Contrôle 2

Calculatrice et documents sont interdits.
En dehors des exceptions précisées dans l'énoncé, tous les résultats doivent être correctement rédigés et rigoureusement justifiés.
Le barème est donné à titre indicatif : 6 - 8 - 6.

Exercice 1 : parties du plan

1. **Préliminaires**

   (a) Démontrer rigoureusement l'inégalité : $\sqrt{2} < \frac{3}{2}$.

   Nous savons que $8 < 9$. Donc en passant à la racine carrée, $\sqrt{8} < \sqrt{9}$, c'est-à-dire $2\sqrt{2} < 3$. Donc $\sqrt{2} < \frac{3}{2}$.

   (b) Démontrer : $\forall \theta \in \mathbf{R},\ \cos(\theta) + \sin(\theta) = \sqrt{2}\cos(\theta - \frac{\pi}{4})$.

   Soit $\theta \in \mathbf{R}$. Utilisons une formule trigonométrique :

   $$\cos(\theta - \tfrac{\pi}{4}) = \cos(\theta)\cos(-\tfrac{\pi}{4}) - \sin(\theta)\sin(-\tfrac{\pi}{4}) = \frac{\sqrt{2}}{2}\cos(\theta) + \frac{\sqrt{2}}{2}\sin(\theta).$$

   Multiplions par $\sqrt{2}$:

   $$\sqrt{2}\cos(\theta - \tfrac{\pi}{4}) = \cos(\theta) + \sin(\theta).$$

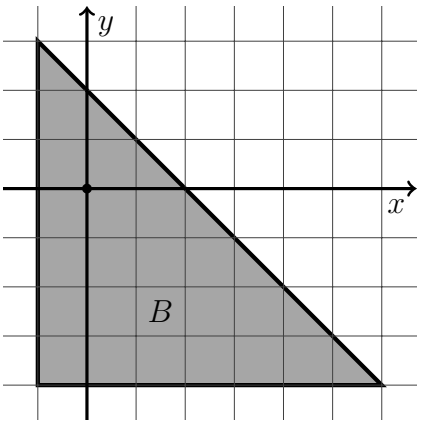
2. **Ensembles**

   Soit $A = \{(2\cos(\theta) + 1, 2\sin(\theta) - 2) \in \mathbf{R}^2 \mid \theta \in \mathbf{R}\}$.

   (a) Cet ensemble est représenté dans le plan par un cercle. Donner sans justification son équation cartésienne, son centre et son rayon.

   (b) Définir mathématiquement l'ensemble B représenté par le triangle grisé ci-contre. (On précise que les bords de l'ensemble sont inclus dans B.)

   (c) Démontrer rigoureusement que $A \subset B$.

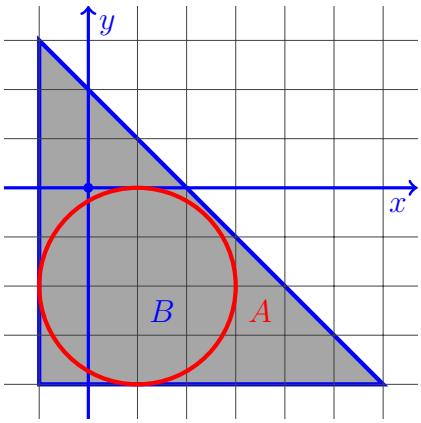


2. (a) Il s'agit du cercle de centre $(1, -2)$ de rayon 2. Son équation cartésienne est : $(x-1)^2 + (y+2)^2 = 4$ (on peut vérifier que $(x, y) = (2\cos(\theta) + 1, 2\sin(\theta) - 2)$ satisfait bien cette égalité. Ainsi :

$$A = \{(x, y) \in \mathbf{R}^2 \mid (x-1)^2 + (y+2)^2 = 4\}.$$

   (b) L'ensemble B est délimité par les droites d'équations : $y = -4$, $x = -1$ et $x + y = 2$. Nous pouvons le définir par :

$$B = \{(x, y) \in \mathbf{R}^2 \mid x \geqslant -1, y \geqslant -4 \text{ et } y \leqslant 2 - x\}.$$



(c) La figure ci-dessus semble confirmer l'inclusion demandée, mais elle ne constitue pas une preuve. Nous observons notamment que A « rentre tout juste »à l'intérieur de B ; la preuve de l'inclusion ne sera peut-être pas évidente et nécessitera peut-être des encadrements fins.

Soit $(x, y) \in A$. Par définition, il s'écrit $(x, y) = (2\cos(\theta)+1, 2\sin(\theta)-2)$ avec $\theta \in \mathbf{R}$.
Nous savons que $\cos(\theta) \geqslant -1$, donc $2\cos(\theta) + 1 \geqslant -1$.
De même, $\sin(\theta) \geqslant -1$, donc $2\sin(\theta) - 2 \geqslant -4$.
Nous avons ainsi vérifié que : $x \geqslant -1$ et $y \geqslant -4$.
Enfin,

$$x + y = 2\cos(\theta) + 1 + 2\sin(\theta) - 2 = 2(\cos(\theta) + \sin(\theta)) - 1 = 2\sqrt{2}\cos(\theta - \tfrac{\pi}{4}) - 1$$

d'après la question 1-b. Or $\cos(\theta - \frac{\pi}{4}) \leqslant 1$ donc $x + y \leqslant 2\sqrt{2} - 1$.
Puis d'après la question 1-a ,$x + y \leqslant 2 \cdot \frac{3}{2} - 1 = 2$.
Nous avons ainsi montré que $y \leqslant 2 - x$.
Ainsi, (x, y) satisfait toutes les conditions définissant l'ensemble B, donc $(x, y) \in B$.
Donc $B \subset A$.

Exercice 2 : plus grand diviseur strict

Pour un entier n, on appelle **plus grand diviseur strict de** n le plus grand entier k tel que $k|n$ et $k < n$.
Par exemple, pour $n = 10$, ses diviseurs sont : 1, 2, 5 et 10 ; son plus grand diviseur strict est $k = 5$. Cette définition ne peut pas s'appliquer aux entiers 0 et 1.

Nous définissons l'application $\varphi : \mathbf{N} \setminus \{0, 1\} \longrightarrow \mathbf{N}^*$, $n \longmapsto$ le plus grand diviseur strict de n

Nous notons respectivement **P**, **Pair** et **Imp** les ensembles des entiers naturels premiers, pairs et impairs.

1. Donner les valeurs de $\varphi(7)$, $\varphi(9)$ et $\varphi(100)$.

   Les diviseurs de 7 sont 1 et 7, donc $\varphi(7) = 1$. De même, on obtient : $\varphi(9) = 3$, $\varphi(100) = 50$.

2. Soit $p \in \mathbf{P}$. Déterminer $\varphi(p)$.

   Soit $p \in \mathbf{P}$. Ses diviseurs sont par définition 1 et p. Donc son plus grand diviseur strict est 1 : $\varphi(p) = 1$.

3. Soit $n \in \mathbf{N}^*$. Déterminer $\varphi(2n)$.

   Soit d un diviseur strict de $2n$. Alors il existe $k \in \mathbf{N}$ tel que $2n = dk$. Comme $d < n$, $k > 1$, donc $k \geqslant 2$. Comme $d = \frac{2n}{k}$, nous concluons que $d \leqslant n$. Autrement dit, tout diviseur strict de $2n$ est inférieur à n. Or n est un diviseur strict de $2n$ ($n < 2n$ car $n \neq 0$), nous concluons que n est le plus grand diviseur strict de $2n$: $\varphi(2n) = n$.

4. Sans justification, donner l'ensemble image $\varphi(\mathbf{Pair} \setminus \{0\})$.

   $\varphi(\mathbf{Pair} \setminus \{0\}) = \mathbf{N}^*$.
   Si nous souhaitons le justifier : par définition de φ, l'image de tout nombre appartient à $\mathbf{N}^*$, donc $\varphi(\mathbf{Pair} \setminus \{0\}) \subset \mathbf{N}^*$. Soit maintenant $n \in \mathbf{N}^*$. D'après la question précédente, $n = \varphi(2n)$, donc tout élément de $\mathbf{N}^*$ admet un antécédent pair. Donc $\mathbf{N}^* \subset \varphi(\mathbf{Pair}\setminus\{0\})$.
   Par double inclusion, le résultat est démontré.

5. Montrer par double inclusion que $\varphi(\mathbf{Imp} \setminus \{1\}) = \mathbf{Imp}$.

   Montrons que $\varphi(\mathbf{Imp} \setminus \{1\}) \subset \mathbf{Imp}$.
   Soit $n \in \mathbf{Imp} \setminus \{1\}$. Comme il est impair, il n'est pas divisible par 2, donc tous ses diviseurs sont impairs. En particulier, son plus grand diviseur strict est impair. Donc $\varphi(n) \in \mathbf{Imp}$. Ainsi $\varphi(\mathbf{Imp} \setminus \{1\}) \subset \mathbf{Imp}$.
   Montrons maintenant $\mathbf{Imp} \subset \varphi(\mathbf{Imp} \setminus \{1\})$. Soit $m \in \mathbf{Imp}$. Posons $n = 3m$. Montrons que $\varphi(n) = m$.Comme m est impair, n l'est aussi. Et m est un diviseur de n. Notons $k = \varphi(n)$ le plus grand diviseur strict de n. Donc $n > k \geqslant m$. Donc $\frac{1}{n} < \frac{1}{k} \leqslant \frac{1}{m}$, donc $1 < \frac{n}{k} \leqslant \frac{n}{m}$. Si $\frac{n}{k} = 2$, alors $n = 2k$, donc n est pair ce qui est faux. Donc $\frac{n}{k} = 3$ et $n = 3k$. Or $n = 3m$, donc $k = m$ et $\varphi(n) = m$. Ainsi, tout entier impair admet un antécédent impair, donc $\mathbf{Imp} \subset \varphi(\mathbf{Imp} \setminus \{1\})$.
   Par double inclusion, l'égalité est démontrée.

6. Déterminer l'ensemble $\varphi^{-1}(\{1\})$ des antécédents de 1 par φ.

   Montrons par double inclusion que : $\varphi^{-1}(\{1\}) = \mathbf{P}$.
   Soit $p \in \mathbf{P}$. D'après 2., $\varphi(p) = 1$, donc p est un antécédent de 1 : $p \in \varphi^{-1}(\{1\})$. Ainsi $\mathbf{P} \subset \varphi^{-1}(\{1\})$.
   Soit maintenant $n \in \varphi^{-1}(\{1\})$. Cela signifie que $\varphi(n) = 1$. Autrement dit, 1 est le plus grand diviseur strict de n. Donc c'est le seul diviseur strict de n. Ainsi n n'a pour diviseurs que 1 et lui-même : c'est un nombre premier. Donc $n \in \mathbf{P}$ et nous déduisons $\varphi^{-1}(\{1\}) \subset \mathbf{P}$.
   Conclusion : $\varphi^{-1}(\{1\}) = \mathbf{P}$.

7. Montrer, toujours par double inclusion, que $\varphi^{-1}(\mathbf{P}) = \{pq \ ; \ p \in \mathbf{P} \text{ et } q \in \mathbf{P}\}$.

   Notons E le second ensemble. Montrons $E \subset \varphi^{-1}(\mathbf{P})$. Soient p et q des nombres premiers et $n = pq$. Alors les diviseurs de n sont : 1, p, q et n. Son plus grand diviseur strict est alors $\max(p, q)$. En particulier, ce plus grand diviseur strict est un nombre premier, donc $\varphi(n) \in \mathbf{P}$. Donc $n \in \varphi^{-1}(\mathbf{P})$.

   Montrons $\varphi^{-1}(\mathbf{P}) \subset E$. Soit $n \in \varphi^{-1}(\mathbf{P})$. Donc $\varphi(n)$ est un nombre premier que nous notons p. Ce nombre étant le plus grand diviseur strict de n, c'est en particulier un diviseur, donc il existe un entier $k > 1$ tel que $n = kp$. Supposons par l'absurde que k

ne soit pas premier. Alors il existe des entiers $a > 1$ et $b > 1$ tels que $k = ab$. Alors $n = abp$ et nous remarquons que bp est un diviseur strict de n strictement supérieur à p. Cela contredit notre définition de p et nous concluons que k est un nombre premier. Donc $n = kp$ est un produti de deux nombres premiers, donc $n \in E$.

Par double inclusion, l'égalité est démontrée.

Exercice 3 : lois de réciprocité quadratique

Soient a et n des entiers naturels.
On dit que a est un **carré modulo** n si : $\exists b \in \mathbf{N}$, $a = b^2 \mod n$.

Nous admettons les résultats suivants (appelés lois de réciprocité quadratique) :
Soient p et q des nombres premiers.
• Si p ou q est congru à 1 modulo 4, alors p est un carré modulo q si et seulement si q est un carré modulo p.
• Si p et q sont congrus à 3 modulo 4, alors p est un carré modulo q si et seulement si q n'est pas un carré modulo p.

Le but de cet exercice est d'appliquer ces propriétés pour déterminer si 43 est un carré modulo 97.

1. Réduire modulo 4 les nombres premiers 5, 7, 11, 43 et 97.
   Réduire également 43 modulo 11 et 97 modulo 43.

   Dans $\mathbf{Z}/4\mathbf{Z}$: $\bar{5} = \bar{1}$, $\bar{7} = \bar{3}$, $\overline{11} = \bar{3}$, $\overline{43} = \bar{3}$ et $\overline{97} = \bar{1}$. Par exemple, le dernier résultat est justifié par l'égalité : $97 = 4 \times 24 + 1$.
   De même, $43 = 3 \times 11 + 10$, donc $43 \equiv 10 \mod 11$ et $97 = 2 \times 43 + 11$, donc $97 \equiv 11 \mod 43$.

2. Écrire la table des carrés dans $\mathbf{Z}/11\mathbf{Z}$. Les nombres 5 et 7 sont-ils des carrés modulo 11 ?

   Dans $\mathbf{Z}/11\mathbf{Z}$, la table des carrés est donnée par :

x	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\overline{10}$
x^2	$\bar{0}$	$\bar{1}$	$\bar{4}$	$\bar{9}$	$\bar{5}$	$\bar{3}$	$\bar{3}$	$\bar{5}$	$\bar{9}$	$\bar{4}$	$\bar{1}$

   D'après la table, 5 est un carré modulo 11 puisque $\bar{5} = \bar{4}^2$, et $\bar{7}$ n'est pas un carré puisqu'il n'apparaît pas dans la table.

3. Le nombre 11 est-il un carré modulo 5 ? Et modulo 7 ? Est-ce conforme aux lois de réciprocité quadratique ?

   On a $11 \equiv 1 \mod 5$ et $1 = 1^2$ est clairement un carré. Donc $11 \equiv 1^2 \mod 5$: 11 est un carré modulo 5. Comme 5 est congru à 1 modulo 4, la première loi de réciprocité quadratique affirme que 11 est un carré modulo 5 ssi 5 est un carré modulo 11. C'est bien le cas puisque nous avons vu que chacun des deux est un carré modulo l'autre.

   De la même manière, $11 \equiv 4 \mod 7$ et $4 = 2^2$ est clairement un carré, donc $11 \equiv 2^2 \mod 7$: 11 est un carré modulo 7. Cette fois, 11 et 7 sont tous deux congrus à 3 modulo 4 ; la seconde loi affirme que 11 est un carré modulo 7 ssi 7 n'est pas un carré modulo 11. Cela est bien conforme à nos résultats.

4. En appliquant plusieurs fois les lois, déterminer si 43 est un carré modulo 97.

   Le nombre 97 est congru à 1 modulo 4. D'après la première loi, 43 est un carré modulo 97 ssi 97 est un carré modulo 43. Or $97 \cong 11 \mod 43$, donc cela revient à dire que 11 est un carré modulo 43.
   Or 11 et 43 sont tous deux congrus à 3 modulo 11, donc 11 est un carré modulo 43 ssi

43 n'est pas un carré modulo 11. Comme $43 \equiv 10 \mod 11$, cela revient à dire que 10 n'est pas un carré modulo 11.
Résumons :

43 carré modulo 97 ssi 11 carré modulo 43 ssi 10 pas un carré modulo 11

Or d'après la table de la question 2., nous pouvons affirmer que 10 n'est pas un carré modulo 11 et ainsi conclure que 43 est un carré modulo 97.
Si nous avions voulu démontrer ce résultat directement, nous aurions dû dresser la table des carrés modulo 97 et observer par exemple que $\overline{43} = \overline{25}^2$ dans $\mathbf{Z}/97\mathbf{Z}$. C'est très fastidieux. Les lois de réciprocité quadratique permettent de ramener ce problème à des calculs modulo des nombres plus petits.