Les p-adiques au lycée

Bernard Le Stum

Université de Rennes 1

Version du 5 novembre 2012

Qu'est-ce qu'un nombre ?

On sait que « trois écureuils », ce n'est pas pareil que « quatre écureuils ». Ce n'est pas non plus la même chose que « trois brosses à dent ». Pourtant, même si la notion d' « écureuil » et celle de « brosse à dent » n'ont rien en commun, on voit que « trois écureuils » et « trois brosses à dent » partagent une caractéristique commune (en plus d'avoir des poils ☺). On dégage ainsi le concept de nombre ; le nombre 3 en l'occurrence. C'est un concept mathématique. Comme la vérité, par exemple, est un concept philosophique.

Les humains primitifs ne disposaient pas vraiment du concept de nombre, faisant seulement parfois la différence entre « un », « deux » et « plusieurs ». Les bébés ou certains animaux font aussi la différence entre « un », « deux » et « plusieurs », mais la confusion arrive ensuite assez vite.

. . . / . . .

Les nombres entiers

L'école de Pythagore, au VIe siècle avant J-C, place les entiers naturels non nuls

$$1, 2, 3, 4, 5, \dots$$

au centre de leur philosophie (ils commençaient en fait à compter à partir de 2 ou 3). Le 0 n'est ajouté que par les indiens au Ve siècle après JC. Les nombres négatifs n'apparaissent eux qu'à l'époque moderne. On considère maintenant l'ensemble de tous les entiers relatifs

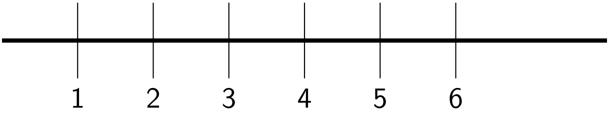
$$\mathbf{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

C'est un anneau : cela signifie que l'on peut ajouter, soustraire et multiplier les entiers relatifs entre eux (mais pas toujours les diviser). Et que les règles auxquelles on s'attend s'appliquent.

$\dots / \dots$

Du discret au continu

Depuis toujours, les bergers doivent « compter » leurs moutons afin de s'assurer de bien ramener le soir tous ceux qu'ils ont emmenés le matin. En fait, ils n'ont pas besoin pour cela de savoir compter. Il leur suffit de faire une entaille sur un bout de bois pour chaque mouton qui entre dans le pré le matin. Et de passer ensuite le doigt sur les entailles au fur et à mesure que les moutons en sortent le soir.

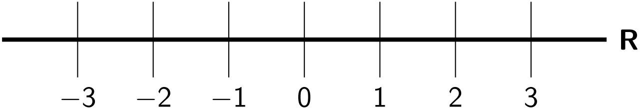


Le bout de bois représente le continu et les entailles le discret (les paradoxes de Xenon sur le continu et le discret ont mis à mal l'école pythagoricienne : Achille et la tortue par exemple – autre débat).

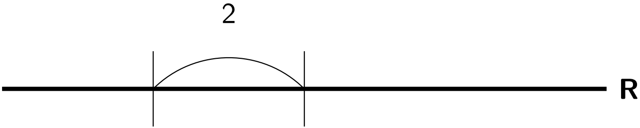
. . . / . . .

Compter ou mesurer

On peut ainsi placer tous les entiers sur la droite réelle :



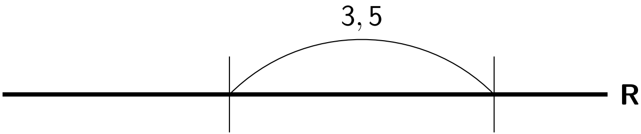
Sur la droite, on ne peut pas vraiment « compter ». On peut seulement mesurer la distance entre deux points. On introduit pour cela les nombres réels, qui sont parfois entiers :

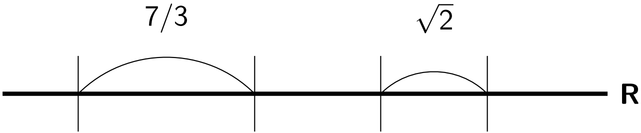


. . . / . . .

Les nombres réels

mais pas tout le temps :





Les nombres réels forment un corps $\mathbf{R}$: on peut les ajouter, les soustraire, les multiplier et les diviser. Il faut bien sûr choisir un sens sur la droite pour mettre des signes.

Les nombres décimaux

Les nombres entiers comme les nombres réels existent indépendemment de leur représentation. Les romains utilisaient un système complexe de lettres majuscules pour représenter les entiers (XLVII pour 47 par exemple). Il aura fallu des siècles pour arriver à ce qu'on appelle la numérotation de position.

Il s'agit d'écrire les entiers naturels comme somme de puissances de 10 :

$$3103 = 3 \times 1000 + 1 \times 100 + 0 \times 10 + 3 \times 1.$$

On introduit les nombres décimaux en autorisant les puissances négatives :

$$18,11 = 1 \times 10 + 8 \times 1 + 1 \times \frac{1}{10} + 1 \times \frac{1}{100}.$$

Quitte à signer les nombres, on obtient ainsi un nouvel anneau $\mathbf{D}$. Mais on ne peut pas toujours diviser dans $\mathbf{D}$ ($\frac{1}{3}$ n'est pas dans $\mathbf{D}$ par exemple).

Notion de base

Si on avait 7 doigts au lieu de 10, on utiliserait probablement un système à 7 chiffres. On écrirait les entiers naturels comme sommes finies

$$n = \cdots + a \times 343 + b \times 49 + c \times 7 + d \times 1$$

avec $a, b, c, \ldots$ entre 0 et 6. C'est un peu ce que font les ordinateurs qui n'ont que 2 doigts ☺, c'est à dire 2 chiffres 0 et 1. En fait, si on fixe un entier naturel $p \geq 2$, on peut toujours écrire tout entier naturel n comme somme finie

$$n = \cdots + a \times p^3 + b \times p^2 + c \times p + d \times 1$$

avec $a, b, c, \ldots$ strictement plus petits que p. Par exemple, si $p = 2$ et $n = 9$, on aura

$$9 = 1 \times 8 + 0 \times 4 + 0 \times 2 + 1 \times 1$$

Et donc 9 s'écrit donc 1001 en binaire. Les babyloniens utilisaient la base 60 et sur internet, on utilise souvent a base 16 (clés WEP par exemple).

Des « décimaux » en base p

Fixons un entier $p \geq 2$ (pensez à $p = 10$ ou $p = 7$ ou $p = 2$ par exemple). On peut considérer les nombres qui s'écrivent comme somme finie

$$x = \cdots + a \times p^2 + b \times p + c \times 1 + d \times \frac{1}{p} + e \times \frac{1}{p^2} + \cdots$$

ou $a, b, c, \ldots$ sont des entiers naturels strictement inférieurs à p (comme on a déjà fait avec $p = 10$). Quitte à signer les nombres, on obtient de nouveau un anneau $\mathbf{D}_p$.

Considérons par exemple le nombre décimal $x = 1,625$. On a

$$x = 1 + \frac{1}{2} + \frac{1}{8}$$

et notre nombre x s'écrit donc $1,101$ en binaire.

$\ldots / \ldots$

Développement des nombres réels

N'importe quel nombre réel peut s'écrire avec une infinité de décimales

$$\frac{1}{3} = 0,3333\ldots, \quad \sqrt{2} = 1,4142\ldots \quad \text{ou} \quad \pi = 3,14159\ldots$$

Inversement, on peut placer n'importe quel nombre avec une infinité de décimales sur la droite réelle. Tout réel positif s'écrit donc comme somme éventuellement infinie à droite

$$\cdots + a_2 \times 100 + a_1 \times 10 + a_0 + a_{-1} \times \frac{1}{10} + a_{-2} \times \frac{1}{100} + \cdots$$

ou les a_i sont des entiers naturels entre 0 et 9.

Ceci reste valable si on remplace 10 par un autre entier naturel $p \geq 2$. Par exemple,

$$\frac{1}{3} = \frac{1}{4} + \frac{1}{16} + \frac{1}{64} + \cdots$$

s'écrit donc $0,0101010\ldots$ en base 2 dans $\mathbf{R}$.

Construction des nombres réels

Oublions un moment que l'on sait ce qu'est un nombre réel. Fixons un entier naturel $p \geq 2$. On considère toutes les expressions éventuellement infinies à droite

$$\cdots + a_2 \times p^2 + a_1 \times p + a_0 + a_{-1} \times \frac{1}{p} + a_{-2} \times \frac{1}{p^2} + \cdots$$

ou les a_i sont des entiers naturels strictement inférieurs à p.

On peut faire des opérations sur ces nombres en opérant sur la partie gauche des nombres.

Prenons par exemple $p = 10$ et calculons x^2 pour $x = 1,4142\ldots$. On fait

$$(1,4)^2 = 1,96 \quad \text{puis} \quad (1,414)^2 = 1,999396 \quad \text{etc.}$$

pour trouver $1,999999\ldots$ que l'on identifie avec 2. On a donc $x^2 = 2$.

Quitte à signer les nombres, on construit ainsi le corps $\mathbf{R}$ nombres réels.

Les nombres p-adiques

On fixe toujours $p \geq 2$ et on considère l'ensemble $\mathbf{Q}_p$ de toutes les expressions éventuellement infinies à gauche

$$\cdots + a_2 \times p^2 + a_1 \times p + a_0 \times 1 + a_{-1} \times \frac{1}{p} + a_{-2} \times \frac{1}{p^2} + \cdots$$

ou les a_i sont des entiers naturels strictement inférieurs à p.

On définit les opérations en opérant sur les parties droite des nombres. Prenons par exemple $p = 10$ et calculons x^2 pour $x = \ldots 9999999999$. On fait

$$(99)^2 = 9801 \quad \text{puis} \quad (9999)^2 = 99980001 \quad \text{etc.}$$

pour trouver $\ldots 000001$ que l'on identifie avec 1. Donc, $x^2 = 1$. On peut aussi calculer $x + 1 = 0$ si bien qu'en fait, $x = -1$.

On obtient donc ainsi l'ensemble $\mathbf{Q}_p$ des nombres p-adiques. Ceux qui n'ont pas de virgule sont les entiers p-adiques dont l'ensemble se note $\mathbf{Z}_p$.

. . . / . . .

Les entiers p-adiques

$\mathbf{Z}_p$ est donc l'ensemble des expressions éventuellement infinies à gauche

$$\cdots + a_3 \times p^3 + a_2 \times p^2 + a_1 \times p + a_0 \times 1$$

ou les a_i sont des entiers naturels strictement inférieurs à p. Par exemple, pour $p = 2$, on trouve toutes les suites infinies à gauche de 0 et de 1.

En fait, $\mathbf{Z}_p$ est un anneau. En particulier, tous les nombres ont un opposé dans $\mathbf{Z}_p$. Par exemple, on a vu que

$$-1 = \ldots 99999999999 \text{ dans } \mathbf{Z}_{10}.$$

On peut souvent diviser dans $\mathbf{Z}_p$. Par exemple, on a

$$\frac{1}{3} = \ldots 10101011 \text{ dans } \mathbf{Z}_2 \quad \text{(exercice)}.$$

Mais on a aussi

$$\pm\sqrt{2} = \ldots 213 \text{ et } \ldots 454 \text{ dans } \mathbf{Z}_7 \quad \text{(exercice)}.$$

La valuation p-adique

La valuation p-adique $v_p(x)$ d'un nombre x est le nombre de zéros à droite dans l'écriture de x en base p si x est entier ou l'opposé du nombre de chiffres après la virgule si x est « décimal ».

Formellement, si on écrit

$$x = \cdots + a_2 \times p^2 + a_1 \times p + a_0 \times 1 + a_{-1} \times \frac{1}{p} + \cdots + a_r \times \frac{1}{p^r}$$

avec $a_r \neq 0$, on aura $v_p(x) = r$.

Par exemple, on a $v_{10}(2400) = 2$ et $v_{10}(1,625) = -3$.

Mais on peut aussi calculer $v_2(2400) = 5$ et $v_2(1,625) = -3$. En effet, en binaire, le nombre décimal 2400 s'écrit 100101100000 et le nombre décimal $1,625$ s'écrit $1,101$.

$\cdots / \cdots$

La valeur absolue p-adique

Si $x \in \mathbf{Q}_p$, la valeur absolue p-adique de x est

$$|x|_p = \frac{1}{p^{v_p(x)}}.$$

Si $x, y \in \mathbf{Q}_p$, la distance p-adique entre x et y est

$$d_p(x, y) = |x - y|_p.$$

Par exemple, $7 \times 11 \times 13$ est 10-adiquement proche de 1 car

$$d_{10}(7 \times 11 \times 13, 1) = |1000|_{10} = \frac{1}{10^3} = 0,001.$$

Ou encore, 3100 est 2-adiquement proche de 28. On peut calculer

$$d_2(3100, 28) = |3100 - 28|_2 = |3072|_2 = \frac{1}{1024} \simeq 0,001$$

car $3072 = 3 \times 2^{10}$ si bien que $v_2(3072) = 10$ et $2^{10} = 1024$.

Géométrie p-adique

Comme on dispose d'une distance sur les nombres p-adiques, on peut faire de la géométrie p-adique.

Théorème

La valeur absolue p-adique satisfait l'inégalité ultramétrique

$$|x+y|_p \leq \max(|x|_p, |y|_p).$$

Conséquence : pour tout x, y, z, on a :

$$d_p(x,z) \leq \max(d_p(x,y), d_p(y,z)).$$

Ça veut dire que, « dans un triangle la longueur d'un côté quelconque est toujours plus petite que (ou égale à) la longueur d'un des autres côtés ».

Géométrie p-adique, suite

On peut démontrer des résultats déconcertants en géométrie p-adique :

Théorème

Tous les triangles sont isocèles.

Démonstration.

Notons a, b, c les longueurs des côtés du triangle. On peut supposer que a est plus petit que (ou égal à) b. L'inégalité ultramétrique nous dit que c est plus petit que a ou plus petit que b. De toutes façons, comme a est plus petit que b, c sera plus petit que b. Donc, le maximum de a et c est plus petit que b. Mais l'inégalité ultramétrique nous dit qu'il est aussi plus grand que b : il doit être égal à b. Il y a donc bien deux côtés qui ont même longueur. $\square$

Géométrie p-adique, fin

On peut faire encore pire :

Théorème

N'importe quel point d'un disque est au centre du disque.

Démonstration.

Soit y un point du disque $D(x, a)$ de centre x et de rayon a. Alors, la distance de x à y est plus petite que a. Si z est un point quelconque du disque $D(x, a)$, alors la distance de x à z sera aussi plus petite que a. Et l'inégalité ultramétrique implique que la distance de y à z est plus petite que a. Ça veut dire que z est dans le disque $D(y, a)$ de centre y et de rayon a. Symétriquement, si z est un point quelconque du disque $D(y, a)$, alors z est dans le disque $D(x, a)$. Les deux disques sont donc identiques. Et y est donc « un » centre du disque $D(x, a)$. $\square$

p pour premier...

Un entier naturel est dit premier s'il a exactement 2 diviseurs : 1 et lui même. Les nombre premiers sont donc

$$2, 3, 5, 7, 11, 13, \ldots$$

(utiliser le crible d'Erathostène pour les trouver « tous »).

Si p est un nombre premier, alors $\mathbf{Q}_p$ est un corps. Mais c'est faux en général. Par exemple, on peut trouver deux entiers 10-adiques non nuls dont le produit est nul :

$$\cdots 112 \times \cdots 125 = \cdots 000.$$

On ne peut donc pas diviser par ces nombres dans $\mathbf{Q}_{10}$.

Pour résumer, si p est premier, on peut diviser dans $\mathbf{Z}_p$ par tous les entiers qui ne sont pas multiple de p ; et dans $\mathbf{Q}_p$, par tous les nombres non nuls.

$\ldots / \ldots$

Les nombres rationnels

Les nombres qui s'écrivent sous la forme $x = \frac{m}{n}$, où m et n sont des entiers relatifs et $n \neq 0$, forment le corps des nombres rationnels

$$\mathbf{Q} := \{0, 1, -1, 2, -2, \frac{1}{2}, -\frac{1}{2}, 3, -3, \frac{1}{3}, -\frac{1}{3}, \frac{2}{3}, -\frac{2}{3} \ldots\}$$

(on peut toujours diviser dans $\mathbf{Q}$). On remarque que $\mathbf{Q}$ contient toujours $\mathbf{D}_p$ (et en particulier tous les nombres décimaux) et est contenu dans $\mathbf{R}$ et dans $\mathbf{Q}_p$. Mais la réciproque n'est pas vraie :

Exemple ($\sqrt{2} \notin \mathbf{Q}$)

Supposons que $\sqrt{2} = \frac{m}{n}$ où m, n sont deux entiers naturels, c'est à dire $m = \sqrt{2} \times n$. En élevant au carré, on trouve que $m^2 = 2n^2$. On voit donc que m^2 est pair si bien que m est pair, disons $m = 2r$. On a donc $4r^2 = 2n^2$, et en simplifiant, on trouve $n^2 = 2r^2$ si bien que n^2 est pair. Et donc n est pair, c'est à dire $n = 2s$. On a donc $\sqrt{2} = \frac{2r}{2s} = \frac{r}{s}$ avec $r < m$ et $s < n$. Et ainsi de suite. Contradiction.

$\ldots / \ldots$

Un résultat global

Théorème (du produit)

Si x est un nombre rationnel, le produit de toutes les valeurs absolues de x est égal à 1.

En fait, il s'agit de faire le produit de toutes les valeurs absolues p-adiques pour p premier, et de la valeur absolue habituelle (dite archimédienne).

Prenons par exemple $x = -6,3$. On a bien sûr $|x| = 6,3$. On calcule $|x|_2 = 2$, $|x|_3 = \frac{1}{9}$, $|x|_5 = 5$, $|x|_7 = \frac{1}{7}$ et $|x|_p = 1$ sinon. Et on a bien

$$6,3 \times 2 \times 5 \times \frac{1}{9} \times \frac{1}{7} = 1.$$

Conséquence : pour étudier la valeur absolue archimédienne d'un nombre, il suffit de connaître ses valeurs absolues p-adiques.

– Merci à vous –