Imagination et mathématiques: deux exemples

Alain VALETTE*

Texte de l'exposé prononcé le 18 décembre 2007 à l'occasion du Colloque *"ImaginatioN"* organisé par l'Institut de Psychologie et Education de l'UniNE

1 Préambule

Il y a cet aspect dual des mathématiques : d'une part un langage, extrêmement précis et codifié, qui permet son application aux autres sciences ; d'autre part une science comme les autres, qui a néanmoins pour spécificité de questionner des objets un peu particuliers, puisqu'il s'agit d'objets du monde des idées [1]. Dans cet exposé, nous ne considèrerons que le second aspect, en prenant le point de vue d'un mathématicien actif engagé dans une activité de recherche.

2 L'imagination est partout en mathématiques !

2.1 Avant

Avant de débuter une recherche, l'imagination sert à se poser de bonnes questions, à la fois *intéressantes* et *accessibles*.

On réalise particulièrement cet aspect des choses quand on devient soi-même directeur de thèse et qu'on doit donner un sujet de thèse à un doctorant : il faut des questions intéressantes (pour qu'il ait une chance de trouver un poste plus tard), ni trop faciles (dans ce cas, le directeur connaît vraisemblablement la réponse), ni trop difficiles (l'étudiant ne dispose que de 4 ans pour produire une thèse).

2.2 Pendant

On peut distinguer deux grandes phases dans la recherche en mathématiques :

Phase d'invention ou de découverte : L'imagination est là pour deviner quelle forme aura la solution d'un problème, et quelles seront les principales étapes qui mèneront à la solution. (Méthodes : exploitation des analogies, extrapolation à partir d'un exemple bien choisi ou bien compris, ...)

*Institut de mathématique de l'université de Neuchâtel

[1] Nous n'entrerons pas ici dans un autre débat : celui de la nature des objets mathématiques.

Phase de vérification : Il s'agit ici de rédiger une *démonstration*, qui doit permettre à un collègue de vérifier ligne par ligne l'exactitude du raisonnement et/ou du calcul. Ici, il n'est plus question d'imagination, mais de *technique*. Cependant, durant ce processus, des obstacles imprévus peuvent survenir qu'il s'agit de gérer. L'imagination fait donc un retour dans la *gestion des imprévus*.

A noter que le produit fini (article, traité) ne comprendra sûrement ni le mot "imagination" ni le mot "intuition" !

"Rien n'est plus fécond, tous les mathématiciens le savent, que ces obscures analogies, ces troubles reflets d'une théorie à une autre, ces furtives caresses, ces brouilleries inexplicables ; rien aussi ne donne plus de plaisir au chercheur. Un jour vient où l'illusion se dissipe ; le pressentiment se change en certitude ; les théories jumelles révèlent leur source commune avant de disparaître ; comme l'enseigne la Gītā *on atteint à la connaissance et à l'indifférence en même temps. La métaphysique est devenue mathématique, prête à former la matière d'un traité dont la beauté froide ne saurait plus nous émouvoir."* (André Weil, [Wei] [2])

2.3 Après

L'enseignant ou l'orateur doit faire preuve d'imagination pour pouvoir, lors d'un cours ou d'un séminaire, transmettre son intuition et ses *images mentales* aux étudiants ou aux auditeurs.

Alors que le mot "image mentale" n'apparaît jamais dans un texte mathématique, il fait un retour en force au niveau d'un cours et surtout d'un exposé de séminaire : il s'agit véritablement de transmettre à ses interlocuteurs l'intuition que l'on peut avoir d'un objet ou d'une situation, et pour s'assurer que ça passe, il faut essayer de susciter les réactions de l'auditoire ! [3]

L'étudiant ou l'auditeur doit aussi faire appel à son imagination, pour entrer dans les images mentales de l'enseignant et questionner celles-ci.

Je dis toujours à mes étudiants : *"Vous ne devez jamais croire ce qu'un prof vous dit, en tout cas pas tout de suite ! Si un enseignant quelqu'il soit essaie de vous convaincre de la véracité d'un raisonnement, votre rôle de scientifiques est de faire preuve d'esprit critique et ne pas prendre ce qu'on vous dit pour argent comptant."* Ce questionnement demande une forme d'imagination bien particulière, consistant à se demander à tout moment comment le raisonnement développé pourrait être faux. Ce ne sont pas nécessairement les meilleurs étudiants, scolairement parlant, qui en sont capables ...

Après ces considérations générales, je vais illustrer mon propos sur deux exemples, l'un en géométrie, l'autre en algèbre ; ces exemples ont en commun qu'à mon avis il fallait une bonne dose d'imagination pour concevoir les démonstrations sous-jacentes.

[2] André Weil est une des figures marquantes des mathématiques du XXème siècle. Le texte cité s'est développé à partir d'une lettre d'André Weil à sa soeur, la philosophe Simone Weil, qui apparemment se demandait comment "fonctionne" un mathématicien.

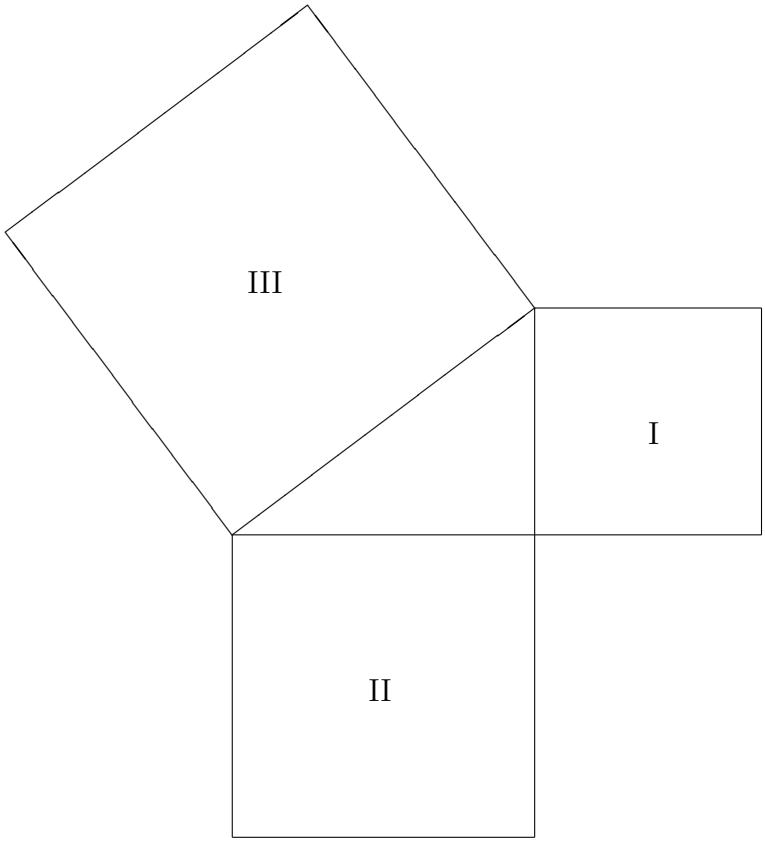
[3] Ceci est à mon avis lié au fait que les mathématiciens préfèrent le contact direct à tous les moyens de communications modernes, et le tableau noir (qui permet de réagir à chaud) aux présentations high-tech.

3 Un exemple en géométrie

Théorème 1 (Pythagore) *L'aire du carré construit sur l'hypoténuse d'un triangle rectangle, est la somme des aires des carrés construits sur les petits côtés.*

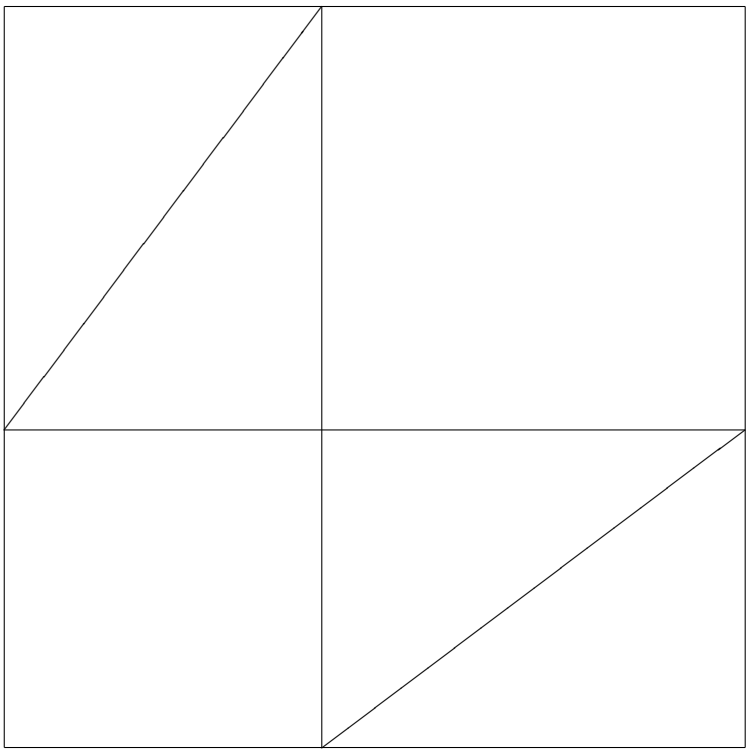
Dans la figure ci-dessous, si I, II, III désignent respectivement les aires du petit, du moyen, et du grand carré, on a :

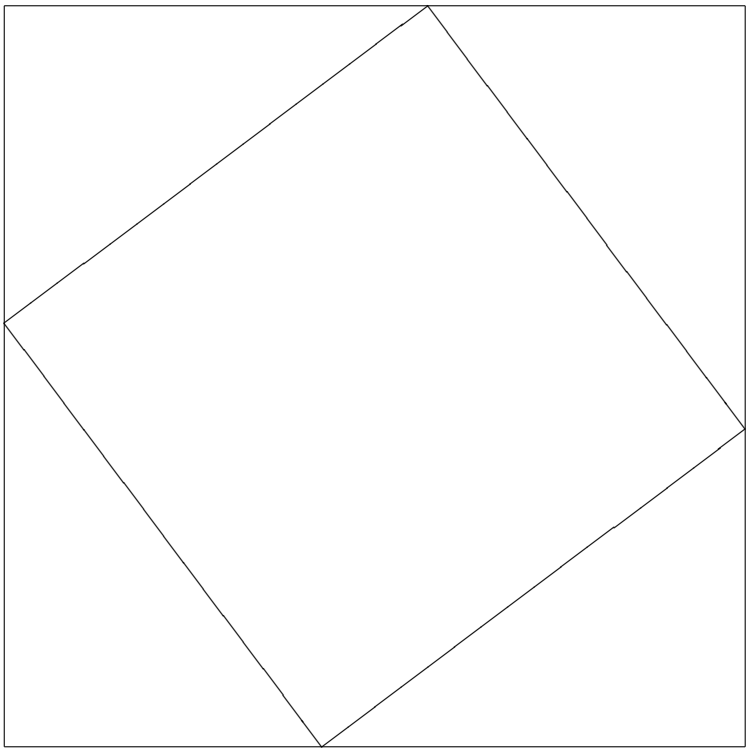
$$I + II = III$$



La page suivante contient une preuve par dissection inspirée d'une preuve chinoise du 3ème siècle avant J.-C.

Je dis que cette figure, sans une phrase, sans une formule, est effectivement une preuve du théorème de Pythagore ! C'est ce que nous appelons dans notre jargon *"proof without words"*. L'imagination critique du spectateur est ici sollicitée, et vous pourriez vous poser des questions comme *"Est-il évident que, dans la seconde figure, la figure centrale est bien un carré ? N'est-ce pas un effet d'optique lié à l'épaisseur du trait ?"*. Réponse : non, car la somme des 3 angles d'un triangle vaut 180 degrés. Autre question possible : *"Peut-on appeler preuve ce qui manifestement qu'un cas particulier, une vérification sur un seul triangle ?"* Réponse : c'est que ce cas particulier est le cas général ! Plus précisément, si je donnais un triangle dont un côté de l'angle droit mesurait $1cm$ et l'autre $1km$, le même raisonnement fonctionne !





4 Transition

"Il y a cette dualité fondamentale, en mathématiques, d'un côté entre la géométrie, qui correspond aux arts visuels, qui correspond à une intuition qui est immédiate : on voit une figure géométrique, boum !, c'est ça, c'est tout, on n'a même pas besoin d'expliquer, on n'a pas envie d'expliquer ! [4]

Et d'un autre côté il y a l'algèbre ; l'algèbre, elle, c'est autre chose, ça n'a rien de visuel, par contre ça a une temporalité, ça s'inscrit dans le temps, c'est le calcul, etc, c'est quelque chose qui évolue. C'est quelque chose de très proche du langage et qui donc a cette précision diabolique du langage." (Alain Connes, [Con] [5])

5 Un exemple en théorie des nombres

5.1 Sommes de carrés

Quels sont les nombres entiers qui sont sommes de 2 carrés parfaits ?

Ce problème a été posé - et résolu ! - par Pierre de Fermat (1601-1655), à mon sens le plus grand mathématicien du 17ème siècle. Le livre de chevet de Fermat était l'*Arithmétique* de Diophante (3ème siècle après J.C.). Dans ce livre, Diophante détermine complètement les triangles rectangles à côtés entiers - par le théorème de Pythagore, cela revient à trouver toutes les solutions entières de l'équation $a^2 + b^2 = c^2$. Fermat s'était demandé quels étaient les nombres entiers qui sont carrés de l'hypoténuse d'un triangle rectangle dont les 2 côtés de l'angle droit sont entiers. Malheureusement, Fermat travaillait en lançant des défis aux autres mathématiciens de l'époque, et n'abattait presque jamais ses propres cartes, de sorte que ses preuves ont presque toutes été perdues ; en particulier, c'est Leonhard Euler (1707-1783) qui a, plus d'un siècle après, donné la première preuve des assertions de Fermat sur les sommes de 2 carrés.

L'identité de Brahmagupta (7ème siècle)

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

montre qu'un produit de sommes de 2 carrés parfaits est encore une somme de 2 carrés parfaits. Le problème est ainsi ramené aux nombres premiers [6].

Je vous parlais d'image mentale. Laissez-moi essayer de vous présenter mon image mentale de la structure multiplicative des nombres naturels : je la vois comme une gigantesque boîte de *Lego*$^{\text{TM}}$, où les blocs de base sont les nombres premiers : il y a des blocs marqués 2, marqués 3, marqués 5, etc... Si je prends deux blocs marqués 3 et un bloc marqué 5, je fabrique l'entier $3^2 \times 5 = 45$. Décomposons les premiers en sommes de 2 carrés.

[4] Commentaire de l'auteur : la preuve que nous venons de voir du théorème de Pythagore me semble illustrer particulièrement bien ce propos !

[5] Alain Connes, Professeur au Collège de France depuis 1985, a aussi obtenu la Médaille Fields en 1982.

[6] Cette assertion demanderait une justification plus détaillée, que nous laissons en exercice.

2	$=$	1^2+1^2	13	$=$	3^2+2^2	31	$=$	$??$
3	$=$	$??$	17	$=$	4^2+1^2	37	$=$	6^2+1^2
5	$=$	2^2+1^2	19	$=$	$??$	41	$=$	5^2+4^2
7	$=$	$??$	23	$=$	$??$	43	$=$	$??$
11	$=$	$??$	29	$=$	5^2+2^2	47	$=$	$??$

Constatation expérimentale : il semble que, à l'exception de $p = 2$, seuls les nombres premiers de la forme $4m + 1$ soient sommes de 2 carrés ! Voici une autre expérience :

x	x^2+1	*Diviseurs premiers de* x^2+1
1	2	2
2	5	5
3	10	$2, 5$
4	17	17
5	26	$2, 13$
6	37	37
7	50	$2, 5$
8	65	$5, 13$
9	82	$2, 41$
10	101	101

Constatation expérimentale : il semble que, à l'exception de $p = 2$, seuls les nombres premiers de la forme $4m + 1$ apparaissent !

Théorème 2 (Fermat 1640 ; Euler 1742) *Soit p un nombre premier différent de 2. Les propriétés suivantes sont équivalentes :*

1) p est de la forme $4m + 1$;

2) Il existe un entier x avec $x^2 + 1$ divisible par p ;

3) p est somme de 2 carrés.

Cet énoncé apparaît dans une lettre de Fermat à Mersenne, du 25 décembre 1640 : *"...Sur le sujet des triangles rectangles, voici mes fondements : 1^o Tout nombre premier, qui surpasse de l'unité un multiple du quaternaire, est une seule fois la somme de deux quarrés et une seule fois l'hypoténuse d'un triangle rectangle..."* [Fer].

Pour illustrer ce que peut être l'imagination en algèbre/théorie des nombres, j'aimerais donner une preuve du Théorème de Fermat-Euler.

5.2 L'outil : congruences et arithmétique modulo n

Nous rencontrons des congruences modulo n, c'est-à-dire des calculs sur des restes de division par n, dans les assertions suivantes :

- "Il est 9 heures du matin, dans 10 heures il sera 7 heures de l'après-midi" *(calcul modulo 12).*
- "Il est 9 heures, dans 20 heures il sera 5 heures" *(calcul modulo 24).*
- "C'est aujourd'hui mardi, dans 10 jours ce sera vendredi" *(calcul modulo 7).*
- "Nous sommes le 18 décembre, dans 65 jours nous serons le 21 février" *(calcul modulo 31).*

On note $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$, qu'on munit de l'addition et de la multiplication modulo n ; voici dans deux cas les tables d'addition et de multiplication (où nous omettons $0 \times x = 0$ dans la table de multiplication) :

$n = 5$:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

.	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$n = 6$:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

.	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

On remarque que tout $x \in \mathbb{Z}_n$ possède un unique opposé, noté $-x$, qui est donné par l'élément $n - x \in \{0, 1, ..., n-1\}$.

Par contre, il n'y a pas nécessairement d'inverse pour la multiplication, comme on le voit avec $n = 6$; par contre, pour $n = 5$, tout élément non nul possède un inverse multiplicatif : comme le montre le lemme suivant, c'est lié au fait que 5 est un nombre premier [7].

Lemme 1 *Si p est premier, tout élément non nul de $\mathbb{Z}_p$ possède un inverse multiplicatif, noté x^{-1}.*

Preuve : [8] On doit montrer que, pour $x \in \mathbb{Z}_p$, $x \neq 0$, il existe $y \in \mathbb{Z}_p$ tel que $xy \equiv 1 \ (mod\ p)$. Pour cela on considère l'application $f : \mathbb{Z}_p \backslash \{0\} \to \mathbb{Z}_p \backslash \{0\} : y \mapsto xy$, et on veut montrer que 1 est dans l'image de f. Pour cela, il suffit de montrer que f est surjective. Et comme on travaille sur un ensemble fini, il suffit de montrer que f est injective : si $y \neq y' \in \mathbb{Z} \backslash \{0\}$: $f(y) \neq f(y')$. Mais $f(y) = f(y')$ implique $x(y - y') \equiv 0 \ (mod\ p)$, ce qui veut dire que p divise $x(y - y')$. *Comme p est premier*, p divise soit x soit $y - y'$, dans les deux cas une contradiction. [9]

Une structure où l'on peut pratiquer les 4 opérations : l'addition, la soustraction, la multiplication et la division (sauf par 0) s'appelle un *corps*. Nous venons de montrer que $\mathbb{Z}_p$ est un corps.

[7] Commentaire : Ayez une petite pensée pour ce lemme chaque fois que vous effectuez une transaction sécurisée sur Internet : c'est ce lemme qui est à la base du système RSA, qui garantit la sécurité de votre paiement !

[8] Cette preuve n'était pas dans l'exposé oral.

[9] Cette preuve est très symptomatique des mathématiques contemporaines, qui met l'accent sur la notion de *fonction* : l'équation $xy = 1$ possède une solution si et seulement si 1 est dans l'image de f, si et seulement si f est surjective, si et seulement si f est injective. Typique de l'imagination requise d'un algébriste !

5.3 Preuve de Fermat-Euler

(**3**) $\Rightarrow$ (**1**) : Le carré d'un nombre pair est $(2k)^2 = 4k^2 \equiv 0 \ (mod\ 4)$; le carré d'un nombre impair est $(2k+1)^2 = 4k^2 + 4k + 1 \equiv 1 \ (mod\ 4)$. Donc modulo 4, les sommes de 2 carrés sont $0, 1, 2$. Donc, si p est somme de 2 carrés, comme p est impair p est congru à 1 modulo 4.

(**1**) $\Leftrightarrow$ (**2**) : On observe que p divise $x^2 + 1$ si et seulement si $x^2 \equiv -1 \ (mod\ p)$, ce qui revient à dire que -1 est un carré modulo p.

Un bref commentaire avant la suite de la preuve. Selon le *livre de Josué* (VI.4-5, [Bib]), les Israélites ont fait tomber les remparts de la ville de Jericho en en faisant 7 fois le tour en jouant de la trompette. La preuve qui suit, un petit bijou très représentatif de l'imagination en mathématiques, procède du même principe : on donne l'impression de s'écarter complètement du problème, qui tout à coup tombe sans effort ! Cette preuve est tirée de [AZ] [10]. Evidemment, il n'est pas simple pour l'enseignant de motiver cette preuve...[11]

Pour $x \in \mathbb{Z}_p \backslash \{0\}$, on définit le paquet de x comme

$$P_x = \{x, -x, x^{-1}, -x^{-1}\}.$$

On vérifie facilement que deux paquets sont soit disjoints, soit égaux :

$$P_x \cap P_y \neq \emptyset \ \Rightarrow \ P_x = P_y,$$

et fournissent donc une partition de $\mathbb{Z}_p \backslash \{0\}$.

Par exemple, pour $p = 11$, la partition est $\{1, 10\}$, $\{2, 9, 6, 5\}$, $\{3, 8, 4, 7\}$; pour $p = 13$, c'est $\{1, 12\}$, $\{2, 11, 7, 6\}$, $\{3, 10, 9, 4\}$, $\{5, 8\}$.

Le paquet "général" contient 4 éléments, mais il peut y avoir des coïncidences. Par exemple, on a toujours

$$P_1 = P_{-1} = \{1, -1\}.$$

Etudions systématiquement les coïncidences :

- Le cas $x \equiv -x \ (mod\ p)$ est impossible car p est impair.
- Le cas $x \equiv x^{-1} \ (mod\ p)$ est équivalent à $x^2 \equiv 1 \ (mod\ p)$. Cette équation a deux solutions dans $\mathbb{Z}_p$, à savoir $x = \pm 1$, qui mènent au paquet P_1.
- Le cas $x \equiv -x^{-1} \ (mod\ p)$ est équivalent à $x^2 \equiv -1 \ (mod\ p)$. Ici résonne une petite clochette : on commence à soupçonner que cette décomposition en paquets pourrait avoir un lien avec le problème posé ! L'équation $x^2 \equiv -1 \ (mod\ p)$ a soit 0 solution, soit 2 solutions $\pm x_0$, qui mènent au paquet $P_{x_0} = \{x_0, -x_0\}$ (pour $p = 13$, c'est le paquet $\{5, 8\}$).

Morale : $\mathbb{Z}_p \backslash \{0\}$, ensemble à $p-1$ éléments est partitionné en paquets de 4 éléments, à l'exception de un ou deux paquets exceptionnels à 2 éléments, le paquet P_1 étant toujours présent, l'autre paquet à 2 éléments étant présent si et seulement si -1 est un carré dans $\mathbb{Z}_p$. Donc :

[10] Un extrait de l'introduction de ce livre fascinant et inclassable : *"Paul Erdös often talked about The Book, in which God maintains the perfect proofs of mathematical theorems."*

[11] Je m'en tire en général par un *"Vous ne pouvez pas m'empêcher de faire ça !"*

- si $p = 4m + 1$, le second paquet exceptionnel doit être présent, et -1 est un carré ;
- si $p = 4m + 3$, le second paquet exceptionnel ne peut exister, et -1 n'est pas un carré.

Génial !

(**2**) $\Rightarrow$ (**3**) (esquisse [12]) : D'après Gauss, on introduit l'anneau

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

des nombres complexes dont la partie réelle et la partie imaginaire sont entières. "Anneau" veut dire : on peut y pratiquer l'addition, la soustraction et la multiplication. Dans un anneau, on peut définir un nombre premier de deux façons :

- comme un élément qui n'admet pas de diviseurs non triviaux ;
- ou comme un élément qui, chaque fois qu'il divise un produit, divise au moins un des des facteurs.

Dans $\mathbb{Z}$, ces deux définitions sont équivalentes (exemple : 6 n'est pas premier, car 6 divise $12 = 3 \times 4$, mais 6 ne divise ni 3 ni 4). Plus généralement, dans un anneau "principal", les deux définitions sont équivalentes. On montre que $\mathbb{Z}[i]$ est principal (voir [Sam]).

Si p divise $x^2 + 1$, on peut factoriser dans $\mathbb{Z}[i]$:

$$x^2 + 1 = (x + i)(x - i)$$

et remarquer que, dans $\mathbb{Z}[i]$, p ne divise ni $x + i$ ni $x - i$. Donc p divise un produit sans diviser aucun des facteurs, donc p n'est pas premier dans $\mathbb{Z}[i]$. Comme $\mathbb{Z}[i]$ est principal, p y admet une factorisation non triviale $p = z_1 z_2$.

Pour poursuivre, on fait appel au *module* d'un nombre complexe : si $z = a + bi$:

$$|z| = \sqrt{a^2 + b^2}.$$

On utilisera :

- $|z_1 z_2| = |z_1||z_2|$ (avatar de l'identité de Brahmagupta) ;
- $|z|^2 \in \mathbb{N}$ pour $z \in \mathbb{Z}[i]$.

Avec $p = z_1 z_2$, on a alors $p^2 = |p|^2 = |z_1|^2 |z_2|^2$, factorisation dans $\mathbb{N}$. Mais comme p est premier, les seules factorisations de p^2 dans $\mathbb{N}$ sont $p^2 = p^2 \times 1 = p \times p = 1 \times p^2$; comme $p = z_1 z_2$ est une factorisation non triviale dans $\mathbb{Z}[i]$, on en tire

$$|z_1|^2 = |z_2|^2 = p\,;$$

si $z_1 = a + bi$, on a donc $p = a^2 + b^2$ et p est somme de 2 carrés. [13]

[12] Cette partie ne figurait pas dans l'exposé oral ; elle a été ajoutée par souci d'être complet. Notons que, mathématiquement, c'est la partie "dure" de la preuve : à partir d'une information "faible" (sur des congruences), on doit déduire une information "forte" (à savoir une égalité dans $\mathbb{Z}$).

[13] Cette démonstration illustre un principe : pour résoudre un problème, il est intéressant et utile de lui mettre de la *structure* : ici, d'une part le fait que $\mathbb{Z}[i]$ est un anneau principal, d'autre part les propriétés de l'application $z \mapsto |z|^2$ de $\mathbb{C}$ dans $\mathbb{R}^+$.

6 Conclusion

Les mathématiques contemporaines offrent un certain nombre de *structures* (groupes, anneaux, corps, ..., variétés, espaces métriques, ..., espaces de mesures, processus stochastiques, ..., espaces fonctionnels, opérateurs différentiels, ...).

L'imagination en mathématiques consiste, en vue de la résolution d'un problème, à combiner de façon adéquate diverses structures parmi la panoplie à disposition. Plus rarement, elle consiste à constater l'inadéquation des structures existantes pour la résolution du problème donné, et à forger, *sous l'effet de la nécessité* de nouvelles structures mieux adaptées.

Références

[AZ] Martin Aigner et Günther M. Ziegler. *Proofs from the Book*. Springer-Verlag Berlin Heidelberg, 1998, 199 pages, ISBN 3-540-63698-6.

[Bib] *La Bible, Ancien Testament*. Bibliothèque de la Pléiade, NRF, 1956.

[Con] *Alain Connes, Médaille d'or 2004 du CNRS*. DVD 15 minutes, CNRS images, 2004.

[Fer] Pierre de Fermat. *Oeuvres, Livre II*. Editées par P. Tannery et C. Henry, Gauthier-Villars, 1891.

[Sam] Pierre Samuel. *Théorie algébrique des nombres*. Coll. Méthodes, Hermann, Paris, 1971.

[Wei] André Weil. *De la métaphysique aux mathématiques*. Oeuvres scientifiques, Springer, 1979, vol. 2 (1951-1964), 408-412.

Adresse de l'auteur :

Institut de Mathématiques
11, rue Emile Argand
Case postale 158
CH-2009 Neuchâtel - SUISSE
`alain.valette (AT) unine.ch`