Les nombres p-adiques
Daniel Barsky et Gilles Christol

Au début de notre siècle, le mathématicien allemand Kurt Hensel[1] inventait les nombres p-adiques. Que désigne ce vocable un peu curieux ? Des nombres abstraits et difficiles à représenter, mais aussi des entités qui permettent aux spécialistes de la théorie des nombres de construire de puissants outils d'étude. Des objets mathématiques sans lesquels le célèbre théorème de Fermat, pour ne citer que lui, n'aurait pu être démontré. Et qui alimentent les spéculations de certains physiciens sur la nature de l'espace et du temps.

Quelle est la longueur de la diagonale d'un carré dont le côté mesure 1 mètre ? En chœur, les élèves d'une classe de lycée répondront sans hésiter : $\sqrt{2}$ mètre ! Et ils donneront cette réponse probablement sans se douter que $\sqrt{2}$, et les nombres qui lui ressemblent, étaient une source d'ennuis sérieux pour les mathématiciens, depuis l'Antiquité jusqu'à une époque assez récente. Car si les nombres entiers et les fractions qu'ils permettent de former se sont facilement fait accepter, il n'en a pas été de même des nombres dits irrationnels comme $\sqrt{2}$ ou π, qui ont un développement décimal illimité et non périodique (tel $\pi = 3,14159...$). C'est seulement au siècle dernier que les irrationnels ont été définis de manière entièrement satisfaisante, avec la construction rigoureuse de l'ensemble $\mathbb{R}$ des nombres réels à partir du corps $\mathbb{Q}$ des nombres rationnels (qui comprend les entiers et les rapports d'entiers). L'ensemble $\mathbb{Q}$ des nombres rationnels était, pour plusieurs raisons, incomplet. Nous avons fait allusion à l'une d'entre elles : il n'y a pas assez de nombres rationnels pour représenter tous les points d'une droite, comme le montre l'exemple de la diagonale d'un carré. Adjoindre les nombres irrationnels aux nombres rationnels pour former le corps $\mathbb{R}$ des nombres réels (voir l'encadré "Corps, distance, valeur absolue") était indispensable pour donner un fondement solide à toute l'analyse mathématique classique (limites, fonctions, intégration, équations différentielles, etc.) et pour la faire progresser.

Au tournant du siècle, cependant, en 1902, le mathématicien allemand Kurt Hensel inventa des objets, les "nombres p-adiques", qui constituent une manière différente de compléter l'ensemble des nombres rationnels. Le corps des nombres p-adiques ne ressemble pas à celui des nombres réels, et est beaucoup moins intuitif. En particulier, les nombres p-adiques ne se prêtent pas à une interprétation géométrique aussi simple que les nombres réels ou même les nombres complexes (fig. 1). Entités relativement abstraites, ils ont mis du temps à prouver leur utilité ; mais aujourd'hui, les nombres p-adiques possèdent un statut central dans beaucoup de branches des mathématiques comme la théorie algébrique des nombres (étude des racines des polynômes à coefficients entiers) ou la géométrie algébrique (étude des solutions d'équations polynomiales à plusieurs variables).

Référence : Magazine La Recherche, juillet-août 1995, vol. 26, Numéro spécial Nombres.

Daniel Barsky est directeur de recherche au CNRS et travaille à l'université Paris-Nord (Villetaneuse). Il s'intéresse aux fonctions L p-adiques.

Gilles Christol est professeur à l'université Paris 6, et travaille sur les équations différentielles dans les corps p-adiques.

Transcription : Denise Vella-Chemla, 21.4.2022.

[1] Le mathématicien allemand Kurt Hensel (1861-1941) inventa les nombres p-adiques, au début du XX^e siècle. Il était un élève du célèbre théoricien des nombres Leopold Kronecker. Hensel enseigna à Berlin, puis à l'université de Marburg.

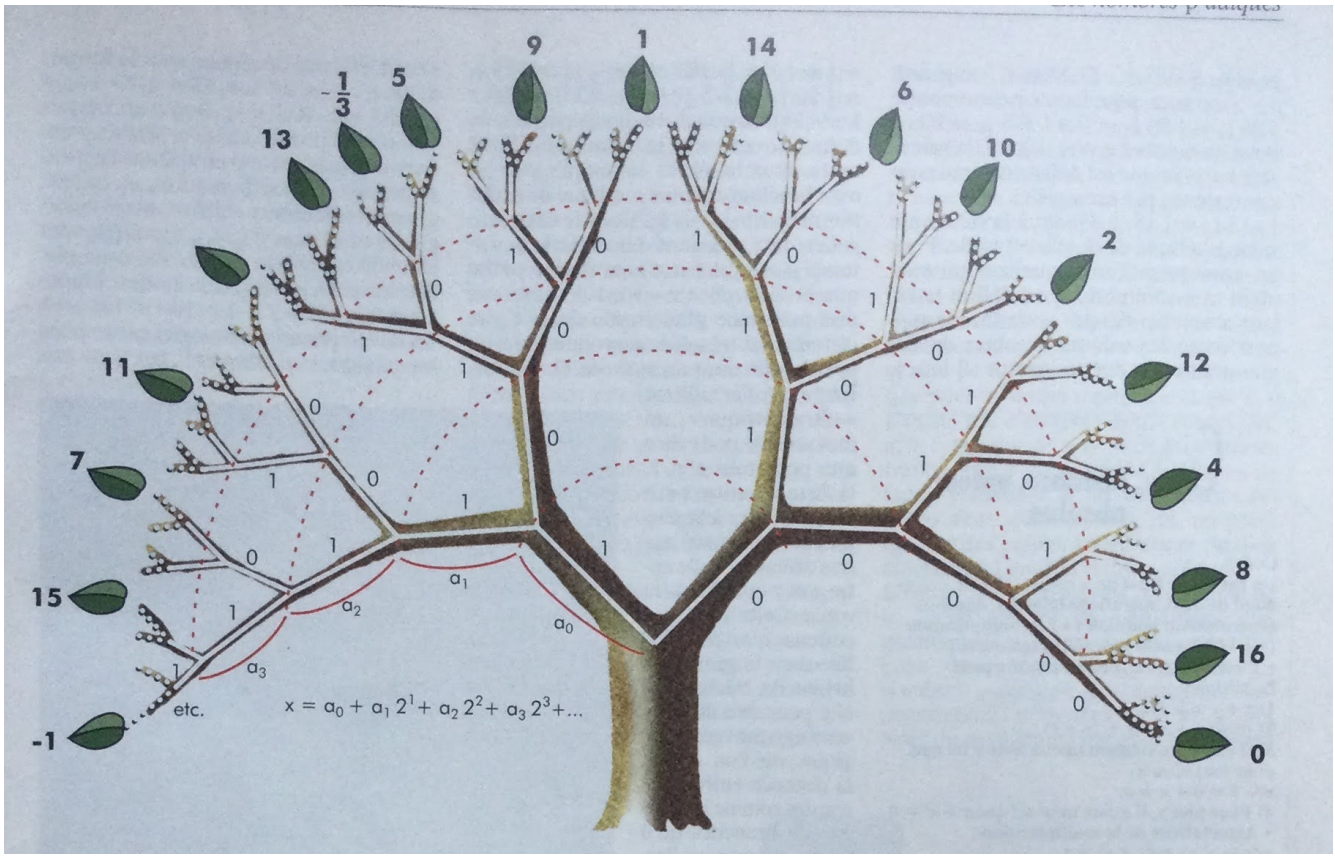

FIGURE 1. Cet arbre infini où chaque branche se divise en deux permet de donner une représentation imagée des nombres 2-adiques. Plus précisément, il représente ici les "entiers 2-adiques", qui s'écrivent sous la forme $a_0 + a_1 2^1 + a_2 2^2 + a_3 2^3 + ...$, où les coefficients a_0, a_1, a_2, etc. valent 0 ou 1. A chaque ramification, on associe un coefficient, valant 0 pour la branche de droite et 1 pour la branche de gauche. De cette façon, chaque "feuille" de l'arbre (obtenue après une infinité de ramifications) peut être identifiée à un "entier 2-adique". Les entiers usuels faisant partie des entiers 2-adiques, quelques-uns d'entre eux ont été indiqués (par exemple -1, qui s'écrit $1 + 2^1 + 2^2 + 2^3 + ...$: tous ses coefficients sont égaux à 1).

Que sont donc les nombres p-adiques ? Plusieurs manières de les définir existent. La démarche originale, celle de Hensel, portait sur les nombres algébriques, nombres qui sont solutions d'une équation polynomiale à coefficients entiers. Hensel introduit les nombres p-adiques en cherchant à représenter les nombres algébriques sous la forme de séries de puissances d'un nombre premier p. Mais la voie historique n'est pas la plus facile à présenter, même si elle permet de mieux comprendre le contexte dans lequel les nombres p-adiques ont été inventés. Nous en avons choisi une autre, davantage calquée sur la construction du corps $\mathbb{R}$ des nombres réels. Quelques préambules sont nécessaires. En particulier, nous avons besoin de préciser les notions de "valeur absolue" et de "distance".

Bien qu'ils soient peu intuitifs, les nombres p-adiques possèdent aujourd'hui un statut central dans plusieurs branches des mathématiques.

Pour un nombre rationnel x, la "valeur absolue" usuelle de x est notée $|x|$ et vaut simplement x si ce nombre est positif, et $-x$ sinon ; en d'autres termes, la valeur absolue de x est toujours positive, $|3| = 3, |-12| = 12, |-4/5| = 4/5$, etc. La valeur absolue de x peut être interprétée comme

la distance de x à 0. Plus généralement, la distance entre deux nombres rationnels x et y est le nombre $|x-y|$. Par exemple, la distance entre -4 et $+8$ vaut 12. Remarque très importante pour la suite : valeur absolue et distance sont dotées de propriétés que l'on peut formuler en termes plus abstraits (voir l'encadré "Corps, distance, valeur absolue"). Aussi, sur un ensemble donné, il est souvent possible de définir une et même plusieurs "distances", qui ne ressemblent pas forcément à la distance géométrique et intuitive à laquelle nous sommes habitués. Nous le verrons avec la distance dite p-adique, mais auparavant il nous faut expliquer en quoi la notion de distance intervient pour "compléter" le corps des nombres rationnels.

La valeur absolue et la distance que nous avons explicitées plus haut sont indispensables pour faire de l'analyse. Par exemple, elles permettent de donner un sens précis à l'affirmation "le nombre $5,12$ est voisin (ou proche) du nombre $5,11$", ou encore à l'énoncé "la suite $u_n = 1/n$ tend vers 0 lorsque n tend vers l'infini". Prenons maintenant l'exemple de la suite $(1+1/1)^1, (1+1/2)^2, (1+1/3)^3, (1+1/4)^4$, etc. Ces nombres rationnels valent respectivement $2, 2,25, 2,37..., 2,44...$, etc., et se rapprochent (au sens de la distance définie plus haut !) peu à peu d'une certaine limite e. Or on peut démontrer que cette limite n'est pas un nombre rationnel ; autrement dit, e ne peut pas s'écrire sous la forme a/b où a et b sont des entiers.

Pour de multiples raisons (commodité, rigueur, cohérence, etc.), les mathématiciens souhaitaient compléter le corps $\mathbb{Q}$ des rationnels de façon à inclure les nombres qui, comme e, sont des limites d'une suite de nombres rationnels. La procédure est technique mais assez simple. Il nous suffira de savoir qu'elle consiste à raisonner sur les suites de nombres rationnels qui se rapprochent les uns des autres (c'est ici en particulier qu'intervient la distance), et qu'elle identifie - d'une certaine façon - les nombres réels à toutes les suites possibles jouissant de cette propriété. Outre les nombres rationnels, l'ensemble $\mathbb{R}$ ainsi construit contient les nombres dits irrationnels, C'est-à-dire ceux dont le développement décimal comporte une infinité de chiffres après la virgule, sans qu'ils se répètent de façon périodique (par exemple $\pi = 3,14159265358....$ ou $e = 2,718281828459....$).

La construction ci-dessus de $\mathbb{R}$ fait appel de façon essentielle à la distance que nous avions définie sur les nombres rationnels, puisqu'on considère les suites de nombres rationnels devenant de plus en plus "proches". Mais nous avons aussi dit qu'il pouvait exister plusieurs "distances" différentes. Au début du siècle, on s'est aperçu qu'on peut munir le corps $\mathbb{Q}$ des rationnels de distances appelées p-adiques. Un théorème dû au mathématicien Alexander Ostrowski, en 1935, montre même que la distance habituelle et les distances p-adiques sont les seules distances intéressantes dont puisse être muni l'ensemble des rationnels. Si, pour compléter $\mathbb{Q}$, on emploie la distance p-adique au lieu de la distance usuelle, on obtient non pas le corps $\mathbb{R}$ des réels, mais le "corps des nombres p-adiques", noté $\mathbb{Q}_p$.

Il est temps à présent d'expliquer la notion de distance p-adique. Commençons par la "valeur absolue p-adique" d'un nombre entier positif n. Ici, p désigne un certain nombre premier comme 3, 7, 19, etc., c'est-à-dire un entier positif qui n'est divisible que par 1 et par lui-même. La valeur de p étant choisie, on peut essayer de diviser n par p et ses puissances successives p^2, p^3, p^4, etc. Si la plus grande puissance par laquelle n est divisible est p^r, alors la valeur absolue p-adique de n est, par définition, $1/p^r$. On note : $|n|_p = 1/p^r$. En d'autres termes, la valeur absolue p-adique d'un entier positif n est d'autant plus petite que n est davantage divisible par p. Par exemple,

pour $p = 5$, la valeur absolue 5-adique de 26 est $|26|_5 = 1$ car $26 = 5^0 \times 2 \times 13$, celle de 50 vaut $|50|_5 = 1/25$ puisque $50 = 2 \times 5^2$, et celle de 375 vaut $|375|_5 = 1/125$ puisque $375 = 3 \times 5^3$. Mais si l'on choisit $p = 3$, on aura, pour les mêmes nombres : $|26|_3 = |50|_3 = 1$ et $|375|_3 = 1/3$.

Pour un nombre entier négatif, la valeur absolue p-adique est définie comme pour son opposé par exemple : $|-15|_p = |15|_p$. Quant à la valeur absolue p-adique de 0, elle est nulle. Pour un nombre rationnel quelconque m/n, où m et n sont entiers, on définit la valeur absolue p-adique en faisant le rapport entre les valeurs absolues du numérateur et du dénominateur : $|m/n|_p = |m|_p/|n|_p$. Par exemple : $|26/375|_5 = |26|_5/|375|_5 = 1/(1/125) = 125$.

La valeur absolue p-adique permet de définir directement la distance p-adique entre deux nombres rationnels x et y : c'est la valeur absolue p-adique de la différence, soit $|x - y|_p$. Dans le cas particulier où x et y sont des entiers, la distance p-adique est d'autant plus petite que la différence $x - y$ est divisible par une puissance plus élevée de p. Cette distance est très déconcertante par rapport à celle dont nous avons l'habitude. En particulier, elle est "ultramétrique", un mot savant pour dire que pour tous x, y, z, la distance entre x et z est inférieure à la plus grande des deux autres distances, celle entre x et y et celle entre y et z. Cette propriété curieuse n'est pas vérifiée dans la géométrie habituelle. Néanmoins, elle peut être illustrée avec un arbre généalogique, où l'on définit la distance entre deux cousins comme le nombre de branches qu'il faut parcourir sur l'arbre pour aller de l'un à l'autre en passant par un ancêtre commun (fig. 2). Il est facile de constater que la distance entre deux cousins de même génération est au plus égale à la plus grande des distances qui séparent ces deux cousins d'un troisième, appartenant à la même génération que les deux autres.

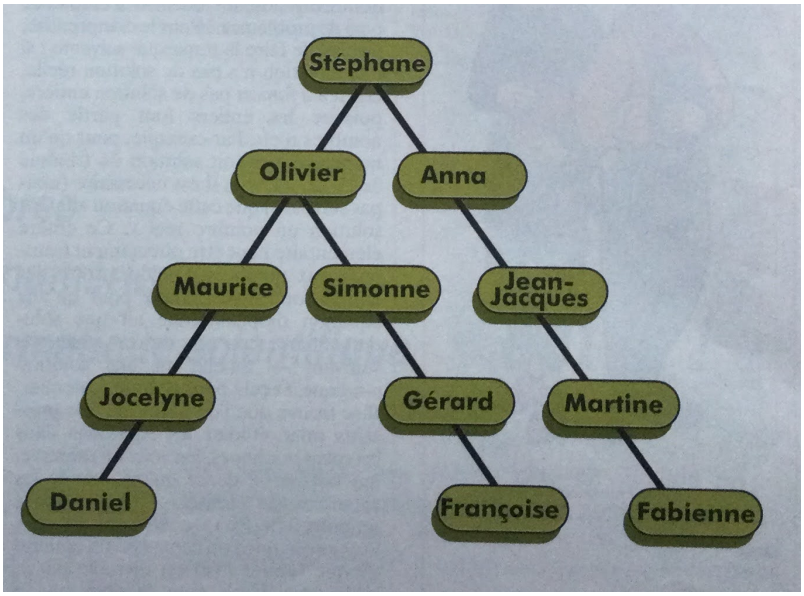

FIGURE 2. Figure 2. Une distance p-adique est ultramétrique, ce qui signifie que pour tous x, y, z, la distance $d(x, y)$ entre x et y est inférieure ou égale à la plus grande des distances $d(x, z)$ et $d(z, y)$. Cette propriété peut être illustrée sur un arbre généalogique, en comptant le nombre de branches qui séparent deux cousins de même génération et en considérant ce nombre comme la distance entre ces deux cousins. Ici, par exemple, la distance entre Daniel et Françoise vaut 6, et celle entre Françoise et Fabienne vaut 8. La distance entre Daniel et Fabienne doit donc être inférieure ou égale à la plus grande des deux autres, c'est-à-dire à 8 - ce qu'on vérifie immédiatement.

Corps, distance, valeur absolue

Corps

Un ensemble K est un "corps" s'il est muni de deux opérations internes, appelées généralement addition ($+$) et multiplication ($\times$), vérifiant les propriétés suivantes :
• K est un groupe commutatif pour l'addition :
1) $x + y = y + x$
2) $(x + y) + z = x + (y + z)$
3) Il existe un élément neutre noté 0 tel que, pour tout x, on a $x + 0 = 0 + x = x$.
4) Pour tout x, il existe un x' tel que $x + x' = 0$.
• Associativité de la multiplication : $x \times (y \times z) = (x \times y) \times z$
• Distributivité de la multiplication par rapport à l'addition :
$x \times (y + z) = x \times y + x \times z$ et $(x + y) \times z = x \times z + y \times z$
• Il existe un élément neutre $e \neq 0$ pour la multiplication : $x \times e = e \times x = x$.
• Tout $x \neq 0$ possède un inverse x'', c'est-à-dire tel que $x \times x'' = x'' \times x = e$.

Quand la multiplication est commutative ($x \times y = y \times x$), on dit que K est un corps commutatif. L'ensemble $\mathbb{Q}$ des nombres rationnels, l'ensemble $\mathbb{R}$ des nombres réels, l'ensemble $\mathbb{Q}_p$ des nombres p-adiques, l'ensemble $\mathbb{C}$ des nombres complexes sont des exemples de corps commutatifs.

Distance

Une distance sur un ensemble E est une application d qui, à tout couple (x, y) d'éléments de E, associe un nombre réel positif ou nul $d(x, y)$ et vérifiant :
• $d(x, y) = d(y, x)$
• $d(x, y) > 0$ si $x \neq y$ et $d(x, x) = 0$
• $d(x, z) \leq d(x, y) + d(y, z)$. La distance est dite ultramétrique si $d(x, z) \leq \max(d(x, y), diy, z))$. Les distances p-adiques sont des exemples de distances ultramétriques.

Valeur absolue

Une valeur absolue définie sur un corps K est une application qui, à tout élément x de K, fait correspondre un nombre réel positif ou nul noté $|x|$ et telle que :
• $x > 0$ si $x \neq 0$ et $|0| = 0$
• $|x + y| \leq |x| + |y|$
(pour une valeur absolue ultramétrique,
$|x + y| \leq \max(|x], [y]))$
• $|x \times y| = |x| \times |y|$

Dans ces conditions, l'expression $d(x, y) = |x - y|$ définit une distance sur le corps K.

Comme nous l'avons dit à plusieurs reprises, l'ensemble $\mathbb{Q}_p$ des nombres p-adiques est obtenu en complétant le corps des rationnels, en faisant usage de la distance p-adique (bien sûr, il faut au préalable choisir la valeur du nombre premier p). Cela semble certainement très abstrait, mais on peut donner une représentation plus concrète des nombres p-adiques, un peu à la façon dont les nombres réels possèdent une représentation sous forme d'un développement décimal. Un nombre réel s'écrit, en base décimale, sous la forme : $a_q 10^q + ... + a_3 10^3 + a_2 10^2 + a_1 10^1 + a_0 + a_1 10^{-1} + a_{-2} 10^{-2} + ...$, ou q est un certain entier positif, et les a_i sont des entiers compris entre 0 et 9. Dans l'écriture usuelle, les coefficients a_0, a_1, a_2, etc. correspondent aux chiffres avant la virgule, tandis que a_{-1}, a_{-2} etc. désignent les chiffres après la virgule. Par exemple, l'écriture $23,14$ équivaut au développement $2 \times 10^1 + 3 + 1 \times 10^{-1} + 4 \times 10^{-2}$. Un développement analogue existe pour les nombres p-adiques ; ce sont les "développements de Hensel". On peut en effet démontrer qu'un nombre p-adique peut toujours s'écrire sous la forme $a_{-n} p^{-n} + a_{-n+1} p^{-n+1} + ... + a_0 + a_1 p^1 + a_2 p^2 + ...$ où n est un certain

entier positif, et où chaque coefficient entier a_i est compris entre 0 et $p-1$. Le développement de Hensel d'un nombre p-adique peut comporter une infinité de puissances positives de p - ce qui ne signifie pas que ces nombres sont infiniment "grands", étant donné que c'est la distance p-adique qui fournit les critères de grandeur. Pour les nombres rationnels, qui font partie de l'ensemble $\mathbb{Q}_p$ des nombres p-adiques, les coefficients a_i du développement de Hensel se répètent à partir d'un certain rang (de la même façon que, dans le corps $\mathbb{R}$ des nombres réels, les décimales d'un nombre rationnel se répètent périodiquement à l'infini).

Voici un exemple particulièrement simple de développement de Hensel d'un nombre rationnel. Choisissons $p = 5$ et cherchons le développement de Hensel de $-1/4$. On écrit ce nombre sous la forme $1/(1-5)$ et on utilise la formule bien connue de la série géométrique : $1+x+x^2+x^3+... = 1/(1-x)$, formule valable à condition que la valeur absolue de x soit inférieure à 1. Comme la valeur absolue 5-adique de 5 vaut $1/5$, qui est inférieur à 1, la formule peut s'appliquer. Cela donne $-1/4 = 1 + 5 + 5^2 + 5^3 + ...$, qui est le développement de Hensel de $-1/4$. Les coefficients, à partir de a_0 sont tous égaux à 1. Mais ce qui précède n'est qu'un exemple, et le développement de Hensel n'est généralement pas aussi facile à obtenir.

On peut imaginer les nombres p-adiques comme les feuilles d'un arbre infini dont chaque branche se ramifie en p branches secondaires, lesquelles se divisent à leur tour, et ainsi de suite.

Ce type de développement permet, soit dit en passant, de donner une représentation géométrique des nombres p-adiques. Imaginons un arbre dont chaque branche se ramifie en p branches secondaires, celles-ci se divisant à leur tour et ainsi de suite à l'infini. Si l'on numérote $0, 1, 2, .., p-1$ les branches issues de chaque nœud, on peut représenter chaque coefficient a_n du développement de Hensel d'un nombre p-adique par l'une des branches de l'arbre, cette branche étant elle-même issue de la branche-mère correspondant au coefficient a_{n-1}. De cette façon, on assimile chacun des nombres p-adiques à l'une des "feuilles" de l'arbre, qui sont les extrémités de cette ramification à l'infini. L'exemple le plus simple à dessiner est celui du corps $\mathbb{Q}_2$ des nombres 2-adiques (fig. 1). On part d'une branche-mère, qui se divise en deux branches-filles. On décide par exemple que la branche de droite correspond à la valeur 0, et que celle de gauche est associée à la valeur 1, ces nombres 0 et 1 étant les deux valeurs possibles pour le coefficient a_0 (par exemple), puis on répète le processus à l'infini. Un nombre 2-adique étant défini par une suite infinie de 0 ou 1 (les valeurs des coefficients du développement de Hensel), il peut être identifié à un certain chemin à travers l'arbre ou, ce qui revient au même, à l'une des "feuilles" qui terminent la ramification infinie.

Tout ce qui précède l'indique, le maniement des nombres p-adiques n'est pas aussi aisé que celui des nombres réels. Mais une fois dépassées ces difficultés initiales, il devient possible de développer une analyse p-adique, c'est-à-dire examiner des objets mathématiques classiques comme les suites, les séries, les fonctions, les équations algébriques, les équations différentielles, etc. en se plaçant dans le monde des nombres p-adiques et non dans le monde des nombres réels. Certains résultats y sont plus simples qu'en analyse classique (par exemple, toute série $u_1 + u_2 + ... + u_n + ...$ dont le terme général u_n tend vers 0 quand n tend vers l'infini converge vers une certaine limite). Mais aussi des phénomènes nouveaux apparaissent et ce sont, bien sûr, les plus intéressants à étudier.

A quoi servent les nombres p-adiques et l'analyse qu'ils permettent de développer ? Pour les mathématiciens au moins, à beaucoup de choses. Nous ne pourrons en donner ici qu'un bref et incomplet aperçu. Tout d'abord, une remarque : il y a deux manières d'utiliser les nombres p-adiques. Soit en ne considérant qu'une seule distance p-adique et, dans ce cas, le nombre premier p choisi joue un rôle privilégié, soit en faisant intervenir simultanément toutes les distances qu'on peut définir sur les nombres rationnels (tant les distances p-adiques que la distance classique). L'intérêt de cette deuxième approche réside dans une formule dite "du produit" qui lie toutes ces distances : le produit de toutes les valeurs absolues p-adiques d'un nombre rationnel m/n est égal à l'inverse de la valeur absolue ordinaire de m/n (cette formule se démontre facilement en décomposant m et n en leurs facteurs premiers). En combinant ces deux approches, on peut obtenir des résultats qui s'expriment de manière classique, c'est-à-dire dont l'énoncé ne fait pas intervenir les nombres p-adiques. Là réside une bonne part de l'utilité des nombres p-adiques. L'exemple sans doute le plus frappant en est la démonstration du fameux théorème de Fermat, menée à bien il y a quelques mois par Andrew Wiles, à l'université de Princeton[2]. Ce théorème dit que pour un entier n plus grand que 2, il n'existe pas d'entiers positifs et non nuls a, b, c, tels que $a^n + b^n = c^n$. La démonstration utilise les nombres p-adiques de façon essentielle à de nombreuses reprises alors que l'énoncé, lui, ne porte que sur des entiers ordinaires et est bien antérieur à l'invention des p-adiques.

L'équation de Fermat est un exemple de ce qu'on appelle les "équations diophantiennes", dont l'étude constitue l'une des premières applications des nombres p-adiques. Les équations diophantiennes, nommées ainsi en l'honneur du mathématicien grec Diophante qui en étudia quelques-unes au IV^{e} siècle, sont des équations polynomiales en une ou plusieurs variables, avec des coefficients entiers ($3x^4 + 5y^6 - 2xy = 0$ par exemple). Elles interviennent très souvent en mathématiques et dans leurs applications. Beaucoup d'équations polynomiales simples n'ont pas de solutions lorsqu'on les cherche dans les nombres réels : c'est le cas de l'équation $x^2 + 1 = 0$. Pour les résoudre, les mathématiciens du XVI^{e} siècle ont inventé les nombres complexes, en introduisant le symbole $\sqrt{-1}$. Mais une autre possibilité passe par les nombres p-adiques: on peut démontrer que, si p est un nombre premier de la forme $4n+1$, il existe un nombre p-adique x tel que $x^2+1 = 0$. Pour le choix $p = 5$, les calculs montrent que son développement de Hensel débute par $2+5+2\times5^2+5^3+3\times5^4+4\times5^5+....$ Cet exemple illustre le fait qu'une équation dépourvue de solution réelle peut posséder une solution p-adique.

Généralement, lorsqu'on parle d'équations diophantiennes, on sous-entend que l'on cherche des solutions qui sont des nombres entiers. En quoi les nombres p-adiques aident-ils à étudier ce type de problèmes ? Pour le comprendre, il suffit de faire la remarque suivante : si une équation n'a pas de solution réelle, elle n'a a fortiori pas de solution entière, puisque les entiers font partie des nombres réels. Par exemple, pour qu'un nombre entier soit solution du trinôme $3x^2 + 2x - 1 = 0$, il est nécessaire (mais pas suffisant) que cette équation ait pour solution un nombre réel x. Ce critère élémentaire peut être directement transposé aux nombres p-adiques, dont les entiers font aussi partie : pour qu'une équation diophantienne ait une solution entière, il est nécessaire - mais pas suffisant - qu'elle ait une solution p-adique, et cela pour chaque p premier.

Il se trouve que l'on a des moyens puissants pour étudier les équations dans les corps p-adiques.

[2]**La Recherche a publié** : (I) Catherine Goldstein, "Le théorème de Fermat", mars 1994. (II) Catherine Goldstein, "La conjecture de Fermat est enfin un théorème", juin 1995.

En voici un exemple, qui fait partie de ce qu'on appelle les "lemmes de Hensel". Donnons-nous un polynôme $P(x)$ à coefficients entiers. Supposons que l'on connaisse un entier n tel que l'entier $P(n)$ est divisible par p, mais avec $P'(n)$ non divisible par p (où $P'(x)$ est la dérivée de $P(x)$). Alors il existe un nombre p-adique x tel que $P(x) = 0$. Par exemple, si $P(x) = x^2 + 1$, sa dérivée est $P'(x) = 2x$; on a donc $P(2) = 5$ et $P'(2) = 4$. Le nombre 4 n'étant pas divisible par 5, on en conclut que le polynôme $x^2 + 1$ possède une racine dans l'ensemble $\mathbb{Q}_5$ des nombres 5-adiques. Nous avions donné plus haut les premiers termes du développement de Hensel de cette racine.

C'est à l'aide de tels moyens qu'on parvient éventuellement à trouver un nombre premier p pour lequel l'équation n'a pas de solution dans les nombres p-adiques. On en conclut alors qu'elle n'a pas de solution dans les entiers. Un autre résultat important appelé "principe de Hasse" en l'honneur de Helmut Hasse, élève de Hensel, énonce la réciproque pour les équations diophantiennes de degré 2 en une ou plusieurs variables : si une telle équation a une solution p-adique pour tout nombre premier p et une solution réelle, alors elle a une solution entière. Ce "principe" n'est malheureusement pas vrai en général. Trouver les conditions dans lesquelles le principe de Hasse est vérifié est un problème qui a été très étudié mais qui reste encore largement ouvert.

Les mathématiques p-adiques sont-elles dans une situation analogue à celle des géométries non euclidiennes au siècle dernier ? Ont-elles aussi un lien étroit avec la réalité physique ?

L'emploi des nombres p-adiques a aussi été étendu aux fonctions. Notamment à la "fonction zêta de Riemann", une fonction remarquable par les résultats purement arithmétiques qu'elle permet d'obtenir. Cette fonction $\zeta(s)$ est définie par $\zeta(s) = 1 + 1/2^s + 1/3^s + 1/4^s + ...$ pour $s > 1$. Comme l'a montré Bernhard Riemann au XIX$^{\text{e}}$ siècle, elle peut être prolongée pour toute valeur complexe de la variable (sauf pour $s = 1$). La fonction ainsi construite est étroitement liée aux propriétés des nombres premiers (voir l'article de Henri Cohen dans ce numéro). La fonction zêta de Riemann a été généralisée dans de nombreux domaines des mathématiques. En particulier, toujours au siècle dernier, l'Allemand Peter Gustav Lejeune-Dirichlet, lors de ses recherches sur les nombres premiers contenus dans une progression arithmétique, a introduit des fonctions de la variable complexe appelées aujourd'hui "fonctions L de Dirichlet", très utiles en arithmétique.

En 1964, les mathématiciens Tomio Kubota et Heinrich W. Leopoldt parvenaient à développer les techniques nécessaires pour construire des analogues p-adiques des fonctions zêta et L. Ces nouveaux objets, qui sont des fonctions d'une variable p-adique à valeur dans les nombres p-adiques, permettent d'obtenir des renseignements précieux de nature arithmétique, complémentaires de ceux fournis par les fonctions zêta et L classiques, mais qu'il n'est malheureusement pas possible d'expliquer ici. Quoi qu'il en soit, c'est à partir des années 1960, grâce aussi aux travaux de l'Américain Bernard Dwork sur les fonctions zêta associées à des "variétés algébriques" (ensembles de solutions d'une famille de polynômes à plusieurs variables), que l'analyse p-adique a pris son essor et acquis ses lettres de noblesse en mathématiques.

Mais les méthodes p-adiques n'interviennent pas qu'en mathématiques pures. On les voit maintenant apparaître dans des domaines inattendus comme les probabilités ou la physique théorique. Une des raisons en est que les nombres p-adiques fournissent un exemple simple de structure en

arbre. Par exemple, dans l'étude théorique des propriétés thermodynamiques des verres de spin (matériaux désordonnés contenant des particules aimantées, dont l'orientation doit s'ajuster pour minimiser les interactions magnétiques), la technique dite "des répliques" consiste à considérer n échantillons identiques, à calculer l'énergie d'interaction magnétique, puis à faire tendre formellement, dans les calculs, l'entier n vers 0. En fait, un examen attentif montre que la technique des répliques revient à prendre une suite d'entiers qui tend "p-adiquement" vers zéro pour tous les nombres premiers p à la fois (par exemple, la suite $n \to n! = 1 \times 2 \times 3 \times ... \times (n-1) \times n$ possède cette propriété car, pour tout nombre premier p, $n!$ est divisible par des puissances de p de plus en plus grandes lorsque n tend vers l'infini).

Les applications de l'analyse p-adique à la physique pourraient même aller au delà des aspects strictement techniques. Des physiciens théoriciens se livrent par exemple à des spéculations sur la structure de l'espace et du temps à très petite échelle. Les lois de la relativité et de la physique quantique semblent indiquer qu'il n'est pas possible de mesurer des longueurs inférieures à une valeur extraordinairement petite, appelée longueur de Planck, et qui est de l'ordre de 10^{-35} mètre. L'existence d'une distance minimale suggère à certains théoriciens qu'à cette échelle, la structure ultime de l'espace-temps pourrait se décrire non pas en termes de nombres réels, mais en termes de structure p-adique. Pour l'instant, ce ne sont que des études spéculatives, mais il n'est pas exclu qu'elles aboutissent un jour à des conclusions vérifiables par des expériences.

La situation à laquelle donnent lieu les nombres p-adiques est en un sens très analogue à celle de la géométrie. Au siècle dernier, on a découvert que la géométrie ordinaire ou euclidienne n'est pas la seule géométrie qui puisse être envisagée, mais que l'on pouvait construire différentes géométries non euclidiennes. On pensait au début que la géométrie euclidienne était la seule qui soit adaptée à la description du monde physique : l'avènement de la théorie de la relativité a montré qu'il n'en est rien. Les nombres p-adiques ont été et sont la source de grands progrès en arithmétique et en géométrie algébrique. Peut-être découvrira-t-on qu'ils ont aussi, à l'instar des géométries non euclidiennes, un lien étroit avec la réalité physique.

Pour en savoir plus

- Z.I. Borevitch et I.R. Chafarevitch, Théorie des nombres, Gauthier-Villars, 1967.
- G. Christol, "p-adic numbers and ultrametricity" dans From Number Theory to Physics (Waldschmidt et al., eds.), Springer, 1992.
- R. Rammal et al., "Ultrametricity for physicists", Rev. Mod. Phys., 58, 1986.
- Y. Amice, Les nombres p-adiques, PUF, 1975.
- B. Dwork, G. Gerotto, F. Sullivan, "An Introduction to G-Functions", Annals of Math. Studies, 133, Princeton University Press, 1994.
- N. Koblitz, p-adic numbers, p-adic analysis and Zeta functions, 2nd ed. Springer-Verlag, 1984.
- V.S. Vladimirov, I.V. Volovich et E.I. Zelenov, p-adic analysis and mathematical physics, World Scientific, 1994.