Université Claude Bernard - Lyon 1 | **Semestre d'automne 2025–2026**

L1 | UE : Algèbre 1 pour les Mathématiques

Sujet blanc pour préparer le Contrôle Terminal

CORRECTION

Aucun document ou dispositif électronique n'est autorisé pendant l'épreuve.

Les réponses doivent toutes être soigneusement justifiées, et la rédaction la plus précise possible.

Exercice 1 Questions de cours (1 + 3 = 4 points)

1. Enoncer le Théorème fondamental de l'Arithmétique (on ne demande pas la preuve !).

   Correction. Soit $n \geq 2$ un entier, alors il existe une unique écriture de n sous la forme

   $$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

   où, pour tout $i \in \{1, ..., k\}$, p_i est un nombre premier, $\alpha_i \in \mathbb{N}^*$ et $p_1 < p_2 < ... < p_k$.

2. Soient a et b deux entiers naturels non-nuls. Montrer qu'il existe $(u, v) \in \mathbb{Z}^2$ tels que

   $$au + bv = \mathrm{PGCD}(a, b).$$

   Correction. Raisonnons par récurrence forte et, pour tout $b \in \mathbb{N}^*$, définissons la proposition

   $$P(b) : \text{"}\forall a \in \mathbb{N}^*, \exists (u, v) \in \mathbb{Z}^2, au + bv = \mathrm{PGCD}(a, b)\text{"}.$$

   Initialisation : Si $b = 1$, alors, pour tout $a \in \mathbb{N}^*$, il est clair que $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(a, 1) = 1 = a \times 0 + b \times 1$, donc le couple $(u, v) = (0, 1)$ convient. Ainsi, $P(1)$ est vraie.

   Hérédité (alternative à la version du CM) : Soit $b \in \mathbb{N}^*$. Supposons que $P(k)$ est vraie pour tout $k \in \{1, ..., b\}$. Montrons que $P(b + 1)$ est vraie. Soit $a \in \mathbb{N}^*$, alors la division euclidienne de $b + 1$ par a donne : $b + 1 = aq + r$ avec $0 \leqslant r < a$. Comme $P(r)$ est vraie, alors il existe $(u, v) \in \mathbb{Z}^2$ tels que $au + rv = \mathrm{PGCD}(a, r)$. Or $\mathrm{PGCD}(a, r) = \mathrm{PGCD}(a, b)$ et on obtient ainsi

   $$\mathrm{PGCD}(a, b) = au + rv = au + (b + 1 - aq)v = a(u - qv) + (b + 1)v$$

   et donc $P(b + 1)$ est vraie.

   Conclusion : On en déduit donc que, $\forall b \in \mathbb{N}^*$, $\forall a \in \mathbb{N}^*$, $\exists (u, v) \in \mathbb{Z}^2$, $au + bv = \mathrm{PGCD}(a, b)$.

Exercice 2 Equations complexes (2 + 2 = 4 points)

1. Déterminer les racines carrées de $9 + 40i$.

   Correction. Soit $z = x + iy$, $(x, y) \in \mathbb{R}^2$, on cherche à résoudre $z^2 = 9 + 40i$. On a donc :

   $$z^2 = (x + iy)^2 = x^2 - y^2 + 2ixy = 9 + 40i,$$
   $$|z|^2 = x^2 + y^2 = |9 + 40i| = \sqrt{9^2 + 40^2} = \sqrt{1681} = 41.$$

   On obtient donc $\begin{cases} x^2 - y^2 = 9 \\ x^2 + y^2 = 41 \\ 2xy = 40 \end{cases}$, et ainsi $2x^2 = 41+9 = 50$, d'où $x \in \{-5, 5\}$ et $2y^2 = 41-9 = 32$ d'où $y \in \{-4, 4\}$. Comme $xy = 20 > 0$, alors x et y ont même signe, donc les racines de $9 + 40i$ sont $-5 - 4i$ et $5 + 4i$.

2. Résoudre dans $\mathbb{C}$ l'équation $iz^2 + (1-5i)z - 2 + 6i = 0$.

Correction. Le discriminant de ce polynôme du second degré est

$$\Delta = (1-5i)^2 - 4i(-2+6i) = 1 - 25 - 10i + 8i + 24 = -2i.$$

Comme $-2i = 2e^{-i\frac{\pi}{2}}$, les racines carrées de Δ sont donc δ et $-\delta$ avec

$$\delta = \sqrt{2}e^{-i\frac{\pi}{4}} = \sqrt{2}\left(\cos\left(-\frac{\pi}{4}\right) + i\sin\left(-\frac{\pi}{4}\right)\right) = \sqrt{2}\left(\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right) = 1 - i.$$

Les solutions de l'équation sont donc

$$z_1 = \frac{-(1-5i)+(1-i)}{2i} = \frac{4i}{2i} = 2 \quad \text{et} \quad z_2 = \frac{-(1-5i)-(1-i)}{2i} = \frac{-2+6i}{2i} = -\frac{1}{i} + 3 = 3 + i.$$

<u>Exercice 3</u> Polynômes (1.5 + 0.5 + 1 + 1 = 4 points)

Pour tout $n \in \mathbb{N}^*$, on définit le polynôme $P_n = (X+1)^n - nX - 1$ et on note Z_n l'ensemble des racines de P_n dans $\mathbb{C}$, sans prendre en compte leurs multiplicités.

1. Factoriser P_2, P_3 et P_4 dans $\mathbb{R}[X]$ et déterminer Z_2, Z_3 et Z_4.

Correction. On calcule et on factorise :

$$\begin{aligned}
P_2 &= (X+1)^2 - 2X - 1 = X^2, \\
P_3 &= (X+1)^3 - 3X - 1 = X^3 + 3X^2 = X^2(X+3) \\
P_4 &= (X+1)^4 - 4X - 1 = X^4 + 4X^3 + 6X^2 = X^2(X^2 + 4X + 6).
\end{aligned}$$

P_2 et P_3 sont bien factorisés avec des polynômes irréductibles de $\mathbb{R}[X]$. Quant à P_4, on remarque que le discriminant de $X^2 + 4X + 6$ vaut $\Delta = 16 - 24 = -8 < 0$ donc ce polynôme est irréductible et P_4 est bien factorisé dans $\mathbb{R}[X]$. Les racines complexes de P_4 sont donc

$$X_1 = \frac{-4 + i\sqrt{8}}{2} = -2 + i\sqrt{2} \quad \text{et} \quad X_2 = \frac{-4 - i\sqrt{8}}{2} = -2 - i\sqrt{2}.$$

On trouve alors

$$Z_2 = \{0\}, \quad Z_3 = \{0, -3\} \quad \text{et} \quad Z_4 = \{0, -2 + i\sqrt{2}, -2 - i\sqrt{2}\}.$$

2. Montrer que, pour tout $n \in \mathbb{N}^*$, X^2 divise P_n.

Correction. Soit $n \in \mathbb{N}^*$. Il suffit de remarquer que X^2 divise P_n si et seulement si 0 est racine de P_n de multiplicité au moins 2. On calcule :

$$P_n(0) = 1^n - 1 = 0,$$

et comme $P_n' = n(X+1)^{n-1} - n$, on a

$$P_n'(0) = n \times 1^{n-1} - n = 0,$$

donc 0 est bien racine de P_n de multiplicité au moins 2, donc X^2 divise P_n.

3. Déterminer le PGCD de P_4 et P_3 en utilisant les factorisations de la question 1, puis avec l'algorithme d'Euclide.

   Correction. On rappelle que

$$P_3 = X^2(X+3) \quad \text{et} \quad P_4 = X^2(X^2+4X+6).$$

   Comme la seule racine de $X+3$ est -3 et que ce n'est pas une racine de X^2+4X+6, on en déduit que X^2 est le PGCD de P_3 et P_4.

   Avec l'algorithme d'Euclide :

$$X^4+4X^3+6X^2 = (X+1)(X^3+3X^2)+3X^2$$
$$X^3+3X^2 = \left(\frac{1}{3}X+1\right)(3X^2).$$

   On en déduit, en renormalisant, que le PGCD recherché est X^2.

4. Soit $n \in \mathbb{N}^*$. On note R_n le reste de la division euclidienne de P_n par X^2-1.
   Montrer que $R_n(1) = 2^n - n - 1$ et $R_n(-1) = n-1$, puis en déduire l'expression de R_n.

   Correction. Soit $n \in \mathbb{N}^*$. On sait qu'il existe deux polynômes Q_n et R_n tels que

$$P_n(X) = (X^2-1)Q_n(X) + R_n(X), \quad d^\circ R \leqslant 1.$$

   Donc $R_n(X) = a_nX + b_n$ avec $(a_n, b_n) \in \mathbb{R}^2$. On évalue cette équation en $X = 1$ et $X = -1$ et on trouve :

$$P_n(1) = 2^n - n - 1 = R_n(1) \quad \text{et} \quad P_n(-1) = n-1 = R_n(-1),$$

   d'où le système $\begin{cases} 2^n - n - 1 = a_n + b_n \\ n - 1 = -a_n + b_n \end{cases}$, ce qui permet de trouver $2b_n = 2^n - 2$ et donc $b_n = 2^{n-1} - 1$ ce qui donne $a_n = b_n - n + 1 = 2^{n-1} - n$. Le reste recherché est donc

$$R_n = \left(2^{n-1} - n\right) X + 2^{n-1} - 1.$$

Exercice 4 Arithmétique (1 + 1 + 1 + 1 = 4 points)

Pour tout $n \in \mathbb{N}$, on définit $a_n = 2^n + 3^n$.

1. En utilisant les congruences, montrer que, $\forall n \in \mathbb{N}$, $5 \mid a_{2n+3}$.

   Correction. Soit $n \in \mathbb{N}$, alors on a

$$a_{2n+3} = 2^{2n+3} + 3^{2n+3} = 8 \times 4^n + 27 \times 9^n \equiv 3 \times 4^n + 2 \times 4^n \; [5] \equiv 5 \times 4^n \; [5] \equiv 0 \; [5],$$

   donc $5 \mid a_{2n+3}$.

2. En utilisant l'algorithme d'Euclide, déterminer le PGCD de 275 et 35.

   Correction. Par l'algorithme d'Euclide, on a :

$$275 = 7 \times 35 + 30$$
$$35 = 30 + 5$$
$$30 = 5 \times 6 + 0,$$

   donc $\mathrm{PGCD}(275, 35) = 5$.

3. Résoudre dans $\mathbb{Z}^2$ l'équation $a_3x + a_5y = 3$. Résoudre de même l'équation $a_3x + a_5y = 10$.

   Correction. On cherche à résoudre :

   — $35x + 275y = 3$. Comme $\mathrm{PGCD}(275, 35) = 5$ ne divise pas 3, l'équation n'admet pas de solution dans $\mathbb{Z}^2$.

   — $35x + 275y = 10$. Cette fois-ci, $\mathrm{PGCD}(275, 35) = 5$ divise 10, donc l'équation admet des solutions. Cherchons une solution particulière de l'équation en déterminant les coefficients de Bézout de 275 et 35. On remonte l'algorithme d'Euclide et on trouve

   $$5 = 35 - 30 = 35 - (275 - 7 \times 35) = 8 \times 35 - 275.$$

   Donc, en multipliant par 2, on trouve

   $$35 \times (16) + 275 \times (-2) = 10,$$

   donc $(16, -2)$ est une solution particulière de cette équation, qui est équivalente à $7x + 55y = 2$ où 7 et 55 sont donc premiers entre eux. L'ensemble des solutions de l'équation est donc

   $$S = \{(16 + 55k, -2 - 7k) : k \in \mathbb{Z}\}.$$

4. Montrer que pour tout $n \in \mathbb{N}$, a_n et a_{n+1} sont premiers entre eux.

   Indication : *Calculer $a_{n+1} - 3a_n$ et $a_{n+1} - 2a_n$.*

   Correction. Pour tout $n \in \mathbb{N}$, on a

   $$a_{n+1} - 3a_n = 2^{n+1} + 3^{n+1} - 3(2^n + 3^n) = 2^{n+1} - 3 \times 2^n = 2^n(2 - 3) = -2^n.$$

   Le PGCD de a_{n+1} et a_n divise donc 2^n, c'est donc une puissance de 2. De même, on a, pour tout $n \in \mathbb{N}$,

   $$a_{n+1} - 2a_n = 2^{n+1} + 3^{n+1} - 2(2^n + 3^n) = 3^{n+1} - 2 \times 3^n = 3^n(3 - 2) = 3^n.$$

   Le PGCD de a_{n+1} et a_n divise donc 3^n, c'est donc une puissance de 3. On en déduit donc que la seule possibilité est que $\mathrm{PGCD}(a_n, a_{n+1}) = 1$, donc ces deux nombres sont premiers entre eux.

Exercice 5 **Entiers de Gauss (0.5 + 1 + 1 + 1.5 = 4 points)**

On considère l'ensemble $\mathbb{Z}[i] = \{z = a + ib : (a, b) \in \mathbb{Z}^2\}$ ainsi que l'application $N : \mathbb{Z}[i] \to \mathbb{R}$, $z \mapsto \overline{z}z$, appelé *stathme* de $\mathbb{Z}[i]$.

1. Montrer que pour tout $z \in \mathbb{Z}[i]$, $N(z) \in \mathbb{N}$.

   Correction. Soit $z \in \mathbb{Z}[i]$, alors $z = a + ib$ avec $(a, b) \in \mathbb{Z}^2$. Ainsi, $N(z) = |z|^2 = a^2 + b^2 \in \mathbb{N}$.

2. Montrer que pour tout $(z, z') \in \mathbb{Z}[i]^2$, $zz' \in \mathbb{Z}[i]$ et $N(zz') = N(z)N(z')$.

   Correction. Soit $z = a + ib$, $(a, b) \in \mathbb{Z}^2$ et $z' = m + in$, $(m, n) \in \mathbb{Z}^2$, alors

   $$zz' = (a + ib)(m + in) = am - bn + i(bm + an).$$

   Comme $am - bn \in \mathbb{Z}$ et $bm + an \in \mathbb{Z}$, $zz' \in \mathbb{Z}[i]$. De plus, on a

   $$N(zz') = |zz'|^2 = |z|^2|z'|^2 = N(z)N(z').$$

3. Soit $z \in \mathbb{Z}[i] \backslash \{0\}$ tel que $z^{-1} \in \mathbb{Z}[i]$. Montrer que $N(z) = 1$.
   Correction. Soit $z \in \mathbb{Z}[i] \backslash \{0\}$ tel que $z^{-1} \in \mathbb{Z}[i]$, alors, comme $zz^{-1} = 1$ et
   $$1 = N(1) = N(zz^{-1}) = N(z)N(z^{-1}).$$
   Mais comme $N(z) \in \mathbb{N}$ et $N(z^{-1}) \in \mathbb{N}$ et ont pour produit 1, ils sont donc égaux à 1 tous les deux, et donc en particulier $N(z) = 1$.
4. En déduire $\{z \in \mathbb{Z}[i] \backslash \{0\} : z^{-1} \in \mathbb{Z}[i]\}$.
   Correction. Soit $z \in \mathbb{Z}[i] \backslash \{0\}$ tel que $z^{-1} \in \mathbb{Z}[i]$, alors, en notant $z = a + ib$, $(a, b) \in \mathbb{Z}^2$, on obtient
   $$N(z) = a^2 + b^2 = 1.$$
   Comme a et b sont des entiers relatifs, alors $a > 1$ ou $b > 1$ implique que $a^2 + b^2 > 1$, donc les seules possibilités sont :
   - $a = 1$ et $b = 0$, et on trouve $z = 1$,
   - $a = -1$ et $b = 0$, et on trouve $z = -1$,
   - $a = 0$ et $b = 1$, et on trouve $z = i$,
   - $a = 0$ et $b = -1$, et on trouve $z = -i$.

   Ainsi, $\{z \in \mathbb{Z}[i] \backslash \{0\} : z^{-1} \in \mathbb{Z}[i]\} = \{1, -1, i, -i\}$.