

Entiers quadratiques : unités de $\mathbb{Z}[\sqrt{2}]$ et polygones réguliers du réseau Deux exercices de terminale et ce qu'ils cachent

Michel Hua

Octobre 2026

Résumé

On part de deux exercices de terminale. Le premier demande si un triangle équilatéral peut avoir ses sommets sur un quadrillage. Le second demande de montrer que chaque puissance $(1 + \sqrt{2})^q$ s'écrit $\sqrt{n+1} + \sqrt{n}$ avec n entier. Les deux se résolvent en quelques lignes, mais chacun cache une idée plus générale. Derrière le second, il y a le groupe des unités de l'anneau $\mathbb{Z}[\sqrt{2}]$: on montre que ce sont exactement les $\pm(1 + \sqrt{2})^k$, ce qui résout l'équation de Pell-Fermat $x^2 - 2y^2 = \pm 1$, et que cet anneau est euclidien. Derrière le premier, il y a un argument de trace : une rotation qui préserve un réseau a une trace entière. On en déduit que le seul polygone régulier à sommets entiers dans le plan est le carré.

Leçons concernées. 126 (Exemples d'équations en arithmétique), 122 (Anneaux principaux), 191 (Exemples d'utilisation des techniques d'algèbre en géométrie), 102 (Groupe des nombres complexes de module 1, racines de l'unité).

Développements possibles. Théorème 2.5 et corollaire 2.6 (unités de $\mathbb{Z}[\sqrt{2}]$ et équation $x^2 - 2y^2 = \pm 1$) ; proposition 2.11 et exercice 4 ; théorème 3.3 avec l'exercice 5. Le fichier `EntiersQuadratiques.lean` vérifie avec Mathlib le lemme 2.1, la proposition 2.3, le corollaire 2.6, les propositions 2.8, 2.11 et 3.1, le théorème 3.3 (par le théorème de Niven plutôt que par la trace) et l'exercice 2.

Prérequis. Irrationalité de $\sqrt{2}$, anneaux et groupes, anneaux principaux, matrices 2×2 , rotations du plan.

Notations. Dans tout le texte, $d \geq 2$ est un entier qui n'est pas un carré parfait. On note $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$ et $\mathbb{Q}(\sqrt{d}) = \{r + s\sqrt{d} : r, s \in \mathbb{Q}\}$. Ce sont des sous-anneaux de $\mathbb{R}$.

Table des matières

1	Deux questions de terminale	2
2	Unités de $\mathbb{Z}[\sqrt{d}]$ et équation de Pell-Fermat	3
2.1	Norme et conjugaison	3
2.2	Structure du groupe des unités	4
2.3	Retour à l'exercice	5
2.4	Compléments	6
3	Polygones réguliers à sommets entiers	6
3.1	Le triangle équilatéral	6
3.2	Tous les polygones réguliers	7

4	Retour aux deux questions	8
5	Exercices	9
6	Corrigés	9

1 Deux questions de terminale

Première question. Sur une feuille quadrillée, peut-on dessiner un triangle équilatéral dont les trois sommets sont des nœuds du quadrillage ? On essaie. Le triangle $(0, 0)$, $(2, 0)$, $(1, 2)$ est isocèle, mais ses côtés valent 2 , $\sqrt{5}$ et $\sqrt{5}$. On n'arrive jamais à égaliser les trois (figure 1). Nous verrons pourquoi : la hauteur d'un triangle équilatéral de côté ℓ vaut $\frac{\sqrt{3}}{2}\ell$, et $\sqrt{3}$ est irrationnel.

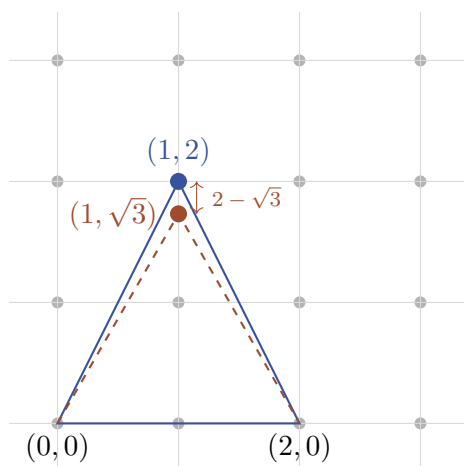


FIG. 1 : Sur la base $(0, 0)$, $(2, 0)$, le troisième sommet du triangle équilatéral est $(1, \sqrt{3})$: il tombe entre deux nœuds. Le nœud le plus proche, $(1, 2)$, donne un triangle seulement isocèle.

Seconde question. Développons les premières puissances de $1 + \sqrt{2}$:

q	1	2	3	4	5
$(1 + \sqrt{2})^q$	$1 + \sqrt{2}$	$3 + 2\sqrt{2}$	$7 + 5\sqrt{2}$	$17 + 12\sqrt{2}$	$41 + 29\sqrt{2}$
	$\sqrt{1} + \sqrt{2}$	$\sqrt{9} + \sqrt{8}$	$\sqrt{49} + \sqrt{50}$	$\sqrt{289} + \sqrt{288}$	$\sqrt{1681} + \sqrt{1682}$

À chaque fois, on obtient la somme des racines de deux entiers *consécutifs*. L'exercice demande de montrer que c'est toujours le cas : pour tout $q \in \mathbb{N}$, il existe $n \in \mathbb{N}$ tel que

$$(1 + \sqrt{2})^q = \sqrt{n+1} + \sqrt{n}.$$

Si l'on écrit $(1 + \sqrt{2})^q = a_q + b_q\sqrt{2}$, cela revient à dire que a_q^2 et $2b_q^2$ sont consécutifs, c'est-à-dire que $a_q^2 - 2b_q^2 = \pm 1$.

Ce qu'on va faire. La seconde question parle d'une équation, $x^2 - 2y^2 = \pm 1$, et la section 2 la résout complètement. La bonne notion est celle d'*unité* d'un anneau. La première question parle de géométrie, et la section 3 la généralise à tous les polygones réguliers. Dans les deux cas, l'outil de base est le même : un nombre irrationnel ne peut pas être égal à un quotient d'entiers.

2 Unités de $\mathbb{Z}[\sqrt{d}]$ et équation de Pell-Fermat

2.1 Norme et conjugaison

Pour calculer dans $\mathbb{Z}[\sqrt{d}]$, on veut pouvoir identifier les coefficients : si $a + b\sqrt{d} = a' + b'\sqrt{d}$, on aimerait conclure $a = a'$ et $b = b'$. C'est exactement l'irrationalité de $\sqrt{d}$.

Lemme 2.1. *Le réel $\sqrt{d}$ est irrationnel. Par conséquent, si $r, s \in \mathbb{Q}$ vérifient $r + s\sqrt{d} = 0$, alors $r = s = 0$. En particulier, l'écriture d'un élément de $\mathbb{Q}(\sqrt{d})$ sous la forme $r + s\sqrt{d}$ est unique.*

Démonstration. Supposons $\sqrt{d} = p/q$ avec $p, q \geq 1$ et $p \wedge q = 1$. Alors $p^2 = dq^2$. Si un nombre premier ℓ divisait q , il diviserait p^2 , donc p . C'est impossible puisque $p \wedge q = 1$. Donc $q = 1$ et $d = p^2$ est un carré, ce qui est exclu.

Si maintenant $r + s\sqrt{d} = 0$ avec $s \neq 0$, on aurait $\sqrt{d} = -r/s \in \mathbb{Q}$. Donc $s = 0$, puis $r = 0$. L'unicité de l'écriture s'obtient en appliquant ceci à la différence de deux écritures. $\square$

Dans la feuille d'origine, on montrait par une récurrence que $(1 + \sqrt{2})^q = a_q + b_q\sqrt{2}$, puis, par une seconde récurrence, que $(1 - \sqrt{2})^q = a_q - b_q\sqrt{2}$ avec les *mêmes* coefficients. Cette seconde récurrence cache un fait simple : changer $\sqrt{2}$ en $-\sqrt{2}$ respecte les opérations. On donne un nom à cette opération.

Définition 2.2. La *conjugaison* est l'application $\sigma : \mathbb{Q}(\sqrt{d}) \rightarrow \mathbb{Q}(\sqrt{d})$, $r + s\sqrt{d} \mapsto r - s\sqrt{d}$. Elle est bien définie grâce au lemme 2.1. La *norme* est $N(x) = x\sigma(x)$, c'est-à-dire

$$N(r + s\sqrt{d}) = (r + s\sqrt{d})(r - s\sqrt{d}) = r^2 - ds^2.$$

L'équation $x^2 - 2y^2 = \pm 1$ s'écrit donc $N(x + y\sqrt{2}) = \pm 1$. La proposition suivante rassemble ce qu'on sait de la norme. Le point important est le troisième : les solutions de l'équation sont exactement les éléments inversibles de l'anneau.

Proposition 2.3. 1. σ est un automorphisme de l'anneau $\mathbb{Q}(\sqrt{d})$, égal à son propre inverse, qui envoie $\mathbb{Z}[\sqrt{d}]$ dans lui-même.
 2. La norme est multiplicative : $N(xy) = N(x)N(y)$. Elle est entière sur $\mathbb{Z}[\sqrt{d}]$, et $N(x) = 0$ si et seulement si $x = 0$.
 3. Un élément $x \in \mathbb{Z}[\sqrt{d}]$ est inversible dans $\mathbb{Z}[\sqrt{d}]$ si et seulement si $N(x) = \pm 1$. Dans ce cas, $x^{-1} = N(x)\sigma(x)$.

Démonstration. 1. L'additivité est claire. Pour la multiplicativité, on écrit $x = r + s\sqrt{d}$ et $x' = r' + s'\sqrt{d}$. On a $xx' = (rr' + dss') + (rs' + r's)\sqrt{d}$, et

$$\sigma(x)\sigma(x') = (r - s\sqrt{d})(r' - s'\sqrt{d}) = (rr' + dss') - (rs' + r's)\sqrt{d} = \sigma(xx').$$

Enfin $\sigma(1) = 1$ et $\sigma \circ \sigma = \text{id}$. Si r, s sont entiers, $r - s\sqrt{d}$ est dans $\mathbb{Z}[\sqrt{d}]$.

2. On a $N(xx') = xx'\sigma(x)\sigma(x') = x\sigma(x) \cdot x'\sigma(x') = N(x)N(x')$. Pour $x \in \mathbb{Z}[\sqrt{d}]$, $N(x) = a^2 - db^2 \in \mathbb{Z}$. Supposons $N(r + s\sqrt{d}) = 0$. Si $s \neq 0$, alors $d = (r/s)^2$ et $\sqrt{d} = |r/s| \in \mathbb{Q}$, ce qui contredit le lemme 2.1. Donc $s = 0$, puis $r^2 = 0$.

3. Si $xy = 1$ avec $x, y \in \mathbb{Z}[\sqrt{d}]$, alors $N(x)N(y) = N(1) = 1$. Ce sont deux entiers de produit 1, donc $N(x) = \pm 1$. Réciproquement, si $N(x) = \pm 1$, on a $x \cdot N(x)\sigma(x) = N(x)^2 = 1$, et $N(x)\sigma(x)$ est bien dans $\mathbb{Z}[\sqrt{d}]$. $\square$

La multiplicativité de la norme répond déjà à la question de départ. Comme $N(1 + \sqrt{2}) = 1 - 2 = -1$, on a $N((1 + \sqrt{2})^q) = (-1)^q$, c'est-à-dire $a_q^2 - 2b_q^2 = (-1)^q$. La feuille d'origine ne faisait pas autre chose, avec σ caché dans la seconde récurrence. Mais on peut aller plus loin et se demander si les $(1 + \sqrt{2})^q$ sont les *seules* solutions.

2.2 Structure du groupe des unités

Le groupe des unités $\mathbb{Z}[\sqrt{d}]^\times$ contient toujours 1 et -1 . On veut décrire les autres. L'idée est de les ranger sur la droite réelle : on va voir qu'il y a une plus petite unité strictement plus grande que 1, et que toutes les autres en sont des puissances. Le lemme suivant dit qu'une unité > 1 a des coefficients positifs, ce qui empêche les unités de s'accumuler près de 1.

Lemme 2.4. *Si $u = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]^\times$ vérifie $u > 1$, alors $a \geq 1$ et $b \geq 1$. En particulier $u \geq 1 + \sqrt{d}$.*

Démonstration. L'idée est que le conjugué d'une grande unité est petit. Par la proposition 2.3, $u\sigma(u) = \pm 1$, donc $\sigma(u) = \pm 1/u$ appartient à $] -1, 1[$. On récupère les coefficients par demi-somme et demi-différence :

$$2a = u + \sigma(u) > 1 - 1 = 0, \quad 2b\sqrt{d} = u - \sigma(u) > 1 - 1 = 0.$$

Comme a et b sont entiers, $a \geq 1$ et $b \geq 1$. □

Théorème 2.5. *Si $\mathbb{Z}[\sqrt{d}]^\times \neq \{\pm 1\}$, alors $\mathbb{Z}[\sqrt{d}]^\times$ possède un plus petit élément ε_d strictement supérieur à 1, et*

$$\mathbb{Z}[\sqrt{d}]^\times = \{\pm \varepsilon_d^k : k \in \mathbb{Z}\} \simeq \{\pm 1\} \times \mathbb{Z}.$$

On dit que ε_d est l'unité fondamentale de $\mathbb{Z}[\sqrt{d}]$.

L'idée de la preuve est celle de la division euclidienne, mais pour la multiplication. Si u est une unité positive, on l'encadre entre deux puissances consécutives de ε_d . En divisant par la plus petite, on obtient une unité comprise entre 1 et ε_d . Par minimalité de ε_d , ce « reste » vaut 1.

Démonstration. Existence de ε_d . Soit u une unité différente de ± 1 . Comme u est réel, $|u| \neq 1$. L'un des quatre réels $u, -u, u^{-1}, -u^{-1}$ est donc > 1 ; c'est une unité, notée M . Par le lemme 2.4, une unité $a + b\sqrt{d}$ comprise dans $]1, M]$ vérifie $1 \leq a \leq M$ et $1 \leq b \leq M/\sqrt{d}$. Il n'y en a donc qu'un nombre fini, et il y en a au moins une, M lui-même. On note ε_d la plus petite.

Descente. Soit u une unité. Quitte à remplacer u par $-u$, on suppose $u > 0$. Comme $\varepsilon_d > 1$, il existe un unique $k \in \mathbb{Z}$ tel que $\varepsilon_d^k \leq u < \varepsilon_d^{k+1}$, à savoir $k = \lfloor \ln u / \ln \varepsilon_d \rfloor$. Alors $v = u \varepsilon_d^{-k}$ est une unité, et $1 \leq v < \varepsilon_d$. Par minimalité de ε_d , on ne peut pas avoir $v > 1$. Donc $v = 1$ et $u = \varepsilon_d^k$.

Isomorphisme. L'application $(\pm 1, k) \mapsto \pm \varepsilon_d^k$ est un morphisme de groupes, surjectif d'après ce qui précède. Il est injectif : si $\pm \varepsilon_d^k = 1$, alors le signe est $+$ (car $\varepsilon_d^k > 0$), puis $k = 0$ (car $\varepsilon_d > 1$). □

Le théorème ne dit pas comment trouver ε_d . Pour $d = 2$, le lemme 2.4 le donne immédiatement : une unité > 1 est au moins $1 + \sqrt{2}$, et $1 + \sqrt{2}$ est une unité.

Corollaire 2.6. 1. $\mathbb{Z}[\sqrt{2}]^\times = \{\pm(1 + \sqrt{2})^k : k \in \mathbb{Z}\}$.

2. Pour $q \in \mathbb{N}$, écrivons $(1 + \sqrt{2})^q = a_q + b_q\sqrt{2}$. Les solutions dans $\mathbb{N}^2$ de $x^2 - 2y^2 = 1$ sont les (a_q, b_q) avec q pair. Celles de $x^2 - 2y^2 = -1$ sont les (a_q, b_q) avec q impair.

Démonstration. 1. On a $N(1 + \sqrt{2}) = -1$, donc $1 + \sqrt{2}$ est une unité > 1 et le théorème s'applique. Par le lemme 2.4, toute unité > 1 est $\geq 1 + \sqrt{2}$. Donc $\varepsilon_2 = 1 + \sqrt{2}$.

2. Soit $(x, y) \in \mathbb{N}^2$ avec $x^2 - 2y^2 = \pm 1$. Alors $u = x + y\sqrt{2}$ est une unité. Elle n'est pas nulle, donc $(x, y) \neq (0, 0)$ et $u \geq 1$. Par le point 1, $u = (1 + \sqrt{2})^q$ avec $q \in \mathbb{Z}$. On a $q \geq 0$, car $(1 + \sqrt{2})^q < 1$ pour $q < 0$. Par unicité de l'écriture, $(x, y) = (a_q, b_q)$, et le signe est $N((1 + \sqrt{2})^q) = (-1)^q$.

Réciproquement, chaque (a_q, b_q) est dans $\mathbb{N}^2$. En effet, en multipliant par $1 + \sqrt{2}$, on obtient la récurrence $a_{q+1} = a_q + 2b_q$, $b_{q+1} = a_q + b_q$, avec $(a_0, b_0) = (1, 0)$. □

Exemple 2.7. Voici les premières valeurs :

q	0	1	2	3	4	5	6	7
a_q	1	1	3	7	17	41	99	239
b_q	0	1	2	5	12	29	70	169

On vérifie par exemple $99^2 - 2 \cdot 70^2 = 9801 - 9800 = 1$ et $239^2 - 2 \cdot 169^2 = 57121 - 57122 = -1$. Les deux suites vérifient aussi $x_{q+2} = 2x_{q+1} + x_q$, puisque $1 + \sqrt{2}$ est racine de $X^2 - 2X - 1$. La figure 2 montre ces points sur les deux hyperboles $x^2 - 2y^2 = \pm 1$: multiplier par $1 + \sqrt{2}$ fait sauter d'une branche à l'autre en s'éloignant de l'origine.

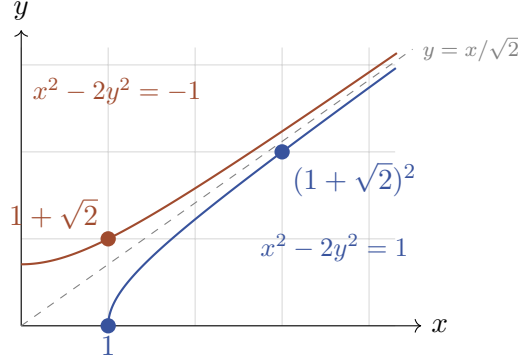


FIG. 2 : Les deux hyperboles $x^2 - 2y^2 = \pm 1$ et leurs premiers points entiers du premier quadrant ; le suivant est $(7, 5)$. Ils alternent d'une branche à l'autre : (a_q, b_q) est sur $x^2 - 2y^2 = (-1)^q$.

2.3 Retour à l'exercice

On a maintenant tout ce qu'il faut. Rien dans l'argument n'est propre à $1 + \sqrt{2}$: il suffit de partir d'une solution de $a^2 - db^2 = \pm 1$ à coefficients positifs. On énonce donc le résultat dans cette généralité.

Proposition 2.8. Soit $(a, b) \in \mathbb{N}^2$ tel que $a^2 - db^2 = \eta \in \{-1, 1\}$. Pour $q \in \mathbb{N}$, on écrit $(a + b\sqrt{d})^q = A_q + B_q\sqrt{d}$. Alors $A_q, B_q \in \mathbb{N}$ et $A_q^2 - dB_q^2 = \eta^q$. Les entiers A_q^2 et dB_q^2 sont donc consécutifs, et

$$(a + b\sqrt{d})^q = \sqrt{n+1} + \sqrt{n}, \quad n = \min(A_q^2, dB_q^2).$$

De plus, cet entier n est unique.

Démonstration. On a $A_0 = 1$ et $B_0 = 0$. En multipliant par $a + b\sqrt{d}$, on obtient $A_{q+1} = aA_q + dbB_q$ et $B_{q+1} = bA_q + aB_q$. Par récurrence, ce sont des entiers positifs.

Par multiplicativité de la norme, $A_q^2 - dB_q^2 = N((a + b\sqrt{d})^q) = N(a + b\sqrt{d})^q = \eta^q$. Comme $A_q \geq 0$ et $B_q \geq 0$, on peut écrire $A_q = \sqrt{A_q^2}$ et $B_q\sqrt{d} = \sqrt{dB_q^2}$. Ce sont les racines de deux entiers consécutifs, d'où la forme annoncée.

Enfin, la fonction $t \mapsto \sqrt{t+1} + \sqrt{t}$ est strictement croissante sur $\mathbb{R}_+$, donc deux valeurs différentes de n donnent deux réels différents. $\square$

Exemple 2.9. Pour $d = 2$ et $a = b = 1$, on retrouve l'exercice. On a $n = 2b_q^2$ si q est pair et $n = a_q^2$ si q est impair. Par exemple

$$(1 + \sqrt{2})^5 = 41 + 29\sqrt{2} = \sqrt{1682} + \sqrt{1681}, \quad (1 + \sqrt{2})^6 = 99 + 70\sqrt{2} = \sqrt{9801} + \sqrt{9800}.$$

Avec $d = 3$ et $(a, b) = (2, 1)$, on obtient de même $(2 + \sqrt{3})^2 = 7 + 4\sqrt{3} = \sqrt{49} + \sqrt{48}$.

Remarque 2.10. La preuve n'utilise pas vraiment que d n'est pas un carré. Si on remplace σ par le développement du binôme, on obtient directement $(a - b\sqrt{d})^q = A_q - B_q\sqrt{d}$: seuls les termes qui contiennent une puissance impaire de $\sqrt{d}$ changent de signe.

2.4 Compléments

On a utilisé l'anneau $\mathbb{Z}[\sqrt{2}]$ comme un cadre de calcul. Il a une propriété de plus, qui le rapproche de $\mathbb{Z}$: on peut y faire des divisions euclidiennes. La norme joue le rôle de la valeur absolue.

Proposition 2.11. *L'anneau $\mathbb{Z}[\sqrt{2}]$ est euclidien pour le stathme $x \mapsto |N(x)|$. En particulier, il est principal, donc factoriel.*

Démonstration. L'idée est la même que dans $\mathbb{Z}$: on calcule le quotient exact dans $\mathbb{Q}(\sqrt{2})$, puis on l'arrondit à l'élément de $\mathbb{Z}[\sqrt{2}]$ le plus proche.

L'anneau $\mathbb{Z}[\sqrt{2}]$ est intègre, comme sous-anneau de $\mathbb{R}$. Soit $x, y \in \mathbb{Z}[\sqrt{2}]$ avec $y \neq 0$. Dans $\mathbb{Q}(\sqrt{2})$, on écrit $x/y = x\sigma(y)/N(y) = r + s\sqrt{2}$ avec $r, s \in \mathbb{Q}$. On choisit des entiers m, n avec $|r - m| \leq \frac{1}{2}$ et $|s - n| \leq \frac{1}{2}$. On pose $q = m + n\sqrt{2}$ et $\rho = x - qy$, qui sont dans $\mathbb{Z}[\sqrt{2}]$. Avec $\alpha = r - m$ et $\beta = s - n$, on a $\rho = y(\alpha + \beta\sqrt{2})$, donc

$$|N(\rho)| = |N(y)| \cdot |\alpha^2 - 2\beta^2| \leq |N(y)| \max(\alpha^2, 2\beta^2) \leq \frac{1}{2} |N(y)| < |N(y)|.$$

La première inégalité vient de ce que α^2 et $2\beta^2$ sont deux réels positifs : leur différence est majorée en valeur absolue par le plus grand des deux. $\square$

Remarque 2.12. Le même argument montre que $\mathbb{Z}[\sqrt{3}]$ est euclidien, avec $|\alpha^2 - 3\beta^2| \leq \frac{3}{4}$. Il ne marche plus pour d grand, et le résultat devient faux : $\mathbb{Z}[\sqrt{10}]$ n'est pas principal. En effet $2 \cdot 3 = (4 + \sqrt{10})(4 - \sqrt{10})$, et 2 est irréductible sans être premier. Il est irréductible car aucun élément n'est de norme ± 2 , puisque $x^2 \equiv \pm 2 \pmod{5}$ n'a pas de solution. Il n'est pas premier car il ne divise ni $4 + \sqrt{10}$ ni $4 - \sqrt{10}$.

Remarque 2.13 (Fractions continues). On a $\sqrt{2} = [1; 2, 2, 2, \dots]$, et les réduites $1, \frac{3}{2}, \frac{7}{5}, \frac{17}{12}, \frac{41}{29}, \dots$ sont exactement les a_q/b_q . Voici pourquoi. Si $a^2 - 2b^2 = \pm 1$ avec $b \geq 1$, alors $|a - b\sqrt{2}| = 1/(a + b\sqrt{2})$ et $a \geq b$, donc

$$\left| \frac{a}{b} - \sqrt{2} \right| = \frac{1}{b(a + b\sqrt{2})} < \frac{1}{2b^2}.$$

Le critère de Legendre dit alors que a/b est une réduite de $\sqrt{2}$. En général, l'unité fondamentale de $\mathbb{Z}[\sqrt{d}]$ se lit sur la période du développement en fraction continue de $\sqrt{d}$.

Remarque 2.14 (Dirichlet). Le théorème 2.5 suppose qu'il existe une unité autre que ± 1 . C'est toujours vrai (Lagrange) : l'équation $x^2 - dy^2 = 1$ a une solution non triviale, ce qui se démontre avec le théorème d'approximation de Dirichlet. C'est un cas particulier du théorème des unités de Dirichlet : pour un corps de nombres K ayant r_1 plongements réels et r_2 paires de plongements complexes, $\mathcal{O}_K^\times \simeq \mu(K) \times \mathbb{Z}^{r_1+r_2-1}$. Attention, $\mathbb{Z}[\sqrt{d}]$ n'est pas toujours l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$: pour $d = 5$, celui-ci est $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, d'unité fondamentale le nombre d'or.

3 Polygones réguliers à sommets entiers

3.1 Le triangle équilatéral

On revient à la première question. On en donne deux preuves. La première est celle de la feuille d'origine : elle traduit « équilatéral » par une rotation et sépare parties réelle et imaginaire. La seconde compare deux calculs de l'aire, et elle est plus courte.

Proposition 3.1. *Il n'existe pas de triangle équilatéral, non réduit à un point, dont les sommets sont dans $\mathbb{Z}^2$.*

Preuve de la feuille d'origine. On identifie $\mathbb{R}^2$ à $\mathbb{C}$, de sorte que $\mathbb{Z}^2$ devient $\mathbb{Z}[i]$. Soit A, B, C trois points de $\mathbb{Z}[i]$ formant un triangle équilatéral, d'affixes a, b, c . Quitte à échanger B et C , le triangle est direct. Cela veut dire qu'on passe de $\overrightarrow{AB}$ à $\overrightarrow{AC}$ par la rotation d'angle $\pi/3$:

$$c - a = \omega(b - a), \quad \omega = e^{i\pi/3} = \frac{1}{2} + i\frac{\sqrt{3}}{2}.$$

Posons $b - a = u + iv$ et $c - a = s + it$, avec $u, v, s, t \in \mathbb{Z}$. En développant et en séparant parties réelle et imaginaire, on obtient

$$2s - u = -v\sqrt{3}, \quad 2t - v = u\sqrt{3}.$$

Par le lemme 2.1 appliqué à $d = 3$, la première égalité donne $v = 0$ et la seconde $u = 0$. Donc $B = A$, puis $C = A$. $\square$

Preuve par l'aire. Soit $A, B, C \in \mathbb{Z}^2$ formant un triangle équilatéral de côté $\ell > 0$. On calcule son aire de deux façons.

- Par le déterminant : l'aire vaut $\frac{1}{2}|\det(B - A, C - A)|$, qui est dans $\frac{1}{2}\mathbb{Z}$.
- Par la géométrie : l'aire vaut $\frac{\sqrt{3}}{4}\ell^2$, où $\ell^2 = \|B - A\|^2$ est un entier non nul.

En égalant, $\sqrt{3} = 2|\det(B - A, C - A)|/\ell^2$ serait rationnel, ce qui est absurde. $\square$

3.2 Tous les polygones réguliers

Le carré, lui, se dessine sans difficulté sur un quadrillage. Que se passe-t-il pour l'hexagone, l'octogone, le pentagone ? On va voir que le carré est le seul. Commençons par dire précisément ce qu'est un polygone régulier : on part d'un sommet et on tourne autour du centre, toujours du même angle.

Définition 3.2. Soit $n \geq 3$ et P un plan affine euclidien, de direction V . Un *polygone régulier* à n sommets de P est une famille $(P_k)_{k \in \mathbb{Z}/n\mathbb{Z}}$ de la forme $P_k = O + R^k(v)$, où $O \in P$, $v \in V$ est non nul, et R est la rotation vectorielle de V d'angle $2\pi/n$ pour l'une des deux orientations.

Théorème 3.3. *Soit $n \geq 3$. Il existe un polygone régulier à n sommets dont les sommets sont dans $\mathbb{Z}^2$ si et seulement si $n = 4$.*

Voici l'idée. Les côtés du polygone sont des vecteurs à coordonnées entières, et la rotation R les envoie les uns sur les autres. Elle préserve donc un réseau, et sa matrice dans une base de ce réseau est à coefficients entiers. Or la trace d'une matrice ne dépend pas de la base, et la trace d'une rotation d'angle θ vaut $2 \cos \theta$. Donc $2 \cos(2\pi/n)$ est entier, ce qui laisse très peu de possibilités. La figure 3 montre la situation pour le carré.

Démonstration. Le carré $(0, 0), (1, 0), (1, 1), (0, 1)$ convient pour $n = 4$. Réciproquement, soit (P_k) un polygone régulier à sommets dans $\mathbb{Z}^2$, $P_k = O + R^k(v)$, et soit $\theta = 2\pi/n \in]0, 2\pi/3]$.

Étape 1 : les vecteurs côtés. Posons $w_k = P_{k+1} - P_k = R^k(Rv - v)$. Ce sont des vecteurs de $\mathbb{Z}^2$, comme différences de points de $\mathbb{Z}^2$, et $R(w_k) = w_{k+1}$ pour tout $k \in \mathbb{Z}/n\mathbb{Z}$. Le vecteur $w_0 = Rv - v$ est non nul, car R ne fixe que le vecteur nul puisque $\theta \notin 2\pi\mathbb{Z}$. Les vecteurs w_0 et $w_1 = Rw_0$ sont indépendants, car $\theta \notin \pi\mathbb{Z}$.

Étape 2 : le réseau. Soit $L = \sum_k \mathbb{Z}w_k$ le sous-groupe de $\mathbb{Z}^2$ engendré par les w_k . Comme R permute les w_k , on a $R(L) = L$. C'est un sous-groupe de $\mathbb{Z}^2$, donc un $\mathbb{Z}$ -module libre de rang fini. Des vecteurs de $\mathbb{Z}^2$ indépendants sur $\mathbb{Z}$ le sont sur $\mathbb{Q}$ (on chasse les dénominateurs), donc sur $\mathbb{R}$ (le rang d'une matrice rationnelle ne dépend pas du corps). Le rang de L est donc au

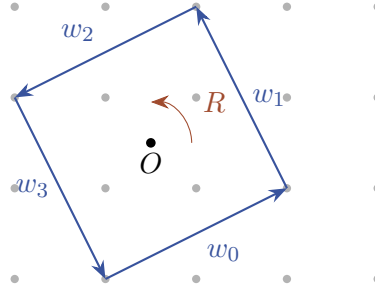


FIG. 3 : Un carré de $\mathbb{Z}^2$ et ses vecteurs côtés. La rotation R d'un quart de tour envoie w_k sur w_{k+1} ; ils engendrent le réseau L de la preuve.

plus 2. Il vaut 2 puisque L contient w_0 et w_1 . Une $\mathbb{Z}$ -base (e_1, e_2) de L est ainsi une base de $\mathbb{R}^2$.

Attention, on ne peut pas se contenter de $L' = \mathbb{Z}w_0 + \mathbb{Z}w_1$: on sait que $R(w_1) = w_2$ est dans $\mathbb{Z}^2$, mais pas qu'il est dans L' . C'est pour cela qu'on prend tous les w_k .

Étape 3 : la trace. Comme $R(e_1)$ et $R(e_2)$ sont dans L , la matrice de R dans la base (e_1, e_2) est à coefficients entiers. Donc $\text{tr } R = 2 \cos \theta \in \mathbb{Z}$. Or $\theta \in]0, 2\pi/3]$ donne $2 \cos \theta \in [-1, 2[$. Donc $2 \cos \theta \in \{-1, 0, 1\}$, c'est-à-dire $\theta \in \{2\pi/3, \pi/2, \pi/3\}$, ou encore $n \in \{3, 4, 6\}$.

Étape 4 : conclusion. Le cas $n = 3$ est exclu par la proposition 3.1. Si $n = 6$, les sommets P_0, P_2, P_4 s'écrivent $O + (R^2)^j(v)$ pour $j = 0, 1, 2$, où R^2 est la rotation d'angle $2\pi/3$. Ils forment un triangle équilatéral à sommets dans $\mathbb{Z}^2$, ce qui est exclu. Il reste $n = 4$. $\square$

Remarque 3.4. La preuve vaut aussi pour les polygones étoilés, où R est la rotation d'angle $2\pi m/n$ avec $m \wedge n = 1$: la condition $2 \cos(2\pi m/n) \in \{-1, 0, 1\}$ donne encore $n \in \{3, 4, 6\}$. Elle vaut aussi mot pour mot dans $\mathbb{Z}^d$ (exercice 5). Seule l'étape 4, qui exclut $n = 3$ et $n = 6$, utilise la dimension 2.

Remarque 3.5 (Racines de l'unité). En termes complexes, si les sommets z_k sont dans $\mathbb{Z}[i]$, alors $e^{2i\pi/n} = (z_2 - z_1)/(z_1 - z_0)$ est dans $\mathbb{Q}(i)$. Le théorème 3.3 dit donc que les racines de l'unité de $\mathbb{Q}(i)$ sont ± 1 et $\pm i$. On peut aussi le voir ainsi. Une racine primitive n -ième de l'unité est de degré $\varphi(n)$ sur $\mathbb{Q}$ (irréductibilité des polynômes cyclotomiques). Si elle est dans $\mathbb{Q}(i)$, on a $\varphi(n) \leq 2$, donc $n \in \{1, 2, 3, 4, 6\}$. Et $e^{2i\pi/3} = \frac{-1+i\sqrt{3}}{2}$ n'est pas dans $\mathbb{Q}(i)$.

Remarque 3.6 (Entiers d'Eisenstein). Sur le réseau hexagonal $\mathbb{Z}[j]$, avec $j = e^{2i\pi/3}$, la situation s'inverse : il y a des triangles équilatéraux et des hexagones réguliers, mais pas de carré, puisque $i \notin \mathbb{Q}(j) = \mathbb{Q}(i\sqrt{3})$. Le plan $x + y + z = 0$ coupe $\mathbb{Z}^3$ selon une copie de ce réseau, ce qui explique l'exercice 5.

4 Retour aux deux questions

Le triangle. Aucun triangle équilatéral n'a ses sommets sur un quadrillage, parce que $\sqrt{3}$ est irrationnel. Plus généralement, le carré est le seul polygone régulier qu'on puisse y dessiner. La raison profonde est que la rotation d'un quart de tour est la seule rotation non triviale (avec le demi-tour) qui préserve le quadrillage.

Les puissances de $1 + \sqrt{2}$. On a bien $(1 + \sqrt{2})^q = \sqrt{n+1} + \sqrt{n}$ pour un unique $n \in \mathbb{N}$, parce que la norme est multiplicative et que $N(1 + \sqrt{2}) = -1$. Mieux : le corollaire 2.6 montre que les coefficients des $(1 + \sqrt{2})^q$ sont les *seules* solutions positives de $x^2 - 2y^2 = \pm 1$. Les nombres de la forme $\sqrt{n+1} + \sqrt{n}$ qui sont dans $\mathbb{Z}[\sqrt{2}]$ sont donc exactement les puissances de $1 + \sqrt{2}$, puisqu'un tel nombre s'écrit $x + y\sqrt{2}$ avec $x, y \geq 0$ et $x^2 - 2y^2 = \pm 1$.

5 Exercices

Exercice 1. Calculer $(1 + \sqrt{2})^q$ pour $1 \leq q \leq 5$, et l'écrire sous la forme $\sqrt{n+1} + \sqrt{n}$.

Exercice 2. Montrer que l'unité fondamentale de $\mathbb{Z}[\sqrt{3}]$ est $2 + \sqrt{3}$, que toutes les unités de $\mathbb{Z}[\sqrt{3}]$ sont de norme 1, et résoudre $x^2 - 3y^2 = 1$ dans $\mathbb{N}^2$.

Exercice 3. Déterminer les nombres triangulaires $\frac{n(n+1)}{2}$, $n \geq 1$, qui sont des carrés parfaits.

Exercice 4. Soit p un nombre premier tel que 2 soit un carré modulo p . Montrer qu'il existe $(x, y) \in \mathbb{Z}^2$ tel que $p = x^2 - 2y^2$. Traiter $p = 7$ et $p = 17$.

Exercice 5. Soit $d \geq 2$. Montrer qu'un polygone régulier à n sommets dont les sommets sont dans $\mathbb{Z}^d$ n'existe que pour $n \in \{3, 4, 6\}$, et que les trois cas sont réalisés dans $\mathbb{Z}^3$.

6 Corrigés

Exercice 1. On utilise la récurrence $a_{q+1} = a_q + 2b_q$, $b_{q+1} = a_q + b_q$:

$$\begin{aligned} 1 + \sqrt{2} &= \sqrt{2} + \sqrt{1}, & 3 + 2\sqrt{2} &= \sqrt{9} + \sqrt{8}, & 7 + 5\sqrt{2} &= \sqrt{50} + \sqrt{49}, \\ 17 + 12\sqrt{2} &= \sqrt{289} + \sqrt{288}, & 41 + 29\sqrt{2} &= \sqrt{1682} + \sqrt{1681}. \end{aligned}$$

Les valeurs de n sont donc 1, 8, 49, 288, 1681, conformément à la proposition 2.8.

Exercice 2. On suit la méthode du corollaire 2.6. On a $N(2 + \sqrt{3}) = 4 - 3 = 1$, donc $2 + \sqrt{3}$ est une unité > 1 . Montrons que c'est la plus petite. Soit $u = a + b\sqrt{3}$ une unité > 1 . Par le lemme 2.4, $a, b \geq 1$.

- Si $b = 1$, alors $a^2 = 3 \pm 1$, donc $a = 2$ et $u = 2 + \sqrt{3}$.
- Si $b \geq 2$, alors $u \geq 1 + 2\sqrt{3} > 2 + \sqrt{3}$, puisque $\sqrt{3} > 1$.

Donc $\varepsilon_3 = 2 + \sqrt{3}$, et $\mathbb{Z}[\sqrt{3}]^\times = \{\pm(2 + \sqrt{3})^k\}$ par le théorème 2.5. Toutes ces unités sont de norme $N(2 + \sqrt{3})^k = 1$. On le voit aussi directement : $x^2 - 3y^2 = -1$ imposerait $x^2 \equiv 2 \pmod{3}$, ce qui est impossible. Comme dans le corollaire 2.6, les solutions de $x^2 - 3y^2 = 1$ dans $\mathbb{N}^2$ sont les coefficients de $(2 + \sqrt{3})^k$, $k \geq 0$: (1, 0), (2, 1), (7, 4), (26, 15), (97, 56), ...

Exercice 3. L'idée est de compléter le carré pour faire apparaître une équation de Pell-Fermat. En multipliant par 8 et en ajoutant 1, on obtient

$$\frac{n(n+1)}{2} = m^2 \iff 4n^2 + 4n + 1 = 8m^2 + 1 \iff (2n+1)^2 - 2(2m)^2 = 1.$$

On pose $x = 2n+1$ et $y = 2m$. Réciproquement, si $x^2 - 2y^2 = 1$, alors x est impair, donc $x^2 \equiv 1 \pmod{8}$, donc $8 \mid 2y^2$ et y est pair. Par le corollaire 2.6, les solutions avec $n \geq 1$ correspondent à $x + y\sqrt{2} = (1 + \sqrt{2})^{2k} = (3 + 2\sqrt{2})^k$, $k \geq 1$:

$$(x, y) = (3, 2), (17, 12), (99, 70), (577, 408), \dots \quad (n, m) = (1, 1), (8, 6), (49, 35), (288, 204), \dots$$

Par exemple $\frac{49 \cdot 50}{2} = 1225 = 35^2$.

Exercice 4. L'idée est de factoriser $a^2 - 2$ dans $\mathbb{Z}[\sqrt{2}]$, puis d'utiliser que cet anneau est principal. Soit $a \in \mathbb{Z}$ avec $p \mid a^2 - 2 = (a - \sqrt{2})(a + \sqrt{2})$.

- L'élément p n'est pas inversible dans $\mathbb{Z}[\sqrt{2}]$, car $N(p) = p^2 \neq \pm 1$.
- Il ne divise ni $a - \sqrt{2}$ ni $a + \sqrt{2}$ dans $\mathbb{Z}[\sqrt{2}]$. Sinon, on aurait $a \pm \sqrt{2} = p(u + v\sqrt{2})$, donc $pv = \pm 1$.

Ainsi p n'est pas premier dans $\mathbb{Z}[\sqrt{2}]$. Comme cet anneau est principal (proposition 2.11), irréductible équivaut à premier, et p n'est donc pas irréductible : $p = \pi\rho$ avec π, ρ non inversibles. Alors $N(\pi)N(\rho) = p^2$ avec $|N(\pi)| \neq 1$ et $|N(\rho)| \neq 1$, donc $N(\pi) = \pm p$. En écrivant $\pi = x + y\sqrt{2}$, on a $x^2 - 2y^2 = \pm p$. Si le signe est $-$, on remplace π par $\pi(1 + \sqrt{2})$, de norme $-N(\pi) = p$.

Pour $p = 7$, on a $3^2 \equiv 2$ et $7 = 3^2 - 2 \cdot 1^2$. Pour $p = 17$, on a $6^2 \equiv 2$ et $17 = 5^2 - 2 \cdot 2^2$.

Inversement, si $p = x^2 - 2y^2$ est impair, alors x est impair, et $p \equiv 1 - 2y^2 \equiv 1$ ou $7 \pmod{8}$. Avec la seconde loi complémentaire de réciprocité quadratique, un premier impair p est de la forme $x^2 - 2y^2$ si et seulement si $p \equiv \pm 1 \pmod{8}$.

Exercice 5. Soit (P_k) un polygone régulier à n sommets dans $\mathbb{Z}^d$, contenu dans un plan affine de direction V , et soit R la rotation de V correspondante. On reprend les étapes 1 à 3 de la preuve du théorème 3.3. Les vecteurs $w_k = P_{k+1} - P_k$ sont dans $\mathbb{Z}^d \cap V$, et R les permute. Le groupe L qu'ils engendrent est un sous-groupe de $\mathbb{Z}^d$, donc libre de rang fini. Une $\mathbb{Z}$ -base de L est formée de vecteurs entiers indépendants sur $\mathbb{Z}$, donc sur $\mathbb{R}$, contenus dans le plan V . Le rang est donc au plus 2, et il vaut 2 puisque w_0 et w_1 sont indépendants. On conclut comme dans le théorème que $2\cos(2\pi/n) \in \mathbb{Z}$, donc $n \in \{3, 4, 6\}$.

Les trois cas sont réalisés dans $\mathbb{Z}^3$ (figure 4).

- $n = 4$: le carré $(0, 0, 0), (1, 0, 0), (1, 1, 0), (0, 1, 0)$.
- $n = 3$: le triangle $(1, 0, 0), (0, 1, 0), (0, 0, 1)$, de côté $\sqrt{2}$.
- $n = 6$: les six points

$$(1, -1, 0), (1, 0, -1), (0, 1, -1), (-1, 1, 0), (-1, 0, 1), (0, -1, 1).$$

Vérifions le dernier cas. Ces points sont les $\rho^k(1, -1, 0)$, $0 \leq k \leq 5$, avec $\rho(x, y, z) = (-y, -z, -x)$. L'application ρ est une isométrie linéaire de $\mathbb{R}^3$ qui stabilise le plan $V = \{x + y + z = 0\}$. On calcule $\rho^2(x, y, z) = (z, x, y)$ et $\rho^3 = -\text{id}$. La restriction de ρ à V est donc d'ordre exactement 6, puisque ni ρ^2 ni ρ^3 n'y induisent l'identité. Une isométrie d'ordre 6 d'un plan euclidien est une rotation d'angle $\pm\pi/3$, car les symétries orthogonales sont d'ordre 2. Les six points forment donc un hexagone régulier de centre 0 et de rayon $\sqrt{2}$.

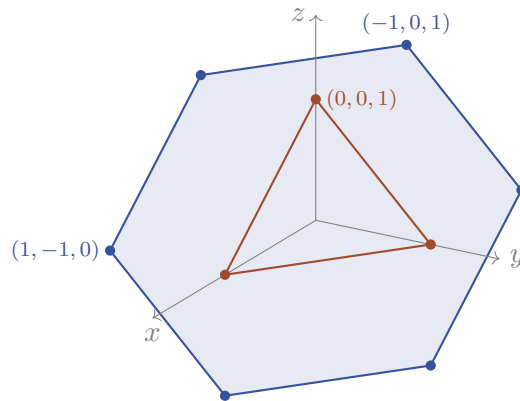


FIG. 4 : Dans $\mathbb{Z}^3$: l'hexagone régulier formé des permutations de $(1, -1, 0)$, dans le plan $x + y + z = 0$, et le triangle équilatéral $(1, 0, 0), (0, 1, 0), (0, 0, 1)$, dans le plan $x + y + z = 1$.

On remarque que la preuve par l'aire de la proposition 3.1 ne s'applique plus dans $\mathbb{Z}^3$: l'aire du triangle $(1, 0, 0), (0, 1, 0), (0, 0, 1)$ vaut $\frac{\sqrt{3}}{2}$, qui n'est pas dans $\frac{1}{2}\mathbb{Z}$.

Références

- [1] P. Samuel, *Théorie algébrique des nombres*, Hermann.

- [2] D. Duverney, *Théorie des nombres*, Dunod.
- [3] G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press.
- [4] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer.
- [5] X. Gourdon, *Les maths en tête. Algèbre et probabilités*, Ellipses.

Source. Feuille d'exercices de terminale S (2003).