PUISSANCES FRACTIONNAIRES DES NOMBRES p-ADIQUES

Résumé

Après avoir rappelé la définition et les propriétés de la valuation, nous établissons intuitivement les règles d'existence de la racine carrée p-adique d'un nombre puis celles de l'existence d'une puissance fractionnaire. Nous réfléchissons en même temps sur les éventuelles relations d'inclusion entre les différents ensembles de nombres p-adiques, celui des réels, et celui des nombres complexes.

Introduction

Nous avons vu dans « 1 Représentation p-adique » que tous les **nombres rationnels** avaient une représentation usuelle et une infinité de représentations p-adiques (une pour chaque valeur de p).

On sait également qu'il existe des nombres qui ne sont pas rationnels et que l'on qualifie de **réels** comme π ou $\sqrt{2}$ par exemple. Nous rencontrerons également dans ce fichier les **nombres complexes** qui font intervenir $i = \sqrt{-1}$.

Pour continuer notre exploration, nous tentons de calculer la racine carrée d'un nombre rationnel en représentation p-adique, puis, de façon plus générale, une puissance fractionnaire.

Comme nous l'avons fait dans « 1 Représentation p-adique », nous abordons ce sujet de façon pragmatique et ludique sans trop rechercher de démonstrations générales.

Notre devise pourrait être, comme il a déjà été écrit : « **Montrer plutôt que démontrer** ».

Pour rester concret, nous continuons à utiliser des exemples pris dans les nombres 5-adiques en essayant de ne pas trop restreindre la généralité.

Valuation

La notion de valuation simplifie beaucoup l'expression d'un certain nombre de propriétés.

Nous lui consacrons un fichier (« A1 Valuation ») qu'il est vivement conseillé de lire. Nous rappelons ici ses propriétés essentielles.

Les nombres sans virgule qui se terminent par un ou plusieurs 0 sont des multiples de p. Leur valuation est égale au nombre de 0 à droite de ce nombre. Par conséquent, le «0| p-adique a une valuation infinie.

Les nombres à virgule sont des nombres sans virgule ne se terminant pas par 0 divisés par une puissance de p. Leur valuation est l'opposé du nombre de chiffres après la virgule.

Tous les autres nombres p-adiques ont une valuation nulle. Ces derniers sont appelés **unités p-adiques**.

Les **unités p-adiques** sont donc des nombres **sans virgule** qui **ne se terminent pas par 0**.

Si a est un nombre p-adique et u une unité p-adique, on peut écrire $a = u \times 10^n$ où n est la valuation p-adique de a (un entier relatif).

Nous montrons dans l'annexe « A3 Valuation » les propriétés suivantes :

$$v(a \times b) = v(a) + v(b) \text{ donc } v(a^n) = n v(a).$$

$$v(b / a) = v(b) - v(a).$$

$$v(a + b) \geq \text{Min}(v(a), v(b))$$

$$v(a) \neq v(b) \text{ entraine toujours } v(a + b) = \text{Min}(v(a), v(b))$$

La propriété concernant la valuation d'une somme ne nous servira pas dans ce fichier.

Racine carrée

Condition d'existence

Dans le monde des nombres « habituels », on sait que seuls les réels positifs ou nuls ont deux racines carrées réelles (et opposées). On sait également que tous les nombres complexes (donc éventuellement réels) possèdent deux racines carrées complexes (donc éventuellement réelles) opposées.

Dans le monde des nombres p-adiques, il en est tout autrement. Montrons d'abord que certains nombres p-adiques n'ont pas de racine carrée.

Comme pour les nombres réels, on admet que la recherche de la racine carrée du nombre p-adique a est équivalente à la résolution de l'équation $x^2 = a$.

Les propriétés de la valuation nous permettent de dire que la valuation d'un carré est obligatoirement paire puisque $v(x^2) = 2 v(x)$. L'équation $x^2 = a$ n'a donc pas de solution p-adique si $v(a)$ est impaire (c'est-à-dire si le nombre p-adique a se termine par un nombre impair de 0 ou si a possède un nombre impair de chiffres après la virgule).

En conséquence, **une infinité de nombres p-adiques n'ont donc pas de racine carrée.**

Si $v(a)$ est paire, on introduit l'unité p-adique u associée au nombre a : $a = u \times 10^{2n}$.

On appelle x la racine carrée de a et t l'unité p-adique telle que $t^2 = u$.

On a donc $x^2 = t^2 \times 10^{2n}$ donc $x = t \times 10^n$

On doit donc chercher les solutions de l'équation $t^2 = u$ où t et u sont des unités p-adiques, sans être certain que cette équation possède une solution.

Nous abordons cette question dans le cas particulier des nombres 5-adiques.

Reprenons la table de multiplication des entiers modulo 5 (les mathématiciens appellent cet ensemble $\mathbb{Z}/5\mathbb{Z}$) sans la ligne et la colonne 0.

Les nombres situés sur la diagonale donnent le dernier chiffre à droite du carré de n'importe quelle unité 5-adique.

x	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Le dernier chiffre du carré d'une unité 5-adique est donc obligatoirement **1** ou **4**.

Les unités 5-adiques se terminant par 2 ou 3 n'ont donc pas de racine carrée.

Mais **2** possède une racine carrée 7-adique car $3^2 = 2 \pmod{7}$.

On regroupe les deux conditions d'existence des solutions de l'équation $x^2 = a$:

Quand on écrit **a** sous la forme $a = u p^n$, l'équation $x^2 = a$ possède des solutions 5-adiques si et seulement si **n** est pair et si l'unité 5-adique **u** se termine par **1** ou **4**.

Calcul d'une racine carrée

Il reste cependant à s'assurer que l'on a un moyen de calculer la racine carrée des nombres qui possèdent les propriétés ci-dessus.

Pour cela, il suffit de mettre en œuvre un algorithme proche de celui que seuls les lycéens de plus de 60 ans connaissent encore.

Avec cet algorithme antédiluvien, on peut calculer, par exemple, la racine carrée 5-adique de $6 \sim 11$.

On obtient **...1 2 4 0 3 1** et son opposé **...3 2 0 4 1 4**.

Une vérification s'impose peut-être pour les incrédules ?

	...1 2 4 0 3 1
x	...1 2 4 0 3 1
-----	...1 2 4 0 3 1
	...3 2 1 4 3
	...0 0 0 0
	...2 2 4
	...1 2
	...1
-----	...0 0 0 1 1

	...3 2 0 4 1 4
x	...3 2 0 4 1 4
-----	...3 3 3 2 2 1
	...2 0 4 1 4
	...3 2 2 1
	...0 0 0
	...3 3
	...2
-----	...0 0 0 1 1

On perd évidemment la périodicité des chiffres propre aux nombres rationnels, comme dans la représentation usuelle. On considère les 6 chiffres indiqués comme une approximation du résultat, de même que 2,44949 est une approximation de $\sqrt{6}$ en représentation usuelle et en base 10.

On dira que $\sqrt{6}$ appartient à $\mathbb{R}$ et $\sqrt{6}$ à $\mathbb{Q}_5$, même si l'écriture concrète de ce nombre n'est pas la même dans les deux ensembles.

Racines carrées de -1

De toute évidence la règle d'existence des racines carrées 5-adiques énoncée ci-dessus s'applique également aux nombres négatifs que l'on sait reconnaître (voir « A2 Changement de représentation ») mais qui s'écrivent sans le signe « moins ».

En particulier, $-1 \sim \mathbf{4}$ possède une racine carrée 5-adique puisque sa valuation est 0 et qu'il se termine par 4.

Le calcul avec l'algorithme du paragraphe précédent donne les 6 derniers chiffres des deux racines carrées 5-adiques de -1 : **...431212** et **...013233**. Ces deux nombres sont évidemment opposés l'un de l'autre.

Ces deux écritures de $\sqrt{-1}$ sont donc associées aux nombres complexes i et $-i$, sans que l'on puisse savoir lequel des deux est associé à i ou à $-i$.

$\mathbb{Q}_5$ n'est donc pas inclus dans $\mathbb{R}$ puisqu'il contient des éléments de $\mathbb{C}$!

Mais $\sqrt{-1}$ n'est pas un nombre p -adique pour toute valeur de p . En effet, le nombre 7-adique associé à -1 est $\mathbf{6}$ et les carrés 7-adiques se terminent par 1, 2 ou 4.

Cependant, nous verrons dans le paragraphe suivant que tous les ensembles $\mathbb{Q}_p$ contiennent des nombres complexes. Donc $\mathbb{Q}_p$ n'est jamais inclus dans $\mathbb{R}$.

Racine $n^{\text{ième}}$

On généralise le problème précédent en cherchant les conditions d'existence des solutions de l'équation $x^n = a$, où a est un nombre p -adique rationnel et n un entier strictement positif.

Pour traiter le cas des nombres 5-adiques, nous écrivons d'abord le tableau des puissances successives des entiers modulo 5.

On ne va pas plus loin que x^4 car on retrouve le **petit théorème de Fermat** qui dit que si p est premier et x entier, non nul, et premier avec p , alors, $x^{p-1} = 1$ (modulo p).

x	x^2	x^3	x^4
1	1	1	1
2	4	3	1
3	4	2	1
4	1	4	1

Les conditions d'existence des solutions de l'équation $x^n = a$ peuvent donc se formuler de façon voisine de celles de l'équation $x^2 = a$.

La condition sur la valuation est simple à exprimer : **cette équation n'a des solutions que si la valuation de a est un multiple de n** (en tenant compte évidemment des multiples négatifs).

Pour la condition sur le dernier chiffre, on ne rentrera pas dans le détail car ça n'a pas un grand intérêt et on peut traiter le problème au cas par cas.

Racines $(p-1)^{\text{ième}}$ de 1

Pour continuer notre réflexion sur les éventuelles relations d'inclusion entre $\mathbb{Q}_p$, $\mathbb{R}$ et $\mathbb{C}$, il est intéressant d'examiner cette question.

Le problème est classique en représentation usuelle et on sait de façon générale que l'équation $x^n = 1$ possède n solutions complexes données par $\exp\left(\frac{2ik\pi}{n}\right)$ avec k entier variant de 0 à $n-1$.

Donc pour $n = p - 1$, les solutions sont $\exp\left(\frac{2ik\pi}{p-1}\right)$.

Pour les nombres p -adiques, le petit théorème de Fermat nous permet d'affirmer que si u est une unité p -adique, alors u^{p-1} se termine par 1.

On en déduit que l'équation $x^{p-1} = 1$ possède $p - 1$ solutions que l'on peut considérer comme les représentations p -adiques des nombres complexes $\exp\left(\frac{2ik\pi}{p-1}\right)$.

Quel que soit p , l'ensemble $\mathbb{Q}_p$ contient donc des nombres complexes.

Nous ne creuserons pas davantage ces questions difficiles et, pour en terminer définitivement avec les relations d'inclusion, je cite une phrase de Bruno Winckler (Université de Bordeaux) qui a éclairé ma lanterne lors de ma « découverte » des nombres p -adiques :

« Un théorème de logique permet de prouver, et c'est extrêmement ténu, que tous les nombres p -adiques peuvent être "vus" comme des nombres complexes, "à une transformation près" qu'il est impossible d'expliciter en général... ».

Conclusion

Le cas général des puissances fractionnaires se traite comme la racine $n^{\text{ième}}$ puisque l'équation $x^{n/m} = a$ se ramène à $x^n = a^m = b$.

Les conditions d'existence des solutions de l'équation $x^{n/m} = a$ permettent évidemment de dire si $a^{m/n}$ est un nombre p -adique mais ne permettent pas de les calculer.

Dans la représentation usuelle, l'équation $x^{n/m} = a$ possède une seule solution réelle quand a est strictement positif. Elle est donnée par $x = \exp\left(\frac{1}{n} \ln(a^m)\right)$.

Si a est un nombre négatif ou complexe, il faut faire intervenir les fonctions exponentielle et logarithme à argument complexe, ce qui est simple pour la première et nettement plus délicat pour la seconde.

Mais si a est un nombre écrit en représentation p-adique, on ne sait pas encore comment calculer le logarithme ou l'exponentielle de ce nombre.

Nous abordons cette question dans le fichier « Exponentielle et Logarithme ».