Corrigé du contrôle 2

Exercice 1 **Cubique de Tschirnhausen**

On souhaite représenter la courbe $\mathcal{C}$ du plan définie par l'équation cartésienne $3y^2 = x^2 - x^3$:

$$\mathcal{C} = \{(x, y) \in \mathbf{R}^2 \mid 3y^2 = x^2 - x^3\}.$$

1. Démontrer que $\mathcal{C} = \{(1 - 3t^2, t - 3t^3); t \in \mathbf{R}\}$.
   Indication : pour démontrer l'une des inclusions, on pourra poser $t = \frac{y}{x}$.
2. Considérer plusieurs valeurs de t dans $[-2, 2]$ et représenter quelques points de $\mathcal{C}$. Représenter ensuite l'allure générale de la courbe.

Montrons l'égalité par double inclusion.
- Notons $A = \{(1-3t^2, t-3t^3); t \in \mathbf{R}\}$ et montrons $A \subset \mathcal{C}$. Soit $(x, y) \in A$. Par définition de A, ce point s'écrit sous la forme $(1-3t^2, t-3t^3)$ avec $t \in \mathbf{R}$. Pour montrer qu'il appartient à $\mathcal{C}$, il suffit de montrer qu'il satisfait l'égalité $3y^2 = x^2 - x^3$. Calculons $3y^2 = 3(t-3t^3)^2 = 3t^2 - 18t^4 + 27t^6$. D'autre part

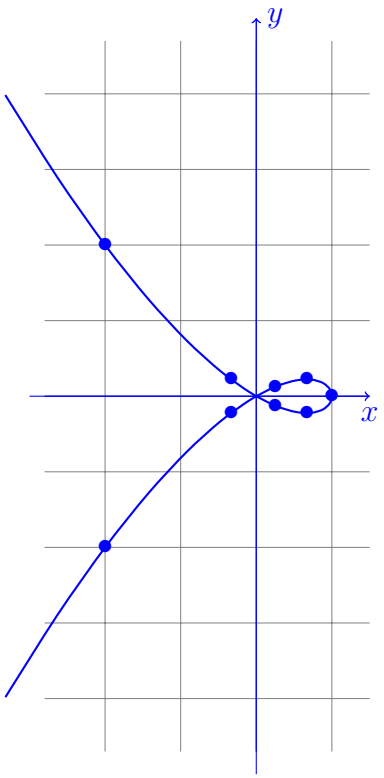
$$x^2 - x^3 = (1 - 3t^2)^2 - (1 - 3t^2)^3 = (1 - 6t^2 + 9t^4) - (1 - 9t^2 + 27t^4 - 27t^6) = 3t^2 - 18t^4 + 27t^6.$$

On obtient bien $3y^2 = x^2 - x^3$, donc $(x, y) \in \mathcal{C}$. On a ainsi démontré que $A =\subset \mathcal{C}$.

- Montrons maintenant $\mathcal{C} \subset A$. Soit $(x, y) \in \mathcal{C}$. Il s'agit de trouver un nombre réel t tel que (x, y) puisse s'écrire $(1 - 3t^2, t - 3t^3)$. Suivons l'indication et posons $t = \frac{y}{x}$ si $x \neq 0$. Alors $y = tx$. Comme $(x, y) \in \mathcal{C}$, on a $3y^2 = x^3 - x^2$. Remplaçons y : $3t^2x^2 = x^3 - x^2$. Comme on a supposé $x \neq 0$, on peut simplifier : $3t^2 - 1 - x$, donc $x = 1 - 3t^2$ et $y = tx = t - 3t^3$. On a ainsi montré que si $x \neq 0$, alors $(x, y) = (1 - 3t^2, t - 3t^3)$ avec $t = \frac{y}{x} \in \mathbf{R}$. Donc $(x, y) \in A$.
Il ne faut pas oublier le cas $x = 0$. On a alors $y = 0$ et on peut vérifier que $(0, 0) = (1-3t^2, t-3t^3)$ avec $t = \frac{1}{\sqrt{3}}$.
Dans tous les cas, $(x, y) \in A$ et donc $\mathcal{C} \subset A$.

Par double inclusion on a démontré $\mathcal{C} = A$.

La courbe $\mathcal{C}$ était définie de façon implicite par une équation cartésienne. Nous disposons maintenant d'une définition paramétrique qui rend bien plus simple sa représentation (notamment avec un ordinateur). Il suffit en effet de faire varier t et de calculer les points de $\mathcal{C}$ correspondants pour les représenter de manière précise. Pour se donner une idée de la courbe on peut prendre $t = 0, \pm\frac{1}{3}, \pm\frac{1}{2}, \pm\frac{2}{3}, \pm 1, \pm 2, etc$ et on sait déjà qu'elle passe par l'origine.



Exercice 2 **Homographie du plan complexe**

On considère l'application

$$\begin{array}{rccc} f: & \mathbf{C}\setminus\{1\} & \to & \mathbf{C} \\ & z & \mapsto & \dfrac{2z+i}{z-1} \end{array}$$

1. Démontrer que f est injective.

   Soient z et z' dans $\mathbf{C}\setminus\{1\}$ tels que $f(z)=f(z')$. Montrons que $z=z'$.
   On a $\frac{2z+i}{z-1}=\frac{2z'+i}{z'-1}$, donc $(2z+i)(z'-1)=(2z'+i)(z-1)$. Donc $2zz'+iz'-2z-i=2z'z+iz-2z'-i$. En passant tous les termes à gauche de l'égalité il reste $(i+2)(z'-z)=0$ et on en déduit $z'-z=0$ donc $z=z'$. La fonction f est bien injective.

2. Déterminer l'image I de f.

   Montrons que $I=\mathbf{C}\setminus\{2\}$. Il est clair que pour tout $z\in\mathbf{C}$, $\frac{2z+i}{z-1}\neq 2$ sinon on en déduirait $i=-2$. Donc $\forall z\in\mathbf{C}\setminus\{1\}, f(z)\neq 2$ et on en déduit $I\subset\mathcal{C}\setminus\{2\}$.
   Montrons maintenant l'autre inclusion. Soit $y\in\mathcal{C}\setminus\{2\}$. Posons $z=\frac{y+i}{y-2}$. Remarquons que $z\neq 1$. Et $f(z)=\frac{2\frac{y+i}{y-2}+i}{\frac{y+i}{y-2}-1}=\frac{(2+i)y}{i+2}=y$. Donc y est dans l'image de f. Ainsi tous les éléments de $\mathcal{C}\setminus\{2\}$ sont dans I. Finalement l'image de f est $I=\mathcal{C}\setminus\{2\}$.

   Remarque : z a été obtenu après un travail d'analyse au brouillon. On a simplement résolu l'équation $\frac{2z+i}{z-1}=y$.

3. Donner l'application réciproque de f définie de I vers $\mathbf{C}\setminus\{1\}$.

   Comme f est injective et surjective sur son image I, elle définit une bijection de $\mathbf{C}\setminus\{1\}$ vers I. Sa bijection réciproque a été déterminée dans la question précédente. Il s'agit de

l'application $f^{-1} : y \mapsto \frac{y+i}{y-2}$. On a déjà vérifié que pour tout y dans I, $f(f^{-1}(y)) = y$. Et on peut également vérifier que pour tout z dans $\mathbf{C} \setminus \{1\}$, $f^{-1}(f(z)) = \frac{\frac{2z+i}{z-1}+i}{\frac{2z+i}{z-1}-1} = z$. Ainsi, f^{-1} est bien la bijection réciproque de f.

4. Déterminer, sans démonstration, les ensembles $f(\mathbf{R} \setminus \{1\})$ et $f^{-1}(i\mathbf{R})$.

On place les images $f(0) = -i$, $f(2) = 4+i$, $f(-1) = 1-\frac{i}{2}$, $f(3) = 3+\frac{i}{2}$ et on conjecture que $f(\mathbf{R}\setminus\{1\})$ est la droite d'équation $y = \frac{1}{2}x - 1$ privée du point $(2, 0)$. Démontrons-le : Soit $x \in \mathbf{R}\setminus\{1\}$. Alors $f(x) = \frac{2x+i}{x-1}$ qui correspond au point $(\frac{2x}{x-1}, \frac{1}{x-1})$ du plan. On peut vérifier que ce point satisfait l'équation de la droite : $\frac{1}{x-1} = \frac{1}{2}\frac{2x}{x-1} - 1$. Réciproquement, on peut vérifier que tout point $(x, \frac{1}{2}x - 1)$ de la droite (hormis $(2, 0)$) est l'image d'un réel par f : c'est l'image de $\frac{x}{x-2}$.

On place les images $f^{-1}(i) = \frac{2}{5} - \frac{4}{5}i$, $f^{-1}(-i) = 0$, $f^{-1}(0) = -\frac{i}{2}$, $f^{-1}(2i) = \frac{3}{4} - \frac{3}{4}i$, $f^{-1}(-2i) = \frac{3}{4} - \frac{3}{4}i$ et on conjecture que l'image réciproque de $i\mathbf{R}$ est le cercle de centre $\frac{1}{2} - \frac{i}{4}$ et de rayon $\frac{\sqrt{5}}{4}$ privé du point 1.
Pour le démontrer, on vérifie que pour tout nombre réel y, $|f^{-1}(y) - (\frac{1}{2} - \frac{i}{4})| = \frac{\sqrt{5}}{4}$ et réciproquement que tout point du cercle (hormis 1) est bien envoyé par f sur l'axe imaginaire pur.

Exercice 3 **Théorème de Wilson**

Le théorème de Wilson affirme que si p est un nombre premier, alors $(p-1)! \equiv -1 \mod p$. Nous allons démontrer ce théorème.

1. Vérifier le théorème pour $p = 5$ et $p = 11$.

$4! = 24$ et on a bien $24 \equiv -1$ modulo 5. Pour $p = 11$, il est hors de question de calculer 10!. Calculons progressivement 10! en réduisant le résultat modulo 11 à chaque étape. Dans $\mathbf{Z}/11\mathbf{Z}$, $\overline{2!} = \bar{2}$, $\overline{3!} = \bar{3}$, $\overline{4!} = \overline{24} = \bar{2}$, $\overline{5!} = \bar{5} \times \bar{2} = \overline{10}$, $\overline{6!} = \bar{6} \times \overline{10} = \overline{60} = \bar{5}$, $\overline{7!} = \bar{7} \times \bar{5} = \overline{35} = \bar{2}$, $\overline{8!} = \bar{8} \times \bar{2} = \overline{16} = \bar{5}$, $\overline{9!} = \bar{9} \times \bar{5} = \overline{45} = \bar{1}$ et enfin $\overline{10!} = \overline{10} \times \bar{1} = \overline{10} = -\bar{1}$. Ainsi on obtient bien pour $p = 11$ que $(p-1)!$ est congru à -1 modulo p.

2. Le théorème reste-t-il vrai si p n'est pas premier ?

Prenons $p = 6$. Alors $(p-1)! = 5! = 120$ qui est un multiple de 6. Donc $(p-1)!$ est ici égal à 0 modulo p. On a trouvé un contre-exemple au théorème de Wilson si on autorise p à ne pas être premier.

Passons à la démonstration du théorème. Soit $p \in \mathcal{P}$ et plaçons-nous dans $\mathbf{Z}/p\mathbf{Z}$.

3. Soient $\bar{a}$ et $\bar{b}$ dans $\mathbf{Z}/p\mathbf{Z}$. Montrer que si $\bar{a}\bar{b} = \bar{0}$, alors $\bar{a} = \bar{0}$ ou $\bar{b} = \bar{0}$.

On suppose que $\bar{a}\bar{b} = \bar{0}$. Cela signifie dans $\mathbf{Z}$ que ab est un multiple de p. Or p est un nombre premier. D'après le lemme d'Euclide, on en déduit que p divise a ou p divise b. Dans $\mathbf{Z}/p\mathbf{Z}$, cela signifie que $\bar{a} = \bar{0}$ ou $\bar{b} = \bar{0}$.
Remarque : ce résultat n'est plus vrai si on ne suppose pas p premier. Par exemple, modulo 6, on a $\bar{2} \times \bar{3} = \bar{0}$ pourtant $\bar{2}, \bar{3} \neq \bar{0}$.

4. En déduire que l'équation $x^2 - \bar{1} = \bar{0}$ n'a que deux solutions dans $\mathbf{Z}/p\mathbf{Z}$.

Soit $x \in \mathbf{Z}/p\mathbf{Z}$ tel que $x^2 - \bar{1} = \bar{0}$. Factorisons : $(x-\bar{1})(x+\bar{1}) = \bar{0}$. D'après la propriété précédente, on a le droit d'en déduire $x - \bar{1} = \bar{0}$ ou $x + \bar{1} = \bar{0}$. Les solutions de l'équation sont ainsi $x = \bar{1}$ et $x = -\bar{1}$.

5. Soit $\bar{x} \in \mathbf{Z}/p\mathbf{Z}$ avec $\bar{x} \neq \bar{0}$.
À l'aide de l'égalité de Bézout, montrer qu'il existe $\bar{y} \in \mathbf{Z}/p\mathbf{Z}$ tel que $\bar{x}\bar{y} = \bar{1}$.
Montrer de plus à l'aide des questions précédentes que $\bar{y}$ est unique et que si $\bar{x} \neq \pm\bar{1}$, alors $\bar{y} \neq \bar{x}$.

Soit $x \in \mathbf{Z}$ un représentant de $\bar{x}$. Comme $\bar{x} \neq 0$, on en déduit que x n'est pas un multiple de p. Et comme p est premier, on en déduit que x et p sont premier entre eux. On peut appliquer le théorème de Bézout : il existe des entiers relatifs y et z tels que $xy + zp = 1$. Réduisons cette égalité modulo p : $\bar{x}\bar{x} + \bar{z}\bar{p} = \bar{1}$. Comme $\bar{p} = \bar{0}$ il reste $\bar{x}\bar{y} = \bar{1}$.
Montrons l'unicité de $\bar{y}$. Soient $\bar{y}$ et $\bar{y}'$ tels que $\bar{x}\bar{y} = \bar{x}\bar{y}' = \bar{1}$. Alors $\bar{x}(\bar{y} - \bar{y}') = \bar{0}$. D'après la question 3, on peut en déduire $\bar{x} = \bar{0}$ ou $\bar{y} - \bar{y}' = \bar{0}$. Comme $\bar{x} \neq \bar{0}$, on en déduit $\bar{y} = \bar{y}'$.
Autre raisonnement possible : si $\bar{x}\bar{y} = \bar{y}'$, alors $\bar{y}\bar{x}\bar{y} = \bar{y}\bar{x}\bar{y}'$ et comme $\bar{y}\bar{x} = \bar{1}$, il reste $\bar{y} = \bar{y}'$.
Montrons la dernière remarque. Si $\bar{y} = \bar{x}$, alors on a obtenu $\bar{x}^2 = \bar{1}$. Or on a montré que les seuls solutions de cette équation sont $\bar{x} = \pm\bar{1}$. Donc si $\bar{x} \neq \pm\bar{1}$, alors $\bar{y} \neq \bar{x}$.

6. Démontrer le théorème de Wilson.
Dans le produit $(p-1)!$ on regroupera chaque entier a (sauf 1 et $p-1$) avec l'entier b de la question précédente lui correspondant.

Récapitulons : tout élément $\bar{a}$ de $\mathbf{Z}/p\mathbf{Z}$ admet un inverse dans $\mathbf{Z}/p\mathbf{Z}$ et sauf pour $\bar{1}$ et $-\bar{1}$, cet inverse est différent de lui. Considérons le produit $(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-2) \cdot (p-1)$ et réduisons-le modulo p. On peut regrouper dans ce produit chaque élément avec son inverse qui lui est différent (sauf pour $\bar{1}$ et $\overline{p-1} = -\bar{1}$). Leur produit fait $\bar{1}$ et on obtient finalement $\overline{(p-1)!} = \bar{1} \times (-\bar{1}) \times \bar{1} \times \bar{1} \times \cdots \times \bar{1} = -\bar{1}$.

Pour bien comprendre cette démonstration, regardons un exemple : pour $p = 11$, commençons par chercher les inverses des éléments de $\mathbf{Z}/11\mathbf{Z}$: $\bar{2} \times \bar{6} = \bar{1}$, $\bar{3} \times \bar{4} = \bar{1}$, $\bar{5} \times \bar{9} = \bar{1}$, et $\bar{7} \times \bar{8} = \bar{1}$. Alors

$$\overline{10!} = \bar{1} \cdot (\bar{2} \cdot \bar{6}) \cdot (\bar{3} \cdot \bar{4}) \cdot (\bar{5} \cdot \bar{9}) \cdot (\bar{7} \cdot \bar{8}) \cdot \bar{10} = \bar{1} \cdot \bar{1} \cdot \bar{1} \cdot \bar{1} \cdot \bar{1} \cdot (-\bar{1}) = -\bar{1}.$$