Équation de Pell-Fermat

On portera une attention particulière à **la rédaction** et à **la propreté** de la copie.
En particulier tout **graphe ou schéma** pertinent et correctement annoté sera **valorisé**.
Les résultats devront être mis en valeur dès que possible.

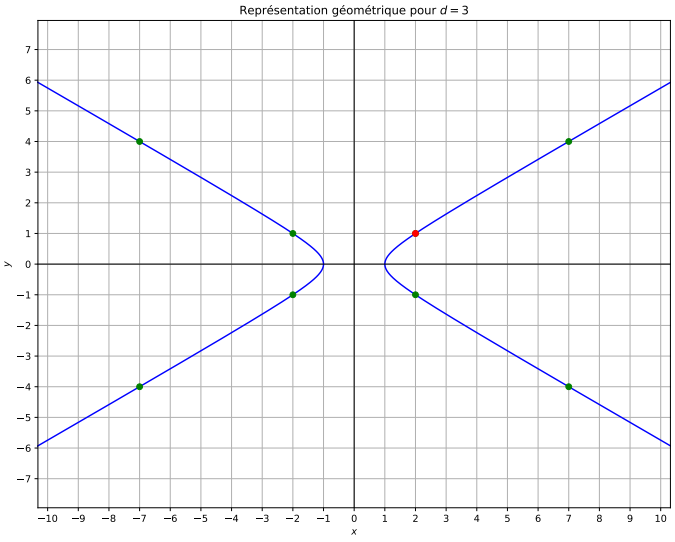
Indiquez sur votre copie le temps approximatif pris pour le devoir.

Contexte

L'objectif de ce problème est de d'étudier l'équation diophantienne de Pell-Fermat, c'est à dire de déterminer tous les couples $(x, y) \in \mathbb{Z}^2$ tels que

$$x^2 - dy^2 = 1. \qquad \text{(PF)}$$

- La partie 0 établit un disjonction de cas selon la valeur de d.
- La partie 1 étudie la structure de l'anneau $\mathbb{Z}[\sqrt{d}]$, et relie un sous-groupe G du groupe de ses inversibles à l'ensemble des solutions de l'équation de Pell-Fermat.
- La partie 2 étudie la structure du groupe G obtenu à la partie précédente.
- La partie 3 déterminer une asymptotique du nombre de solutions $(x, y) \in \mathbb{N}^2$ telles que $x \leq k$.
- Enfin la partie 4 démontre l'existence d'une solution non triviale admise dans les parties précédentes, en se ramenant à un problème d'approximation d'irrationnels quadratiques par des rationnels.
- Facultativement, la partie 5 interprète géométriquement les parties précédentes.



Notations

Dans tout le devoir on utilisera les notations suivantes:
- Dans tout le sujet $d \in \mathbb{N}^*$ est un entier naturel non nul fixé.
  On peut remarquer dès à présent qu'en dehors de la partie 0 on supposera de plus que d n'est pas un carré parfait.
- On note (PF) l'équation dite de Pell-Fermat:
$$x^2 - dy^2 = 1. \qquad \text{(PF)}$$
  d'inconnue $(x, y) \in \mathbb{Z}^2$.
- On note $\mathcal{S}_{(\text{PF})}$ l'ensemble des solutions de l'équation (PF), c'est à dire
$$\mathcal{S}_{(\text{PF})} = \left\{(x, y) \in \mathbb{Z}^2 \middle| x^2 - dy^2 = 1\right\}.$$
- On appellera ensemble des solutions *non triviales* de (PF) l'ensemble $\mathcal{S}_{(\text{PF})} \backslash \{(1, 0), (-1, 0)\}$ (voir partie 0).
- On notera
$$\mathbb{Z}[\sqrt{d}] = \left\{a + b\sqrt{d}, (a, b) \in \mathbb{Z}^2\right\}.$$
- Pour $x \in \mathbb{R}$ on notera $\lfloor x \rfloor$ la partie entière de x, c'est à dire le plus grand entier plus petit que x.
- Pour $x \in \mathbb{R}$ on notera $\{x\} = x - \lfloor x \rfloor$ la partie fractionnaire de x.

0 Préliminaires arithmétiques

0.1. Montrer que $(1, 0)$ et $(-1, 0)$ sont solutions de l'équation de Pell-Fermat (PF).
On appellera ces solutions *solutions triviales* et toute autre solution *solution non triviale*.

0.2. On suppose dans cette question que d est un carré parfait (c'est à dire qu'il existe $\delta \in \mathbb{N}$ tel que $d = \delta^2$).
Montrer que l'équation de Pell-Fermat (PF) n'admet pas de solution non triviale.

0.3. On suppose dans cette question que d n'est pas un carré parfait.
Montrer que $\sqrt{d} \notin \mathbb{Q}$.

Dans la suite on suppose que d n'est pas un carré parfait.
De plus dans les parties 2 et 3 on admettra que, dans ce cas, l'équation (PF) admet au moins une solution non-triviale.
Ce résultat sera démontré en partie 4.

---

1 Étude de $\mathbb{Z}[\sqrt{d}]$

1.4. Montrer que $\mathbb{Z}[\sqrt{d}]$ muni des opérations + et × usuelles est un anneau commutatif.
1.5. Montrer que l'application

$$\varphi : \begin{array}{c} \mathbb{Z}^2 \to \mathbb{Z}[\sqrt{d}] \\ (a,b) \mapsto a + b\sqrt{d} \end{array}$$

est un isomorphisme de groupes additifs.
Traduire l'injectivité de φ en termes d'unicité.
1.6. Montrer que l'on peut définir une application

$$\sigma : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}[\sqrt{d}]$$

telle que

$$\forall (a,b) \in \mathbb{Z}^2, \sigma\left(a + b\sqrt{d}\right) = a - b\sqrt{d}.$$

1.7. Montrer que

$$\sigma : \begin{array}{c} \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}[\sqrt{d}] \\ z \mapsto \sigma(z) \end{array}$$

est un automorphisme d'anneaux de $\mathbb{Z}[\sqrt{d}]$.
1.8. Soit $z \in \mathbb{Z}[\sqrt{d}]$ et $(a,b) \in \mathbb{Z}^2$ tel que $z = a + b\sqrt{d}$.
Exprimer a et b en fonction de z et $\sigma(z)$.
On pourra noter dans la suite $\pi_1(z) = a$ et $\pi_2(z) = b$.
Commenter.
Pour $z \in \mathbb{Z}[\sqrt{d}]$, on définit la *norme* de z, notée $N(z)$, par $N(z) = z \times \sigma(z)$.
1.9. Montrer que

$$\forall z \in \mathbb{Z}[\sqrt{d}]\ ,\quad N(z) \in \mathbb{Z}$$

et

$$\forall z \in \mathbb{Z}[\sqrt{d}]\ ,\quad N(z) = 0 \Leftrightarrow z = 0.$$

1.10. Montrer que

$$\forall (z_1, z_2) \in \mathbb{Z}[\sqrt{d}]\ ,\quad N(z_1 z_2) = N(z_1)N(z_2)$$

1.11. Soit $z \in \mathbb{Z}[\sqrt{d}]$.
Montrer que

$$z \in \left(\mathbb{Z}[\sqrt{d}]\right)^\times \ \Leftrightarrow\ N(z) \in \{-1, +1\}.$$

1.12. Montrer que

$$G = \left\{ z \in \mathbb{Z}[\sqrt{d}] \,\middle|\, N(z) = 1 \right\}$$

muni du produit × est un groupe.
1.13. Expliciter une bijection entre G et l'ensemble $\mathcal{S}_{(\mathrm{PF})}$.

2 Structure du groupe G

On rappelle que l'on admet dans cette partie que $\mathcal{S}_{(\mathrm{PF})} \neq \{(1,0),(-1,0)\}$.

2.14. Montrer que
$$H = G \cap]0,+\infty[$$
est un groupe.

2.15. Expliciter un isomorphisme de groupe entre G et $H \times \{-1,+1\}$.

2.16. Montrer que
$$H \cap]1,+\infty[\neq \emptyset.$$

2.17. Soient $z_1, z_2 \in H$ et $(a_1,b_1),(a_2,b_2) \in \mathbb{Z}^2$ tels que $z_1 = a_1 + b_1\sqrt{d}$ et $z_2 = a_2 + b_2\sqrt{d}$.
Montrer que
$$z_1 < z_2 \Rightarrow b_1 < b_2.$$
Interpréter ce résultat en termes de l'application π_2.

2.18. En déduire que
$$\xi = \min\left(H \cap]1,+\infty[\right)$$
est bien défini.

2.19. Expliquer succinctement pourquoi, pour tout $n \in \mathbb{Z}$, $\xi^n \in H$.

2.20. Soit $x \in H$.
Montrer qu'il existe et un unique $n \in \mathbb{Z}$ tel que
$$\xi^n \leq x < \xi^{n+1}.$$

2.21. Soit $x \in H$ et n tel que $\xi^n \leq x < \xi^{n+1}$.
Montrer que $x = \xi^n$.

2.22. Déduire des question précédentes que
$$H = \{\xi^n, n \in \mathbb{Z}\}$$

2.23. Conclure qu'il existe un et unique $(a_1,b_1) \in \mathbb{Z}^2$ tels que $a_1 + b_1\sqrt{d} > 1$ et
$$G = \left\{\varepsilon(a_1 + b_1\sqrt{d})^n, (n,\varepsilon) \in \mathbb{Z} \times \{-1,+1\}\right\}.$$
Commenter.

3 Estimée asymptotique du nombre de solutions

On rappelle le résultat suivant démontré à la partie 2:

Il existe un et unique $(a_1,b_1) \in \mathbb{Z}^2$ tels que $a_1 + b_1\sqrt{d} > 1$ et $G = \left\{\varepsilon(a_1 + b_1\sqrt{d})^n, (n,\varepsilon) \in \mathbb{Z} \times \{-1,+1\}\right\}$.

3.24. Montrer que pour tout $n \in \mathbb{N}$ on a
$$(a_1 + b_1\sqrt{d})^n = a_n + b_n\sqrt{d}$$
où $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in \mathbb{Z}^{\mathbb{N}}$ sont définies par
$$\begin{cases} a_0 = 1 \\ b_0 = 0 \end{cases}$$
et
$$\forall n \in \mathbb{N}, \begin{cases} a_{n+1} = a_n a_1 + d b_n b_1 \\ b_{n+1} = a_n b_1 + a_1 b_n \end{cases}$$

3.25. Pour tout $n \in \mathbb{N}$ on pose $X_n = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$.
Expliciter une matrice $A \in \mathrm{M}_2(\mathbb{Z})$ telle que
$$\forall n \in \mathbb{N}, X_{n+1} = AX_n.$$

3.26. Montrer que
$$\forall n \in \mathbb{N},\ A^n = \begin{pmatrix} \dfrac{\xi^n + \sigma(\xi)^n}{2} & d\dfrac{\xi^n - \sigma(\xi)^n}{2\sqrt{d}} \\ \dfrac{\xi^n - \sigma(\xi)^n}{2\sqrt{d}} & \dfrac{\xi^n + \sigma(\xi)^n}{2} \end{pmatrix}.$$

3.27. Soit $n \in \mathbb{N}$.
Déduire de la question précédente une expression explicite de a_n et b_n en fonction de ξ et de n.

3.28. Donner un équivalent simple quand $k \to +\infty$ de

$$\text{card}\left(\mathcal{S}_{(\text{PF})} \cap [\![-k, k]\!] \times \mathbb{R}\right)$$

4 Existence d'une solution non triviale

4.29. Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ et $C \in \mathbb{R}_+$. Montrer que

$$\left|\frac{a}{b} - \sqrt{d}\right| \leq \frac{C}{b^2} \Rightarrow |a^2 - db^2| \leq (2\sqrt{d} + C)C.$$

4.30. Soit $x \in \mathbb{R}$ et $N \in \mathbb{N}^*$.
Montrer qu'il existe $k, l \in [\![0, N]\!]$ tels que $k \neq l$ et

$$|\{kx\} - \{lx\}| \leq \frac{1}{N}.$$

4.31. Soit $x \in \mathbb{R}$ et $N \in \mathbb{N}^*$.
En déduire qu'il existe $p, q \in \mathbb{Z} \times \mathbb{N}^*$ tels que

$$\left|x - \frac{p}{q}\right| \leq \frac{1}{Nq}.$$

4.32. Soit $x \in \mathbb{R}\backslash\mathbb{Q}$.
Montrer qu'il existe une infinité de couples $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tels que

$$\left|x - \frac{p}{q}\right| \leq \frac{1}{q^2}.$$

4.33. En utilisant les questions précédentes montrer qu'il existe $\eta \in \mathbb{Z}$ tel que l'ensemble

$$\left\{z \in \mathbb{Z}[\sqrt{d}] \middle| N(z) = \eta\right\}$$

est infini.

On fixe dans la suite un tel $\eta \in \mathbb{Z}$.

4.34. Montrer qu'il existe $z_1, z_2 \in \mathbb{Z}[\sqrt{d}]$ tels que
- $|z_1| \neq |z_2|$,
- $N(z_1) = N(z_2) = \eta$,
- $\pi_1(z_1) \equiv \pi_1(z_2)[\eta]$,
- $\pi_2(z_1) \equiv \pi_2(z_2)[\eta]$.

On fixe désormais de tels z_1, z_2.

4.35. Montrer que $\dfrac{z_1\sigma(z_2)}{\eta} \in \mathbb{Z}[\sqrt{d}]$.

4.36. Conclure que (PF) admet au moins une solution non triviale.

5 Bonus facultatif: Interprétation géométrique

Ne traiter cette partie que si toutes les autres parties ont été traitée.
De nombreux schémas sont attendus dans cette partie.

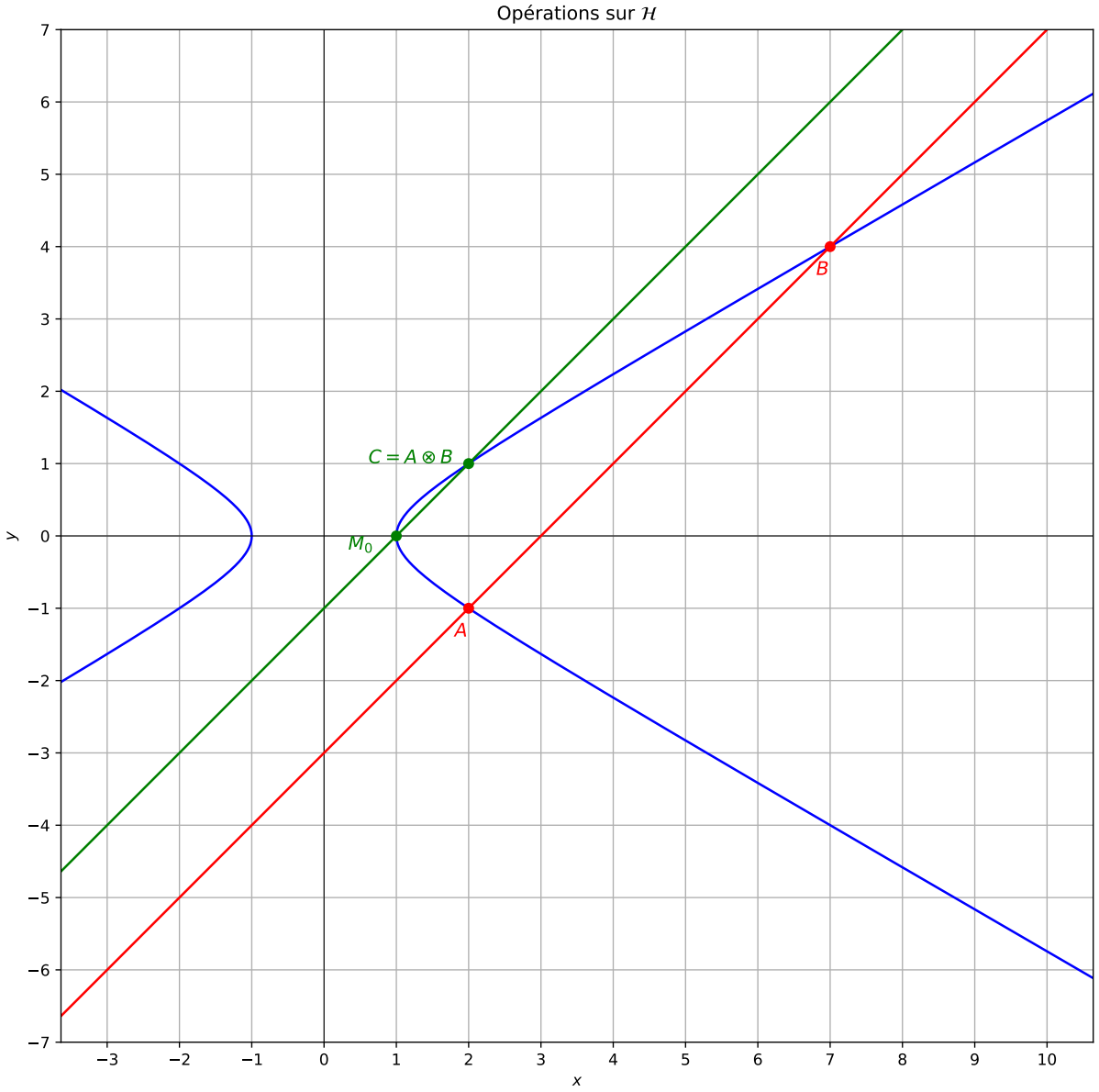
Dans cette partie on note

$$\mathcal{H} = \left\{(x, y) \in \mathbb{R}^2 \middle| x^2 - dy^2 = 1\right\}$$

et

$$\mathcal{H}^{\mathbb{Z}} = \mathcal{H} \cap \mathbb{Z}^2.$$

On note aussi M_0 le point de coordonnées $(1, 0)$.
Soient A, B deux points de $\mathcal{H}$.
On note Δ_{AB} la droite passant par A et B si $A \neq B$ et la tangente à $\mathcal{H}$ en A si $A = B$.
On note aussi $\widetilde{\Delta_{AB}}$ la droite parallèle à Δ_{AB} et passant par M_0.



5.37. Soient A, B de points de $\mathcal{H}$.

Montrer qu'il existe un unique point C tel que $\widetilde{\Delta_{AB}} \cap \mathcal{H} = \{M_0, C\}$.

On note alors

$$A \otimes B = C.$$

5.38. Interpréter géométriquement les résultats des parties précédentes.