DM 1 · C1. Le théorème de Noël

Fermat, Mersenne, et les nombres qui se cassent en deux carrés

---

LE PLAN DE L'ÉDIFICE

	PARTIE	NIVEAUX	S'APPUIE SUR
0.	Prologue · le cadeau du 25 décembre	△▲	l'exercice 19 de l'Atelier
I.	L'identité qui multiplie les carrés	△▲	le prologue et l'exercice 19
II.	Un monde où l'on peut diviser	▲♦	la partie I et l'exercice 28
III.	Bézout, irréductibles, et le lemme d'Euclide	△▲♦	la partie II
IV.	Le théorème de Noël	△▲♦	la partie III
V.	Pour continuer le voyage	♦	tout ce qui précède

Facultatif, et pour longtemps. Tout travail sincère, même partiel, est valorisé ; un travail bâclé ne l'est jamais. Ce document peut vous accompagner plusieurs années : certaines questions vous attendront en prépa ou à l'université. Horizon raisonnable : 3 à 4 semaines. Et si vous bloquez, écrivez : dire où l'on bloque et pourquoi est déjà du travail mathématique, souvent le plus formateur. Vérifiez toujours les hypothèses d'un résultat avant de l'utiliser.

△ fondations : accessible avec le cours · ▲ construction : recul et autonomie · ♦ sommet : défis, ou invitations pour plus tard

---

PROLOGUE

Le cadeau du 25 décembre

Voici deux listes. À gauche : 5, 13, 17, 29, 37, 41. À droite : 3, 7, 11, 19, 23, 31. Ce sont tous des nombres premiers, et ils se ressemblent comme des frères. Pourtant les six de gauche se cassent en deux carrés, $5 = 1 + 4$, $13 = 4 + 9$, $17 = 1 + 16$, et ainsi de suite ; les six de droite s'y refusent obstinément, et vous pouvez essayer longtemps. Personne, en général, ne trouve cela étrange. C'est pourtant l'un des faits les plus profonds de l'arithmétique, la réponse tient dans un reste de division par 4, et la démonstration passe par un pays de nombres que le chapitre vient tout juste de construire.

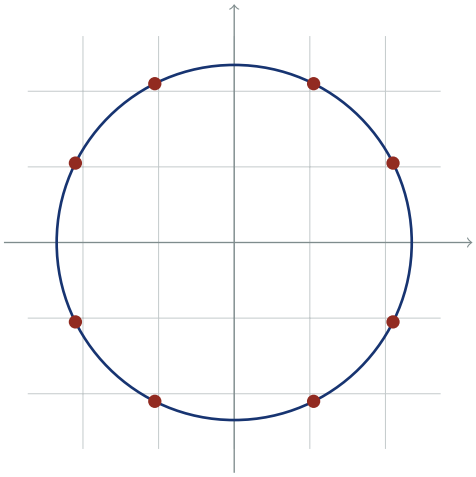
Quatre hommes jalonnent cette histoire : un géomètre d'Alexandrie du troisième siècle, un ingénieur militaire hollandais qui joue du luth, un magistrat de Toulouse qui fait des mathématiques la nuit, et un Suisse installé à Berlin qui y consacrera sept ans de sa vie. À la fin du voyage, vous saurez pourquoi certains nombres premiers se brisent et d'autres non, et vous aurez démontré un théorème que son auteur lui-même n'a jamais démontré.

Le point de départ, vous l'avez déjà calculé. À l'exercice 19 de l'Atelier, l'identité de Diophante appliquée à

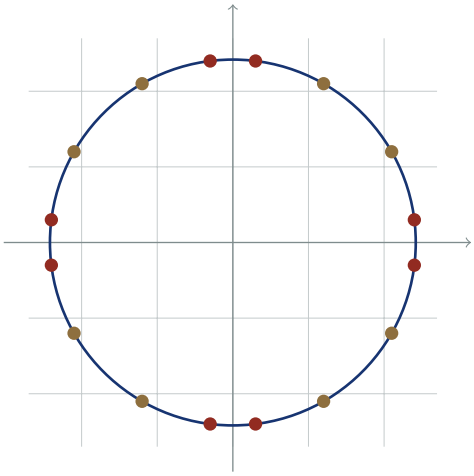
$5 = 1^2 + 2^2$ et $13 = 2^2 + 3^2$ vous a donné 65 de **deux** façons :

$$65 = 1^2 + 8^2 = 4^2 + 7^2.$$

Or 5 et 13 ne s'écrivent, chacun, que d'une seule. Voilà les trois faits que ce devoir doit expliquer, et l'on peut déjà les regarder.



$5 = 1^2 + 2^2$
huit points, une seule écriture



$65 = 1^2 + 8^2 = 4^2 + 7^2$
seize points, deux écritures

Un entier est somme de deux carrés lorsque le cercle centré à l'origine et de rayon sa racine carrée passe par un point à coordonnées entières. Compter les écritures, c'est compter ces points. Les deux figures ne sont pas à la même échelle : ici l'on compte, on ne mesure pas.

Q1. Le tri.

a) △ Pour chacun des nombres 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 et 37, dire s'il est somme de deux carrés d'entiers naturels, et donner l'écriture quand elle existe. On autorise le carré 0^2.

b) △ Ranger ceux de la liste qui sont impairs en deux colonnes, selon que leur reste dans la division euclidienne par 4 vaut 1 ou 3. Comparer avec le résultat du a).

c) △ Formuler une conjecture. Le nombre 2 mérite-t-il une place à part ?

Q2. La moitié facile. Une conjecture n'est pas un théorème, et celle-ci a deux sens. Commençons par celui qui se démontre en dix lignes.

a) △ Soit $n \in \mathbb{Z}$. En distinguant selon la parité de n, démontrer que le reste de n^2 dans la division euclidienne par 4 vaut 0 ou 1.

b) △ En déduire que, pour tous $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$, le reste de $a^2 + b^2$ dans la division euclidienne par 4 vaut 0, 1 ou 2.

c) △ Conclure : **aucun** nombre premier de la forme $4k + 3$ n'est somme de deux carrés.

Vous venez de démontrer la moitié du théorème. C'est la moitié facile, et elle ne coûte que la parité. L'autre moitié, celle qui affirme que tout premier $4k + 1$ *est* somme de deux carrés, occupera tout le reste de ce devoir. Notez la dissymétrie : pour interdire, il suffit d'un obstacle ; pour garantir, il faut *construire* a et b, et ils ne se donnent pas.

> AMSTERDAM 1625, TOULOUSE 1640, BERLIN 1749
>
> Le théorème porte le nom de Fermat, et c'est une injustice de plus. **Albert Girard** l'énonce le premier, en 1625, quinze ans avant lui : c'est le même Girard qui, quatre ans plus tard, affirmera que toute équation de degré n possède n solutions. **Fermat** le réénonce le 25 décembre 1640, dans une longue lettre au père Marin Mersenne, moine minime qui tient à lui seul la boîte aux lettres mathématique de l'Europe. Il y expose ce qu'il appelle ses *fondements* pour toutes les questions de sommes de carrés, ajoute qu'il en possède la démonstration, et ne la donne pas. Fermat n'a d'ailleurs jamais publié une ligne de mathématiques de son vivant : il énonce, il affirme avoir démontré, et il passe à autre chose. Il faudra attendre **Euler**, qui commence en 1742 et annonce enfin sa preuve à Goldbach le 12 avril 1749. Sept ans pour deux lignes écrites un soir de Noël.

PARTIE I — *s'appuie sur le prologue et sur l'exercice 19*

L'identité qui multiplie les carrés

Avant de chercher, il faut réduire le problème. Et pour cela, il faut remarquer que les sommes de deux carrés se comportent bien vis-à-vis de la multiplication, ce que l'exercice 19 a établi et que voici sous sa forme utile.

> **R1 – L'IDENTITÉ DE DIOPHANTE, VUE PAR LE CONJUGUÉ**
>
> Pour tout $z = a + ib$ avec $a \in \mathbb{R}$ et $b \in \mathbb{R}$, on note $\mathrm{N}(z) = z\,\overline{z} = a^2 + b^2$, appelée la **norme** de z. Alors, pour tous $z \in \mathbb{C}$ et $w \in \mathbb{C}$,
>
> $$\mathrm{N}(z\,w) = \mathrm{N}(z)\ \mathrm{N}(w),$$
>
> ce qui s'écrit, en coordonnées : pour tous $a \in \mathbb{R}$, $b \in \mathbb{R}$, $c \in \mathbb{R}$ et $d \in \mathbb{R}$,
>
> $$\left(a^2 + b^2\right)\left(c^2 + d^2\right) = (ac - bd)^2 + (ad + bc)^2.$$
>
> *Conséquence immédiate : le produit de deux sommes de deux carrés est une somme de deux carrés.* **(Établi à l'exercice 19 de l'Atelier : on ne le redémontre pas.)**

Q3. Fabriquer à la chaîne.

a) △ En partant de $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$ et $17 = 1^2 + 4^2$, écrire $5 \times 13 \times 17$ comme somme de deux carrés. Vérifier le résultat par le calcul direct du produit.

b) △ Recommencer en échangeant 1 et 2 dans l'écriture de 5. Obtient-on la même chose ?

c) ▲ Soient $n \in \mathbb{N}^*$ et $p_1, \dots, p_n$ des entiers naturels tous sommes de deux carrés. Démontrer par récurrence sur n que leur produit est somme de deux carrés.

Q4. Le crible. On veut maintenant voir le phénomène sur tous les entiers, et pas seulement sur les nombres premiers.

a) △ Dresser la liste des entiers de 1 à 25 qui sont sommes de deux carrés d'entiers naturels. On s'autorisera 0, de sorte que 1, 4 et 9 y figurent.

b) △ Repérer dans cette liste les nombres obtenus comme produits de deux entiers plus petits de la liste. La question Q3c est-elle visible à l'œil nu ?

c) △ **Attention au sens de la flèche.** Justifier, à l'aide du seul nombre 9, que la réciproque de Q3c est fausse : un produit peut être somme de deux carrés sans que ses facteurs le soient. Garder ce contre-exemple en réserve, il servira à la question Q14.

Q5. Ce qu'il reste, et pourquoi c'est difficile.

a) △ Écrire 2 comme somme de deux carrés. Le prologue avait raison de lui donner une place à part : pourquoi ne peut-il être ni de la forme $4k+1$ ni de la forme $4k+3$?

b) △ Énoncer précisément, en une phrase, l'énoncé qu'il reste à démontrer.

c) ▲ Le nombre $2\,017$ est premier et vaut $4 \times 504 + 1$. *Si* la conjecture de Q1c est vraie, il est donc somme de deux carrés : cherchez a et b. Combien d'essais faut-il faire, au pire, pour y arriver par tâtonnement ? Que se passerait-il avec un nombre premier à trente chiffres ?

La question c) dit tout : chercher a et b n'est pas une méthode, c'est une loterie. Il nous faut un argument qui *garantisse* leur existence sans les exhiber. Et cet argument, on va aller le chercher là où le chapitre nous a appris à regarder : dans un monde plus grand.

PARTIE II — *s'appuie sur la partie I et sur l'exercice 28*

Un monde où l'on peut diviser

Dans $\mathbb{Z}$, tout part d'un seul énoncé : la division euclidienne. C'est elle qui donne le PGCD, puis Bézout, puis le lemme d'Euclide, puis la décomposition en facteurs premiers. Toute l'arithmétique tient à ce fil. La question de cette partie est donc simple à formuler, et sa réponse est le cœur du devoir : *existe-t-il une division euclidienne dans $\mathbb{Z}[i]$?* Si oui, toute l'arithmétique s'y transporte, et avec elle les outils qui nous manquent.

> **R2 – L'ANNEAU DES ENTIERS DE GAUSS**
>
> On note $\mathbb{Z}[i] = \{a + ib \mid a \in \mathbb{Z},\ b \in \mathbb{Z}\}$. Cet ensemble est stable par addition et par multiplication ; la norme N y est à valeurs dans $\mathbb{N}$ et reste multiplicative ; et les seuls éléments de $\mathbb{Z}[i]$ qui y sont inversibles sont 1, -1, i et $-i$, c'est-à-dire exactement ceux de norme 1.
>
> **(Établi à l'exercice 28 de l'Atelier : on ne le redémontre pas.)**

> **DÉFINITION – DIVISIBILITÉ DANS $\mathbb{Z}[i]$**
>
> Soient $z \in \mathbb{Z}[i]$ et $w \in \mathbb{Z}[i]$. On dit que z **divise** w **dans** $\mathbb{Z}[i]$, et l'on note $z \mid w$, lorsqu'il existe $u \in \mathbb{Z}[i]$ tel que $w = z\,u$.

Q6. Des entiers qui se cassent.

a) △ Vérifier que $2 = (1+i)(1-i)$, puis que $5 = (1+2i)(1-2i)$ et $13 = (2+3i)(2-3i)$.

b) △ Démontrer que, pour tous $z \in \mathbb{Z}[i]$ et $w \in \mathbb{Z}[i]$, si $z \mid w$ dans $\mathbb{Z}[i]$ alors $\mathrm{N}(z)$ divise $\mathrm{N}(w)$ dans $\mathbb{Z}$.

c) ▲ En déduire que 3 n'est le produit d'aucun couple d'éléments non inversibles de $\mathbb{Z}[i]$. *On pourra raisonner sur les normes possibles.*

d) ▲ Que viennent de montrer les questions a) et c) réunies, à propos de 2, 5, 13 d'un côté et de 3 de l'autre ? Rapprocher du tri de la question Q1.

Vous tenez la piste. Certains nombres premiers ordinaires *se cassent* en entrant dans $\mathbb{Z}[i]$, et d'autres résistent ; et pour l'instant, ceux qui se cassent sont exactement ceux qui sont sommes de deux carrés. Ce n'est pas un hasard : si $p = z\,\overline{z}$ avec $z = a + ib$, $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$, alors $p = a^2 + b^2$, et réciproquement. **Le théorème de Fermat est donc, mot pour mot, une question de divisibilité dans $\mathbb{Z}[i]$.** Reste à savoir y diviser.

Q7. La division euclidienne. On cherche, pour $z \in \mathbb{Z}[i]$ et $w \in \mathbb{Z}[i]$ non nul, à écrire $z = q\,w + r$ avec $q \in \mathbb{Z}[i]$, $r \in \mathbb{Z}[i]$ et $\mathrm{N}(r) < \mathrm{N}(w)$.

a) △ On prend $z = 8 + 5i$ et $w = 2 + 3i$. Calculer le quotient $\dfrac{z}{w}$ sous forme algébrique. Appartient-il à $\mathbb{Z}[i]$?

b) ▲ Placer ce quotient dans le plan, repérer le point de $\mathbb{Z}[i]$ le plus proche de lui, et l'appeler q. Calculer alors $r = z - q\,w$, puis $\mathrm{N}(r)$ et $\mathrm{N}(w)$. Conclure sur cet exemple.

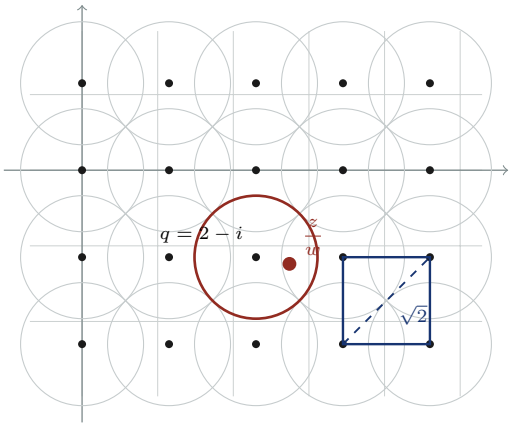
c) ▲ **Le point qui décide de tout.** Démontrer que, pour tout $x \in \mathbb{C}$, il existe $q \in \mathbb{Z}[i]$ tel que

$$\mathrm{N}(x - q) \leqslant \frac{1}{2}.$$

On raisonnera séparément sur chacune des deux coordonnées. Géométriquement, cela dit qu'aucun point du plan n'est à une distance supérieure à $\dfrac{\sqrt{2}}{2}$ du nœud le plus proche, et c'est ce que montre la figure ci-dessous.

d) ♦ En déduire le théorème général : pour tous $z \in \mathbb{Z}[i]$ et $w \in \mathbb{Z}[i]$ non nul, il existe $q \in \mathbb{Z}[i]$ et $r \in \mathbb{Z}[i]$ tels que $z = q\,w + r$ et $\mathrm{N}(r) < \mathrm{N}(w)$. *On appliquera le c) au complexe $\dfrac{z}{w}$, puis on multipliera par w en se souvenant que* N *est multiplicative (R1).*

e) ▲ Dans $\mathbb{Z}$, le couple $(q\,;r)$ de la division euclidienne est unique. Ici, il ne l'est pas toujours : trouver une situation géométrique où quatre choix de q conviennent également. Cela gêne-t-il pour la suite ?



aucun point du plan n'échappe au disque de rayon $\dfrac{\sqrt{2}}{2}$ centré sur un nœud : c'est toute la démonstration

R3 – DIVISION EUCLIDIENNE DANS $\mathbb{Z}[i]$

Pour tous $z \in \mathbb{Z}[i]$ et $w \in \mathbb{Z}[i]$ avec $w \neq 0$, il existe $q \in \mathbb{Z}[i]$ et $r \in \mathbb{Z}[i]$ tels que

$$z = q\,w + r \qquad \text{et} \qquad \mathrm{N}(r) < \mathrm{N}(w).$$

Le couple $(q\,;r)$ n'est pas nécessairement unique.

GÖTTINGEN, 1832

Gauss n'a pas inventé ces nombres pour Fermat. Il les introduit dans son second mémoire sur les résidus biquadratiques, en 1832, pour un tout autre problème : comprendre les puissances quatrièmes modulo un nombre premier. Les sommes de deux carrés en tombent comme un fruit mûr, presque en passant. C'est une constante de cette histoire : on agrandit le monde pour une raison, et l'on récolte des théorèmes qu'on ne cherchait pas.

PARTIE III *s'appuie sur la partie II*

Bézout, irréductibles, et le lemme d'Euclide

Vous venez d'obtenir la clé. Tout ce que l'arithmétique de $\mathbb{Z}$ déduit de la division euclidienne va se transporter dans $\mathbb{Z}[i]$, avec les mêmes démonstrations. Vous ferez ce travail dans $\mathbb{Z}$ aux chapitres A1, A2 et A3 ; la curiosité de ce devoir est que vous allez le faire *d'abord* ailleurs. Avant de démontrer, prenez l'outil en main.

Q8. Deux divisions à la main.

a) △ Effectuer la division euclidienne de $z = 11 + 3i$ par $w = 1 + 8i$ dans $\mathbb{Z}[i]$, en suivant la méthode de Q7 : calculer $\dfrac{z}{w}$, choisir le nœud le plus proche, en déduire q puis r, et vérifier que $\mathrm{N}(r) < \mathrm{N}(w)$.

b) △ Recommencer avec $z = 1 + 8i$ et $w = 2 - 4i$.

c) △ Vous venez d'amorcer un algorithme d'Euclide dans $\mathbb{Z}[i]$. Poursuivez-le jusqu'à obtenir un reste nul. Quel est le dernier reste non nul ?

> **DÉFINITION – IRRÉDUCTIBLE**
>
> Un élément π de $\mathbb{Z}[i]$, non nul et non inversible, est dit **irréductible** lorsque, pour tous $z \in \mathbb{Z}[i]$ et $w \in \mathbb{Z}[i]$, l'égalité $\pi = z\,w$ entraîne que z ou w est inversible dans $\mathbb{Z}[i]$.

Q9. Reconnaître un irréductible.

a) ▲ Démontrer que, pour tout $z \in \mathbb{Z}[i]$, si $\mathrm{N}(z)$ est un nombre premier de $\mathbb{Z}$, alors z est irréductible dans $\mathbb{Z}[i]$.

b) △ En déduire que $1 + i$, $1 + 2i$ et $2 + 3i$ sont irréductibles dans $\mathbb{Z}[i]$.

c) △ La réciproque du a) est fausse : démontrer que 3 est irréductible dans $\mathbb{Z}[i]$ alors que $\mathrm{N}(3) = 9$ n'est pas premier. *La question Q6c a déjà fait tout le travail.*

Q10. Bézout, sans changer une virgule. Soient $a \in \mathbb{Z}[i]$ et $b \in \mathbb{Z}[i]$, non tous les deux nuls. On note

$$I = \{a\,u + b\,v \mid u \in \mathbb{Z}[i],\ v \in \mathbb{Z}[i]\}\,.$$

a) ▲ Justifier que I contient au moins un élément non nul, puis qu'il existe dans I un élément non nul d dont la norme est minimale parmi les normes des éléments non nuls de I. *On se souviendra que* N *est à valeurs dans* $\mathbb{N}$ *(R2).*

b) ♦ Soit $x \in I$. Effectuer la division euclidienne de x par d (R3) et démontrer que le reste appartient à I. En déduire que d divise tous les éléments de I, donc en particulier a et b.

c) ▲ Démontrer que tout diviseur commun de a et de b divise d. *On utilisera l'appartenance de* d *à* I.

d) ♦ **Le lemme d'Euclide.** Soit π un irréductible de $\mathbb{Z}[i]$ et soient $z \in \mathbb{Z}[i]$, $w \in \mathbb{Z}[i]$ tels que $\pi \mid z\,w$. Démontrer que $\pi \mid z$ ou $\pi \mid w$. *On supposera que* π *ne divise pas* z*, on appliquera ce qui précède au couple* $(\pi\,;z)$*, et l'on multipliera par* w *la relation obtenue.*

Prenez la mesure de ce que vous venez de faire. Vous avez reconstruit, dans un anneau que personne ne vous avait présenté, toute la mécanique qui fait marcher l'arithmétique. Et vous ne vous êtes servi que d'une seule chose : le fait qu'aucun point du plan n'est trop loin d'un nœud du réseau.

> BERLIN, 12 AVRIL 1749
>
> Euler, lui, n'avait pas ces outils. Il attaque le théorème par la *descente infinie*, la méthode que Fermat disait employer : supposer une solution, en fabriquer une strictement plus petite, recommencer, et buter sur l'impossibilité d'une suite infinie strictement décroissante d'entiers naturels. Sa démonstration est longue et pénible ; celle que vous allez écrire, avec les outils de Gauss, tiendra en une page. Le théorème n'a pas changé. C'est le monde dans lequel on le regarde qui a changé.

PARTIE IV — *s'appuie sur la partie III*

Le théorème de Noël

Tout est en place, sauf une chose. Pour casser p dans $\mathbb{Z}[i]$, il va falloir y trouver un multiple de p qui se factorise, et le candidat naturel est m^2+1, car pour tout $m \in \mathbb{Z}$ on a $m^2+1 = (m+i)(m-i)$. Encore faut-il qu'un tel m existe. C'est le seul point que ce devoir vous demande d'admettre.

> **R4 – LE PONT VERS L'ARITHMÉTIQUE**
>
> Soit p un nombre premier tel que $p = 4k+1$ pour un certain $k \in \mathbb{N}^*$. Alors il existe $m \in \mathbb{N}$ tel que p divise m^2+1 dans $\mathbb{Z}$.
>
> *Ce résultat est une conséquence du théorème de Wilson. Vous en aurez les outils au chapitre A3 ; ici, on l'admet.* *(ce résultat peut être admis pour la suite)*

Q11. Prendre R4 en main.

a) △ Vérifier R4 sur $p = 5$ avec $m = 2$, sur $p = 13$ avec $m = 5$, sur $p = 17$ avec $m = 4$ et sur $p = 29$ avec $m = 12$.

b) △ Trouver un entier m convenable pour $p = 37$, puis pour $p = 41$.

c) △ Écrire 29, 37 et 41 comme sommes de deux carrés, puis vérifier sur chacun que le produit $z\,\overline{z}$ correspondant redonne bien le nombre premier de départ. C'est exactement la cassure que la question suivante va démontrer en général.

Q12. La cassure. Dans toute cette question, p est un nombre premier de la forme $4k+1$ et m est un entier fourni par R4.

a) △ Justifier que p divise $(m+i)(m-i)$ dans $\mathbb{Z}[i]$.

b) ▲ Démontrer que p ne divise ni $m+i$ ni $m-i$ dans $\mathbb{Z}[i]$. *On écrira $m+i = p\,(u+iv)$ avec $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$, et l'on regardera la partie imaginaire.*

c) ▲ En déduire, grâce au lemme d'Euclide, que p **n'est pas** irréductible dans $\mathbb{Z}[i]$.

d) ▲ Il existe donc $z \in \mathbb{Z}[i]$ et $w \in \mathbb{Z}[i]$, tous deux non inversibles, tels que $p = z\,w$. Prendre les normes et en déduire que $\mathrm{N}(z) = p$.

e) △ Conclure : en écrivant $z = a + ib$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$, on obtient $p = a^2 + b^2$.

Le théorème est démontré. Relisez la chaîne : un lemme d'arithmétique, une factorisation qui n'existe que dans $\mathbb{Z}[i]$, le lemme d'Euclide, et une norme. Aucune recherche de a et b, aucun tâtonnement. **On n'a pas trouvé les deux carrés : on a démontré qu'ils ne pouvaient pas ne pas exister.**

les nombres premiers qui se cassent dans $\mathbb{Z}[i]$ sont exactement ceux de la forme $4k+1$, plus le cas isolé de 2

Q13. Et « d'une seule façon ». Fermat annonçait aussi l'unicité, et c'est elle qui explique le contraste des deux cercles du prologue. On admet pour cette question le résultat suivant.

> **R5 – DÉCOMPOSITION EN IRRÉDUCTIBLES**
>
> Tout élément non nul et non inversible de $\mathbb{Z}[i]$ s'écrit comme produit d'irréductibles de $\mathbb{Z}[i]$, et cette écriture est unique à l'ordre des facteurs près et à multiplication près par des inversibles.
>
> *La démonstration se calque sur celle du théorème fondamental de l'arithmétique, que vous établirez au chapitre A3 : on raisonne par récurrence forte, ici sur la norme.* *(ce résultat peut être admis pour la suite)*

a) ▲ Soit p premier de la forme $4k+1$ et soit $p = a^2 + b^2$ une écriture donnée par Q12, avec $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$. Quitte à remplacer a par $|a|$ et b par $|b|$, ce qui ne change pas a^2+b^2, on suppose désormais $a \in \mathbb{N}$ et $b \in \mathbb{N}$. Démontrer alors que $z = a + ib$ et $\overline{z} = a - ib$ sont irréductibles dans $\mathbb{Z}[i]$.

b) ♦ Soit $p = c^2 + d^2$ une autre écriture, avec $c \in \mathbb{N}$ et $d \in \mathbb{N}$. En posant $z' = c + id$, démontrer que z' est un diviseur irréductible de p dans $\mathbb{Z}[i]$, puis, grâce à R5, que z' est égal à z ou à $\overline{z}$ à un inversible près.

c) ♦ En déduire que $\{c\,;d\} = \{a\,;b\}$: l'écriture est unique à l'ordre des deux carrés près.

d) ▲ Revenir aux deux cercles du prologue. Combien de points à coordonnées entières porte le cercle de rayon $\sqrt{5}$? Celui de rayon $\sqrt{65}$? Proposer une explication de la différence à l'aide de la factorisation $65 = 5 \times 13$. *La démonstration complète demanderait d'appliquer R5 aux quatre facteurs irréductibles de 65 : une conjecture argumentée suffit ici.*

Q14. Ce que le devoir laisse ouvert. Le théorème traite les nombres premiers. Les autres entiers restent à trier, et la question Q4c vous attendait ici.

a) △ Parmi 9, 15, 21, 45, 50 et 98, lesquels sont sommes de deux carrés ?

b) ▲ Décomposer chacun en facteurs premiers et observer l'exposant des facteurs premiers de la forme $4k+3$. Conjecturer un critère valable pour tout entier naturel non nul.

c) ♦ Démontrer le sens *suffisant* : si tout facteur premier de la forme $4k+3$ figure à un exposant pair, alors l'entier est somme de deux carrés. *Tout est en place : $2 = 1^2 + 1^2$, la question Q12 pour les facteurs de la forme $4k+1$, l'écriture $\left(q^{\,b}\right)^2 + 0^2$ pour les autres, et Q3c pour recoller le tout.* Le sens réciproque, lui, demande davantage que ce devoir : il vous attend sur le compagnon.

PARTIE V

s'appuie sur tout ce qui précède

Pour continuer le voyage

Le compte est bon. Le tri du prologue, celui que personne ne trouve étrange, est désormais un théorème : un nombre premier impair se casse en deux carrés si et seulement si son reste dans la division par 4 vaut 1, et il ne se casse alors que d'une seule manière.

Regardez le chemin. Vous avez pris une identité vieille de dix-sept siècles, vous en avez fait une norme ; vous avez remarqué qu'aucun point du plan n'est loin d'un nœud du réseau, et vous en avez tiré une division euclidienne ; de cette division vous avez déduit Bézout, puis le lemme d'Euclide ; et de ce lemme, en trois lignes, un théorème que Girard avait énoncé en 1625, que Fermat avait affirmé sans le prouver en 1640, et qu'Euler avait mis sept ans à démontrer autrement.

C'est la dernière leçon du chapitre, et la plus utile. On n'a pas rendu le théorème plus facile : on a changé le monde dans lequel on le regardait, et il est devenu facile tout seul. Fabriquer un monde de nombres n'est donc pas un luxe de théoricien. C'est un outil, et vous venez de vous en servir.

Q15. Trois portes qui restent ouvertes.

a) ♦ Le théorème garantit l'existence de a et b mais ne les fabrique pas. En vous inspirant de l'algorithme d'Euclide de la question Q8, imaginer une méthode qui, partant de p et de m, *produise* effectivement a et b. *Indication : calculer le PGCD de p et de $m + i$ dans $\mathbb{Z}[i]$.*

b) ♦ Le résultat R5 est admis ici. Dans d'autres anneaux construits sur le même modèle, il est **faux**. Cherchez, dans l'ensemble des nombres de la forme $a+b\sqrt{-5}$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$, deux factorisations différentes du nombre 6.

c) ♦ Combien y a-t-il de points à coordonnées entières sur le cercle de rayon $\sqrt{n}$, pour n quelconque ? La réponse porte un nom et se démontre avec les outils de ce devoir, poussés un cran plus loin.

> BRUNSWICK, 1877
>
> La question b) n'est pas une farce. Dans l'anneau qu'elle vous fait visiter, 6 s'écrit de deux façons irréductibles différentes, et toute l'arithmétique s'effondre. Richard Dedekind en tire la conclusion qui fonde l'algèbre moderne : plutôt que de renoncer, il forge en 1871 un objet neuf, l'*idéal*, pour lequel l'unicité redevient vraie, et il en donne six ans plus tard la grande exposition. Le geste vous est désormais familier. C'est celui de tout le chapitre : quand un énoncé bute sur un mur, on agrandit le monde jusqu'à ce que le mur disparaisse.

LA SUITE SUR LE COMPAGNON NUMÉRIQUE

Cinq contenus vous attendent sur le compagnon numérique du chapitre : le sens réciproque de la question Q14, celui que ce devoir n'a pas les moyens d'établir ; la démonstration d'Euler par descente infinie, celle de 1749, à comparer avec la vôtre ; la méthode du PGCD dans $\mathbb{Z}[i]$ annoncée en Q15a, puis l'algorithme de Cornacchia qui en est la traduction sans nombres complexes ; la réponse à Q15c, c'est-à-dire le compte exact des points à coordonnées entières sur un cercle de rayon $\sqrt{n}$; et le récit de l'anneau où 6 se factorise deux fois.

ANNEXE · COUPS DE POUCE

À consulter librement : un coup de pouce n'est pas une solution, et y recourir n'enlève rien à la valeur du travail.

Q2a. Écrivez $n = 2k$ puis $n = 2k+1$, et développez le carré. Dans les deux cas, un facteur 4 apparaît.

Q6c. Si $3 = zw$ avec z et w non inversibles, alors $9 = \mathrm{N}(z)\,\mathrm{N}(w)$ avec $\mathrm{N}(z) \neq 1$ et $\mathrm{N}(w) \neq 1$: la seule possibilité est $\mathrm{N}(z) = \mathrm{N}(w) = 3$. Reste à voir si 3 est une norme, c'est-à-dire si $3 = a^2 + b^2$ a une solution entière.

Q7c. Tout réel est à distance au plus $\dfrac{1}{2}$ d'un entier. Appliquez-le à la partie réelle de x, puis à sa partie imaginaire, et sommez les deux carrés : chacun ne dépasse pas $\dfrac{1}{4}$.

Q7d. Appliquez le c) au complexe $\dfrac{z}{w}$: il fournit un q tel que $\mathrm{N}\left(\dfrac{z}{w} - q\right) \leqslant \dfrac{1}{2}$. Or $r = z - qw$ s'écrit $\left(\dfrac{z}{w} - q\right) w$, et N est multiplicative (R1) : il vient $\mathrm{N}(r) \leqslant \dfrac{\mathrm{N}(w)}{2}$. Concluez en remarquant que w est non nul, donc que $\mathrm{N}(w) \geqslant 1$, ce qui rend l'inégalité *stricte*.

Q8c. Le dernier reste non nul a pour norme 5. Si vous trouvez autre chose, refaites le choix du nœud le plus proche : à l'étape 2, deux nœuds sont à égale distance.

Q10b. Le reste s'écrit $r = x - \lambda d$, avec $\lambda \in \mathbb{Z}[i]$. Si x et d sont tous deux dans I, une combinaison de la forme $x - \lambda d$ y est encore : revenez à la définition de I.

Q10d. Trois étapes, et la première est un petit lemme à établir au passage. **Un.** Les diviseurs d'un irréductible π sont les inversibles et les associés de π : si $\pi = \delta\varepsilon$, l'irréductibilité donne δ inversible, ou bien ε inversible et alors δ est associé à π. **Deux.** Supposons que π ne divise pas z : par le lemme, tout diviseur commun de π et de z est inversible, donc l'élément d construit en a) et b) pour le couple $(\pi\,;z)$ est inversible. **Trois.** Comme $d \in I$, il s'écrit $d = \pi u_0 + z v_0$; multipliez par d^{-1}, qui appartient à $\mathbb{Z}[i]$, pour obtenir $\pi u + z v = 1$, puis multipliez cette dernière égalité par w.

Q12b. Si $m + i = p(u + iv)$, alors en identifiant les parties imaginaires on obtient $1 = pv$ avec $v \in \mathbb{Z}$, ce qui force p à diviser 1.

Q13b. Commencez par observer que z' divise p dans $\mathbb{Z}[i]$, puisque $p = z'\overline{z'}$.

Q13c. Écrivez ce que donne la question b) : $z' = \varepsilon z$ ou $z' = \varepsilon\overline{z}$, avec ε inversible, donc $\varepsilon \in \{1\,;-1\,;i\,;-i\}$. Il y a huit cas ; multiplier par i ne fait qu'échanger les deux coordonnées en changeant un signe. Six cas s'éliminent d'un coup en remarquant que a et b sont tous deux non nuls, puisque p est premier.

Q15b. Le nombre 6 s'écrit 2×3, mais aussi $\left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right)$. Il reste à se convaincre qu'aucun des quatre facteurs ne se casse davantage, en raisonnant sur la quantité $a^2 + 5b^2$.

Annexe B · Le laboratoire des deux carrés

Le programme suivant cherche, pour un entier n donné, un couple $(a\,;b)$ d'entiers naturels tel que $n = a^2 + b^2$, et renvoie `None` lorsqu'il n'en existe aucun.

```python
from math import isqrt

def deux_carres(n):
    a = 0
    while a * a <= n:
        reste = n - a * a
        b = isqrt(reste)
        if b * b == reste:
            return (a, b)
        a = a + 1
    return None

for n in range(1, 51):
    print(n, deux_carres(n))

# A completer : n'afficher que les PREMIERS, et verifier Q1c.
```

Valeurs de contrôle : `deux_carres(45)` rend $(3\,;6)$, `deux_carres(98)` rend $(7\,;7)$, `deux_carres(15)` rend `None`, et `deux_carres(2017)` rend $(9\,;44)$.

Deux prolongements, si le cœur vous en dit : compter, pour chaque n, le *nombre* d'écritures et non la première trouvée ; puis chronométrer le programme sur un nombre premier à dix chiffres, afin de mesurer ce que coûte la loterie de la question Q5c.