

- modulo q si q est un carré modulo p sur une horloge ayant p heures. Par exemple, 5 est un carré parfait modulo 11, puisque $5=16=4^2$ et 11 est un carré modulo 5, puisque $11=1=1^2$.

«Je trouve cela très surprenant», confie Peter Scholze. «À première vue, ces deux choses n'ont rien en commun.» «Vous pouvez interpréter beaucoup de théories algébriques modernes comme de simples tentatives de généraliser cette loi», explique Jared Weinstein.

Au milieu du xx^e siècle, les mathématiciens ont découvert un lien étonnant entre les lois de réciprocité et ce qui avait l'air d'être un sujet totalement différent: la géométrie hyperbolique (un exemple de modèle d'espace hyperbolique est le pavage «Anges et démons», d'Escher). Ce

lien fait partie intégrante du programme de Langlands (voir l'encadré page 86), une série de conjectures et de théorèmes interconnectés portant sur les relations entre la théorie des nombres, la géométrie et l'analyse. Quand ces conjectures sont prouvées, elles se révèlent souvent extrêmement puissantes. Par exemple, la preuve du dernier théorème de Fermat a consisté à résoudre une petite – mais loin d'être triviale – partie du programme Langlands.

Les mathématiciens ont progressivement pris conscience que ce programme s'étend bien au-delà du cas du disque hyperbolique: il peut aussi être étudié dans des espaces hyperboliques de dimension supérieure et d'autres contextes variés. Peter Scholze a montré comment

L'ÉTRANGE MONDE P -ADIQUE

Notre manière habituelle (décimale) d'écrire des nombres consiste à les représenter comme une somme de puissances de dix avec des facteurs (des coefficients) compris entre 0 et 9. Ainsi, 347 est une forme abrégée de $3 \times 10^2 + 4 \times 10^1 + 7 \times 10^0$.

En fait, on peut identifier tout nombre réel avec la suite de ses chiffres: $a_n a_{n-1} \dots a_1 a_0, a_{-1} a_{-2} a_{-3} \dots$ est essentiellement identique à: $a_n \times 10^n + a_{n-1} \times 10^{n-1} \dots a_1 \times 10 + a_0 + a_{-1} \times 10^{-1} + a_{-2} \times 10^{-2} + a_{-3} \times 10^{-3} \dots$ les chiffres a_i étant compris entre 0 et 9. Dans ce contexte, les séquences à l'infini de chiffres 0,999... et 1,000... représentent le même nombre.

De manière générale, en mathématiques, une suite est un ensemble de quantités, par exemple de nombres, dont les éléments sont pourvus de numéros (des indices): a_n désigne l'élément de rang n d'une suite, du coefficient de 10^n dans l'exemple précédent.

Habituellement, les indices vont de 1 à l'infini: $a_1, a_2, a_3 \dots$. C'est différent avec les nombres réels qui peuvent nécessiter une infinité de coefficients à indice négatif. Par exemple, $\pi = 3,14159$ s'écrit: $3 \times 10^0 + 1 \times 10^{-1} + 4 \times 10^{-2} + 1 \times 10^{-3} + 5 \times 10^{-4} + 9 \times 10^{-5} \dots$

où $a_0 = 3, a_{-1} = 1, a_{-2} = 4, a_{-3} = 1, a_{-4} = 5, a_{-5} = 9 \dots$

Le fait que la base soit 10 n'a aucune signification mathématique. Dans ce qui suit, il sera même plus intéressant de choisir pour base un nombre premier p . Un nombre réel écrit en base p est donc une suite de chiffres entre 0 et $p-1$, qui peut en contenir un nombre infini d'éléments d'indice négatif (après la virgule), mais seulement un nombre fini d'indice positif. Peut-on imaginer l'inverse? Quels seraient les nombres obtenus en autorisant une infinité de termes à gauche de la virgule, mais seulement un nombre fini de termes à sa droite?

Ces nombres sont dits p -adiques. Leur comportement déconcerte et réclame du temps pour s'y s'habituer. Et contrairement aux nombres réels, ils sont complètement inadaptés pour décrire les processus naturels. Néanmoins, on peut calculer avec eux presque comme on a l'habitude de le faire depuis l'école primaire. Ainsi, pour les nombres 5-adiques, comme pour les nombres habituels en base 5, on a $4+1=10$. Cependant, on a aussi $\dots 4444+1=0$, car il y a une retenue à chaque addition, qui se propage à l'infini vers la gauche. La division doit également être effectuée dans l'ordre inverse de celui de la méthode scolaire.

Les nombres p -adiques forment un corps, c'est-à-dire un ensemble où les quatre opérations arithmétiques de base peuvent être effectuées sans restriction – sauf la division

par zéro. On désigne ce corps par le symbole $\mathbb{Q}_p$.

Quand dit-on de deux nombres réels qu'ils sont proches?

Lorsque leur différence a un zéro avant la virgule et beaucoup de zéros après. La question est plus complexe avec deux nombres p -adiques: ils sont proches quand leur différence a beaucoup de zéros avant la virgule (et seulement des zéros derrière) ou, ce qui revient au même, est divisible par une puissance élevée de p . Le fait qu'il existe encore une infinité de chiffres plus à gauche est sans importance. Avec cette définition de la proximité, on peut définir des suites de nombres p -adiques ainsi que leurs limites. Toutefois, on ne peut pas ordonner les nombres p -adiques sur une ligne aussi facilement que les nombres réels.

Le calcul de puissances, définies par multiplication répétée d'un nombre, compte parmi les opérations qui sont toujours possibles dans un corps. Ce n'est pas le cas des racines. Parmi les nombres réels, il n'existe pas de x ayant la propriété $x^2 = -1$. Les mathématiciens remédient à ce défaut en ajoutant, quasiment par décret, un nouveau nombre appelé i , dont ils ne demandent rien d'autre que la propriété $i^2 = -1$ (ils «ajoutent au corps des nombres réels une racine de -1 »). Ainsi, ils construisent à partir des nombres réels les nombres complexes. Un procédé similaire est possible avec les nombres p -adiques. On ajoute de préférence au corps $\mathbb{Q}_p$ une racine p -ième de p . Cependant, contrairement au cas des nombres complexes, ceci ne résout pas une fois pour toutes le problème du calcul de racines. Il s'avère nécessaire d'ajouter également la p -ième racine de la p -ième racine, la p^2 -ième racine de ce nombre, et ainsi de suite. Cela conduit à l'extension de corps infinie de $\mathbb{Q}_p$, la «tour infinie» évoquée dans le texte principal.

Le corps $\mathbb{Q}_p$ des nombres p -adiques a une autre propriété remarquable: on peut pourvoir ses éléments (des suites de chiffres entre 0 et $p-1$, dont une infinité à un indice positif, mais seulement un nombre fini à indice négatif sont non nuls) de nouvelles règles de calcul, ce qui conduit à un corps complètement différent.

Ces nouvelles règles de calcul viennent de la théorie de l'analyse complexe (la théorie des fonctions). On y étudie de préférence des fonctions représentables par des séries entières, c'est-à-dire des sommes infinies de la forme $f(z) = a_0 + a_1 z + a_2 z^2 + a_3 z^3 \dots$

Si l'on ne veut pas exclure des fonctions telles que $1/z$ ou $2/z^3 + 3z^2$, on doit étendre les sommes à des «séries de Laurent», où des coefficients d'indice négatif peuvent apparaître. Pour $1/z$, on a alors $a_{-1} = 1$, et pour $2/z^3 + 3z^2$, $a_{-3} = 2$ et $a_2 = 3$.