} \times \frac{(p-1)!}{(i-1)!(p-1)-(i-1))!} = \frac{p}{i}\binom{p-1}{i-1}$$

donc $p\underbrace{\binom{p-1}{i-1}}_{\in \mathbb{Z}} = i\underbrace{\binom{p}{i}}_{\in \mathbb{Z}}$ donc $p \mid i\binom{p}{i}$,

or $p \wedge i = 1$ (car p premier et p ne divise pas i car $i \in [\![1, p-1]\!]$),

donc le théorème de Gauss permet d'affirmer que $p \mid \binom{p}{i}$.

$$\boxed{\text{Ainsi, } u_p \equiv (-2)^{\frac{p-1}{2}}\ [p].}$$

ii. Montrer que $\overline{u_p}$ est une racine de $X^2 - 1$ dans $\mathbb{Z}/p\mathbb{Z}$. Quelle est la forme factorisée de $X^2 - 1$ dans le corps $\mathbb{Z}/p\mathbb{Z}$? Que peut-on en déduire concernant la congruence de u_p modulo p ?

- Puisque, d'après la question précédente, $u_p \equiv (-2)^{\frac{p-1}{2}}\ [p]$, on a

$$u_p^2 \equiv ((-2)^{\frac{p-1}{2}})^2\ [p]\ \equiv (-2)^{p-1}\ [p]$$

or p est premier et $p \wedge (-2) = p \wedge 2 = 1$ (car deux nombres premiers distincts sont premiers entre eux) donc le petit théorème de Fermat donne

$$(-2)^{p-1} \equiv 1\ [p]$$

donc, par transitivité de la congruence modulo p,

$$u_p^2 \equiv 1\ [p] \quad \text{ce qui se reformule de manière équivalente en} \quad \overline{u_p}^2 = 1$$

$$\boxed{\text{Ainsi, } \overline{u_p} \text{ est une racine de } X^2 - 1 \text{ dans } \mathbb{Z}/p\mathbb{Z}.}$$

- ⋆ $1^2 \equiv 1\ [p]$ et $(p-1)^2 \equiv (-1)^2\ [p] \equiv (-1)^2 \equiv 1\ [p]$ donc $\overline{1}$ et $\overline{p-1}$ sont deux racines distinctes (car $p \geqslant 3$ donc $0 \leqslant 1 < p-1$ donc 1 et $p-1$ sont deux représentants distincts dans le système $[\![0, p-1]\!]$ de représentants des classes modulo p) de X^2-1 dans $\mathbb{Z}/p\mathbb{Z}$,
  ⋆ X^2-1 est de degré 2,
  ⋆ X^2-1 est unitaire,
  donc X^2-1 n'a pas d'autres racines, ces deux racines sont simples et sa forme factorisée est

$$\boxed{X^2-1 = (X-\overline{1})(X-\overline{p-1}) = (X-1)(X+1)}$$

- D'après les deux points précédents, $\overline{u_p}$ est une racine de X^2-1 dans $\mathbb{Z}/p\mathbb{Z}$ et les racines de X^2-1 dans ce corps sont $\{\overline{1}, -\overline{1}\}$ donc

$$\boxed{u_p \equiv 1\ [p] \text{ ou } u_p \equiv -1\ [p]}$$

(d) Étude des termes d'indices une puissance de 2. Notons v la suite définie par

$$v_0 = 1\ ,\ v_1 = -1\ ,\ \forall n \in \mathbb{N}\ ,\ v_{n+2} = -2v_{n+1} - 3v_n$$

ce qui correspond, comme pour la suite u, au cas particulier de l'étude précédente pour $b=2$ et $c=3$.

i. Montrer que $\forall n \in \mathbb{N}\ ,\ v_n = \dfrac{\alpha^n + \overline{\alpha}^n}{2}$ où α est une racine du trinôme X^2+2X+3.

Appliquons la formule établie dans la question II.4(b) pour

$$\alpha = -1 + i\sqrt{2}\ ,\ u_0 = 1\ ,\ u_1 = -1$$

$$\begin{aligned}
\forall n \in \mathbb{N}\ ,\ v_n &= \frac{\alpha\overline{\alpha}^n - \overline{\alpha}\alpha^n}{\alpha - \overline{\alpha}} - \frac{\alpha^n - \overline{\alpha}^n}{\alpha - \overline{\alpha}} \\
&= \frac{\alpha\overline{\alpha}^n - \overline{\alpha}\alpha^n - \alpha^n + \overline{\alpha}^n}{\alpha - \overline{\alpha}} \\
&= \frac{(\alpha+1)\overline{\alpha}^n - (\overline{\alpha}+1)\alpha^n}{\alpha - \overline{\alpha}} \quad \text{or } \alpha+1 = i\sqrt{2},\ \overline{\alpha}+1 = -i\sqrt{2} \text{ et } \alpha - \overline{\alpha} = 2i\mathrm{Im}(\alpha) = 2i\sqrt{2} \\
&= \frac{\overline{\alpha}^n + \alpha^n}{2}
\end{aligned}$$

$$\boxed{\text{Ainsi, } \forall n \in \mathbb{N},\ v_n = \frac{\alpha^n + \overline{\alpha}^n}{2}.}$$

---

ii. En reconnaissant une identité remarquable, déterminer, pour tout $n \in \mathbb{N}$, une relation simple entre $u_{2^{n+1}}$, u_{2^n} et v_{2^n}.

Rappelons l'expression explicite de u_n en fonction de n et α qui se déduit directement de la question II.4(b) :

$$\forall n \in \mathbb{N}\ ,\ u_n = \frac{\alpha^n - \overline{\alpha}^n}{\alpha - \overline{\alpha}}$$

Observons alors que, pour tout $n \in \mathbb{N}$,

$$u_{2^{n+1}} = \frac{\alpha^{2^{n+1}} - \overline{\alpha}^{2^{n+1}}}{\alpha - \overline{\alpha}} = \frac{(\alpha^{2^n})^2 - (\overline{\alpha}^{2^n})^2}{\alpha - \overline{\alpha}} = \frac{(\alpha^{2^n} - \overline{\alpha}^{2^n})(\alpha^{2^n} + \overline{\alpha}^{2^n})}{\alpha - \overline{\alpha}} = u_{2^n} \times 2v_{2^n}$$

$$\boxed{\text{Ainsi, } \forall n \in \mathbb{N},\ u_{2^{n+1}} = u_{2^n} \times 2v_{2^n}.}$$

---

iii. En déduire, par récurrence, que $u_{2^n} \equiv 0\ [2^n]$ pour tout $n \in \mathbb{N}$.

Notons tout d'abord qu'une récurrence immédiate à partir de la propriété de récurrence définie pour tout $n \in \mathbb{N}$ par

$$\mathcal{Q}(n)\ :\ \text{« } u_n \in \mathbb{Z} \text{ et } u_{n+1} \in \mathbb{Z},\ v_n \in \mathbb{Z} \text{ et } v_{n+1} \in \mathbb{Z} \text{ ».}$$

permet d'une part de justifier que la question a bien un sens (car la suite u est à valeurs entières) et d'autre part que la suite v est également à valeurs entières.
Considérons la propriété $\mathcal{P}(\cdot)$ définie pour tout $n \in \mathbb{N}$ par

$$\mathcal{P}(n)\ :\ \text{« } u_{2^n} \equiv 0\ [2^n] \text{ ».}$$

⋆ $u_1 = 1$ donc $u_{2^0} \equiv 1\ [1] \equiv 0\ [1] \equiv 0\ [2^0]$ donc $\mathcal{P}(0)$ est vraie.
⋆ (*pour le plaisir, inutile dans une rédaction définitive*)
$u_2 = -2u_1 - 3u_0 = -2$ donc $u_2 \equiv -2\ [2] \equiv 0\ [2] \equiv 0\ [2^1]$ donc $\mathcal{P}(1)$ est vraie.
⋆ Soit $n \in \mathbb{N}$ fixé quelconque tel que $\mathcal{P}(n)$ est vraie.
La véracité de $\mathcal{P}(n)$ donne $2^n \mid u_{2^n}$,
donc $2 \times 2^n \mid 2u_{2^n}$,
si bien que $2^{n+1} \mid u_{2^n} \times 2v_{2^n}$ car $v_{2^n} \in \mathbb{Z}$,
or, en reprenant la relation établie dans la question précédente $u_{2^{n+1}} = u_{2^n} \times 2v_{2^n}$,
donc $2^{n+1} \mid u_{2^{n+1}}$ ce qui prouve $\mathcal{P}(n+1)$.
Ainsi, $\forall n \in \mathbb{N},\ u_{2^n} \equiv 0\ [2^n]$.

III Corps $\mathbb{Q}[N]$

Cette partie est consacrée à l'étude de l'ensemble $\mathbb{Q}[N] = \{Q(N) \mid Q \in \mathbb{Q}[X]\}$ où N est la matrice introduite dans la partie II.

III.1. Montrer que $\mathbb{Q}[N] = \{sN + tI_2 \mid (s,t) \in \mathbb{Q}^2\}$.
Pour l'inclusion directe, on pourra utiliser le résultat de la question II.2.

⋆ Soient $(s,t) \in \mathbb{Q}^2$ fixés quelconques.
Posons $Q = sX + t \in \mathbb{Q}[X]$.
Par définition de $\mathbb{Q}[N]$, $sN + tI_2 = Q(N) \in \mathbb{Q}[N]$.
Par conséquent, $\{sN + tI_2 \mid (s,t) \in \mathbb{Q}^2\} \subset \mathbb{Q}[N]$.
⋆ Soit $M \in \mathbb{Q}[N]$ fixé quelconque.
Il existe $Q \in \mathbb{Q}[X] : M = Q(N)$.
— **Méthode 1.** Nous avons vu dans la question II.2 que toutes les puissances entières de N s'expriment comme des combinaisons linéaires de I_2 et N. Par conséquent, puisque M est une combinaison linéaire de puissances de N, alors M est une combinaison linéaire de combinaisons linéaires de I_2 et N, donc c'est une combinaison linéaire de I_2 et N.
L'argument proposé ci-dessus est incomplet : il ne faut pas seulement justifier que M est une combinaison linéaire de I_2 et N, il faut aussi prouver que les coefficients d'une telle combinaison linéaire peuvent être choisis rationnels et compte tenu de la formule établie dans la question II.2, cela n'a rien d'évident : les coefficients dont l'expression est explicitée sont a priori complexes. Néanmoins, dans la question II.2, la division euclidienne de X^m par P, qu'elle soit effectuée dans $\mathbb{C}[X]$ ou dans $\mathbb{Q}[X]$ possède le même reste et le même quotient. En effet, notons respectivement $\hat{Q_m}$ et $\hat{R_m}$ le quotient et le reste de la division euclidienne de X^m par P dans $\mathbb{Q}[X]$. Alors

$$(\hat{Q_m}, \hat{R_m}) \in \mathbb{Q}[X]^2\ ,\ X^m = \hat{Q_m}P + \hat{R_m} \quad \text{et} \quad \deg \hat{R_m} < \deg P$$

donc, par unicité du quotient et du reste de la division euclidienne de X^m par P dans $\mathbb{C}[X]$,

$$Q_m = \hat{Q_m} \quad \text{et} \quad R_m = \hat{R_m}$$

Ainsi, $R_m \in \mathbb{Q}[X]$ si bien que les coefficients des expressions des puissances de N écrites comme combinaisons linéaires de I_2 et N sont rationnels de sorte que M peut s'obtenir comme une combinaison linéaire à coefficients rationnels de I_2 et N.
— **Méthode 2.**
Effectuons la division euclidienne de Q par P dans $\mathbb{Q}[X]$:

$$\exists (A,B) \in \mathbb{Q}[X]^2\ :\ Q = AP + B \quad \text{et} \quad \deg B < \deg P = 2$$

Puisque $\deg B \leqslant 1$, $\exists (s,t) \in \mathbb{Q}^2\ :\ B = sX + t$ de sorte qu'en prenant l'image de l'égalité polynomiale

$$Q = AP + sX + t$$

par le morphisme d'évaluation en N (morphisme d'anneaux de l'anneau $\mathbb{Q}[X]$ dans l'anneau $\mathcal{M}_2(\mathbb{Q})$) :

$$Q(N) = A(N) \times \underbrace{P(N)}_{=0} + sN + tI_2$$

donc $Q(N) = sN + tI_2$.
Par conséquent, $\mathbb{Q}[N] \subset \{sN + tI_2 \mid (s,t) \in \mathbb{Q}^2\}$.

$\boxed{\text{Ainsi, } \mathbb{Q}[N] = \{sN + tI_2 \mid (s,t) \in \mathbb{Q}^2\}.}$

III.2. En déduire que $\mathbb{Q}[N]$ est un sous-anneau commutatif de $\mathcal{M}_2(\mathbb{Q})$.

- ⋆ $\mathbb{Q}[N] \subset \mathcal{M}_2(\mathbb{Q})$ et $(\mathcal{M}_2(\mathbb{Q}), +, \times)$ est un anneau de référence (attention, il n'est pas commutatif).
- ⋆ $I_2 = \underbrace{0}_{\in\mathbb{Q}} + \underbrace{1}_{\in\mathbb{Q}}.I_2$ donc $\mathbb{Q}[N] \neq \emptyset$ et contient le neutre multiplicatif de l'anneau $\mathcal{M}_2(\mathbb{Q})$.
- ⋆ Soient $(M, M') \in \mathbb{Q}[N]^2$ fixés quelconques.
  Il existe $(s,t,s',t') \in \mathbb{Q}^4$ tels que $M = sN + tI_2$ et $M' = s'N + t'I_2$.
  D'une part,
$$M - M' = \underbrace{(s-s')}_{\in\mathbb{Q}} + \underbrace{(t-t')}_{\in\mathbb{Q}} I_2 \quad \text{donc } M - M' \in \mathbb{Q}[N].$$
  D'autre part, en utilisant que $P(N) = 0 \iff N^2 = -bN - cI_2$,
$$MM' = ss'N^2 + stN + ts'N + tt'I_2 = \underbrace{(st' + ts' - bss')}_{\substack{\in\mathbb{Q} \\ \text{car } c\in\mathbb{Q}}} N + \underbrace{(tt' - css')}_{\substack{\in\mathbb{Z} \\ \text{car } b\in\mathbb{Q}}} I_2 \quad \text{donc } MM' \in \mathbb{Q}[N].$$
- ⋆ Attention, l'anneau $\mathcal{M}_2(\mathbb{Q})$ n'est pas commutatif donc, contrairement à la question I.2(a), la commutativité n'est pas héritée de l'anneau ambiant. Dans l'expression obtenue ci-dessus pour MM', on observe que t et t' d'une part, s et s' d'autre part jouent des rôles symétriques si bien que $M'M$ possède exactement la même expression d'où $MM' = M'M$, ce qui prouve la commutativité de la loi multiplicative sur $\mathbb{Q}[N]$.
  $\boxed{\text{Ainsi, } \mathbb{Q}[N] \text{ est un sous-anneau commutatif de } \mathcal{M}_2(\mathbb{Q}).}$

III.3. Cette question propose l'étude d'un exemple qui sera généralisée dans la question suivante.

(a) Effectuer explicitement la division euclidienne de $P = X^2 + bX + c$ par $X + 2$.

En posant la division euclidienne, on trouve
$$\boxed{P = X^2 + bX + c = (X+2)(X+b-2) + c - 2b + 4.}$$

(b) En évaluant en -2, justifier que le reste est non nul.

Si l'on prend l'image de l'identité ci-dessus par le morphisme d'évaluation en -2, on obtient
$$P(-2) = \underbrace{(-2+2)}_{=0}(-2+b-2) + c - 2b + 4 = c - 2b + 4$$
or les racines de P sont complexes non réelles (car $\Delta < 0$)
$$\boxed{\text{donc le reste de la division, qui vaut } P(-2) = c - 2b + 4 \text{ est non nul.}}$$

(c) En déduire que $N + 2I_2$ est une matrice inversible dans $\mathbb{Q}[N]$ et préciser son inverse.

Prenons l'image de l'identité
$$X^2 + bX + c = (X+2)(X+b-2) + c - 2b + 4$$
par le morphisme d'évaluation en N, on obtient
$$\underbrace{P(N)}_{=0} = (N + 2I_2)(N + (b-2)I_2) + (c - 2b + 4)I_2$$
or $c - 2b + 4 \neq 0$ d'après la question précédente d'où
$$(N + 2I_2)(N + (b-2)I_2) = (2b - c - 4)I_2 \quad \text{donc} \quad (N + 2I_2) \times \frac{1}{2b-c-4}(N + (b-2)I_2) = I_2$$

De plus, $N+2I_2$ et $\dfrac{1}{2b-c-4}(N+(b-2)I_2)$ commutent (elles appartiennent à $\mathbb{Q}[N]$ qui est un anneau commutatif) donc $N+2I_2$ est inversible et son inverse est $\underbrace{\dfrac{1}{2b-c-4}}_{\in\mathbb{Q}}N+\underbrace{\dfrac{(b-2)}{2b-c-4}}_{\in\mathbb{Q}}I_2 \in \mathbb{Q}[N]$.

Ainsi, $N+2I_2$ est une matrice inversible dans $\mathbb{Q}[N]$ d'inverse $\dfrac{1}{2b-c-4}N+\dfrac{(b-2)}{2b-c-4}I_2$.

III.4. (a) Soient $(s,t)\in\mathbb{Q}^2$ tels que $s\neq 0$. Posons $M=sN+tI_2$.
Prouver l'existence de $M'\in\mathbb{Q}[N]$ telle que $MM'=M'M=I_2$.

Notons respectivement Q et R le quotient et le reste de la division euclidienne de $P=X^2+bX+c$ par $sX+t$.
Par définition de la division euclidienne,

$$P=(sX+t)Q+R \quad \text{et} \quad \deg R<\deg(sX+t)=1 \quad (s\neq 0)$$

donc R est un polynôme constant : $\exists r\in\mathbb{Q}\ :\ R=r$.
Prenons l'image de la division euclidienne ci-dessus par le morphisme d'évaluation en $-\dfrac{t}{s}$:

$$P\left(-\frac{t}{s}\right)=\underbrace{\left(-s\times\frac{t}{s}+t\right)}_{=0}Q\left(-\frac{t}{s}\right)+r \quad \text{donc} \quad r=P\left(-\frac{t}{s}\right)$$

or les racines de P sont complexes non réelles (car $\Delta<0$),
donc le reste r de la division est non nul.
Prenons l'image de la division euclidienne ci-dessus par le morphisme d'évaluation en N :

$$\underbrace{P(N)}_{=0}=(sN+tI_2)Q(N)+rI_2$$

donc

$$-rI_2=(sN+tI_2)Q(N) \quad \text{donc} \quad (sN+tI_2)\left(-\frac{1}{r}Q(N)\right)=I_2$$

Or $(sN+tI_2)$ et $-\dfrac{1}{r}Q(N)$ commutent (elles appartiennent à $\mathbb{Q}[N]$ qui est un anneau commutatif) donc $sN+tI_2$ est inversible et son inverse est $-\dfrac{1}{r}Q(N)\in\mathbb{Q}[N]$ (évaluation en N de $-\dfrac{1}{r}Q\in\mathbb{Q}[X]$).

Ainsi, $sN+tI_2$ est une matrice inversible dans l'anneau $\mathbb{Q}[N]$.

(b) À l'aide de la question précédente, montrer que $\mathbb{Q}[N]$ est un corps.

- ⋆ $(\mathbb{Q}[N],+,\times)$ est un anneau commutatif d'après la question III.2.
- ⋆ Soit $M\in\mathbb{Q}[N]$ fixée quelconque telle que $M\neq 0$.
  Compte tenu de la description de $\mathbb{Q}[N]$ établie dans la question III.1, il existe $(s,t)\in\mathbb{Q}^2 : M=sN+tI_2$.
  - — Si $s\neq 0$, alors nous avons établi dans la question III.4(a) que M est un élément inversible de l'anneau $\mathbb{Q}[N]$.
  - — Sinon, $s=0$ donc $M=tI_2$, or $M\neq 0$ donc $t\neq 0$ si bien que la matrice $\dfrac{1}{t}I_2$ existe et vérifie

$$M\times\frac{1}{t}I_2=I_2$$

De plus, M et $\dfrac{1}{t}I_2$ commutent et $\dfrac{1}{t}I_2\in\mathbb{Q}[N]$ donc M est un élément inversible de l'anneau $\mathbb{Q}[N]$.
Ainsi, tout élément non nul de $\mathbb{Q}[N]$ est inversible dans l'anneau $\mathbb{Q}[N]$.

Ainsi, $\mathbb{Q}[N]$ est un corps.
