MPSI 1

Mathématiques
DS 05

Samedi 13 janvier – 8h-12h

- Durée : 4 heures.
- Toute calculatrice ou appareil électronique est interdit.
- Le sujet est constitué de deux problèmes : un d'analyse et un d'algèbre.
- Le sujet est **long** : il **ne faut pas** essayer de tout faire. Un sujet long vous permet de **choisir** ce qui vous inspire le plus. Repérez les questions indépendantes, les parties indépendantes des autres, etc.
- Prenez **10-15 minutes** pour lire le sujet en entier et décider de la stratégie que vous adopterez.
- **Encadrez, soulignez vos résultats** et **numérotez vos pages**.
- À tout moment, vous pouvez admettre le résultat d'une question pour pouvoir continuer : il suffit de le préciser clairement sur la copie.
- Si vous voyez ce qui semble être une erreur d'énoncé, indiquez-le sur la copie.
- Essayez de changer de copie, au moins de page, lorsque vous changez d'exercice ou de partie.
- Laissez de la place dans une marge à gauche pour pouvoir noter plus facilement le devoir.
- Une réponse fausse, si elle ne laisse pas paraître de calculs intermédiaires, compte 0 points ; avec calculs intermédiaires elle peut rapporter quelques points.

♫ Bon courage ! ♫

En début de copie, merci d'indiquer votre objectif personnel pour ce devoir.

Problème 1. Théorème de Sarkovskii

« Period Three implies chaos[1] *»*

Soit I un intervalle, $f : \mathrm{I} \to \mathrm{I}$, n un entier.

- Si $k \in \mathbb{N}$, on note $f^k = \underbrace{f \circ f \circ \cdots \circ f}_{k \text{ fois}}$ avec par convention $f^0 = \mathrm{Id}_\mathrm{I}$.
- Un point x de I est dit **de période** n si $f^n(x) = x$ et pour tout k dans $[\![1, n-1]\!]$, $f^k(x) \neq x$.

Nous allons démontrer le théorème de Sarkovskii, qui s'énonce simplement sous cette forme :

Théorème 1

Si f est continue et admet un point de période 3, alors f admet un point de période n pour tout n dans $\mathbb{N}$.

A. Questions préliminaires

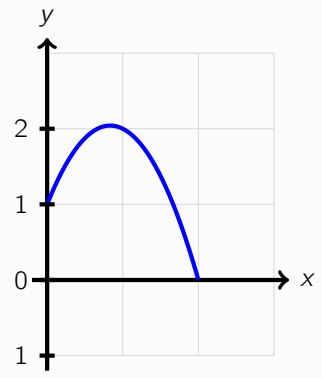
1. On note

$$P : x \mapsto -\frac{3}{2}x^2 + \frac{5}{2}x + 1 = -\frac{1}{2}(x-2)(3x+1).$$

Représenter à main levée le graphe de P et vérifier que 0 est un point de période 3 de P.

Correction

On a le graphe suivant



On calcule, $P(0) = 1$, $P(1) = 2$, $P(2) = 0$, ce qui signifie bien que 0 est un point de période 3.

2. Si I est un segment $[a, b]$ et $f : \mathrm{I} \to \mathrm{I}$ est continue, démontrer que f admet un point fixe.

1. J. Yorke, T-Y. Li, *Period Three Implies Chaos*, American Mathematical Monthly 82 (1975), 985-992.

Correction

C'est un exercice corrigé en classe. On considère $g : x \mapsto f(x) - x$. Alors

- g est continue,
- $g(a) = f(a) - a \geqslant 0$, car $f(a) \in [a, b]$,
- $g(b) = f(b) - b \leqslant 0$ car $f(b) \in [a, b]$.

Donc, par le théorème des valeurs intermédiaires, on dispose de $x_0 \in [a, b]$ tel que $g(x_0) = 0$, i.e. tel que $f(x_0) = x_0$.

3. Si $f : \mathrm{I} \to \mathrm{I}$ est continue, si α et β sont deux points de I et $[\alpha, \beta] \subset f([\alpha, \beta])$, démontrer que f admet un point fixe dans $[\alpha, \beta]$.

Correction

C'est aussi un exercice corrigé en classe. On considère $g : x \mapsto f(x) - x$.
Comme $[\alpha, \beta] \subset f([\alpha, \beta])$, on dispose de $(a, b) \in [\alpha, \beta]^2$ tels que $f(a) = \alpha$ et $f(b) = \beta$. Alors

- g est continue,
- $g(a) = f(a) - a = \alpha - a \leqslant 0$, car $a \in [\alpha, \beta]$,
- $g(b) = f(b) - b = \beta - b \geqslant 0$ car $b \in [\alpha, \beta]$.

Donc, par le théorème des valeurs intermédiaires, on dispose de $x_0 \in [\alpha, \beta]$ tel que $g(x_0) = 0$, i.e. tel que $f(x_0) = x_0$.

B. Un lemme utile

Notre but est de montrer le lemme suivant

Lemme 2

Soit f une fonction continue de I dans I, soit $K = [\alpha, \beta]$ un segment de I. On suppose que $K \subset f(\mathrm{I})$. Alors il existe $(c, d) \in \mathrm{I}^2$ tels que $K = f([c, d])$.

On se donne donc une fonction f continue de I dans I et $K = [\alpha, \beta]$ un segment de I non réduit à un point ($\alpha < \beta$). On suppose que $K \subset f(\mathrm{I})$.

4. Justifier qu'il existe $(a, b) \in \mathrm{I}^2$ tels que $f(a) = \alpha$ et $f(b) = \beta$.

Correction

Comme on supose que $K \subset f(\mathrm{I})$, $\alpha \in f(\mathrm{I})$ donc on dispose de a dans I tel que $f(a) = \alpha$. De même pour β.

On suppose, pour éviter de multiplier les cas à traiter, que $a < b$.

5. Soit $A = \{x \in [a, b], f(x) = \beta\}$. Justifier l'existence de $v = \min A$. On considère de même $u = \max B$ où $B = \{x \in [a, v], f(x) = \alpha\}$.

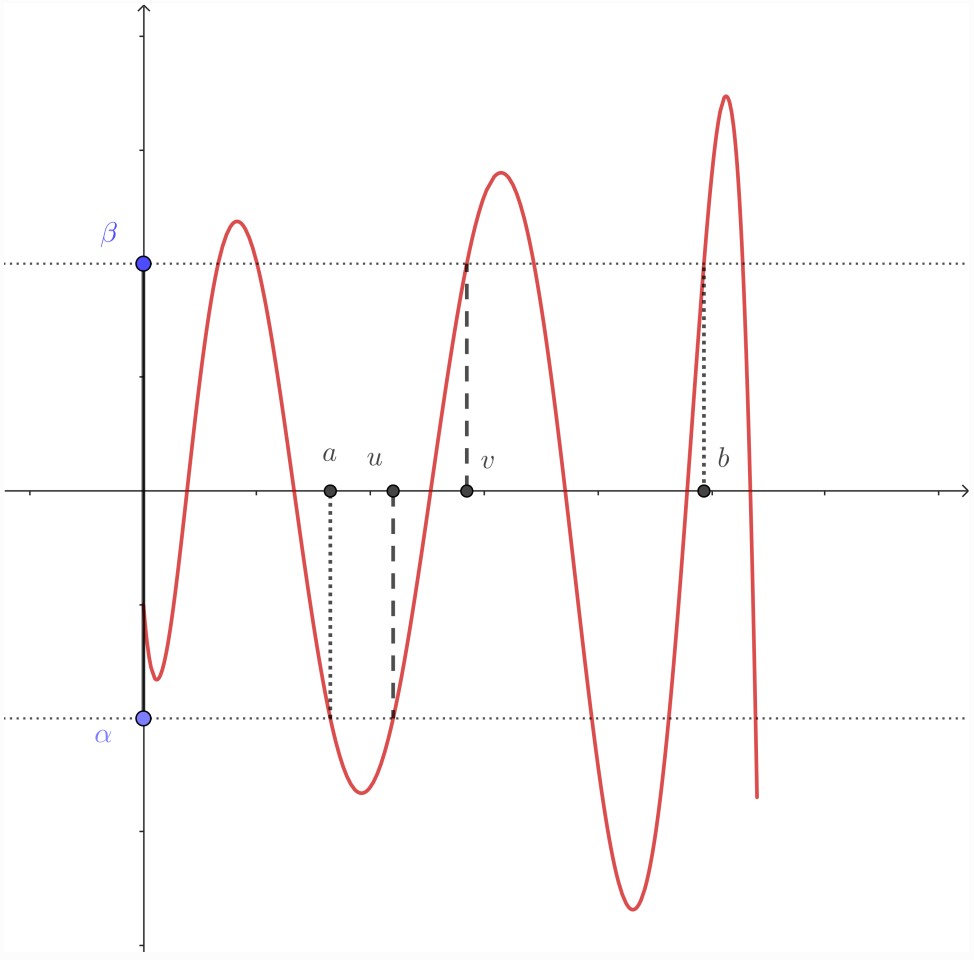
Correction

La partie A est une partie non vide de $\mathbb{R}$, car $b \in A$, minorée par a, donc elle admet une borne inférieure v. Il faut montrer que $v \in A$.
Par caractérisation séquentielle de la borne inférieure, on dispose de $(v_n)_{n\in\mathbb{N}}$ une suite d'éléments de A telle que $v_n \underset{n\to+\infty}{\longrightarrow} v$.
Par continuité de f, $f(v_n) \underset{n\to+\infty}{\longrightarrow} f(v)$. Mais, pour tout n dans $\mathbb{N}$ $f(v_n) = \beta$. Donc, par unicité de la limite, $f(v) = \beta$.
Ainsi, $v \in A$, donc $v = \min(A)$.

6. Illustrer par un dessin clair la situation et démontrer que $K = f([u, v])$.

Correction

On dessine : on a pris a et b des antécédents quelconques de α et β, et on a montré qui étaient alors u et v.



Déjà, comme $f(u) = \alpha$ et $f(v) = \beta$, on sait, par continuité de f et en vertu du théorème des valeurs intermédiaires, que $[\alpha, \beta] \subset f([u, v])$.

Supposons, par l'absurde, qu'on n'ait pas l'égalité $[\alpha,\beta] = f([u,v])$. Alors on disposerait de $w \in [u,v]$ tel que $f(w) \notin [\alpha,\beta]$.

- si $f(w) < \alpha$, alors $w > u$. Mais, par le théorème des valeurs intermédiaires, comme $f(w) < \alpha < \beta = f(v)$ et f est continue, on disposerait de $x \in]w,v[$ tel que $f(x) = \alpha$. Mais alors $x \in B$ et $x > u$, ce qui contredit la maximalité de u.
- on fait de même si $f(w) > \beta$.

Ainsi, on a bien $\boxed{[\alpha,\beta] = f([u,v])}$.

C. Preuve du théorème

On suppose que f est continue sur I (toujours à valeurs dans I) et admet un point $a \in \mathrm{I}$ de période 3. On note $b = f(a)$ et $c = f(b)$. On fixe un entier $n \in \mathbb{N}$. Les points a, b, c sont deux à deux distincts, étant donné que a est de période 3.
Il faudrait traiter plusieurs cas, mais **nous allons nous focaliser sur le cas $a < b < c$.** On note $J = [a, b]$ et $K = [b, c]$.

C-I. Une suite de segments

7. Démontrer que $K \subset f(J)$, que $J \subset f(K)$ et que $K \subset f(K)$.

Correction

On sait que $f(a) = b$ et $f(b) = c$. Ainsi, par le théorème des valeurs intermédiaires, pour tout M dans $[b, c]$, on dispose de x dans $[a, b]$ tel que $f(x) = M$. Donc $f([a, b]) \supset [b, c]$, c'est-à-dire $\boxed{K \subset f(J)}$.
De la même manière, comme $f(b) = c$ et $f(c) = a$, on en déduit, par le théorème des valeurs intermédiaires, que $[a, c] \subset f([b, c])$, donc $\boxed{J \cup K \subset f(K).}$ Les deux derniers résultats sont donc prouvés.

8. Démontrer qu'il existe une suite de segments $(L_0, \dots, L_{n-2})$ vérifiant

$$L_0 = K \text{ et } \forall i \in [\![1, n-2]\!],\ f(L_i) = L_{i-1},$$

vérifiant $L_{n-2} \subset L_{n-3} \subset \cdots \subset L_1 \subset L_0$ et, pour tout i dans $[\![0, n-2]\!]$, $f^i(L_i) = K$.

Correction

Il s'agit de bien appliquer le lemme 2.

- On pose $L_0 = K$. En particulier, $f^0(L_0) = L_0 = K$.
- Ensuite, $K \subset f(K)$, i.e. $L_0 \subset f(L_0)$, donc, par le lemme 2, on dispose de $L_1 \subset L_0$ tel que $f(L_1) = L_0$. Alors $f^1(L_1) = L_0 = K$.
- Mais alors $L_1 \subset L_0 = f(L_1)$ donc, par le lemme 2, on dispose de $L_2 \subset L_1$ tel que $f(L_2) = L_1$. Donc $f^2(L_2) = f(L_1) = L_0$.

On poursuit la construction par récurrence : si $L_0, \dots, L_i$ sont construits, on sait que $L_i \subset L_{i-1} = f(L_i)$, donc on dispose de L_{i+1} dans L_i vérifiant $f(L_{i+1}) = L_i$.
De plus, $f^{i+1}(L_{i+1}) = f^i(f(L_{i+1})) = f^i(L_i) = K$, par hypothèse de récurrence.

9. Démontrer que $J \subset f^{n-1}(L_{n-2})$.
En déduire l'existence de $L_{n-1} \subset L_{n-2}$ tel que $f^{n-1}(L_{n-1}) = J$.

Correction

On sait que $f^{n-1}(L_{n-2}) = f(f^{n-2}(L_{n-2})) = f(K)$ et on a vu à la question 7. que $J \subset f(K)$.
Donc $J \subset f^{n-1}(L_{n-2})$.
Comme f^{n-1} est continue, toujours par le lemme 2, on dispose de $L_{n-1} \subset L_{n-2}$ tel que $J = f^{n-1}(L_{n-1})$.

10. De même, démontrer qu'il existe $L_n \subset L_{n-1}$ vérifiant $f^n(L_n) = K$.

Correction

Il suffit de remarquer que, par la question 7., on sait que $K \subset f(K) = f^n(L_{n-1})$.
Encore et toujours par le lemme, on dispose de $L_n \subset L_{n-1}$ vérifiant $f^n(L_n) = K$.

C-II. Fin de la preuve

11. Montrer que f^n admet au moins un point fixe dans L_n. On notera x_0 l'un de ces points fixes.

Correction

On sait que $L_n \subset L_{n-1} \subset \cdots \subset L_1 \subset L_0 = K = f^n(L_n)$. Donc $L_n \subset f^n(L_n)$. Par la question 3., on sait que f^n admet un point fixe dans L_n.

12. Montrer que $x_0 \notin \{b, c\}$.

Correction

Résumons un peu ce que l'on sait ! On sait que

$$L_n \subset L_{n-1} \subset L_{n-2} \subset \cdots \subset L_1 \subset L_0 = K.$$

Donc, comme $x_0 \in L_n$, x_0 est dans tous les autres L_i ! Ainsi,

- $x_0 \in K$,
- pour tout i dans $[\![0, n-2]\!]$, $f^i(x_0) \in f^i(L_i) = K$,
- $f^{n-1}(x_0) \in f^{n-1}(L_{n-1}) = J$.

Supposons par l'absurde que $x_0 \in \{b, c\}$:

- si $x_0 = b = f(a)$, alors $f^2(x_0) = f^3(a) = a$, mais $a \notin K$, **absurde !**
- si $x_0 = c = f^2(a)$, alors $f(x_0) = f^3(a) = a$, mais $a \notin K$, **absurde !**

Donc $x_0 \notin \{b, c\}$.

13. Conclure que x_0 est de période n.

Correction

Déjà, $f^n(x_0) = x_0$.
Ensuite, si on avait $k < n$ tel que $f^k(x_0) = x_0$, alors :

- ou bien $k = n-1$, donc $f^{n-1}(x_0) = x_0$, ce qui est absurde car $f^{n-1}(x_0) \in J$ et $x_0 \notin J$ (car $x_0 \neq b$)
- ou bien $k < n-1$, mais alors quel que soit i, $f^i(x_0) \in K$, ce qui est absurde aussi car $f^{n-1}(x_0) \notin K$.

On en déduit que pour tout k dans $[\![1, n-1]\!]$, $f^k(x_0) \neq x_0$, donc x_0 est de période n.

Problème 2. L'équation de Pell-Fermat

Mathématiques indiennes et européennes.

Soit $\omega \in \mathbb{N}^*$, qui ne soit pas le carré d'un entier. Le but de ce problème est de déterminer l'ensemble des solutions de l'équation de Pell-Fermat :

$$a^2 - \omega b^2 = 1, \qquad (PF_\omega)$$

d'inconnues a et b dans $\mathbb{Z}$. On nomme S_ω l'ensemble des solutions :

$$S_\omega = \{(a,b) \in \mathbb{Z}^2,\ a^2 - \omega b^2 = 1\}.$$

On remarque que $(1,0)$ et $(-1,0)$ sont solutions triviales de (PF_ω) : on appellera **solution non triviale** de (PF_ω) toute solution différente de $(1,0)$ et $(-1,0)$. On note enfin

$$G_\omega = \{(a,b) \in \mathbb{Z}^2,\ a^2 - \omega b^2 = 1 \text{ ou } a^2 - \omega b^2 = -1\}.$$

1. Établir l'identité de Brahmagupta (mathématicien indien, 598-670) : pour tous a, b, c, d entiers relatifs,

$$(a^2 - \omega b^2)(c^2 - \omega d^2) = (ac + \omega bd)^2 - \omega(ad + bc)^2.$$

Correction

Soient a, b, c, d quatre entiers relatifs. Développons chacun des membres de l'égalité à démontrer. D'une part,

$$(a^2 - \omega b^2)(c^2 - \omega d^2) = a^2c^2 - \omega a^2d^2 - \omega b^2c^2 + \omega^2 b^2 d^2.$$

D'autre part,

$$\begin{aligned}(ac + \omega bd)^2 - \omega(ad + bc)^2 &= a^2c^2 + 2ac\omega bd + \omega^2 b^2 d^2 - \omega a^2 d^2 - 2\omega adbc - \omega b^2 c^2 \\ &= a^2c^2 - \omega a^2 d^2 - \omega b^2 c^2 + \omega^2 b^2 d^2 \\ &= (a^2 - \omega b^2)(c^2 - \omega d^2).\end{aligned}$$

L'identité de Brahmagupta est donc démontrée.

A. Étude d'un anneau

On définit

$$\mathbb{Z}[\sqrt{\omega}] = \left\{a + \sqrt{\omega} b,\ (a,b) \in \mathbb{Z}^2\right\}.$$

2. Montrer que $\mathbb{Z}[\sqrt{\omega}]$ est un sous-anneau de $(\mathbb{R}, +, \times)$.

Correction

Déjà $1 = 1 + \sqrt{\omega} \times 0$, donc $1 \in \mathbb{Z}[\sqrt{\omega}]$.
Ensuite, soient x et y dans $\mathbb{Z}[\sqrt{\omega}]$. Alors on dispose de $(a, b, c, d) \in \mathbb{Z}^4$ tels que $x = a + \sqrt{\omega}b$ et $y = c + \sqrt{\omega}d$. Alors

$$x - y = (a - c) + (b - d)\sqrt{\omega}, \text{ avec } (a - c) \in \mathbb{Z} \text{ et } (b - d) \in \mathbb{Z},$$

donc $x - y \in \mathbb{Z}[\sqrt{\omega}]$.
De même,

$$xy = (a+\sqrt{\omega}b)(c+\sqrt{\omega}d) = ac+\sqrt{\omega}ad+\sqrt{\omega}bc+\omega bd = (ac+\omega bd)+\sqrt{\omega}(ad+bc),$$

avec $(ac + \omega bd) \in \mathbb{Z}$ et $(ad + bc) \in \mathbb{Z}$. Donc $xy \in \mathbb{Z}[\sqrt{\omega}]$.
Donc $\mathbb{Z}[\omega]$ est un anneau.

3. Démontrer que, sous l'hypothèse « ω n'est pas le carré d'un entier », on a $\sqrt{\omega} \notin \mathbb{Q}$.

Correction

Si ω n'est pas un carré, alors on dispose de $p \in \mathbb{P}$ tel que $v_p(\omega)$ est impair. Supposons alors que $\sqrt{\omega} \in \mathbb{Q}$: on disposerait de $(a, b) \in (\mathbb{N}^*)^2$ tels que $\sqrt{\omega} = \dfrac{a}{b}$. Ainsi, $\omega = \dfrac{a^2}{b^2}$, donc $b^2\omega = a^2$.
Mais alors

$$v_p(b^2\omega) = v_p(a^2),$$

donc

$$2v_p(b) + v_p(\omega) = 2v_p(a),$$

ce qui est absurde ! Donc $\sqrt{\omega} \notin \mathbb{Q}$!

4. Démontrer que tout élément de $\mathbb{Z}[\sqrt{\omega}]$ s'écrit de manière unique sous la forme $a+\sqrt{\omega}b$.

Correction

Soient (a, b, c, d) quatre entiers tels que $a+\sqrt{\omega}b = c+\sqrt{\omega}d$. Alors $a-c = \sqrt{\omega}(b-d)$. Si $b - d \neq 0$, alors $\sqrt{\omega} = \dfrac{a-c}{b-d} \in \mathbb{Q}$, ce qui est absurde. Donc $b - d = 0$, i.e. $b = d$. Donc $a = c$. D'où l'unicité de l'écriture.

On définit, pour $s = a + \sqrt{\omega}b \in \mathbb{Z}[\sqrt{\omega}]$, la norme de s, par $\mathcal{N}(s) = a^2 - \omega b^2$.

5. Montrer que pout tous s et t de $\mathbb{Z}[\sqrt{\omega}]$, $\mathcal{N}(st) = \mathcal{N}(s)\mathcal{N}(t)$.

Correction

Soient s et t dans $\mathbb{Z}[\sqrt{\omega}]$, (a, b, c, d) quatre entiers tels que $s = a+\sqrt{\omega}b$ et $t = c+\sqrt{\omega}d$. Alors

$$\begin{aligned} st &= (a + \sqrt{\omega}b) \times (c + \sqrt{\omega}d) \\ &= ac - \omega bd + \sqrt{\omega}(ad + bc). \end{aligned}$$

Donc

$$\begin{aligned}\mathcal{N}(st) &= (ac-\omega bd)^2-\omega(ad+bc)^2\\ &= (a^2-\omega b^2)(c^2-\omega d^2) \text{ par l'identité de Brahmagupta.}\\ &= \mathcal{N}(s)\mathcal{N}(t).\end{aligned}$$

D'où le résultat.

6. Montrer que pour tout s de $\mathbb{Z}[\sqrt{\omega}]$, s est inversible pour la loi $\times$ si, et seulement si $\mathcal{N}(s)=1$ ou $\mathcal{N}(s)=-1$. Exprimer le cas échéant l'inverse de s pour $\times$.

Correction

Soit s dans $\mathbb{Z}[\omega]$. Montrons le résultat par double implication.

- $\Leftarrow$ Supposons que s est inversible pour $\times$. Alors on dispose de $t\in\mathbb{Z}[\omega]$ tel que $st=1$. Alors $\mathcal{N}(st)=\mathcal{N}(1)=1$, i.e. $\mathcal{N}(s)\mathcal{N}(t)=1$. Or par définition, $\mathcal{N}(s)$ et $\mathcal{N}(t)$ sont deux entiers, de produit égal à 1, donc $\mathcal{N}(s)$ divise 1, donc $\mathcal{N}(s)=1$ ou $\mathcal{N}(s)=-1$.
- $\Rightarrow$ Supposons que $\mathcal{N}(s)=1$. $s\in\mathbb{Z}[\sqrt{\omega}]$ donc on dispose de a et b entiers tels que $s=a+\sqrt{\omega}b$. Alors $a^2-\omega b^2=1$, c'est-à-dire que $(a-\sqrt{\omega}b)(a+\sqrt{\omega}b)=1$, donc s est inversible d'inverse $a-\sqrt{\omega}$.

On rappelle que l'on note $\mathcal{U}(\mathbb{Z}[\sqrt{\omega}])$ l'ensemble des éléments de $\mathbb{Z}[\sqrt{\omega}]$ inversibles pour $\times$; $(\mathcal{U}(\mathbb{Z}[\sqrt{\omega}]),\times)$ est un groupe.

7. Montrer que l'équation (PF_ω) admet une solution non triviale si et seulement si $\mathcal{U}(\mathbb{Z}[\sqrt{\omega}])$ n'est pas réduit à $\{-1,1\}$.

Correction

Montrons encore une fois le résultat par double implication.

- $\Leftarrow$ Supposons qu'il existe une solution non triviale (a,b) de (PF_ω). Alors $a^2-\omega b^2=1$, i.e. $\mathcal{N}(a+\sqrt{\omega}b)=1$, i.e. $a+\sqrt{\omega}b$ est inversible dans $\mathbb{Z}[\sqrt{\omega}]$ et $a+\sqrt{b}\notin\{-1,1\}$ car (a,b) n'est pas triviale.
- $\Rightarrow$ Supposons qu'il existe un élément $a+\sqrt{b}=s$ non trivial et inversible dans $\mathbb{Z}[\sqrt{\omega}]$. Alors $\mathcal{N}(s)=\pm1$. Si $\mathcal{N}(s)=1$, alors $a^2-\omega b^2=1$ et c'est gagné. Sinon, posons $t=s^2$. Alors $\mathcal{N}(t)=\mathcal{N}(s\times s)=\mathcal{N}(s)^2=(-1)^2=1$ et c'est gagné.

B. Le groupe de Brahmagupta de l'ensemble des solutions

B-I. Une loi sur G_ω

On définit, pour (a,b) et (c,d) deux couples d'entiers, la loi $\star$ par

$$(a,b)\star(c,d)=(ac+\omega bd,ad+bc).$$

8. Démontrer que $\star$ est une loi de composition interne sur G_ω.

Correction

Soient (a,b) et (c,d) dans G_ω. Montrons que $(a,b)\star(c,d)\in G_\omega$. On sait que $(a,b)\star(c,d)=(ac+\omega bd, ad+bc)$. Pour montrer que $(a,b)\star(c,d)\in G_\omega$, il faut montrer que $(ac+\omega bd)^2-\omega(ad+bc)^2=\pm 1$. Or, par l'identité de Brahmagupta,

$$(ac+\omega bd)^2-\omega(ad+bc)^2=(a^2-\omega b^2)(c^2-\omega d^2).$$

Or, $(a,b)\in G_\omega$ donc $a^2-\omega b^2=\pm 1$. De même pour $x^2-\omega d^2$. Donc $(ac+\omega bd)^2-\omega(ad+bc)^2=\pm 1$. Donc $(a,b)\star(c,d)\in G_\omega$. Donc $\star$ est une loi de composition interne sur G_ω.

9. Montrer que $(G_\omega,\star)$ est un groupe, qu'il est abélien, et que S_ω est un sous-groupe de G_ω.

Correction

$(G_\omega,\star)$ est un ensemble muni d'une loi de composition interne. Montrons qu'il s'agit d'un groupe.

- Montrons que $\star$ est associative. Soient (a,b), (c,d), (e,f) trois éléments de G_ω. Alors

$$\begin{aligned}\Big((a,b)\star(c,d)\Big)\star(e,f)&=(ac+\omega bd,ad+bc)\star(e,f)\\&=(aec+\omega ebd+\omega adf+\omega bcf, acf+\omega fbd+ade+bce)\end{aligned}$$

et

$$\begin{aligned}(a,b)\star\Big((c,d)\star(e,f)\Big)&=(a,b)\star(ce+ndf,cf+de)\\&=(ace+\omega adf+\omega bcf+\omega bde, acf+ade+bcd+\omega bdf)\\&=\Big((a,b)\star(c,d)\Big)\star(e,f).\end{aligned}$$

Donc la loi est associative.

- Montrons que G_ω admet un élément neutre. Posons $\varepsilon=(1,0)$. Alors $\varepsilon\in G_\omega$ car $1^2-\omega\times 0^2=1$. Soit alors (a,b) dans G_ω. Alors $(a,b)\star(1,0)=(0,1)\star(a,b)=(a,b)$. Donc ε est l'élément neutre pour $\star$ dans G_ω.
- Montrons que tout élément de G_ω admet un inverse pour $\star$. Soit (a,b) dans G_ω. Alors

$$(a,b)\star(a,-b)=(a^2+\omega\times b\times(-b),a\times(-b)+ab)=(a^2-\omega b^2,0).$$

Or, $(a,b)\in G_\omega$, donc $a^2-\omega b^2=1$, donc $(a,b)\star(a,-b)=\varepsilon$. De même $(a,-b)\star(a,b)=\varepsilon$.

Donc G_ω est un groupe. De plus si (a,b) et (c,d) sont dans G_ω,

$$(a,b)\star(c,d)=(ac+\omega bd,ad+bc)=(ca+\omega db,da+cb)=(c,d)\star(a,b).$$

Donc G_ω est abélien.
Enfin, on montre que S_ω est un sous-groupe de G_ω :

- déjà, $(1,0) \in S_\omega$,
- ensuite, soient (a,b) et (c,d) dans S_ω. Alors $(a,b) \star (c,d) \in S_\omega$ par le même argument que la question précédente.
- enfin, si $(a,b) \in S_\omega$, $(a,b)^{-1} = (a,-b)$ et $a^2 - \omega(-b)^2 = a^2 - \omega b^2 = 1$, donc $(a,b)^{-1} \in S_\omega$.

10. Démontrer que l'application φ qui à tout élément (a,b) de $(G_\omega, \star)$ associe $a+\sqrt{\omega}b$ est à valeurs dans $(\mathcal{U}(\mathbb{Z}[\sqrt{\omega}]), \times)$, et qu'il s'agit d'un isomorphisme de groupes.

Correction

Procédons en plusieurs étapes :

- déjà, si $(a,b) \in G_\omega$, alors $\mathcal{N}(a+\sqrt{\omega}b) = a^2 - \omega b^2 = \pm 1$, donc $a+\sqrt{\omega}b \in \mathcal{U}(\mathbb{Z}[\sqrt{\omega}])$.
- ensuite, soient (a,b) et (c,d) dans G_ω. Alors

$$\varphi((a,b)\star(c,d)) = \varphi(ac+\omega bd, ad+bc) = (ac+\omega bd) + \sqrt{\omega}(ad+bc),$$

et

$$\begin{aligned}\varphi(a,b)\times\varphi(c,d) &= (a+\sqrt{\omega}b)(c+\sqrt{\omega}d)\\ &= (ac+\omega bd)+\sqrt{\omega}(ad+bc)\\ &= \varphi((a,b)\star(c,d)),\end{aligned}$$

donc φ est un morphisme de groupes.

- enfin, on montre que φ est bijective : si l'on prend $x \in \mathcal{U}(\mathbb{Z}[\sqrt{\omega}])$, alors on dispose d'un unique couple $(a,b) \in \mathbb{Z}^2$ vérifiant $x = a+\sqrt{\omega}b$. Ce couple vérifie $\mathcal{N}(x) = \pm 1$, i.e. $a^2 - \omega b^2 = \pm 1$, i.e. $(a,b) \in G_\omega$.

Donc φ est bien un isomorphisme de groupes.

B-II. Structure de S_ω

Note pour la suite : attention à la notation « puissance » ! Si vous voyez écrit x^n, faites attention au fait que

- si x est un couple, $x = (a,b)$, alors on parle de la puissance n dans $(G_\omega, \star)$,
- si x est un élément de $\mathbb{Z}[\sqrt{\omega}]$, $x = a+\sqrt{\omega}b$, alors on parle de la puissance n usuelle dans $\mathbb{R}$.

On va étudier un peu plus en détail la structure de l'ensemble des solutions, pour remarquer, et c'est assez formidable, que l'ensemble des solutions est, au signe près, engendré par un seul élément.

On suppose qu'il existe une solution non triviale au problème, que l'on notera (α,β). On considère alors

$$A = \{a+\sqrt{\omega}b,\ a \geqslant 0 \text{ et } \mathcal{N}(a+\sqrt{\omega}b) = 1\} \text{ et } B = A \cap]1,+\infty[.$$

11. Démontrer que si $a+\sqrt{\omega}b \in B$, alors $a \geqslant 0$ et $b \geqslant 1$.
On pourra considérer $\dfrac{1}{a+\sqrt{\omega}b}$ *pour montrer qu'on ne peut pas avoir* $b < 0$.

Correction

Éliminons les cas $b = 0$ et $b < 0$.

- Déjà, **si** $b = 0$, alors comme $\mathcal{N}(a + \sqrt{\omega}b) = 1$, $a^2 = 1$, donc $a = 1$, donc $a + \sqrt{\omega}b$ n'est pas strictement supérieur à 1 !
- Ensuite, **si** $b < 0$, comme $\mathcal{N}(a - \sqrt{\omega}b) = 1$, on a

$$1 > \frac{1}{a + \sqrt{\omega}b} = a - \sqrt{\omega}b,$$

mais, pourtant $-b > 0$ et $a \geqslant 0$, donc $a - \sqrt{\omega}b > 1$, absurde !

Ainsi, $\boxed{\text{nécessairement, } b \geqslant 1.}$

12. Démontrer que B est non vide et admet un plus petit élément. On le note ε. On dispose donc de $(a_0, b_0) \in \mathbb{N}^2$ tels que $\varepsilon = a_0 + \sqrt{\omega}b_0$.

Correction

- Déjà, on montre que B est non vide :
  On suppose que (PF_ω) admet une solution non triviale, (α, β). Quitte à changer le signe, on peut supposer α et β positifs (car si (a, b) est solution, $(-a, b)$, $(a, -b)$ et $(-a, -b)$ sont solutions). Mais alors
  — si $\beta = 0$, alors $\alpha = 1$ (comme $\alpha^2 - \sqrt{\omega}\beta^2 = 1$), ce qui est impossible,
  — sinon, $\beta \geqslant 1$ et $\omega > 1$ donc $\sqrt{\omega} > 1$, donc $\alpha + \sqrt{\omega}\beta > 1$.
  Donc B est non vide.
- On ne peut pas directement utiliser le fait que B admette une borne inférieure, rien ne nous dit qu'il s'agirait d'un plus petit élément.
- On considère alors

$$C = B \cap]1, \alpha + \sqrt{\omega}\beta],$$

c'est-à-dire les éléments de B inférieurs ou égaux à $\alpha = \sqrt{\omega}\beta$. Mais, comme les éléments de B sont de la forme $a + \sqrt{\omega}b$ avec $a \geqslant 0$ et $b \geqslant 1$, on a au maximum α choix pour a et β choix pour b, donc C est un ensemble **fini** ! Ainsi, C admet un plus petit élément, donc B admet un plus petit élément.

On appelle le couple (a_0, b_0) **solution fondamentale** de (PF_ω). Soit (x, y) une autre solution de (PF_ω) avec $x, y \geqslant 0$. On veut montrer qu'il existe $n \in \mathbb{N}$ tel que $(x, y) = (a_0, b_0)^n$. On suppose par l'absurde que ce n'est pas le cas.

13. Démontrer qu'il existe k dans $\mathbb{N}$ tel que $\varepsilon^k < x + \sqrt{\omega}y < \varepsilon^{k+1}$.

Correction

On remarque que $\varepsilon > 1$ donc $\varepsilon^k \underset{k \to +\infty}{\longrightarrow} +\infty$. Ainsi, la partie $\{i \in \mathbb{N},\ \varepsilon^i < x + \sqrt{\omega}y\}$ est une partie bornée de $\mathbb{N}$ (car $\varepsilon^i > x + \sqrt{\omega}y$ à partir d'un certain rang), elle admet donc un plus grand élément k. On a alors $\varepsilon^k < x + \sqrt{\omega}y \leqslant \varepsilon^{k+1}$, et même

$$\boxed{\varepsilon^k < x + \sqrt{\omega}y < \varepsilon^{k+1}},$$

car $x+\sqrt{\omega}y \neq \varepsilon^{k+1}$ (on a supposé que (x,y) n'était pas de la forme $(a_0,b_0)^n$, ce qui revient, par l'isomorphisme φ, à dire que $x+\sqrt{\omega}y$ n'est pas de la forme ε^n).

14. Démontrer que $\dfrac{x+\sqrt{\omega}y}{\varepsilon^k} \in B$, et conclure en précisant toutes les solutions de (PF_ω).

Correction

On sait que $\mathcal{U}(\mathbb{Z}[\sqrt{\omega}])$ est un groupe pour $\times$, donc $\dfrac{x+\sqrt{\omega}y}{\varepsilon^k} \in \mathcal{U}(\mathbb{Z}[\sqrt{\omega}])$. Ensuite, étant données les inégalités précédentes,

$$1 < \frac{x+\sqrt{\omega}y}{\varepsilon^k} < \varepsilon,$$

donc $\dfrac{x+\sqrt{\omega}y}{\varepsilon^k} \in B$ et $\dfrac{x+\sqrt{\omega}y}{\varepsilon^k} < \varepsilon$, **ABSURDE !**

Donc, on en déduit qu'il existe n dans $\mathbb{N}$ tel que $(x,y) = (a_0,b_0)^n$.

Ainsi, en prenant en compte tous les signes possibles, l'ensemble des solutions de (PF_ω) est l'ensemble

$$\{(x,y) \in \mathbb{Z}^2,\ \exists n \in \mathbb{N},\ (|x|,|y|) = (a_0,b_0)^n\}$$

B-III. Résolution dans le cas $\omega = 2$

15. En étudiant tous les cas possibles, démontrer que $(3,2)$ est une solution fondamentale de (PF_2).

Correction

On vient de voir qu'une solution fondamentale est une solution (a,b) telle que $a+b\sqrt{2}$ est supérieur ou égal à 1 et minimal.

Il ne nous reste qu'à distinguer les cas :

- pour $a=0$, $(0,b)$ ne peut pas être solution de PF_2,
- pour $a=1$, on remarque que $1^2-2b^2=1$ si et seulement si $b=0$, ce qui est exclus,
- pour $a=2$, on remarque que $2^2-2b^2=1$ si et seulement si $2b^2=3$, ce qui est excluse,
- pour $a=3$, on remarque que $3^2-2b^2=1$ si et seulement si $b^2=4$, ce qui nous ramène à notre solution.

Ensuite, pour $a>3$, on aura nécessairement $a+\sqrt{2}b > 3+2\sqrt{2}$.

Donc $3+2\sqrt{2}$ est bien une unité fondamentale de $\mathbb{Z}[\sqrt{2}]$, donc $(3,2)$ est une solution fondamentale de PF_2.

16. En déduire que l'ensemble des solutions de PF_2 est l'ensemble des éléments de la forme (a_n,b_n), $(a_n,-b_n)$, $(-a_n,b_n)$ et $(-a_n,-b_n)$ où $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ sont les suites définies par

$a_0 = 1$, $b_0 = 0$ et que

$$\forall n \in \mathbb{N}, \begin{cases} a_{n+1} = 3a_n + 4b_n, \\ b_{n+1} = 2a_n + 3b_n. \end{cases}$$

Correction

On détermine déjà l'ensemble des solutions positives de PF_2. On en déduira toutes les autres. On sait que $(3, 2)$ est une solution fondamentale de PF_2. Donc si (a, b) est une solution de PF_2, on dispose de $n \in \mathbb{N}$ vérifiant $(a, b) = (3, 2)^n$.
Notons $(a_n, b_n) = (3, 2)^n$. Alors $(a_0, b_0) = (1, 0)$ (le neutre pour $\star$) et, si $n \in \mathbb{N}$,

$$(a_{n+1}, b_{n+1}) = (a_n, b_n) \star (3, 2) = (3an + 4b_n, 2a_n + 3b_n),$$

ce qui est exactement la relation donnée ci-dessus !

C. Existence d'une solution non triviale dans le cas général

Cette partie, plus délicate que le reste, est surtout là car je ne voulais pas juste admettre l'existence d'une solution non triviale à Pell-Fermat.
Bhāskara II (1114-1185), un autre mathématicien indien, a en fait trouvé une méthode, dite méthode chakravala (« chakra » signifie boucle/cercle), pour déterminer une solution, mais sans preuve. En prenant certaines de ses idées, et en formalisant mieux les choses, on va faire cette preuve.

On pourra utiliser le principe des tiroirs de Dirichlet :

- (première version) si $(x_1, \dots, x_{n+1})$ est un $n+1$-uplet d'éléments d'un ensemble à n éléments, alors on dispose de $i \neq j$ tels que $x_i = x_j$,
- (deuxième version) si $n < m$, si $(x_1, \dots, x_m)$ sont des éléments d'un ensemble E et que $E = \bigcup_{k=1}^{n} F_k$, alors il existe $(i,j) \in [\![1,m]\!]^2$, il existe k dans $[\![1,n]\!]$ vérifiant $i \neq j$ et $(x_i, x_j) \in F_k^2$.
  « *Si on range m chaussettes dans n tiroirs et $m > n$, alors il y a un tiroir contenant au moins deux chaussettes.* » Cela est aussi vrai si on prend un nombre infini de $(x_i)_{i\in\mathbb{N}}$ (il existe alors un F_k qui contient une infinité de termes).

On munit $\mathbb{Z}^2$ de l'addition coordonnée par coordonnée : $(2,-4)+(3,6) = (2+3,-4+6) = (5,2)$. On admet qu'on a alors un groupe, de neutre $(0,0)$.

17. Démontrer que l'application

$$f : \left| \begin{array}{c} \mathbb{Z}^2 \to \mathbb{R} \\ (a,b) \mapsto a + \sqrt{\omega} b \end{array} \right.$$

est un morphisme de groupes injectif.

Correction

Vérifions déjà qu'il s'agit d'un morphisme de groupes : soient (a,b), (a',b') des éléments de $\mathbb{Z}^2$. Alors

$$f((a,b)+(a',b')) = f(a+a', b+b') = (a+a')+\sqrt{\omega}(b+b') = a+\sqrt{\omega}b+a'+\sqrt{\omega}b' = f(a,b)+f(a',b'),$$

donc f est un morphisme de groupes. De plus, f est injectif : soit $(a,b) \in \ker(f)$. Alors $f(a,b) = 0$, donc $a + \sqrt{\omega}b = 0$. Si $b \neq 0$, alors $\sqrt{\omega} = -\dfrac{a}{b} \in \mathbb{Q}$, absurde ! Donc $b = 0$, donc $a = 0$. Donc f est injectif.

18. Soit $n \in \mathbb{N}^*$. Démontrer qu'il existe deux couples différents (a,b) et (a',b') dans $[\![0,n]\!]^2$ vérifiant

$$|f(a,b) - f(a',b')| \leqslant \frac{1}{n}(1+\sqrt{\omega}),$$

puis qu'il existe A_n et B_n deux entiers relatifs,vérifiant

$$|A_n| \leqslant n,\ |B_n| \leqslant n \text{ et } |A_n + \sqrt{\omega}B_n| \leqslant \frac{1}{n}(1+\sqrt{\omega}).$$

Pour la première partie, on pourra utiliser le principe des tiroirs, en remarquant que si $(a,b) \in [\![0,n]\!]^2$, alors $0 \leqslant f(a,b) \leqslant n(1+\sqrt{\omega})$ et en remarquant l'on peut découper $[0, n(1+\sqrt{\omega})]$ en n^2 intervalles de longueur $\dfrac{1}{n}(1+\sqrt{\omega})$.

Correction

Pour tout (a,b) dans $[\![0,n]\!]^2$, $0 \leqslant f(a,b) \leqslant n(1+\sqrt{\omega})$. Or, on peut découper $[0, n(1+\sqrt{\omega})]$ en n^2 intervalles

$$[0, n(1+\sqrt{\omega})] = \bigsqcup_{k=0}^{n^2-1} \left[\frac{k}{n}(1+\sqrt{\omega}), \frac{k+1}{n}(1+\sqrt{\omega})\right]$$

Donc, comme il y a $(n+1)^2$ couples (a,b) dans $[0, n(1+\sqrt{\omega})]$, par le principe des tiroirs, on dispose de $(a,b) \neq (a',b')$ tels que

$$\boxed{0 < |f(a,b) - f(a',b')| \leqslant \frac{1}{n}(1+\sqrt{\omega})}$$

(on a bien $f(a,b) \neq f(a',b')$ car f est injective)
En posant $A_n = a - a'$ et $B_n = b - b'$, on a le résultat voulu.

19. Démontrer que pour tout n dans $\mathbb{N}^*$,

$$|A_n^2 - \omega B_n^2| \leqslant (1+\sqrt{\omega})^2.$$

Correction

C'est juste un petit calcul :

$$|A_n^2 - \omega B_n^2| = |A_n + \sqrt{\omega}B_n|.|A_n - \sqrt{\omega}B_n| \leqslant \frac{1}{n}(1+\sqrt{\omega})(n + n\sqrt{\omega}) = (1+\sqrt{\omega})^2.$$

20. Démontrer que l'ensemble des valeurs prises par (A_n, B_n), i.e. $\{(A_n, B_n),\ n \in \mathbb{N}^*\}$, est infini.

Correction

Si cet ensemble était fini, l'ensemble des valeurs $\{|A_n + \sqrt{\omega}B_n|, n \in \mathbb{N}\}$ serait fini donc minoré, donc la suite $|A_n + \sqrt{\omega}B_n|$ ne pourrait pas tendre vers 0 !

21. En déduire qu'il existe un entier relatif c vérifiant $|c| \leqslant (1+\sqrt{\omega})^2$ et tel que l'équation

$$x^2 - \omega y^2 = c \qquad (PF_\omega(c))$$

admette une infinité de solutions $(x,y) \in \mathbb{Z}^2$.
On pourra encore appliquer le principe des tiroirs...

Correction

On applique encore le principe des tiroirs ! On sait que pour tout n dans $\mathbb{N}$,

$$-(1+\sqrt{\omega})^2 \leqslant A_n^2 - \omega B_n^2 \leqslant (1+\sqrt{\omega})^2.$$

Or, il y a un nombre infini de valeurs différentes de (A_n, B_n) pour un nombre fini de valeurs possibles de $A_n^2 - \omega B_n^2$. Donc il existe une de ces valeurs, notons-la c, telle que $A_n^2 - \omega B_n^2 = c$ une infinité de fois.

22. En déduire qu'il existe deux couples d'entiers (x,y) et (x',y') dans $\mathbb{N}^* \times \mathbb{Z}$ vérifiant l'équation $(PF_\omega(c))$ ci-dessus, et tels que $x \equiv x'[c]$ et $y \equiv y'[c]$.
Oh, tiens, et si on faisait un principe des tiroirs ?

Correction

Comme il y a une infinité de solutions (x, y) et que, modulo c, x et y ne peuvent prendre que $c+1$ valeurs chacun, il existe, par le principe des tiroirs, une infinité couples (x, y) et (x', y') tels que $x \equiv x'[c]$ et $y \equiv y'[c]$. On peut de plus supposer x et x' strictement positifs : si x est solution, $-x$ aussi, et tous les couples solution ne peuvent avoir une première coordonnée nulle (il n'y a qu'un nombre fini de solutions à l'équation $0 - \omega y^2 = c$).

23. On note $\eta = x + \sqrt{\omega}y$, $\eta' = x' + \sqrt{\omega}y'$ et $\xi = \dfrac{\eta}{\eta'}$. Démontrer que $\xi \in \mathbb{Z}[\omega] \setminus \{-1, 1\}$ et en déduire l'existence d'une solution non triviale à (PF_ω) (l'équation du début du problème).

Correction

Déjà, on remarque que

$$\begin{aligned}\xi &= \frac{\eta}{\eta'} \\ &= \frac{x + \sqrt{\omega}y}{x' + \sqrt{\omega}y'} \\ &= \frac{(x + \sqrt{\omega}y)(x' - \sqrt{\omega}y')}{(x')^2 - \omega(y')^2} \\ &= \frac{(xx' - \omega yy') + \sqrt{\omega}(x'y - xy')}{c}.\end{aligned}$$

Or,

$$\begin{aligned}xx' - \omega yy' &\equiv x^2 - \omega y^2[c] \\ &\equiv 0[c]\end{aligned}$$

et

$$\begin{aligned}x'y - xy' &\equiv xy - xy[c] \\ &\equiv 0[c]\end{aligned}$$

Ainsi, c divise les deux coefficients du numérateur donc $\xi \in \mathbb{Z}[\sqrt{\omega}]$. De plus, $\xi \neq 1$ car $\eta \neq \eta'$ et $\xi \neq -1$ car x et x' sont tous deux strictement positifs.
On a donc trouvé une solution non triviale au problème !