Les nombres p-adiques

Nicolas Billerey

Laboratoire de mathématiques Blaise Pascal
Université Clermont Auvergne

Jeudi 13 février 2020

Sommaire

Sommaire

Bases

- Il est d'usage d'utiliser la base 10 (système décimal) pour représenter les entiers naturels.
- Il n'en a pas toujours été ainsi : diverses civilisations ont employé des bases différentes pour compter (Babyloniens, Mayas, Aztèques,...).
- Aujourd'hui encore les ordinateurs utilisent la base 2 (système binaire) et la base 60 (système sexigésimal) est utile dans les mesures de temps.

Compter en base b

- Comment s'écrivent en base $b = 5$ les nombres suivants ?

$$7,\ 23,\ 73,\ 97,\ 456.$$

- Réponse :

$$7 = \underline{12}_5,\ 23 = \underline{43}_5,\ 73 = \underline{243}_5,\ 97 = \underline{342}_5,\ 456 = \underline{3311}_5.$$

- On dit que

$$1 + 1 \times 5 + 3 \times 5^2 + 3 \times 5^3 = \underline{3311}_5$$

  est le développement 5-adique de 456.

- Calculer en base 5 (sans convertir en base 10 !) :

$$\underline{243}_5 + \underline{342}_5 = \underline{1140}_5 \quad \text{et} \quad \underline{12}_5 \times \underline{43}_5 = \underline{1121}_5.$$

  On vérifie qu'on a bien $\underline{1140}_5 = 170$ et $\underline{1121}_5 = 161$.

Développement 5-adique de -1 ?

On calcule

$$\begin{aligned}
-1 &= 4 + (-1) \times 5 \\
&= 4 + (4 + (-1) \times 5) \times 5 \\
&= 4 + 4 \times 5 + (-1) \times 5^2 \\
&= 4 + 4 \times 5 + (4 + (-1) \times 5) \times 5^2 \\
&= 4 + 4 \times 5 + 4 \times 5^2 + (-1) \times 5^3 \\
&= \dots \\
&= 4 + 4 \times 5 + 4 \times 5^2 + 4 \times 5^3 + 4 \times 5^4 + \dots
\end{aligned}$$

Ainsi,

$$-1 = \underline{\dots 44444}_5 = \sum_{n=0}^{\infty} 4 \times 5^n.$$

? ? ? ?

Les nombres 5-adiques

- On considère l'ensemble

$$\mathbb{Z}_5 = \left\{ \ldots a_3 a_2 a_1 a_0 \mid 0 \leq a_i < 5, \text{ pour tout } i \geq 0 \right\}$$

  de tous les entiers 5-adiques.
- On peut addtionner, soustraire et multiplier deux éléments de $\mathbb{Z}_5$ pour en former un troisième, avec les règles de calcul habituelles.
- L'ensemble $\mathbb{Z}_5$ forme donc un anneau qui contient $\mathbb{Z}$.
- Pour diviser, c'est plus compliqué...

Décomposer un entier 5-adique

- Soit $x = \ldots a_3 a_2 a_1 a_0 = \sum_{n \geq 0} a_n 5^n \in \mathbb{Z}_5$ un entier 5-adique.
- On décompose x ainsi :

$$x = \underbrace{\underbrace{\underbrace{a_0}_{x_1} + a_1 \times 5}_{x_2} + a_2 \times 5^2}_{x_3} + \cdots$$

de sorte que pour tout $n \geq 1$, on a

$$x_n = a_0 + a_1 \times 5 + \cdots + a_{n-1} \times 5^{n-1}.$$

- Les entiers $(x_n)_{n \geq 1}$ vérifient, pour tout $n \geq 1$:

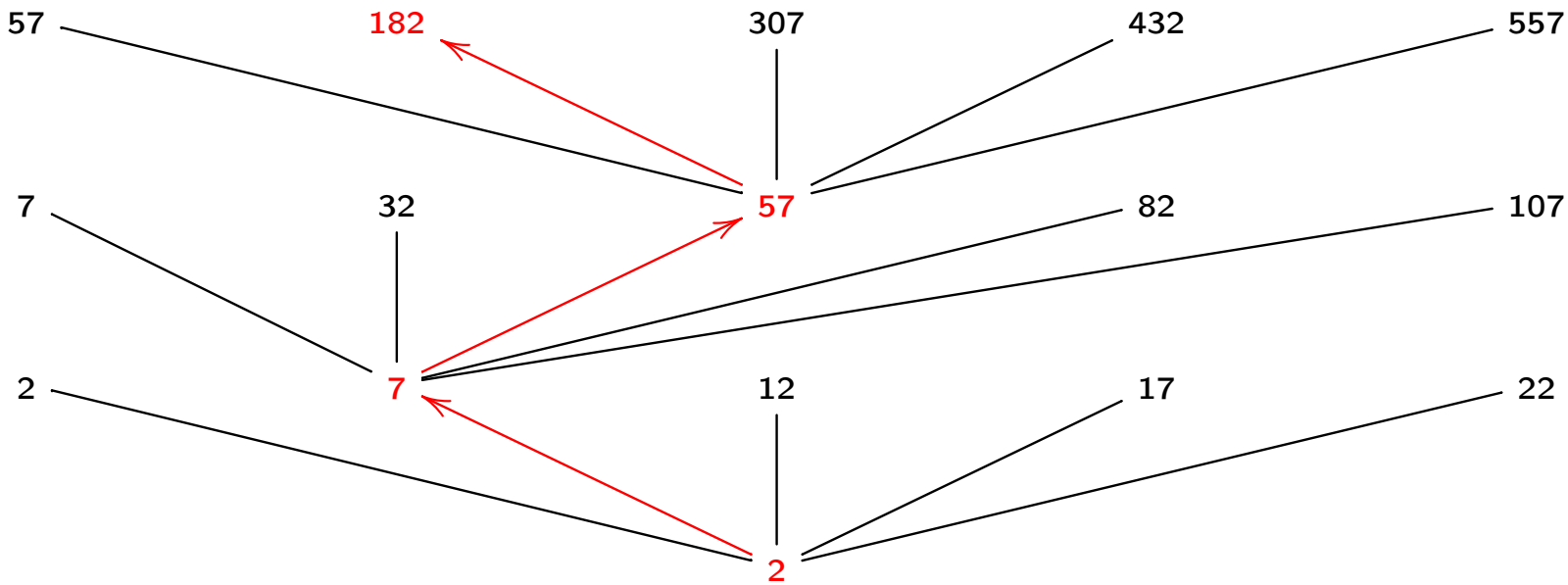
$$0 \leq x_n < 5^n \quad \text{et} \quad x_{n+1} \equiv x_n \pmod{5^n}.$$

Représenter un entier 5-adique

L'entier 5-adique

$$x = \ldots 14114214043404231402233243121 2$$
$$= 2 + 1 \times 5 + 2 \times 5^2 + 1 \times 5^3 + 3 \times 5^4 + \cdots$$

vérifie $(x_n)_{n\geq 0} = (2,\ 7,\ 57,\ 182,\ 2057, \ldots)$ et se représente ainsi :



Entiers 5-adiques et congruences

- Réciproquement, toute suite $(x_n)_{n\geq 1}$ d'entiers vérifiant :

$$0 \leq x_n < 5^n \quad \text{et} \quad x_{n+1} \equiv x_n \pmod{5^n}, \text{ pour tout } n \geq 1,$$

définit un unique entier 5-adique $x = \ldots a_3 a_2 a_1 a_0$.

- Il suffit de poser

$$a_0 = x_1, \; a_1 = \frac{x_2 - x_1}{5}, \; \ldots, \; a_n = \frac{x_{n+1} - x_n}{5^n}, \; \ldots$$

- On en déduit que $\mathbb{Z}_5$ s'identifie (comme anneau) à

$$\varprojlim_n \mathbb{Z}/5^n\mathbb{Z} = \left\{ (x_n)_{n\geq 1} \in \prod_{n\geq 1} \mathbb{Z}/5^n\mathbb{Z} \mid x_{n+1} \equiv x_n \pmod{5^n}, \forall n \geq 1 \right\}.$$

Digression : pourquoi 5 et pas 10 ?

- On aurait pu considérer

$$\begin{aligned}\mathbb{Z}_{10} &= \left\{ \dots a_3 a_2 a_1 a_0 \mid 0 \leq a_i \leq 9, \text{ pour tout } i \geq 0 \right\} \\ &= \left\{ (x_n)_{n\geq 1} \in \prod_{n\geq 1} \mathbb{Z}/10^n\mathbb{Z} \mid x_{n+1} \equiv x_n \pmod{10^n}, \forall n \geq 1 \right\}\end{aligned}$$

  (ou $\mathbb{Z}_2$) au lieu de $\mathbb{Z}_5$.

- Or, pour tout $n \geq 1$, on a, par le lemme chinois,

$$\mathbb{Z}/10^n\mathbb{Z} \simeq \mathbb{Z}/2^n\mathbb{Z} \times \mathbb{Z}/5^n\mathbb{Z}.$$

- On en déduit en particulier que

$$\mathbb{Z}_{10} \simeq \mathbb{Z}_2 \times \mathbb{Z}_5$$

  n'est pas intègre (i.e. il existe des couples d'éléments non nuls dont le produit fait 0).

Division dans $\mathbb{Z}_5$

- Un entier 5-adique $x = (x_n)_{n\geq 1}$ est inversible dans $\mathbb{Z}_5$ si et seulement si, pour tout $n \geq 1$, x_n est inversible dans $\mathbb{Z}/5^n\mathbb{Z}$.
- On en déduit que les éléments inversibles de $\mathbb{Z}_5$ sont précisément ceux qui ne sont pas multiples de 5 dans $\mathbb{Z}_5$:

$$\mathbb{Z}_5^\times = \mathbb{Z}_5 \setminus 5\mathbb{Z}_5.$$

- Par exemple, 3 est inversible dans $\mathbb{Z}_5$ d'inverse

$$\frac{1}{3} = \ldots 3131313132 = 2 + 3 \times 5 + 1 \times 5^2 + 3 \times 5^3 + \cdots$$

- En particulier, l'anneau $\mathbb{Z}_5$ est intègre.

Des entiers aux fractions

- On construit le corps $\mathbb{Q}_5$ des nombres 5-adiques à partir de (l'anneau intègre) $\mathbb{Z}_5$ comme on construit $\mathbb{Q}$ à partir de (l'anneau intègre) $\mathbb{Z}$.
- Tout nombre 5-adique s'écrit donc avec une infinité de chiffres avant la virgule et un nombre fini après !
- Par exemple,

$$x = \ldots 3412043212123001,2104 \in \mathbb{Q}_5.$$

Sommaire

Valuation p-adique

- Tout ce qui a été vu avec 5 se généralise avec p premier quelconque.
- En particulier, on a

$$\mathbb{Z}_p = \left\{(x_n)_{n\geq 1} \in \prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z} \mid x_{n+1} \equiv x_n \pmod{p^n}, \forall n \geq 1\right\}$$

et tout élément x de $\mathbb{Q}_p$ s'écrit de façon unique

$$x = p^N y \quad \text{avec } y \in \mathbb{Z}_p \setminus p\mathbb{Z}_p.$$

- L'entier N s'appelle la valuation de x ; on note $N = v_p(x)$.
- Par exemple, on a

$$v_5(45/11) = 1, \ v_5(\ldots 140142233211, 231041) = -6, \ v_5(8) = 0.$$

Valuation p-adique et distance

- La valuation p-adique vérifie pour tous $x, y \in \mathbb{Q}_p$:
  1. $v_p(0) = -\infty$;
  2. $v_p(xy) = v_p(x) + v_p(y)$;
  3. $v_p(x+y) \geq \min(v_p(x), v_p(y))$.
- On voudrait rendre compte du fait que

$$p^n \xrightarrow[n \to +\infty]{} 0 \quad \text{lorsque } n = v_p(p^n) \to +\infty.$$

- La fonction distance associée devra notamment vérifier

$$|xy|_p = |x|_p |y|_p, \quad \text{quels que soient } x, y \in \mathbb{Q}_p.$$

- Quelle fonction transforme les sommes en produits ?

$\mathbb{Q}_p$ est ultramétrique

- Pour tout $x \in \mathbb{Q}_p$, on pose

$$|x|_p = p^{-v_p(x)}.$$

- La fonction $|\cdot|_p$ est une distance. En particulier, on a :

$$|x|_p = 0 \Leftrightarrow x = 0 \quad \text{et} \quad |xy|_p = |x|_p |y|_p.$$

- Elle vérifie de plus l'inégalité ultramétrique :

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

plus forte que l'inégalité triangulaire !

Topologie dans $\mathbb{Q}_p$

- Deux points de $\mathbb{Q}_p$ sont d'autant plus proches que leur différence est multiple de p.
- Deux boules de $\mathbb{Q}_p$ sont disjointes ou concentriques !
- Chaque point d'une boule en est son centre !
- Tous les triangles sont isocèles !
- Une série à coefficients dans $\mathbb{Q}_p$ converge si et seulement si son terme général tend vers 0 !

Digression : $\mathbb{R}$ et les $\mathbb{Q}_p$

- On aurait pu construire $\mathbb{Q}_p$ par un procédé analogue à celui utilisé pour construire $\mathbb{R}$ à partir de $\mathbb{Q}$:

$$\mathbb{Q}_p = \mathcal{C}(\mathbb{Q}, |\cdot|_p)/\sim,$$

où $\mathcal{C}(\mathbb{Q}, |\cdot|_p)$ désigne l'ensemble des suites de Cauchy de $\mathbb{Q}$ pour la distance p-adique et

$$(x_n) \sim (y_n) \text{ si } (x_n) - (y_n) \text{ converge } (p\text{-adiquement}) \text{ vers } 0.$$

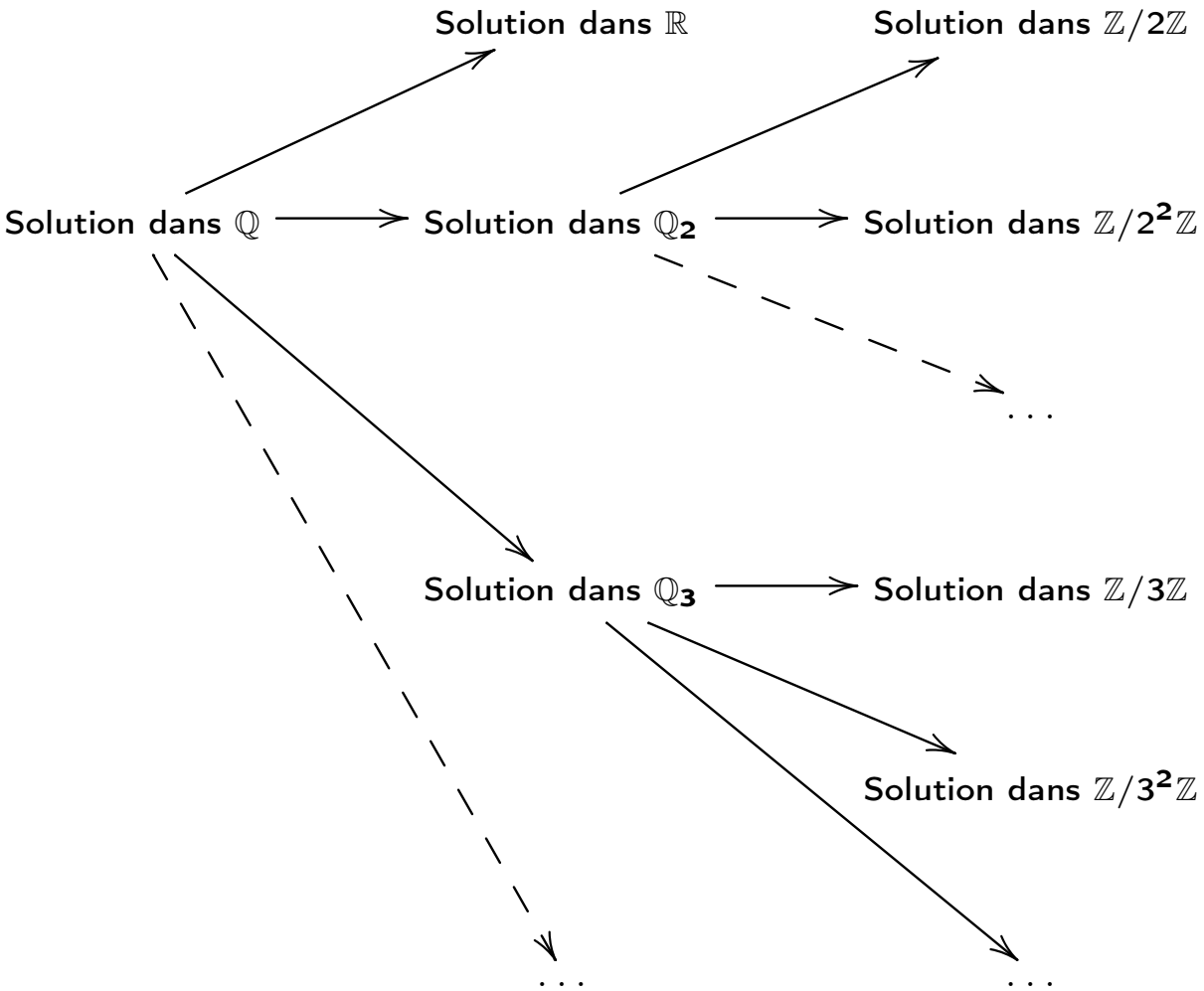
- Ainsi construit, $\mathbb{Q}_p$ est automatiquement un espace complet.
- Un théorème d'Ostrowski affirme que $\mathbb{R}$ et les corps $\mathbb{Q}_p$ avec p premier, forment tous les complétés de $\mathbb{R}$.

Sommaire

Le principe « local-global »

Le principe « local-global » interroge la possibilité de montrer qu'une équation polynomiale donnée admet, ou non, une solution rationnelle en étudiant ses solutions dans $\mathbb{R}$ et chacun des $\mathbb{Q}_p$.

Sens direct : du global au local



Un cas concret

- Vérifions par ce procédé que l'équation

$$x^2 - x - 1 = 0$$

n'a pas de solution rationnelle (ce que l'on sait être le cas !).

- Une telle solution donnerait lieu à un couple $(a, b) \in \mathbb{Z}^2$ tel que $\mathrm{pgcd}(a, b) = 1$ et

$$a^2 - ab - b^2 = 0.$$

- D'où, si b est impair, $a^2 - a - 1 \equiv 0 \pmod 2$ et une contradiction, et de même si a est impair.
- On dit que cette équation présente une obstruction locale (en 2).

Sens réciproque : des solutions approchées aux solutions exactes

- On veut construire une solution exacte à partir d'approximations successives.
- En analyse classique, on dispose de la méthode de Newton.
- Son analogue p-adique s'appelle le lemme de Hensel.

Lemme de Hensel : cas concret

- On cherche une solution $x = \ldots a_4 a_3 a_2 a_1 a_0 \in \mathbb{Z}_5$ à l'équation

$$x^2 + 1 = 0.$$

- On pose $a_0 = 2$ (l'autre choix serait $a_0 = 3$).
- Si x est solution, on a

$$(a_0 + a_1 \times 5)^2 + 1 \equiv 0 \pmod{5^2} \iff a_1 \times 5 \equiv -\frac{a_0^2 + 1}{2 \times a_0} \pmod{5^2}$$
$$\iff a_1 = 1.$$

- Plus généralement, x_{n+1} s'obtient à partir de x_n par la formule

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}, \quad \text{où } f(x) = x^2 + 1 \text{ et } x_n = a_0 + \cdots + a_{n-1} \times 5^{n-1}.$$

- On obtient $x = \ldots 141142140434042314022332431212$.

Sens réciproque : du local au global

L'existence de solutions dans $\mathbb{R}$ et dans chacun des corps $\mathbb{Q}_p$ suffit-elle à assurer de l'existence d'une solution rationnelle ?

Théorème (Hasse–Minkowski)

Toute forme quadratique

$$q(X_1, \ldots, X_n) = \sum_{i \leq j} a_{i,j} X_i X_j$$

à coefficients rationnels représente 0 dans $\mathbb{Q}$ si et seulement si tel est le cas dans $\mathbb{R}$ et dans chacun des $\mathbb{Q}_p$ avec p premier.

Contre-exemple au principe de Hasse

- Le théorème de Hasse–Minkowski ne s'étend pas aux formes de degré > 2.
- Selmer a montré que l'équation cubique

$$3x^3 + 4y^3 + 5z^3 = 0$$

n'admet aucune solution rationnelle (non nulle) mais a des solutions dans $\mathbb{R}$ et dans chacun des corps $\mathbb{Q}_p$.

- L'étude des situations dans lesquelles le principe « local-global » s'applique est un domaine de recherche actif en géométrie arithmétique.

Courbes de Fermat et obstruction locale

Dans le cas des courbes de Fermat, Halberstadt et Kraus ont conjecturé que l'absence de solution (non triviale) s'explique souvent par l'existence d'obstructions locales.

Conjecture

Soient a, b, c trois entiers ne vérifiant aucune relation linéaire à coefficients dans $\{-1, 0, 1\}$. Alors, il existe une constante $g(a, b, c)$ telle que pour tout nombre premier $p > g(a, b, c)$, la courbe d'équation

$$aX^p + bY^p = cZ^p$$

admet au-moins une obstruction locale.

À ce jour, on ne sait pas démontrer un tel énoncé !

Merci pour votre attention !