Devoir Maison n° 8 : corrigé

MPSI Lycée Camille Jullian

20 février 2025

Problème : résolution d'une équation de Pell-Fermat.

A. Quelques généralités.

1. L'équation $y^2 - 4x^2 = 1$ peut se factoriser sous la forme $(y-2x)(y+2x) = 1$. Les nombres $y-2x$ et $y+2x$ étant supposés tous les deux entiers, ils sont donc tous les deux égaux à 1 ou à -1. Or, si $y-2x = y+2x$, alors $x = 0$, et on a donc $y^2 = 1$, ce qui nous donne simplement deux solutions : $(0,1)$ et $(0,-1)$. C'est exactement la même chose quand $d = c^2$: $(y-cx)(y+cx) = 1$, et on en déduit rapidement que $x = 0$ et $y = \pm 1$.
2. Soit G un sous-groupe de $(\mathbb{R}, +)$, tel que $\exists \varepsilon > 0$, $G \cap]0, \varepsilon[= \emptyset$.
   (a) Supposons par l'absurde qu'il existe un deuxième élément $y \in G$ compris dans l'intervalle $]x-\varepsilon, x+\varepsilon[$ (et différent de x). On aurait alors $y - x \in]0, \varepsilon[$ ou $x - y \in]0, \varepsilon[$ (selon que $x < y$ ou $y < x$), ce qui contredit l'hypothèse faite sur le groupe G puisque clairement $y - x$ et $x - y$ sont des éléments de G quand G est un groupe additif.
   (b) Le cas particulier $G = \{0\}$ est bien sûr un sous-groupe additif de $\mathbb{R}$ vérifiant l'hypothèse de l'énoncé. Si on suppose que G n'est pas réduit à 0, alors il existe un élément non nul dans G. Quitte à considérer son opposé, il existe même un élément strictement positif dans G. L'ensemble des éléments strictement positifs de G est alors non vide et minoré, il admet une borne inférieure a qui ne peut pas être nulle (elle est supérieure ou égale à ε avec l'hypothèse faite sur G). Si on suppose que $a \notin G$ (autrement dit que cette borne inférieure n'est pas un minimum), alors par caractérisation de la borne inférieure, il existe un élément de G appartenant à l'intervalle $]a, a+\varepsilon[$ (où ε est le réel vérifiant la condition de l'énoncé). Cela contredit le résultat de la question précédente et prouve donc (par l'absurde) que $a \in G$.
   (c) G étant un groupe additif, il contient tous les multiples de a, donc $a\mathbb{Z} \subset G$. De plus, par définition de a, $G \cap]0, a[= \emptyset$, et les questions précédentes permettent alors d'affirmer qu'il n'existe aucun élement de G dans chaque intervalle de la forme $]ka, (k+1)a[$, quel que soit l'entier raltif k. Les seuls éléments de G sont donc les multiples de a, et $G = a\mathbb{Z}$.
3. Si on note $G = \{\ln(x) \mid x \in H\}$, l'ensemble G est un sous-groupe additif de $\mathbb{R}$ (puisque G est un isomorphisme de groupes de $(\mathbb{R}^{+*}, \times)$ vers $(\mathbb{R}, +)$) qui ne contient aucun élément dans l'intervalle $]0, \ln(1+\varepsilon)[$. En appliquant les résultats de la question précédente, il existe alors un réel strictement positif a tel que $G = a\mathbb{Z}$. Il suffit de noter $b = e^a$ et d'appliquer la fonction exponentielle (isomorphisme réciproque) pour en déduire que $H = \{e^{ka} \mid k \in \mathbb{Z}\} = \{b^k \mid k \in \mathbb{Z}\}$.

B. L'anneau $\mathbb{Z}[d]$.

1. Il faut vérifier les choses suivantes :

- $\mathbb{Z}_d$ est un sous-groupe additif de $\mathbb{Z}$, ce qui est assez évident (il contient $0 = 0 + 0\sqrt{d}$, est stable par passage à l'opposé puisque $-(a + b\sqrt{d}) = -a + (-b)\sqrt{d}$, et stable par somme de façon triviale puisque $(a + b\sqrt{d}) + (c + e\sqrt{d}) = (a + c) + (b + e)\sqrt{d}$, les paramètres a, b, c et e étant supposés entiers, et leur somme l'étant donc aussi).
- le neutre pour le produit appartient à $\mathbb{Z}_d$, puisque $1 = 1 + 0\sqrt{d}$.
- la stabilité par produit nécessite un calcul à peine plus sophistiqué que les précédents : $(a + b\sqrt{d})(c + e\sqrt{d}) = ac + ae\sqrt{d} + bc\sqrt{d} + bed = (ac + bed) + (ae + bc)\sqrt{d} \in \mathbb{Z}_d$, avec comme précédemment tous les paramètres idoines supposés entiers.

2. C'est une classique démonstration par l'absurde qu'on peut désormais rédiger très rapidement : si on suppose $\sqrt{d} = \dfrac{p}{q}$, alors $p^2 = dq^2$, avec p et q tous les deux entiers. Les valuations n-adiques des deux entiers p^2 et q^2 sont toutes paires, quel que soit l'entier premier n (en effet, $v_n(p^2) = 2v_n(p)$ d'après les propriétés vues en cours). On devrait donc avoir, pour tout entier premier n, $v_n(d) = 2v_n(p) - 2v_n(q)$ qui est également un nombre pair. Or, ce n'est pas le cas si d n'est pas un carré d'entier (un nombre dont toutes les valuations n-adiques sont paires est clairement le carré d'un entier dont on obtient la décomposition en facteurs premiers en divisant par 2 toutes les valuations n-adiques de d). C'est aburde, donc d est irrationnel.
3. Pour se simplifier la rédaction, posons (façon « nombres complexes ») $\overline{x} = a - b\sqrt{d}$ pour tout élément $x = a + b\sqrt{d}$ appartenant à $\mathbb{Z}_d$. On a alors $N(x) = x\overline{x}$, et donc $N(xy) = xy\overline{xy}$. Constatons alors que $\overline{x} \times \overline{y} = (a - b\sqrt{d})(c - e\sqrt{d}) = ac + bed - (ae + bc)\sqrt{d} = \overline{xy}$ (avec les notations évidentes). On peut alors terminer le calcul : $N(xy) = xy\overline{xy} = x\overline{x}y\overline{y} = N(x)N(y)$. Si $N(x) = 0$, alors $a^2 - db^2 = 0$, donc $d = \dfrac{a^2}{b^2}$ est rationnel, sauf bien sûr si $b = 0$, ce qui implique $a^2 = a = 0$. Comme d est irrationnel, le seul élément vérifiant $N(x) = 0$ est donc 0.
4. Si $N(x) = 1$, alors $x\overline{x} = 1$, donc $\overline{x}$ est inverse de x (et appartient clairement à $\mathbb{Z}_d$. De même, si $N(x) = -1$, c'est $-\overline{x}$ qui sera l'inverse de x. Réciproquement, si x admet un inverse y dans $\mathbb{Z}_d$, alors $N(xy) = N(1) = 1$, donc $N(x)N(y) = 1$. Comme $N(x)$ et $N(y)$ sont des entiers, ils sont donc égaux tous les deux à ± 1.
5. L'application $N : x \mapsto N(x)$ est d'après les calculs précédents un morphisme de groupes (multiplicatifs) de I_d vers $\{-1, 1\}$. Son noyau (les antécédents de 1 par l'application N) est donc un sous-groupe de I_d, ce qui prouve exactement que U est un sous-groupe de I_d. Ensuite, I_d^+ et U_+ sont simplement des intersections de groupes multiplicatifs avec $\mathbb{R}^{+*}$ qui est lui-même un groupe multiplicatif, donc sont des groupes multiplicatifs. Comme ils sont respectivement inclus dans I_d et dans U, il s'agit bien également de sous-groupes de ces groupes.
6. Supposons donc qu'il existe deux entiers naturels (quitte à prendre les valeurs absolues) vérifiant $a^2 - 3b^2 = -1$. Si on procède modulo 4, on en déduit alors que $a^2 + b^2 \equiv 3[4]$ (puisque $-3b^2 \equiv b^2[4]$, on a le droit de multiplier des congruences). Or, il est impossible d'obtenir 3 comme somme de deux carrés modulo 4 : $0^2 \equiv 0[4]$, $1^2 \equiv 1[4]$, $2^2 \equiv 0[4]$ et $3^2 \equiv 1[4]$, donc on ne peut obtenir que 0, 1 ou 2 en ajoutant deux carrés. Il est impossible d'avoir $N(x) = -1$ dans $\mathbb{Z}_3$, ce qui prouve que tous les éléments de I_3 vérifient $N(x) = 1$, et donc que $I_3 = U$ dans ce cas.

C. Résolution de l'équation de Pell-Fermat.

1. Il y a un sens évident : si a et b sont des entiers tous les deux non nuls, $x = a + b\sqrt{d} > a \geqslant 1$, donc $x > 1$. Réciproquement, supposons $x > 1$, alors son inverse $\overline{x}$ appartient aussi à I_d et doit être strictement compris entre 0 et 1. Autrement dit, on a $0 < a - b\sqrt{d} < 1$ et $1 < a + b\sqrt{d}$. En additionnant les deux inégalités de gauche, on a donc $2a > 1$, donc $a > 0$. Mais on en déduit aussi que $b\sqrt{d} > a - 1 \geqslant 0$, donc $b > 0$.
2. Puisqu'on a supposé que $U^+ \neq \{1\}$, U^+ contient un élément différent de 1 et donc, quitte à passer à l'inverse, un élément strictement supérieur à 1. Mais il ne peut pas contenir d'élément

compris entre 1 et $1+\sqrt{d}$, puisque les éléments de U^+ sont de la forme $a+b\sqrt{d}$, avec a et b entiers non nuls d'après la question précédente. On peut donc appliquer le résultat de la première partie pour obtenir exactement ce qui est demandé par l'énoncé. Si on connaît le générateur $\alpha = a+b\sqrt{d}$ (autrement dit si on connaît les plus petites valeurs de a et b formant un couple de solutions), il suffit alors de calculer $\alpha^n = (a+b\sqrt{d})^n$ et de le mettre sous la forme $a_n + b_n\sqrt{d}$ pour obtenir les autres couples solutions (a_n, b_n). On obtiendra ainsi toutes les solutions consitituées de couples d'entiers naturels, on peut bien sûr changer le signe d'un de cex deux entiers (ou des deux) pour en déduire trivialement toutes les solutions entières relatives.

3. On ne peut pas obtenir de couple $(a,1)$ solution car $a^2 = 3$ ne donne pas vraiment de solutions entières. Si on teste avec $b=2$, on trouve l'équation $a^2 = 9$, et on en déduit donc que $\alpha = 3+2\sqrt{2}$ (et que $(3,2)$ est notre plus petite solution). On calcule alors $\alpha^2 = (3+2\sqrt{2})^2 = 9+12\sqrt{2}+8 = 17+12\sqrt{12}$ pour en déduire que $(17,12)$ est le deuxième couple solution (en effet, $17^2 - 2\times 12^2 = 289 - 2\times 144 = 1$), puis $\alpha^3 = (3+2\sqrt{2})^3 = 27+54\sqrt{2}+72+16\sqrt{2} = 99+70\sqrt{2}$ pour trouver le troisième couple solution $(99,70)$ (eh oui, $99^2 - 2\times 70^2 = 9\,801 - 2\times 4\,900 = 1$).

4. (a) Petit bug dans l'énoncé, on veut $z>1$ et pas $z>0$. À nouveau, il y a une implication évidente. Pour l'autre, on reprend le même type de raisonnement que ci-dessus : si $z = a+b\sqrt{d} > 1$, alors $-\overline{z} = b\sqrt{d} - a \in]0,1[$, donc en additionnant $2b\sqrt{d} > 1$, ce qui revient à dire que $b \in \mathbb{N}^*$. Mais alors $a \geqslant b\sqrt{d} - 1 \geqslant \sqrt{d} - 1 > 0$.

   (b) Exactement de la même façon que pour U^+, le groupe n'admet aucun élément compris entre 1 et $1+\sqrt{d}$, donc est engendré par son plus petit élément strictement supérieur à 1, qu'on va donc noter β. Par hypothèse, $\beta \notin I_d$ (sinon l'équation $a^2 - db^2 = 1$ aurait des solutions mais pas l'équation $a^2 - db^2 = -1$). Par contre, $\beta^2 \in I_d$ puisque $N(\beta^2) = N(\beta)^2 = (-1)^2 = 1$, donc $\beta^2 = \alpha$ (c'est nécessairement le plus petit élément strictement supérieur à 1 de I_d).

5. (a) Commençons par regarder une fois de plus ce qui se passe modulo 4 (oui, je sais, ce n'est pas très logique). On doit avoir $x^2 - y^2 \equiv -1[4]$ (puisque $-13 \equiv -1[4]$). Or, le calcul des carrés modulo 4 effectué plus haut montre qu'une différence de carrés ne peut être égale à -1 que si x est pair, et y impair. Passons alors à une étude modulo 3 : $x^2 + 2y^2 = 2$ (car -13 et -1 sont congrus à 2 modulo 3). Les carrés modulo 3 étant 0, 1 et 1, la seule possibilité est d'avoir $0 + 2\times 1$, donc que x soit multiple de 3 (et accessoirement que y ne soit **pas** multiple de 3, mais on s'en fout). Finalement, x étant à la fois pair et multiple de 3, il est bien multiple de 6.

   (b) Si on se place modulo 13, on doit avoir $x^2 \equiv 12[13]$. Il ne reste donc qu'à calculer joyeusement tous les carrés modulo 13 : $0^2 \equiv 0[13]$, $1^2 \equiv 1[13]$, $2^2 \equiv 4[13]$, $3^2 \equiv 9[13]$, $4^2 \equiv 3[13]$, $5^2 \equiv 12[13]$, $6^2 \equiv 10[13]$, $7^2 \equiv 10[13]$, $8^2 \equiv 12[13]$, $9^2 \equiv 3[13]$, $10^2 \equiv 9[13]$, $11^2 \equiv 4[13]$ et $12^2 \equiv 1[13]$. On constate une belle symétrie, mais surtout que les seules possibilités sont donc $x \equiv 5[13]$ et $x \equiv 8[13]$.

   (c) On cherche un multiple de 6 qui vérifie l'une des deux congruences de la question précédente : ça ne marche évidemment pas pour 6 ni pour 12 mais $18 \equiv 5[13]$. Coup de pot, $18^2 = 324$, donc $18^2 + 1 = 325 = 5\times 65 = 5^2 \times 13$, et le couple $(18,5)$ est solution de notre équation ! On a donc $\beta = 18 + 5\sqrt{13}$.

   (d) Calculons brutalement $\alpha = \beta^2 = (18+5\sqrt{13})^2 = 324 + 180\sqrt{13} + 325 = 649 + 180\sqrt{13}$, ce qui prouve que le couple $(649, 180)$ est la plus petite solution de l'équation $x^2 - 13y^2 = 1$. Il faut calculer la suivante ? Allons-y : $\alpha^2 = (649 + 180\sqrt{13})^2 = 421\ 201 + 233\ 640\sqrt{13} + 421\ 200 = 842\ 401 + 233\ 640\sqrt{13}$. Notre deuxième solution est donc le couple $(842\ 401, 233\ 640)$. Mais oui : $842\ 401^1 = 709\ 639\ 444\ 801$, et $13 \times 233\ 640^2 = 842\ 401^1 = 709\ 639\ 444\ 800$, ça sautait aux yeux.