Sur l'équation de Pell-Fermat

1 L'anneau $\mathbb{Z}[\sqrt{\omega}]$

1. On commence par constater que $\mathbb{Z}[\sqrt{\omega}]$ est bien une partie de $\mathbb{R}$. Soient $x = a+\sqrt{\omega}b$ et $y = c+\sqrt{\omega}b$, avec (a,b) et (c,d) dans $\mathbb{Z}^2$, de sorte que $x, y \in \mathbb{Z}[\sqrt{\omega}]$. On a :

   - $1 = 1+\sqrt{\omega}\times 0 \in \mathbb{Z}[\sqrt{\omega}]$;
   - $x-y = (a-c)+\sqrt{\omega}(b-d) \in \mathbb{Z}[\sqrt{\omega}]$;
   - $xy = (ac+\omega bd)+\sqrt{\omega}(ad+bc) \in \mathbb{Z}[\sqrt{\omega}]$.

   Ainsi, $\mathbb{Z}[\sqrt{\omega}]$ est un sous-anneau de $\mathbb{R}$.

2. Considérons une égalité $a+\sqrt{\omega}b = c+\sqrt{\omega}d$, avec a,b,c,d des entiers. On a donc $a-c = \sqrt{\omega}(d-b)$. On prend le carré : $(a-c)^2 = \omega(d-b)^2$. Si p est un nombre premier, on obtient en prenant les valuations p-adiques que $2v_p(a-c) = v_p(\omega)+2v_p(d-b)$. Si $d \neq b$ alors $a \neq c$ et $v_p(\omega) = 2\big(v_p(a-c)-v_p(d-b)\big)$ est pair pour tout premier p ; ceci implique que ω est un carré parfait, ce qui est contraire aux hypothèses.
   Donc, l'écriture $s = a+\sqrt{\omega}b$, avec $a,b \in \mathbb{Z}$, d'un élément s de $\mathbb{Z}[\sqrt{\omega}]$ est unique.

3. On note $s = a+\sqrt{\omega}b$ et $t = c+\sqrt{\omega}d$. Alors, $N(s) = a^2-\omega b^2$, $N(t) = c^2-\omega d^2$, $st = (ac+\omega bd)+\sqrt{\omega}(ad+bc)$ et donc $N(st) = (ac+\omega bd)^2-\omega(ad+bc^2)$. On vérifie immédiatement[1] que
   $$(ac+\omega bd)^2-\omega(ad+bc)^2 = (a^2-\omega b^2)(c^2-\omega d^2)$$
   et donc que $N(st) = N(s)N(t)$.

4. Si $s \in \mathbb{Z}[\sqrt{\omega}]$ est inversible, on note $t \in \mathbb{Z}[\sqrt{\omega}]$ son inverse. Alors, $st = 1$ et donc, par la question précédente, $N(s)N(t) = N(st) = N(1) = 1$. Comme $N(s)$ et $N(t)$ sont des entiers, ils valent tous deux ± 1.
   Réciproquement, si $N(s) = \pm 1$ avec $s = a+\sqrt{\omega}b$, on a $a+\sqrt{\omega}b)(a-\sqrt{\omega}b) = \pm 1$ et donc, $a-\sqrt{\omega}b$ ou son opposé est l'inverse de s.

5. Considérons x un élément de $\mathscr{U} \neq \{\pm 1\}$. Comme $N(x) = \pm 1$, $N(x^2) = 1$. De plus, $x^2 \neq 1$ (car $x \neq \pm 1$) et $x^2 \neq -1$ (car $x \in \mathbb{R}$) ; l'élément x^2 est donc d'ordre infini dans $(\mathbb{R}_+^*, \times)$; donc les puissances x^{2n}, pour $n \in \mathbb{Z}$ sont deux à deux distinctes. Par la question 3, on a $N(x^{2n}) = N(x^2)^n = 1$ pour tout $n \in \mathbb{Z}$. Donc, $\mathscr{U}^+$ est infini ; donc $\mathscr{E}_\omega^+$ aussi.

[1] C'est l'*identité de Brahmagupta.*

2 Existence d'une solution non triviale

6. Considérons les $(n+1)^2$ valeurs $a+\sqrt{\omega}b$, avec $a,b \in [\![0,n]\!]$; elles sont deux à deux distinctes par la question 2. De plus chacune de ses valeurs appartient à $[0, n(1+\sqrt{\omega})]$ par un encadrement immédiat des coefficients a et b.
On peut découper l'intervalle $[0, n(1+\sqrt{\omega})]$ en n^2 intervalles consécutifs de longueur $\frac{1}{n}(1+\sqrt{\omega})$. Comme $(n+1)^2 > n^2$, on peut trouver un petit intervalle contenant au moins deux valeurs distinctes, qu'on note $a+\sqrt{\omega}b$ et $c+\sqrt{\omega}d$, avec $a,b,c,d \in [\![0,n]\!]$. On pose alors $A_n = a-c$ et $B_n = b-d$. Comme A_n et B_n sont la différence de deux entiers entre 0 et n, ils sont majorés par n en valeur absolue ; comme $A_n+\sqrt{\omega}B_n$ est la différence de deux réels dans un même intervalle de longueur $\frac{1}{n}(1+\sqrt{\omega})$, leur différence est majorée en valeur absolue par cette quantité.

7. Si ces couples étaient en nombre fini, alors la suite $\left(|A_n+\sqrt{\omega}B_n|\right)$ prendrait un nombre fini de valeurs. Or, elle est non nulle et converge vers 0 ; c'est impossible.

8. Soit $n \in \mathbb{N}^*$. On a $|A_n^2-\omega B_n^2| = |A_n-\sqrt{\omega}B_n| \times |A_n+\sqrt{\omega}B_n|$. Par inégalité triangulaire, le premier facteur est inférieur à $|A_n|+\sqrt{\omega}|B_n| \leq n(1+\sqrt{\omega})$; par construction, le deuxième est inférieur à $\frac{1}{n}(1+\sqrt{\omega})$. D'où $|A_n^2-\omega B_n^2| \leq n(1+\sqrt{\omega}) \times \frac{1}{n}(1+\sqrt{\omega}) = (1+\sqrt{\omega})^2$.

9. On dispose d'une infinité de couples (A_n,B_n) mais les valeurs de $|A_n^2-\omega B_n^2|$ sont entières et bornées, donc en nombre fini. Donc, une de ses valeurs est atteinte une infinité de fois (*principe des tiroirs infini*) ; d'où l'existence de $c \in \mathbb{Z}$.

10. D'abord, il existe une infinité de couples $(x,y) \in \mathbb{N} \times \mathbb{Z}$ solutions de $x^2-\omega y^2 = c$ car si (x,y) est un couple solution avec $x \in \mathbb{Z}$, alors $(-x,y)$ est aussi solution. Ensuite, il n'y a qu'au plus deux couples solutions $(0,y)$ car la valeur de y est fixée par la valeur de c. Ainsi, il existe une infinité de couples distincts $(x,y) \in \mathbb{N}^* \times \mathbb{Z}$ à l'équation $x^2-\omega y^2 = c$.
Pour chaque couple (x,y) solution, on peut regarder les classes de x et y modulo c. Il y a au maximum c^2 tels couples de classes, donc un nombre fini. Par principe des tiroirs infini, on peut trouver deux couples (x,y) et (x',y') tels que $x \equiv x'\,[c]$ et $y \equiv y'\,[c]$.

11. On a $\xi = \dfrac{\eta}{\eta'} = 1+\dfrac{\eta-\eta'}{\eta'} = 1+\dfrac{(x-x')+\sqrt{\omega}(y-y')}{x'+\sqrt{\omega}y'}$. Or, $(x'+\sqrt{\omega}y')(x'-\sqrt{\omega}y') = x'^2-\omega y'^2 = c$. Donc,
$$\xi = \left(\frac{x-x'}{c}+\sqrt{\omega}\frac{y-y'}{c}\right)(x'-\sqrt{\omega}y').$$
Comme c divise $x-x'$ et $y-y'$, le premier facteur est dans $\mathbb{Z}[\sqrt{\omega}]$. Donc, $\xi \in \mathbb{Z}[\sqrt{\omega}]$. Comme $\eta' = \xi \times \eta$, $N(\eta') = N(\xi)N(\eta)$; comme $N(\eta') = N(\eta)$, $N(\xi) = 1$. Enfin, $\xi \neq \pm 1$ car η et η' sont distincts et que $x, x' > 0$.

3 Structure des solutions

12. Soit $s = a + \sqrt{\omega}b \in \mathscr{A}$, alors $s^{-1} = a - \sqrt{\omega}b$. Comme $s > 1$, $s^{-1} < s$. Donc, $b > 0$; comme c'est un entier, $b \geq 1$.

13. On considère ξ de norme 1, différent de ± 1 (question 12). Quitte à multiplier par -1, on peut supposer $\xi > 0$. Quitte à prendre son inverse, on peut le supposer > 1. De plus, le coefficient a (quand on écrit $\xi = a + \sqrt{\omega}b$) est nécessairement positif car $a = \dfrac{\xi + \xi^{-1}}{2}$. Ainsi, $\mathscr{A}$ est non vide.
Si $s = a + \sqrt{\omega}b$ est dans $\mathscr{A}$ et si a ou b est supérieur à n, alors $s \geq n$. Ainsi, il n'y a qu'un nombre fini de termes dans $\mathscr{A}$ qui soient inférieurs à un élément donné, par exemple le ξ précédent. Ceci montre que $\mathscr{A}$ admet un plus petit élément ε.

14. Comme $\mathscr{U}^+ \cap \mathbb{R}_+^*$ est un sous-groupe du groupe (multiplicatif) $\mathbb{R}_+^*$, l'ensemble $H = \left\{\ln(x), x \in \mathscr{U}^+ \cap \mathbb{R}_+^*\right\}$ est un sous-groupe du groupe (additif) $\mathbb{R}$; en effet ln est un isomorphisme de groupes de $\mathbb{R}_+^*$ vers $\mathbb{R}$. D'après la question précédente, H ne contient aucun élément strictement entre 0 et $\ln\varepsilon$. Donc, H n'est pas dense dans $\mathbb{R}$; il est donc monogène, engendré par son plus petit élément strictement positif, à savoir $\ln\varepsilon$. On en déduit que $\mathscr{U}^+ \cap \mathbb{R}_+^*$ est engendré (multiplicativement) par ε. De plus, un élément est dans $\mathscr{U}^+$ ssi sa valeur absolue y est ; donc $\mathscr{U}^+$ est l'ensemble des éléments de la forme $\pm\varepsilon^k$, pour $k \in \mathbb{Z}$.
On en déduit facilement que $\mathscr{U}^+$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

15. Pour chacun, on cherche une unité en tatônnant puis on montre qu'on n'a pas plus petit (il y a un nombre fini de cas à vérifier). On trouve

    - $\varepsilon = 3 + 2\sqrt{2}$ pour $\omega = 2$;
    - $\varepsilon = 2 + \sqrt{3}$ pour $\omega = 3$;
    - $\varepsilon = 9 + 4\sqrt{5}$ pour $\omega = 5$ (*la vérification que c'est le plus petit peut être longue...*)

    On calcule alors ε^2 et ε^3 pour avoir des nouveaux couples solutions. On trouve :

    - $(3,2)$; $(17,12)$ et $(99,70)$ pour $\omega = 2$;
    - $(2,1)$; $(7,4)$ et $(26,15)$ pour $\omega = 3$;
    - $(9,4)$; $(161,72)$ et $(2889,1292)$ pour $\omega = 5$.

    On est ravi d'apprendre que $2889^2 - 5 \times 1292^2 = 1$.

Remarques. Deux questions principales demeurent.

- Comment obtenir de façon pratique l'unité fondamentale ε ? Il faut ici aller chercher du côté du développement en fractions continues de $\sqrt{\omega}$.

- L'équation jumelle $x^2 - \omega y^2 = -1$ est apparue dans le calcul des inversibles. Elle peut avoir des solutions (pour $\omega = 2$ p. ex.) ou ne pas en avoir (pour $\omega = 3$ p. ex.). Si p est un nombre premier congru à 3 modulo 4 divisant ω, il n'y a pas de solution car -1 n'est pas un carré modulo p ; donc il ne peut y en avoir que si ω est un produit de puissances de 2 et de premiers impairs congrus à 1 modulo 4. Mais cette condition nécessaire n'est pas suffisante et là encore, le développement en fractions continues permet une meilleure compréhension du phénomène.

Me dire si intéressé(e) par un vieux DS sur ce thème.