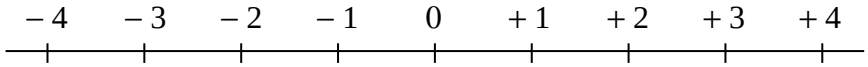
La géométrie des nombres

Christophe Soulé

L'idée première de la géométrie des nombres [1] consiste à considérer les nombres entiers comme contenus dans les nombres réels :

$$\mathbb{Z} \subset \mathbb{R}\,. \tag{1}$$

Une telle inclusion peut nous sembler banale, habitués que nous sommes à imaginer les entiers posés sur la droite des réels :



Mais, comme nous le verrons, cela n'est pas toujours allé de soi, d'autant qu'un tel point de vue est très étranger à l'approche algébrique de la théorie des nombres. Or il conduit pourtant à des résultats étonnants, où la géométrie du continu nous fournit des renseignements cruciaux sur des notions arithmétiques discrètes. Nous présenterons ce domaine des mathématiques à travers quelques antécédents historiques et des exemples pris dans les travaux contemporains.

L'approche géométrique de la théorie des nombres est clairement celle que nous propose les Eléments d'*Euclide* [2]. Ce serait un anachronisme que de vouloir chercher dans ce traité l'assertion que les entiers sont contenus dans les réels, puisque n'y apparaissent que les entiers positifs (zéro exclu), et qu'il faudra attendre le dix-neuvième siècle pour que les nombres réels soient définis de façon précise. Mais le livre V des Eléments, celui sur les proportions, joua un rôle décisif dans le genèse des nombres réels chez

Dedekind. Et les livres VII à IX exposent les propriétés fondamentales des entiers positifs (nombres premiers, factorisation). Il est intéressant de comparer les premières définitions du livre V et celles du livre VII :

Cinquième livre, Définitions :

1. Une grandeur est partie d'une grandeur, la plus petite de la plus grande, quand la plus petite mesure la plus grande.
2. Une grandeur plus grande est multiple d'une grandeur plus petite, quand la plus grande est mesurée par la plus petite.
3. Une raison est certaine manière d'être de deux grandeurs homogènes entr'elles, suivant la quantité.

Septième livre, Définitions :

1. L'unité est ce selon quoi chacune des choses existantes est dite une.
2. Un nombre est un assemblage formé d'unités.
3. Un nombre est une partie d'un nombre, le plus petit du plus grand, lorsque le plus petit mesure le plus grand.

On notera la similitude entre la définition 1 du livre V et la définition 3 du livre VII. Nous pourrions les traduire en disant qu'une grandeur (resp. un nombre) α "est partie" d'une grandeur (resp. d'un nombre β) si un multiple entier de α est égal à β. Les "raisons" (ou proportions) de la définition 3 du livre V seraient des nombres réels positifs et la situation du livre V est bien décrite par la suite exacte que nous a proposé P. Cartier :

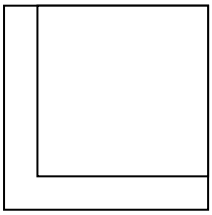
$$1 \to R \to G \to U \to 1\,,$$

où R est le groupe multiplicatif des nombres réels positifs (les "raisons"), U est le groupe abélien libre des unités physiques et G est le groupe des "grandeurs". Le monoïde multiplicatif des entiers positifs agit sur G (une grandeur peut en "mesurer" une autre). Mais les entiers ne sont pas vus pour autant comme des raisons (du moins pas à ce stade de la discussion). L'inclusion (1), même restreinte au nombres positifs, n'est pas une donnée première de la théorie des proportions d'Euclide.

On notera aussi que les résultats du livre V ne sont pas utilisés dans les preuves des livres VII à IX. Certes, les dessins qui viennent à l'appui des démonstrations dans ces chapitres sont curieusement similaires. Mais l'on n'y trouve pas celui des entiers posés sur la droite des réels, et d'ailleurs beaucoup d'historiens doutent que ces croquis aient figuré dans les versions initiales du traité.

En définitive, c'est surtout par sa conception d'ensemble que le livre des Eléments d'Euclide relie théorie des nombres et géométrie. Ce traité est dans l'ensemble un traité de géométrie et seuls trois livres y parlent des nombres entiers. L'arithmétique occupe, somme toute, une place de second rang.

Après de nombreux travaux à partir de l'œuvre de Diophante, les mathématiciens arabes se sont aussi intéressés à celle d'Euclide. Au dixième siècle, *al-Khujandî* annonce avoir démontré qu'un cube n'est jamais la somme de deux cubes. Il ne nous reste sur cette question que le dessin suivant, dû à Abu Ja'far :



Il s'agit là de la projection sur une de ses faces d'un cube contenant un autre cube. L'auteur déduit de cette figure la formule

$$x^3 - y^3 = x^2(x-y) + (x+y)\,(x-y)\,x$$

d'où il résulte, dit-il, que $x^3 - y^3$ ne peut pas être un cube ! [3] [4].

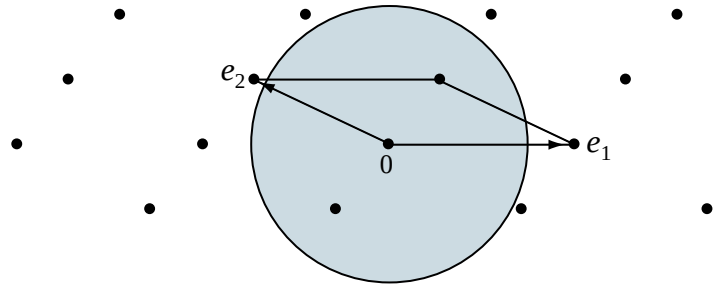
Cet aspect de la préhistoire du théorème de Fermat (on ignore si ce dernier a eu connaissance des travaux ci-dessus) renvoie au thème de notre discussion par le rôle qu'y joue le croquis, bien que celui-ci ne serve qu'à établir une formule algébrique générale. Mais il est aussi intéressant de constater comment les mathématiciens arabes ont su passer des énoncés "bien posés" de Diophante (possédant une solution, en général unique) à un énoncé affirmant l'inexistence d'une solution pour une équation très simple (un énoncé dépourvu d'ailleurs de la moindre conséquence). Notre peur-fascination pour le vide semble être au cœur de notre acharnement à vouloir montrer le théorème de Fermat.

Fermat avait quant à lui une opinion très tranchée (et violente) sur le rapport entre géométrie et arithmétique [5] :

> Il est à peine quelqu'un qui propose des questions purement arithmétiques, il est à peine quelqu'un qui sache les résoudre. Est-ce que l'Arithmétique a plutôt été traitée jusqu'à présent au moyen de la Géométrie que par elle-même ? C'est la tendance qui apparaît dans la plupart des Ouvrages tant anciens que modernes, et dans Diophante lui-même. Car s'il s'est écarté de la Géométrie un peu plus que les autres en astreignant son analyse à ne considérer que les nombres rationnels, il ne s'en est pas dégagé tout à fait, comme le prouvent surabondamment les *Zététiques* de Viète, dans lesquelles la méthode de Diophante est étendue à la quantité continue, et par suite à la Géométrie.
>
> Cependant l'Arithmétique a un domaine qui lui est propre, la théorie des nombres entiers; cette théorie n'a été que très légèrement ébauchée par Euclide et n'a pas été assez cultivée par ses successeurs (à moins qu'elle n'ait été renfermée dans ces livres de Diophante, dont l'injure du temps nous a privés); les arithméticiens ont donc à la développer ou à la renouveler.
>
> Pour éclairer leur marche, je leur propose de démontrer comme théorème ou de résoudre comme problème l'énoncé suivant; s'ils y parviennent, il reconnaîtront au moins que des questions de ce genre ne le cèdent ni pour la subtilité, ni pour la difficulté, ni pour le mode de démonstration, aux plus célèbres de la Géométrie :
>
> Etant donné un nombre non carré quelconque, il y a une infinité de carrés déterminés tels qu'en ajoutant l'unité au produit de l'un d'eux par le nombre donné, on ait un carré.

Ainsi, s'astreindre à ne considérer que des nombres rationnels ne suffit pas à faire de l'arithmétique, car on risque, ce faisant, de ne trouver que des énoncés également valables pour "la quantité continue" ($\mathbb{Q}$ est dense dans $\mathbb{R}$). L'inclusion (1) est dangereuse, elle nous éloigne de l'arithmétique, qui doit s'astreindre à ne traiter que des nombres entiers (positifs). La vraie théorie des nombres n'existe qu'en opposition à la géométrie, et Fermat se propose de faire échapper l'une à l'emprise de l'autre.

L'expression "géométrie des nombres" est due à *Minkowski* ; c'est le titre de son ouvrage "Geometrie der Zahlen" (1896). Il y étudie les réseaux euclidiens. On entend par là la donnée d'un sous-groupe discret Λ dans un espace vectoriel réel de dimension finie $\mathbb{R}^n$, tel que le quotient $\mathbb{R}^n/\Lambda$ soit compact.



On a nécessairement $\Lambda \simeq \mathbb{Z}^n$ et l'inclusion $\Lambda \subset \mathbb{R}^n$ est donc une généralisation à n dimensions de l'inclusion (1). L'énoncé central de la théorie est le suivant :

Théorème 1. [1] *Il existe une constante $C(n)$ telle que, si le volume de $\mathbb{R}^n/\Lambda$ est inférieur à $C(n)$, le réseau Λ contient un vecteur non nul v de longueur $\|v\|$ inférieure à un.*

Le théorème 1 a un nombre considérable de conséquences arithmétiques. Si F est un corps de nombres, i.e. une extension finie du corps $\mathbb{Q}$ des rationnels, et si $\mathcal{O}_F$ est l'anneau des entiers de F, le Théorème 1 permet de montrer que $\mathcal{O}_F$ n'a qu'un nombre fini de classes d'idéaux et que le groupe $\mathcal{O}_F^*$ de ses éléments inversibles est de type fini. Ce théorème sert aussi à la preuve du théorème d'Hermite selon lequel il n'y a qu'un nombre fini de corps de nombres de degré et de discriminant fixés.

Minkowski donne dans [1] une valeur possible pour la constante $C(n)$. Il remarque aussi que la propriété essentielle de la boule unité qui permet de prouver le Théorème 1 est qu'elle est convexe. Le livre [1] est un des premiers textes sur la géométrie des convexes.

Hilbert tenait en très haute estime cet ouvrage de Minkowski. Il le cite dans trois passages de la présentation de ses fameux problèmes. Il écrit ainsi [6] :

> Mais si je place avant tout la rigueur dans le raisonnement comme condition nécessaire à la solution complète d'un problème,

> je n'en élèverai pas moins la voix contre cette opinion que ce ne sont que les questions de l'Analyse ou même de l'Arithmétique qui soient seules susceptibles d'un traitement parfaitement rigoureux. Cette opinion émise de temps à autre par des autorités scientifiques, je la regarde comme absolument erronée.
>
> Une notion si étroite de la condition de rigueur conduirait rapidement à ignorer toutes les conceptions tirées de la Géométrie, de la Mécanique et de la Physique.

et

> La coïncidence entre la pensée géométrique et la pensée arithmétique se révèle encore en ceci : dans les recherches arithmétiques, de même que dans les considérations géométriques, nous ne remontons pas à chaque instant la chaîne des déductions jusqu'aux axiomes ; au contraire, lorsque pour la première fois nous attaquons un problème en Arithmétique, exactement comme en Géométrie, nous employons d'abord une combinaison de raisonnements, rapide, inconsciente, non encore définitive, avec une confiance absolue en un certain sentiment arithmétique et en l'efficacité des symboles arithmétiques; sans cette confiance nous ne pourrions pas plus progresser en Arithmétique que nous ne le pourrions en Géométrie sans la faculté de voir dans l'espace. Comme modèle d'une théorie arithmétique, opérant d'une manière rigoureuse avec les concepts et les symboles de la Géométrie, je citerai l'ouvrage de M. Minkowski : *Geometrie der Zahlen*.

Selon Hilbert, la géométrie peut donc accéder au même niveau de rigueur que l'arithmétique, si elle prend soin d'expliciter ses axiomes. On notera le chemin parcouru depuis Fermat, la théorie des nombres étant maintenant citée en exemple à la géométrie. Plus loin dans [6] (Problème IV, p. 20), Hilbert évoque son article [7] où il cherche à développer axiomatiquement une version non euclidienne de la géométrie de Minkowski.

Au vingtième siècle, la géométrie des nombres a connu des succès considérables. Le Théorème 1 est utilisé dans la plupart des preuves de transcendance et la théorie de l'approximation diophantienne (construction des polynômes auxiliaires). La géométrie des nombres conduit aussi au théorème

de *Mordell-Weil* : si A est une variété abélienne sur un corps de nombres F, le groupe de ses point $\Gamma = A(F)$ est de type fini. La preuve de ce résultat (cf. [8]) consiste d'abord à montrer que, pour tout entier $n > 0$, le quotient $\Gamma/n\Gamma$ est fini. On utilise pour cela le théorème d'Hermite cité plus haut. Ensuite, on montre qu'il existe un produit scalaire sur $\Gamma \otimes \mathbb{R}$ ayant de bonnes propriétés (la hauteur de Néron-Tate). Autrement dit, on cherche à montrer que Γ vérifie les propriétés d'un réseau euclidien.

Les années 80 ont été marquées par la preuve due à Faltings, puis Vojta et Bombieri, de la *conjecture de Mordell* : si X est une courbe lisse projective, de genre au moins deux, sur un corps de nombres F, l'ensemble de ses points $X(F)$ est fini. Les preuves de ces trois auteurs utilisent la géométrie des nombres. C'est particulièrement vrai pour celle de Bombieri, qui repose pour l'essentiel sur l'approximation diophantienne et le théorème de Mordell-Weil.

Quelques années plus tôt, *Arakelov* avait proposé une nouvelle approche géométrique des questions diophantiennes [9]. On peut dire – en paraphrasant une formule connue – que, pour Arakelov, "la géométrie des nombres est une géométrie algébrique", et cela en deux sens complémentaires.

D'abord, la géométrie d'Arakelov fournit une synthèse harmonieuse de la théorie des réseaux euclidiens et de celle des schémas de Grothendieck. Si X est un schéma projectif sur $\mathbb{Z}$ et E un fibré algébrique sur X, le groupe des sections globales $\Lambda = \Gamma(X, E)$ de E sur X est un réseau, isomorphe à $\mathbb{Z}^n$ pour un certain entier n. Choisissons une norme sur la fibre E_x de E en chaque point x de la variété complexe $X(\mathbb{C})$. L'espace vectoriel $\Lambda \otimes \mathbb{R}$ est alors muni de la norme sup :

$$\|s\|_{\sup} = \sup_{x \in X(\mathbb{C})} \|s(x)\|$$

si $s \in \Lambda \otimes \mathbb{R}$. La boule unité de $\| \cdot \|_{\sup}$ est convexe et l'on peut appliquer le théorème de Minkowski au couple $(\Lambda, \| \cdot \|_{\sup})$. La géométrie d'Arakelov permet, sous certaines hypothèses, de calculer le covolume de Λ dans $\Lambda \otimes \mathbb{R}$, et donc de produire des sections $s \in \Lambda$ non nulles et de taille bornée [11].

Par ailleurs, on constate que les énoncés de la géométrie des nombres peuvent se formuler dans des termes très voisins de ceux de la géométrie algébrique. En voici un exemple. Si X est une courbe projective et lisse sur un corps k et E un fibré algébrique sur X, le théorème de Riemann-Roch est

l'égalité

$$h^0(E) - h^1(E) - \deg(E) = (g-1)\,\mathrm{rg}(E)\,, \tag{2}$$

où $h^0(E) = \dim_k \Gamma(X,E)$, $h^1(E) = \dim_k \Gamma(X,E^\vee)$ ($E^\vee$ est le dual de Serre de E), $\deg(E)$ est le degré de E, $\mathrm{rg}(E)$ est son rang, et g désigne le genre de X.

Considérons maintenant un réseau euclidien $\Lambda \subset \mathbb{R}^n$. Notons B la boule unité et

$$\Lambda^\vee = \{v \in \mathbb{R}^n / \forall\, w \in \Lambda\,,\ (v,w) \in \mathbb{Z}\}$$

le dual de Λ. Si $\#\,(\Lambda \cap B)$ est le cardinal de l'ensemble des éléments de Λ contenus dans B, on pose

$$h^0(\Lambda) = \log \#(\Lambda \cap B)$$

et

$$h^1(\Lambda) = \log \#(\Lambda^\vee \cap B)\,.$$

Théorème 2. [10]

$$|h^0(\Lambda) - h^1(\Lambda) + \log(\mathrm{volume}\,(\mathbb{R}^n/\Lambda))| \leq n\log(6) - \log(\mathrm{volume}\,(B))\,. \tag{3}$$

Ce théorème ressemble à la formule (2) et implique le Théorème 1. En effet, si le volume de $\mathbb{R}^n/\Lambda$ est assez petit, puisque $h^0(\Lambda^\vee) \geq 0$, il résulte de (3) que $h^0(\Lambda)$ est non nul, c'est-à-dire que $\Lambda \cap B$ contient un autre point que l'origine.

Il serait intéressant de reformuler la théorie des réseaux euclidiens dans le cadre de la géométrie non commutative de Connes. On aimerait que les nombres réels $h^0(\Lambda)$ et $h^1(\Lambda)$ (resp. $\log(\mathrm{volume}\,(\mathbb{R}^n/\Lambda))$) soient les dimensions (resp. la dimension virtuelle) de certains modules projectifs sur une algèbre de von Neumann bien choisie.

On notera aussi que (3) est une inégalité alors que (2) est une formule exacte. La géométrie des nombres est de nature qualitative. Ainsi le théorème de Mordell-Weil ne dit rien sur le rang de $A(F)$ et l'on ne connaît pas le cardinal de $X(F)$ dans la conjecture de Mordell (bien qu'on sache le majorer). A l'inverse, la théorie algébrique des nombres permet, dans certains cas, de calculer exactement le rang du groupe de Mordell-Weil, le cardinal d'un groupe de classes d'idéaux ou celui d'un groupe de cohomologie.

Comme me l'a fait remarquer L. Clozel, on retrouve cette dichotomie en théorie de Langlands avec, du côté de la géométrie des nombres, les formes automorphes (invariantes par un groupe arithmétique, par exemple le groupe des automorphismes d'un réseau), et, du côté algébrique, la théorie des représentations galoisiennes. Mais peut-on voir l'étude des formes automorphes comme une sorte de géométrie, au sens (très) élargi que A. Connes donne à ce terme ? C'est un problème ouvert (cf. [12]). Le lecteur trouvera aussi dans [13] une alternative au Théorème 2, qui fait intervenir les séries thêta.

Enfin, on peut rapprocher l'idée d'une distinction entre une arithmétique algébrique exacte et une arithmétique qualitative géométrique des études faites ces dernières années sur le rôle de différentes zones cérébrales dans le traitement élémentaire des nombres entiers. Dans l'article [14] S. Dehaene et ses collaborateurs distinguent une région pariétale et bilatérale où s'effectuerait la comparaison des nombres entiers et leur addition approximative, et une région frontale gauche où se feraient les calculs exacts. La première région est connue pour traiter les images, quand la seconde concerne le langage (ce modèle est affiné dans [15], qui distingue trois régions cérébrales aux lieu de deux). Les méthodes expérimentales utilisées dans ces études sont de trois ordres : l'observation des performances en cas de lésion cérébrale, l'enregistrement de l'activité du cerveau, et la psychologie expérimentale. Par exemple, les auteurs de [14] ont calculé la vitesse nécessaire à l'addition exacte ou approximative de nombres à deux chiffres chez des étudiants russes émigrés aux U.S.A., quand la question était posée dans leur langue maternelle ou en anglais. Ils constatent que le choix de la langue affecte l'addition exacte mais pas l'addition approximative. Ceci conforte l'idée que l'addition exacte fait intervenir les zones du langage (du cerveau frontal gauche) et la "représentation verbale des nombres", mais qu'il n'en est pas de même pour l'addition approximative.

On parle couramment aujourd'hui de "géométrie arithmétique". Mais ce syncrétisme terminologique ne doit pas nous cacher la difficulté, sans cesse renouvelée, du rapprochement des différentes branches des mathématiques. L'arithmétique compte mais elle ne sait voir. La géométrie voit mais elle ne sait parler. L'algèbre parle mais elle ne sait compter.

References

[1] M. Minkowski, *Geometrie der Zahlen*, Leipzig, Teubner, (1896).

[2] Euclide, Les Eléments, dans *Les œuvres d'Euclide*, traduites par F. Peyrard, A. Blanchard, (1993).

[3] C. Houzel, *Théorème de Fermat, A travers l'histoire de l'analyse diophantienne*, SMF, (1995).

[4] R. Rashed, *Entre arithmétique et algèbre*, Paris, (1984).

[5] P. Fermat, Second défi aux mathématiciens, 1657, dans *Œuvres de Pierre Fermat*, I. La théorie des nombres, R. Rashed, C. Houzel, G. Christol (1999), A. Blanchard, pp. 258-259.

[6] D. Hilbert, *Sur les problèmes futurs des mathématiques*, Ed. J. Gabay.

[7] D. Hilbert, Über die gerade Linie als Kürzeste Verbindung zweier Punkte, *Math. Annalen* **46** (1895), pp. 91-96.

[8] J.-P. Serre, *Lectures on the Mordell-Weil theorem*, M. Brown Ed., Notes de Michel Waldschmidt. 3ème ed. Aspects of Mathematics. Wiesbaden: Vieweg (1997).

[9] S.Ju. Arakelov, An intersection theory for divisors on an arithmetic surface, *Izv. Akad. Nauk SSSR* **38** (1974), pp. 1179-1192.

[10] H. Gillet, C. Soulé, On the number of lattice points in convex symmetric bodies and their duals, *Israel Journal of Math.* **74**, 2/3 (1991), pp.347-357.

[11] C. Soulé, D.Abramovich, J.-F.Burnol et J.Kramer: *Lectures on Arakelov geometry*, Cambridge Studies in Advanced Mathematics **33**, Cambridge University Press (1992).

[12] A. Connes, Trace formula in noncommutative geometry and the zeroes of the Riemann zeta function, *Selecta Math.* **5** (1999), pp. 29-106.

[13] G. van der Geer, R. Schoof, Effectivity of Arakelov divisors and the theta divisor of a number field, *Selecta Math.* **6** (2000), pp. 377-398.

[14] S. Dehaene, E. Spelke, P. Pinel, R. Stanescu, S. Tsivkin, Sources of mathematical thinking: behavioural and brain-imaging evidence, *Science* **284** (1999), pp. 970-974.

[15] F. Chorbon, L. Cohen, P.F. van de Moortele, S. Dehaene, Differential contributions of the left and right parietal lobules to number processing, *J. of Cognitive Neuroscience* **11** (1999), pp. 617-630.