Les nombres p-adiques

Yann Ollivier

On veut voir ce qui se passe quand on change un peu les règles du calcul usuel. Lorsqu'on passe des nombres entiers aux nombres réels, on s'autorise à utiliser des nombres avec une infinité de chiffres après la virgule. Que se passerait-il si on essayait de calculer avec une infinité de chiffres *avant* la virgule ?

Ce n'est pas simplement un jeu gratuit : on obtient ainsi une théorie algébrique complète, dite p-adique, qui a certaines propriétés un peu plus simples que l'algèbre avec les nombres ordinaires. Elle est souvent étudiée par les mathématiciens, soit pour elle-même, soit pour tester des théorèmes qu'on veut démontrer pour les nombres ordinaires en se « faisant la main » sur le cas p-adique.

1 Les nombres décadiques

Les propriétés des nombres avec une infinité de chiffres à gauche vont différer selon la base dans laquelle on travaille, comme on va le montrer. On commence donc dans la base habituelle : la base 10.

1.1 Addition et multiplication

Un nombre décadique est donc un nombre avec une infinité de chiffres à gauche, tel que $\ldots 1212121212$. On peut additionner les nombres décadiques :

$$\begin{array}{rr} & \ldots 12121212 \\ + & \ldots 95325368 \\ \hline & \ldots 07446570 \end{array}$$

en reportant les retenues comme d'habitude.

Ceci fonctionne bien grâce à la propriété suivante : les n derniers chiffres du nombre $a+b$ ne dépendent que des n derniers chiffres de a et de b.

Question 1 – *Expliquer pourquoi la multiplication des nombres décadiques marche bien aussi.*

Par contre, on ne peut pas tout mélanger, i.e. avoir à la fois des nombres décadiques avec une infinité de chiffres à gauche, et des nombres réels ordinaires avec une infinité de chiffres à droite.

Question 2 – *Expliquer pourquoi la multiplication d'un nombre décadique par un nombre réel ordinaire (avec une infinité de chiffres à droite) ne peut pas marcher.*

1.2 La soustraction

Il peut parfois se produire des propriétés amusantes lorsqu'on additionne des nombres décadiques :

$$\begin{array}{rr} & \ldots 99999997 \\ + & 3 \\ \hline & \ldots 00000000 \end{array}$$

On a envie de dire qu'on a triché : la retenue est partie à l'infini vers la gauche, mais elle existe ! Eh bien non : tout le truc des décadiques consiste justement à dire que 10^n quand n est grand, c'est presque rien : on ne voit que les derniers chiffres, les chiffres trop à gauche ne comptent presque pas.

L'addition ci-dessus n'est absolument pas une contradiction : elle montre simplement qu'en décadiques, on a l'égalité

$$\ldots 99999997 = -3$$

On va montrer que grâce aux décadiques, on peut complètement se passer des signes ! Les nombres éngatifs sont déjà tout prêts.

Question 3 – *Soit n un nombre entier ordinaire. Donner une règle pour calculer son opposé $-n$ en p-adiques.*

Question 4 – *Prouver que, si on sait calculer -1, on sait calculer $-n$ pour n'importe quel nombre n, même si n est un décadique et non un nombre ordinaire.*

On a donc réussi à faire en décadiques trois des quatre opérations usuelles : addition, multiplication, soustraction.

Définition 1 (Anneaux) – *Quand on a trois opérations : l'addition, la soustraction et la multiplication, vérifiant les propriétés habituelles, on dit que les nombres qu'on utilise constituent un* anneau.

1.3 Et la division ?

Il y a des exemples de divisions qui marchent bien en décadiques. Par exemple, pour calculer 1/3, il suffit de remarquer que

$$\begin{array}{rr} & \ldots 66666667 \\ \times & 3 \\ \hline & \ldots 00000001 \end{array}$$

Cet exemple est une autre preuve qu'il ne faut pas mélanger nombres décadiques et nombres réels : sinon, on aurait $\ldots 66666667$ et $0,3333333$ qui vaudraient tous les deux 1/3...

Va-t-on, comme pour la soustraction, pouvoir se passer complètement des fractions et nombres à virgules en décadiques ? Pas tout à fait, parce qu'il y a quand même des problèmes. Regardons la tentative de division en décadiques :

$$\begin{array}{rr} & \ldots ???????? \\ \times & 5 \\ \hline & \ldots 00000001 \end{array}$$

Pour commencer à résoudre cette division, il faut trouver un nombre a entre 0 et 9 tel que a fois 5 se termine par un 1... or ceci n'existe pas.

Donc il n'est pas possible de faire n'importe quelle division en décadiques.

Question 5 – *Dire quels sont les entiers ordinaires qui ont un inverse en décadiques.*

On peut remarquer ci-dessus que l'écriture de 1/3 en décadiques évoque fortement celle de 2/3 en nombres réels. Ça marche aussi pour d'autres nombres :

$$\begin{array}{rr} & \ldots 142857142857143 \\ \times & 7 \\ \hline & \ldots 000000000000001 \end{array}$$

et en nombres réels $1/7 = 0,142857142857\ldots$

Question 6 – *Trouver (et démontrer !) une règle permettant de relier l'écriture décadique de l'inverse d'un nombre, avec l'écriture décimale d'une fraction contenant ce nombre au dénominateur.*

Pour cette question, il sera utile de remarquer qu'en nombres ordinaires, des nombres tels que $0,123123123\ldots$ s'écrivent en fraction 123/999, et qu'en décadiques l'inverse d'un nombre tel que 999 est $\ldots 001001001$ (faites la multiplication !).

À ce stade, on a totalement étudié le problème du calcul des inverses des nombres entiers ordinaires. Savoir calculer des inverses suffit à faire des divisions, en remarquant que

$$a/b = a \times (1/b)$$

2 Des problèmes de limites

2.1 Définition des limites

Pour faire une opération en décadiques, il est absolument indispensable que les derniers chiffres du résultat de l'opération ne dépendent que des derniers chiffres des nombres de départ. (Repensez à l'exemple de la multiplication d'un décadique par un nombre décimal ordinaire à une infinité de chiffres à droite de la virgule.)

L'idée est donc que seuls les chiffres les plus à droite comptent, qu'on voit moins les autres. En d'autres termes : 10^n pour n grand, ça tend vers 0. C'est bien ce qu'on avait vu dans l'addition $\ldots 99999 + 1 = 0$.

Définition 2 (Limite) – *Soient $a_1, a_2, a_3 \ldots$ des nombres décadiques. On dit que cette suite de décadiques tend vers une limite b si, lorsqu'on attend assez longtemps, les derniers chiffres de tous les a_i sont les mêmes que les derniers chiffres de b.*

Par exemple, une suite qui commence par 0 ; 2 ; 1 ; 11 ; 31 ; 421 ; 321 ; 1521 ; 2521 ; 13521 ; 43521 ; 23521 a l'air de se stabiliser vers un nombre se finissant par 3521, puisqu'à partir du dixième terme, ces quatre chiffres ne changent plus.

Donnons une définition plus formelle, qu'il est utile de comprendre :
Définition 3 (Limite, deuxième essai) – *Soit $a_1, a_2, a_3 \ldots$ une suite de nombres décadiques. On dit que cette suite tend vers une limite b si, pour tout nombre de chiffres n qu'on se donne, il existe un i tel que, pour tout $j > i$, les n derniers chiffres de a_j sont les mêmes que les n derniers chiffres de b.*

Par exemple, s'il y a une limite, on sait qu'à partir d'un certain moment, les $n = 15$ derniers chiffres ne vont plus bouger. Mais ce moment peut être très éloigné, par exemple, il se peut qu'il faille attendre le dix millième terme, $i = 10000$, avant que les n derniers chiffres ne changent plus.

À quoi ça sert de définir ça ?

2.2 Limites et division par un décadique

Jusqu'ici, nous n'avions réussi à diviser un décadique que par un nombre ordinaire. Nous n'avions pas tenté des expériences plus osées de division d'un décadique par un autre décadique...

On a bien envie de dire que pour diviser par un décadique, il suffit de diviser par les n derniers chiffres, puis de prendre la limite quand n tend vers l'infini. Autrement dit, on aimerait que pour diviser par $\ldots 33333333$, il suffise de diviser par 3, par 33, par 333, etc. et de voir si on obtient une limite comme ça.

On veut donc montrer très exactement la propriété suivante : que si la suite d'entiers a_i tend vers un décadique b, alors la suite de décadiques $1/a_i$ tend vers l'entier $1/b$. (Attention, on a vu ci-dessus que tous les entiers n'avaient pas d'inverse, par exemple, si'ils se terminaient par 5 ; on suppose donc qu'on n'est pas dans ce cas et que les a_i ont bien des inverses.)

Qu'est-ce qui se passe quand on essaie de changer le dénominateur d'une fraction par une quantité petite ? Ceux qui savent sommer des séries géométriques connaissent sûrement la formule :

$$\frac{1}{1+x} = 1 - x + x^2 - x^3 + x^4 - \ldots$$

qui est valable en nombres ordinaires si $|x| < 1$, autrement dit si x^n tend vers 0 quand n est grand.

Si vous ne connaissez pas cette formule, multipliez le terme de droite par le dénominateur de gauche $1 + x$ et remarquez que tous les termes se téléscopent et qu'il reste 1.

Cette formule se généralise si on a autre chose que 1 au dénominateur :

$$\frac{1}{c+x} = \frac{1}{c}\frac{1}{1+x/c} = \frac{1}{c}\left(1 - (x/c) + (x/c)^2 - (x/c)^3 + \ldots\right)$$

En décadiques, c'est 10^n qui tend vers 0 quand n est grand... Imaginons donc que nous avons un décadique a dont le dernier chiffre est 1. On veut calculer $1/a$. On remarque que $a = 1 + 10b$ où b est un décadique : c'est exactement dire que le dernier chiffre de a est 1.

Mais alors on a envie de dire que, comme ci-dessus,

$$\frac{1}{a} = \frac{1}{1+10b} = 1 - 10b + (10b)^2 - (10b)^3 + (10b)^4 - \ldots$$

Question 7 – *Expliquer pourquoi cette formule est correcte en décadiques.*

Si le dernier chiffre n'est pas un 1, on applique le même truc que ci-dessus, à savoir que

$$\frac{1}{c+10b} = \frac{1}{c}\frac{1}{1+10(b/c)}$$

mais cela nécessite de pouvoir diviser par c. Ce n'est pas toujours possible, mais quand c'est possible, la formule marche.

Question 8 – *Soient x et y deux décadiques. Dire quand il est possible de diviser par y, et écrire la formule pour x/y.*

2.3 La compacité

Bien sûr, si l'on donne une suite de décadiques, elle n'a pas toujours de limite. Par exemple, 1 ; 2 ; 11 ; 22 ; 111 ; 222, etc., ne tend vers rien du tout. On a quand même envie de dire, plutôt qu'elle n'a pas de limite, qu'elle en aurait deux. C'est l'intérêt de la notion de limite extraite.

Si $a_0, a_1, a_2 \ldots$ est une suite, on appelle sous-suite extraite de la suite (a_n) une suite $(a_{n'})$ incluse dans celle-là, c'est-à-dire qu'on ne prend pas tous les termes (mais qu'on en prend quand même une infinité). Par exemple, on peut prendre un terme sur deux, ou bien prendre seulement les termes $a_{n'}$ où n' est un carré, etc.

Ainsi, dans l'exemple de la suite 1 ; 2 ; 11 ; 22 ; 111 ; 222, on a envie de la séparer en deux sous-suites en prenant un terme sur deux, et chacune aura une limite.

Définition 4 (Limite extraite) – *La limite d'une sous-suite d'une suite est appelée* limite extraite *de la suite.*

La suite ci-dessus a donc deux limites extraites $\ldots 111$ et $\ldots 222$.

Si l'on sait bien que toutes les suites n'ont pas de limites, on aimerait bien avoir quand même des limites extraites...

Définition 5 (Compacité) – *Un ensemble (avec une certaine notion de limite) est dit* compact *si toute suite a une limite extraite.*

La compacité est une notion extrêmement importante en mathématiques, qui est utilisée dans tous les domaines. Par exemple, on peut montrer que l'intervalle $[0;1]$ est compact (pour la limite d'une suite de nombres réels). On peut aussi montrer que toute partie du plan qui ne va pas jusqu'à l'infini est compacte (pour la limite de points du plan).

Par contre, l'ensemble des entiers ordinaires n'est pas compact : la bête suite $1, 2, 3, 4 \ldots$ ne tend vers rien du tout.

Mais en y ajoutant les décadiques, il devient compact. Par exemple, de la suite des entiers $1, 2, 3, 4 \ldots$ on peut extraire la sous-suite 1, 11, 101, 1001, 10001, 100001 …, qui dans les décadiques a pour limite 1 ! (Le 1 de devant part à l'infini et disparaît...)

Question 9 (difficile) – *Montrer que l'ensemble des nombres décadiques (y compris les entiers ordinaires) est compact.*

C'est joli, mais à quoi ça sert ?

2.4 Les diviseurs de zéro

Vous avez sans doute déjà remarqué que, si on prend deux nombres a et b se terminant par 2 et 5, leur produit se terminera par un 0. En fouillant un peu, on peut trouver des nombres de trois chiffres dont le produit se termine par trois zéros (par exemple, $\ldots 625 \times \ldots 112 = \ldots 000$), etc.

Définition 6 – *On appelle* diviseurs de zéro *deux nombres non nuls dont le produit est nul.*

Dans les nombres ordinaires, il n'y a pas de diviseurs de 0.

Question 10 – *Peut-on trouver deux nombres décadiques non nuls dont le produit fasse* 0 *?*

(Indice : remarquer que 10^n tend vers 0, que $10 = 2 \times 5$ et utiliser la compacité.)

3 Le problème de la division : fin

On a vu ci-dessus qu'il était impossible en général de diviser en décadiques par certains nombres, par exemple par 2 ou par 5.

Et pourtant, tout le monde sait que $1/2 = 0,5$ et $1/5 = 0,2...$ on aurait bien envie de les rajouter.

Faisons-le.

Définition 7 – *On appelle* nombre décadique à virgule *un nombre ayant une infinité de chiffres à gauche de la virgule, et un nombre fini de chiffres à droite de la virgule.*

(On est obligé de se limiter à un nombre fini de chiffres à droite, sinon on a déjà vu qu'on aura des problèmes pour définir la multiplication, et qu'en plus on risque de se retrouver avec deux nombres différents égaux à 1/3...)

Maintenant, on a le droit de diviser par 2 ou par 5.

Question 11 – *Montrer qu'en décadiques à virgule, on peut diviser par n'importe quel entier ordinaire.*

(Penser qu'un nombre se décompose en facteurs premiers.)

Question 12 – *Dire quels sont les décadiques qui ont un inverse en décadiques à virgule. Dire comment trouver leur inverse, s'il existe.*

Attention : pas tous !

On rappelle qu'un anneau est un ensemble sur lequel on a les opérations ordinaire d'addition, de soustraction et de multiplication, avec les règles habituelles (mais pas forcément la division).

Question 13 – *Montrer que dans un anneau, un diviseur de zéro ne peut jamais avoir d'inverse.*

Si donc vous avez répondu « tous » à la question précédente et que vous avez construit des diviseurs de 0 auparavant, vous avez dit des bêtises.

Pour inverser 2 et 5, on avait simplement rajouté $0,2$ et $0,5$. Mais la question précédente montre qu'on ne peut pas faire pareil pour les diviseurs de zéro : *quelle que soit la manière dont on essaie de rajouter des nouveaux nombres, on n'arrivera jamais à leur trouver des inverses* (à moins de tomber sur une contradiction).

4 Et dans les autres bases ?

On a travaillé en base 10, et on a remarqué tout le long que 2 et 5 nous emmmbêtaient.

On peut essayer d'écrire les nombres en base p (c'est-à-dire qu'un nombre tel que 1234 signifiera $1 \times p^3 + 2 \times p^2 + 3 \times p + 4$ au lieu de $1 \times 1000 + 2 \times 100 + 3 \times 10 + 4$).

Cela fera peut-être disparaître le problème des 2 et des 5...

Définition 8 – *Un entier p-adique est un nombre avec une infinité de chiffres à gauche. Un nombre p-adique à virgule est un nombre avec une infinité de chiffres à gauche, et un nombre fini de chiffres à droite de la virgule.*

Les entiers p-adiques sont notés $\mathbb{Z}_p$. Les p-adiques à virgule sont notés $\mathbb{Q}_p$.

Vérifier la multiplication suivante en base 7 :

$$\begin{array}{rr} & \ldots 254125413_7 \\ \times & 5_7 \\ \hline & \ldots 000000001_7 \end{array}$$

et donc en base 7, l'inverse de 5 est $\ldots 254125413$. Maintenant, 5 a donc un inverse.

On peut reprendre toutes les questions précédentes. Ce qui est très important est que les réponses ne sont pas les mêmes en fonction de p : cela veut dire que les nombres qu'on obtient en autorisant une infinité de chiffres à gauche dépendent de la base dans laquelle on écrit !

Question 14 – *Vérifier que l'addition, la multiplication, la soustraction ne posent pas de problèmes en p-adiques.*

On a donc des anneaux.

Remarquer qu'en base p, l'inverse de p s'écrit simplement $0,1$ dans les p-adiques à virgule : de même que $p \times 10 = 100$ en base p, on a $p \times 0,1 = 1$, autrement dit $0,1 = 1/p$.

Question 15 – *En base p, quels nombres ont des inverses dans $\mathbb{Z}_p$? Et dans $\mathbb{Q}_p$?*

Là encore, il est utile de remarquer que pour savoir diviser par tous les nombres ordinaires, il suffit de savoir diviser par tous les nombres premiers !

Question 16 – *Pour quels p les nombres p-adiques comprennent-ils des diviseurs de 0 ?*

Question 17 – *Conclure de la question précédente que les nombres p-adiques $\mathbb{Q}_p$ ne sont pas tous les mêmes pour tous les p.*

Définition 9 (Corps) – *Quand dans un anneau, tous les éléments (sauf bien sûr 0) ont des inverses, on dit qu'on a un* corps.

Remarquer que les p-adiques sans virgule ne sont pas un corps, parce que p lui-même n'y est jamais inversible (son inverse, c'est toujours $0,1$).

L'étude des corps en général est l'un des domaines les plus importants des mathématiques. Il existe des centaines de théorèmes sur le sujet, et on en découvre de nouveaux chaque année.

Question 18 – *D'après les questions précédentes, pour quels nombres p l'ensemble $\mathbb{Q}_p$ est-il un corps ?*

Souvent, l'ensemble $\mathbb{Q}_p$ est plus facile à traiter que l'ensemble $\mathbb{R}$ des nombres réels. C'est pourquoi, souvent, on essaie de résoudre des problèmes (par exemple des équations) dans $\mathbb{Q}_p$ et, s'il y a des solutions dans $\mathbb{Q}_p$, on essaie de les transférer dans $\mathbb{R}$.