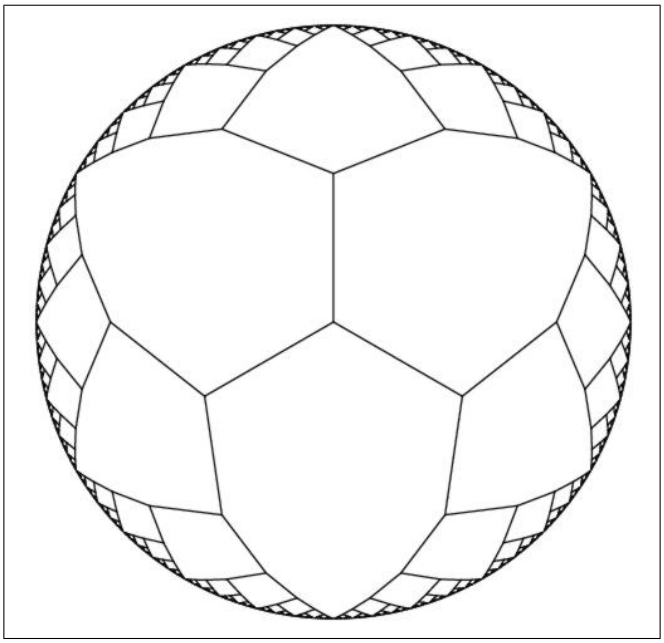
Introduction à l'analyse p-adique

Notes pour le séminaire λ

Bruno Winckler



11 octobre 2012

Table des matières

1 Nombres p-adiques : définition, topologie

Un intérêt de $\mathbb{R}$ par rapport à $\mathbb{Q}$, en plus de sa propriété de borne supérieure qui implique plusieurs théorèmes d'analyse et de topologie, est que c'est un espace complet. Ainsi, la théorie des séries numériques et des séries de fonctions est beaucoup plus riche que sur $\mathbb{Q}$. Par exemple, une série absolument (respectivement normalement) convergente est convergente (respectivement uniformément convergente).

Mais compléter $\mathbb{Q}$ pour avoir $\mathbb{R}$ dépend d'une topologie particulière de $\mathbb{Q}$. Grâce à des topologies différentes, dites p-adiques, on peut obtenir d'autres complétions de $\mathbb{Q}$, qui sont les corps des nombres p-adiques, notés $\mathbb{Q}_p$. Leur intérêt peut être arithmétique : en plus d'obtenir des techniques puissantes issues de l'analyse, passer de $\mathbb{Q}$ à $\mathbb{Q}_p$ nous permet de conserver des informations arithmétiques sur les nombres rationnels. C'est la traduction arithmétique de propriétés analytiques p-adiques que j'expose modestement dans cet exposé, avec quelques exemples qui ne sont que le sommet de l'iceberg.

1.1 Valuation p-adique, complétions de $\mathbb{Q}$

Définition 1.1 (Valuation p-adique)**.** *Soit p un nombre premier. On appelle valuation p-adique l'application $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{+\infty\}$ définie comme suit :*

- *$v_p(0) = +\infty$;*
- *si n est un entier non nul, $v_p(n) = k$ si p^k divise n et p^{k+1} ne divise pas n (p^k est la « plus grande puissance de p dans n ») ;*
- *si $n = \dfrac{a}{b}$ avec a et b des entiers non nuls, alors $v_p(n) = v_p(a) - v_p(b)$.*

Définition 1.2 (Valeur absolue p-adique)**.** *Soit p un nombre premier. On définit la valeur absolue p-adique comme l'application $|\cdot|_p : \mathbb{Q} \to \mathbb{R}_+$ vérifiant $|0|_p = 0$, et $|n|_p = \dfrac{1}{p^{v_p(n)}}$ si n est un rationnel non nul.*

Avec la définition, on voit que $|xy|_p = |x|_p|y|_p$ pour tous rationnels x et y, du fait que :

$$v_p(xy) = v_p(x) + v_p(y).$$

C'est, en fait, propre à ce qu'on appelle une valeur absolue, en toute généralité.

Ainsi, si n s'écrit $\prod_i p_i^{\alpha_i}$ où les α_i sont des entiers, alors $v_{p_i}(n) = \alpha_i$ et $|n|_{p_i} = \frac{1}{p_i^{\alpha_i}}$. Notons que $1 = \prod_i p_i^0$, donc $v_p(1) = 0$ pour tout nombre premier p. Remarquons que $|n|_p < 1$ si, et seulement si p divise le numérateur de n, $|n|_p = 1$ si p n'apparaît pas dans l'expression de n, et $|n|_p > 1$ s'il est au dénominateur.

Exemple. Soit $n = 315 = 3^2 \cdot 5 \cdot 7$. On a $v_3(n) = 2$, $v_5(n) = 1$, $v_7(n) = 1$, et $v_p(n) = 0$ pour tout nombre premier p différent de 3, 5 et 7.

Exemple. On a $v_2\left(\frac{12}{25}\right) = 2$, $v_3\left(\frac{12}{25}\right) = 1$ et $v_5\left(\frac{12}{25}\right) = -2$ (donc $\left|\frac{12}{25}\right|_2 = \frac{1}{4}$, $\left|\frac{12}{25}\right|_3 = \frac{1}{3}$ et $\left|\frac{12}{25}\right|_5 = 25$). Pour p différent de 2, 3 et 5, on a $v_p\left(\frac{12}{25}\right) = 0$ et $\left|\frac{12}{25}\right|_p = 1$.

Exemple. On a $v_p(p^n) = n$ pour tout entier n, donc $|p^n|_p = \frac{1}{p^n}$: plus on est divisible par p, plus on est petit.

Exemple. Soit $n \geqslant 1$ un entier. La valuation p-adique de $n!$ (factorielle n) est $\sum_{k=1}^{+\infty} \left[\frac{n}{p^k}\right]$, où $[x]$ désignera la partie entière de x dans cet exposé. Cette somme est, malgré les apparences, finie, puisque son terme général est nul dès que $p^k > n$, c'est-à-dire $k > \frac{\ln(n)}{\ln(p)}$. L'idée essentielle est que chaque facteur $\left[\frac{n}{p^k}\right]$ compte le nombre de multiples de p^k dans $n!$. Par exemple, $v_2(100!) = 97$ et $v_5(100!) = 24$, ce qui permet de voir que 100! admet 24 zéros à la fin de son écriture décimale, ce que vous pourrez vérifier avec votre logiciel de calcul formel favori. Il est facile de voir que $v_p(n!) \leqslant \frac{n}{p-1}$, ce qui nous sera utile plus tard.

On peut vérifier que $|\cdot|_p$ définit bien une distance sur $\mathbb{Q}$; en fait, elle vérifie bien mieux que l'inégalité triangulaire, puisque pour tout $(x, y) \in \mathbb{Q}$, on a $|x - y|_p \leqslant \max(|x|_p, |y|_p)$ (on parle d'inégalité ultramétrique, et de valeur absolue ultramétrique). Ceci découle de la propriété simple à vérifier $v_p(x - y) \geqslant \min(v_p(x), v_p(y))$ (il y a toujours égalité si $v_p(x) \neq v_p(y)$). Ainsi, $\mathbb{Q}$ muni de la topologie induite par la distance $|\cdot|_p$ définit un espace topologique métrique. On peut vérifier que pour deux valeurs absolues p-adiques différents, les topologies induites sont différentes : par exemple, la suite définie par $(p^n)_{n\geqslant 0}$ converge dans $(\mathbb{Q}, |\cdot|_p)$ (et sa limite est 0), mais pas avec les autres topologies.

Le théorème suivant nous assure qu'on « n'oublie » pas de valeurs absolues :

Proposition 1.3 (Théorème d'Ostrowski)**.** *Les seules valeurs absolues sur $\mathbb{Q}$ sont, à équivalence près, la valeur absolue archimédienne $|\cdot|$ et les valeurs absolues p-adiques $|\cdot|_p$. On note V l'ensemble de ces classes d'équivalence de valeurs absolues (qu'on appelle* places*) sur $\mathbb{Q}$.*

Deux valeurs absolues sont équivalentes si l'une s'écrit comme une puissance strictement positive de l'autre. Deux valeurs absolues équivalentes définissent des topologies équivalentes, c'est pour ça qu'on s'intéresse à leur classe d'équivalence.

Pour chaque place $|\cdot|_v \in V$, on note :

$$\mathbb{Q}_v = \{\text{suites (rationnelles) de Cauchy pour } |\cdot|_v\}/\{\text{suites qui tendent vers 0 pour } |\cdot|_v\}.$$

Dans le cas de la valeur absolue classique, on obtient $\mathbb{R}$. Dans les autres cas, on obtient un nouveau corps complet dans lequel $\mathbb{Q}$ est dense.

Porisme 1.4. *Pour tout p premier, il existe un corps ultramétrique complet $\mathbb{Q}_p$, dont la valeur absolue prolonge la valeur absolue p-adique de $\mathbb{Q}$, et dans lequel $\mathbb{Q}$ est dense.*

Dire qu'il est ultramétrique signifie que sa valeur absolue est ultramétrique.

Dans le cas de $\mathbb{R}$, l'opération de complétion permet d'obtenir des nombres avec des développements décimaux arbitraires après la virgule. Dans le cas p-adique, la complétion implique un phénomène proche et éloigné en même temps : on peut montrer qu'un élément a de $\mathbb{Q}_p$ peut s'écrire $a = \sum_{n=m}^{+\infty} a_n p^n$, où $m \in \mathbb{Z}$ (la convergence est au sens de la valeur absolue p-adique), et $a_n \in [\![0, p-1]\!]$ pour tout $n \geqslant m$. Autrement dit, les nombres p-adiques sont des nombres écrits en base p, avec un nombre infini de chiffres *avant* la virgule ! On note $v_p(a)$ le plus petit entier relatif n tel que $a_n \neq 0$ (et $v_p(0) = \infty$). Cette notion de valuation p-adique prolonge celle sur $\mathbb{Q}$, et encore une fois, on a $|a|_p = \frac{1}{p^{v_p(a)}}$. Alors, on note $\mathbb{Z}_p = \{a \in \mathbb{Q}_p | v_p(a) \geqslant 0\}$ l'anneau des entiers p-adiques, et il est aisé de vérifier que $\mathbb{Q}_p = \mathbb{Z}_p\left[\frac{1}{p}\right]$: c'est le corps des fractions de $\mathbb{Z}_p$. Une autre notation pour un nombre qui s'écrit $\sum_{n=-m}^{+\infty} a_n p^n$ (avec $m \geqslant 0$) est $\overline{\cdots a_2 a_1 a_0, a_{-1} \ldots a_{-m}}^p$.

Proposition 1.5. *L'anneau topologique $\mathbb{Z}$ s'injecte dans $\mathbb{Z}_p$, et y est dense.*

Démonstration. En fait, mieux que $\mathbb{Z}$ (qui appartient bien à $\mathbb{Z}_p$, vu que tous ses éléments n vérifient $v_p(n) \geqslant 0$, et ce pour tout p), l'ensemble $\mathbb{N}$ est dense dans $\mathbb{Z}_p$: si $x = \sum_{k=0}^{+\infty} a_k p^k$ est un entier p-adique, alors la suite $(x_n)_{n\geqslant 0}$ définie par $x_n = \sum_{k=0}^{n} a_k p^k \in \mathbb{N}$ tend vers x : la différence des deux est divisible par p^n, donc la valeur absolue p-adique de $x - x_n$ est majorée par p^{-n}, qui tend vers 0 quand n tend vers l'infini. □

On peut se demander comment caractériser les nombres rationnels au sein des nombres p-adiques. Dans le cas réel, les rationnels sont les nombres dont le développement décimal (impropre ou non) est périodique à partir d'un certain rang. Dans le cas p-adique, le critère est le même : un nombre est rationnel si, et seulement si, son développement p-adique est périodique à partir d'un certain rang.

Exemple. À quoi égale le nombre $\overline{\cdots 1111}^2 = \sum_{n=0}^{+\infty} 2^n$ dans $\mathbb{Q}_2$? Notons x ce nombre. Alors, on a $x = 1 + 2\sum_{n=0}^{+\infty} 2^n$, donc $x = 1 + 2x$, puis $x = -1$. On pouvait le voir « intuitivement » : si on ajoute 1 à ce nombre, alors le chiffre des unités donne 2, mais comme ce nombre doit être 0 ou 1, on met 0 et on reporte la retenue au chiffre des dizaines. Mais alors, avec la retenue, on obtient encore 2 pour le chiffre des dizaines, qu'on doit remplacer par 0 avant de reporter la retenue au chiffre des centaines. Et ainsi de suite, on obtient que des zéros, avec la retenue renvoyée « à l'infini », d'où $x + 1 = 0$.

Exemple. À quoi égale le nombre $\overline{\cdots 1111}^3 = \sum_{n=0}^{+\infty} 3^n$ dans $\mathbb{Q}_3$? Notons x ce nombre. Alors, on a $x = 1+3\sum_{n=0}^{+\infty} 3^n$, donc $x = 1+3x$, puis $x = -\frac{1}{2}$. Cet exemple montre que les entiers ne se reconnaissent pas de la même manière que les rationnels parmi les entiers p-adiques. En fait, les entiers p-adiques dont le développement est périodique à partir d'un certain rang sont les rationnels dont la valuation p-adique est positive, c'est-à-dire les rationnels de la forme $\frac{a}{b}$ où a et b sont premiers entre eux et b non divisible par p.

Ainsi, un nombre p-adique peut être vu comme une série de Laurent dont les coefficients sont dans $\mathbb{Z}/p\mathbb{Z}$, et un entier p-adique peut être vu comme une série formelle dont les coefficients sont aussi dans $\mathbb{Z}/p\mathbb{Z}$. En fait, $\mathbb{Z}_p$ et $\mathbb{Z}/p\mathbb{Z}[[X]]$ sont des anneaux topologiques isomorphes, *via* l'identification $p \leftrightarrow X$.

1.2 Propriétés topologiques, métriques de $\mathbb{Z}_p$ et $\mathbb{Q}_p$

Soit r un réel strictement positif, et x un nombre p-adique. Comme l'espace topologique $\mathbb{Q}_p$ est muni d'une distance, on peut définir des boules ouvertes et fermées : on pose

$$B(x,r) = \{y \in \mathbb{Q}_p; |x-y|_p < r\} \text{ et } B_f(x,r) = \{y \in \mathbb{Q}_p; |x-y|_p \leqslant r\},$$

respectivement les boules ouverte et fermée en x et de rayon r. Comme l'ensemble des valeurs possibles de $|\cdot|_p$ est $p^{\mathbb{Z}}$, on peut considérer uniquement des boules de rayon p^k, où k est un entier relatif. Ces boules sont assez simples à décrire : x_0 est dans la boule fermée de centre x et de rayon p^k si p^k divise $x - x_0$. Autrement dit, tous les termes qui précèdent p^k sont les mêmes dans les développements p-adiques de x et x_0. Si la boule est ouverte, l'étude est la même, à ceci près que le développement p-adique coïncide avant p^{k+1}. Par exemple, si $x = \sum_{n=0}^{+\infty} x_n p^n$ est un entier p-adique et k un entier positif, alors

$$B(x,p^{-k}) = x_0 + x_1 p + \cdots + x_k p^k + p^{k+1}\mathbb{Z}_p.$$

Remarque. Toute boule fermée est ouverte. En effet, $B(x,p^{-k}) = B_f(x,p^{-(k+1)})$.

Remarque. Tout point d'une boule est centre de cette boule, puisqu'on a vu ci-dessus que c'est le développement p-adique du centre tronqué après le terme correspondant à p^k qui caractérise la boule, et que tous les points de cette boule ont le même développement p-adique tronqué.

Remarque. L'anneau $\mathbb{Z}_p$ n'est rien d'autre que la boule fermée de centre 0 et de rayon 1 (et est donc un sous-anneau ouvert de $\mathbb{Q}_p$). Plus généralement, les $p^n\mathbb{Z}_p = B_f(0,p^{-n}) = B(0,p^{-n+1})$ forment une base de voisinages de 0.

L'anneau $\mathbb{Z}_p$ vérifie une autre propriété topologique importante :

Proposition 1.6. *L'anneau topologique $\mathbb{Z}_p$ est compact.*

Démonstration. On a :

$$\mathbb{Z}_p = \bigsqcup_{a \in [\![0,p-1]\!]} (a + p\mathbb{Z}_p)\,.$$

Supposons que $\mathbb{Z}_p$ soit recouvert par des ouverts Ω_j. Montrons qu'on peut en extraire un sous-recouvrement fini. Supposons qu'il n'existe pas de sous-recouvrement fini de $\mathbb{Z}_p$; il existe alors $a_0 \in [\![0, p-1]\!]$ tel que $a_0 + p\mathbb{Z}_p$ ne soit pas recouvert par un sous-recouvrement fini. En recommençant l'opération, il existe $a_1 \in [\![0, p-1]\!]$ tel que $a_0 + a_1 p + p^2\mathbb{Z}_p$ ne soit pas recouvert par un sous-recouvrement fini, et ainsi de suite. Considérons $x = a_0 + a_1 p + a_2 p^2 + etc. \in \mathbb{Z}_p$ obtenu à la limite. Il existe j tel que $x \in \Omega_j$. Il existe alors une boule ouverte centrée en x, de rayon p^{-r}, contenue dans Ω_j. On a

$$B(x, p^{-r}) = a_0 + a_1 p + \cdots + a_r p^r + p^{r+1}\mathbb{Z}_p,$$

et par construction de la suite $(a_n)_{n\geqslant 0}$, cette boule ne peut être recouverte par un sous-recouvrement fini, or cette boule est recouverte par Ω_j, contradiction. □

Porisme 1.7. *L'espace topologique $\mathbb{Q}_p$ est localement compact.*

Voici un exemple d'application du fait que $\mathbb{Z}_p$ soit fermé : écrivons le développement de la série formelle $\sqrt{1+X} = \sum_{n=0}^{+\infty} \binom{1/2}{n} X^n$. On a :

$$\sqrt{1+X} = 1 + \frac{1}{2}X + \frac{\frac{1}{2}\left(\frac{1}{2}-1\right)}{2!}X^2 + \frac{\frac{1}{2}\left(\frac{1}{2}-1\right)\left(\frac{1}{2}-2\right)}{3!}X^3 + \frac{\frac{1}{2}\left(\frac{1}{2}-1\right)\left(\frac{1}{2}-2\right)\left(\frac{1}{2}-3\right)}{4!}X^4 + \text{etc.},$$

ou encore :

$$\sqrt{1+X} = 1 + \frac{1}{2}X - \frac{1}{8}X^2 + \frac{1}{16}X^3 - \frac{5}{128}X^4 + \text{etc.}$$

On remarque que le dénominateur des coefficients devant chaque X^n est une puissance de 2. Ce n'est pas évident *a priori*, puisqu'on divise à chaque étape par factorielle n, et qu'on n'a pas de raison de penser que tous les facteurs de la factorielle (sauf les puissances de 2 éventuellement) sont simplifiés. Voici comment le démontrer à l'aide de la topologie p-adique : il est clair que pour cette topologie, les applications polynomiales sont continues, puisque l'identité est continue, la somme de deux applications continues est continue, de même pour le produit, *etc.* En particulier, l'application polynomiale $x \mapsto \binom{x}{n} = \dfrac{x(x-1)\cdots(x-n+1)}{n!}$ est continue, donc est séquentiellement continue. Si p est un nombre premier impair, on a

$$\lim_{k\to+\infty} \binom{(p^k+1)/2}{n} = \binom{1/2}{n}.$$

Or, pour ce même nombre premier, $\binom{(p^k+1)/2}{n}$ est un entier comme tout coefficient binomial qui se respecte, donc en particulier un p-entier, et appartient à $\mathbb{Z}_p$. Comme $\mathbb{Z}_p$ est fermé, sa limite $\binom{1/2}{n}$ est aussi dans $\mathbb{Z}_p$, donc p ne peut pas apparaître au dénominateur de $\binom{1/2}{n}$. Ceci vaut pour tout p impair, donc seul 2 peut apparaître au dénominateur.

Dans le cas de $\binom{1/2}{n}$, on peut démontrer ce même résultat en remarquant que :

$$\binom{1/2}{n} = \frac{(-1)^{n-1}}{2^{2n-1}}\left(\binom{2n-2}{n-1} - \binom{2n-2}{n}\right),$$

mais l'avantage de la méthode p-adique est qu'elle se généralise au cas des coefficients binomiaux $\binom{r}{n}$ qui apparaissent dans le développement en série de $(1+X)^r$. En adaptant légèrement la méthode exhibée ci-dessus, on peut montrer que le dénominateur de $\binom{r}{n}$ ne contient que des nombres premiers du dénominateur de r : si $r = \frac{a}{b}$, et p ne divise pas b, alors il existe un entier α tel que b divise $p^\alpha - 1$ par le théorème d'Euler ; l'indicatrice $\varphi(b)$ convient. Alors :

$$\binom{a(1-p^{\alpha k})/b}{n}$$

est un entier (même si $a(1-p^{\alpha k})/b$ est négatif, on peut reconnaître un coefficient binomial au signe près), donc un entier p-adique, donc sa limite $\binom{a/b}{n}$ quand k tend vers l'infini est un entier p-adique. Je doute qu'on puisse prouver ce résultat aussi facilement sans le recours p-adique.

Vous pouvez le constater sur cet exemple :

$$(1+X)^{2/15} = 1 + \frac{2}{15}X - \frac{13}{225}X^2 + \frac{364}{10125}X^3 - \frac{3913}{151875}X^4 + \frac{226954}{11390625}X^5 + \text{etc.}$$

Remarque. J'ai exhibé concrètement une suite d'entiers p-adiques tendant vers $\binom{a/b}{n}$ pour ne pas dépayser d'emblée, mais on peut raisonner plus directement ainsi : si p ne divise pas b, alors $r = \frac{a}{b}$ est un entier p-adique, donc par densité il existe une suite $(u_k)_{k\geqslant 0}$ d'entiers tels que $u_k \underset{k\to+\infty}{\longrightarrow} r$. Encore une fois, par continuité des applications polynomiales, la limite $\binom{r}{n}$ de $\left(\binom{u_k}{n}\right)_{k\geqslant 0}$ est un entier p-adique.

Pour résumer les propriétés topologiques : l'anneau $\mathbb{Z}_p$ est compact, et $\mathbb{N}$ est dense dans $\mathbb{Z}_p$. L'espace $\mathbb{Q}_p$ est localement compact et totalement discontinu ; $\mathbb{Z}_p$ en est un sous-anneau ouvert.

2 Séries p-adiques ; logarithme et exponentielle p-adiques

2.1 Généralités

Puisqu'on a une métrique et un espace complet, on peut développer une théorie des séries p-adiques parallèlement à celle des séries numériques, voire une théorie des séries entières. Il y a plusieurs similitudes dans les deux cas, parfois héritées de propriétés algébriques des séries formelles (mais pas toujours : par exemple, le principe des zéros isolés sévit dans le cas p-adique), et bien évidemment des différences, principalement dues au fait que la valeur absolue est ultramétrique. La proposition qui suit est la différence la plus fondamentale :

Proposition 2.1. *Une série p-adique (c'est-à-dire, dont le terme général est un nombre p-adique) converge si, et seulement si son terme général tend vers* 0.

Le fait qu'une série convergente ait son terme général qui tend vers 0 est clair, et est partagé par le cas des séries réelles. C'est sa réciproque qui est réellement intéressante (ou plutôt : p-adiquement intéressante...), et fausse dans le cas réel : par exemple, la série harmonique diverge, bien que son terme général tende vers 0.

Démonstration. Une série de terme général u_n converge si, et seulement si elle vérifie le critère de Cauchy, car $\mathbb{Q}_p$ est complet. Or, comme la valeur absolue est ultramétrique, on a :

$$\left|\sum_{k=n}^{n+m} u_k\right|_p \leqslant \max_{[\![n,n+m]\!]} |u_k|_p.$$

Soit $\varepsilon > 0$. Si la suite $(u_n)_{n\geqslant 0}$ tend vers 0, alors pour n assez grand, on a $|u_n|_p < \varepsilon$. Toujours pour ce n très grand, et indépendamment de m, on a $\left|\sum_{k=n}^{n+m} u_k\right|_p < \varepsilon$, donc la série vérifie le critère de Cauchy, et converge. □

Exemple. La série de terme général p^n converge trivialement, presque par définition de la valeur absolue p-adique. Sa somme vaut $\sum_{n=0}^{+\infty} p^n = \dfrac{1}{1-p}$: c'est un grand classique dans le cadre réel ou formel avec x (de valeur absolue strictement inférieure à 1) ou X à la place de p. À noter que pour $p = 2$, on retrouve ce que j'avais écrit en première partie :

$$-1 = \sum_{n=0}^{+\infty} 2^n = \cdots 11111.$$

Exemple. Si $(u_n)_{n\geqslant 0}$ est une suite d'entiers, alors la série de terme général $\sum_{n\geqslant 0} u_n n!$ converge dans $\mathbb{Q}_p$ pour tout p, et même dans $\mathbb{Z}_p$ (car $\mathbb{Z}_p$ est fermé) : on a évidemment $n! \to 0$ quand $n \to \infty$, et ce n'est pas u_n qui va l'en empêcher. En fait, on peut montrer que tout élément de $\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}$ s'écrit plus ou moins sous cette forme.

Exemple. Soit t un nombre p-adique de valeur absolue strictement inférieure à $p^{-1/(p-1)}$. Alors la série de terme général $(-1)^n \dfrac{t^{2n+1}}{(2n+1)!}$ converge : en effet,

$$\left|\frac{t^{2n+1}}{(2n+1)!}\right|_p = \frac{p^{-(2n+1)v_p(t)}}{|(2n+1)!|_p} < p^{-(2n+1)\left(v_p(t)+\frac{1}{p-1}\right)} \to 0$$

quand $n \to \infty$. Je donne cet exemple parce qu'on peut y reconnaître, dans le cas réel, la fonction sinus. En fait, on peut définir de la même manière le sinus p-adique, noté $\sin_p$. Cependant, j'attire l'attention sur le fait que même si la série définie par ce terme général converge en un certain rationnel à la fois pour la valeur absolue réelle et celle p-adique (et même si la limite est un rationnel dans les deux cas !), les limites ne sont pas forcément les mêmes. Ceci empêche la preuve suivante de l'irrationalité de π, trop belle pour être vraie, d'être vraie :

> *Sophisme.* Supposons que π soit un rationnel, sous la forme $\frac{a}{b}$ avec a et b des entiers premiers entre eux. Soit p un nombre premier impair qui ne divise pas a. Alors,
>
> $$0 = \sin(pb\pi) = \sin(pa) = \sum_{n=0}^{\infty} (-1)^n \frac{(pa)^{2n+1}}{(2n+1)!} \equiv pa \mod p^2,$$
>
> ce qui est absurde.

L'argument est fallacieux parce que $\sin(pa)$ (le sinus réel) est différent de $\sin_p(pa)$, tout simplement. De la même manière, la série 7-adique et la série réelle définies par le terme général $\binom{1/2}{n}\left(\frac{7}{9}\right)^n$ convergent, et toutes les deux vers $\sqrt{1+\frac{7}{9}} = \sqrt{\frac{16}{9}}$ (c'est une égalité

formelle !). Mais dans le cas réel, on obtient $\frac{4}{3}$, tandis que le cas 7-adique « choisit » la racine carrée $-\frac{4}{3}$. En effet, si elle valait $\frac{4}{3}$, alors, comme $\left|\binom{1/2}{n}\left(\frac{7}{9}\right)^n\right|_7 \leqslant \frac{7^{-n}}{|n!|_7} < 1$ pour $n \geqslant 1$, on aurait

$$1 > \left|\sqrt{1+\frac{7}{9}} - 1\right|_7 = \left|\frac{4}{3} - 1\right| = \left|\frac{1}{3}\right| = 1,$$

ce qui est absurde.

On peut aussi parler du rayon de convergence d'une série entière : soit $f = \sum_{n=0}^{+\infty} a_n X^n \in \mathbb{Q}_p[[X]]$ une série formelle. On appelle rayon de convergence de f, et on note r_f, la borne supérieure de l'ensemble (non vide) :

$$\{r \in \mathbb{R}_+; |a_n|_p r^n \to 0\}.$$

Pour tout nombre p-adique x de valeur absolue p-adique inférieure à r_f, la série $\sum_{n\geqslant 0} a_n x^n$ converge. Comme dans le cas réel, on peut montrer que le rayon de convergence égale :

$$\frac{1}{\limsup |a_n|_p^{1/n}}.$$

Dans le cas réel, il peut y avoir des problèmes de convergence sur le « bord », et même un comportement différent en deux points du bord. Je pense à la série qui définit le logarithme, de rayon de convergence 1, convergente en 1, divergente en -1. La situation p-adique est bien plus simple :

Proposition 2.2. *Le domaine de convergence d'une série entière p-adique $f \in \mathbb{Q}_p[[X]]$ est une boule fermée $B_f(0,R)$, où R est soit de la forme p^k avec k entier, soit dans l'ensemble $\{0,\infty\}$.*

Cette proposition est moralement due au fait que la condition nécessaire et suffisante pour que la série converge en x est $|a_n x^n|_p \to 0$, ce qui ne dépend que de la valeur absolue de x, et pas de sa valeur exacte. Donc soit la série converge en tous les x tels que $|x|_p = r_f$ (et alors $R = r_f$), soit elle diverge en tous ces points, et on prend $R = p^{-1} r_f$.

Exemple. Toute série entière à coefficients dans $\mathbb{Z}_p$ converge sur $B(0,1)$.

Exemple. La série entière $\sum_{n\geqslant 0} t^n$ converge sur $B(0,1)$. On a, par ailleurs, $\sum_{n=0}^{+\infty} t^n = \frac{1}{1-t}$ pour tout t dans cette boule.

Exemple. La série entière $\sum_{n\geqslant 0} \frac{t^n}{n!}$ converge sur $B\left(0, p^{-1/(p-1)}\right)$. En effet, si $|t|_p < p^{-1/(p-1)}$, alors :

$$\left|\frac{t^n}{n!}\right|_p = \frac{p^{-n v_p(t)}}{|n!|_p} < p^{-n\left(v_p(t) + \frac{1}{p-1}\right)} \to 0$$

quand $n \to \infty$. On note $\exp_p$ sa somme, par analogie avec l'exponentielle réelle (ou complexe), et on l'appelle exponentielle p-adique. On remarque que dans le cas p-adique, le rayon de convergence de l'exponentielle n'est pas infini ! Ce fait a ses avantages et ses inconvénients. Une analyse plus poussée montre que $\exp_p$ est définie sur $p\mathbb{Z}_p$ si p est impair, sur $4\mathbb{Z}_2$ sinon, et est à valeurs dans $1 + p\mathbb{Z}_p$ dans le premier cas, dans $1 + 4\mathbb{Z}_2$ sinon.

Exemple. De la même manière, on peut définir le logarithme p-adique : la série entière $\sum_{n\geqslant 0}(-1)^{n+1}\frac{t^n}{n}$ converge sur $B(0,1)$. En effet, $\left|\frac{1}{n}\right|_p = p^{v_p(n)}$, et $\lim_{n\to\infty}|a_n|_p^{1/n} = 1$. Donc le rayon de convergence égale 1 (on peut aussi calculer le rayon de convergence de sa dérivée formelle parce qu'il est nettement plus simple, et s'avère être le même que celui de la série). Si $|t|_p = 1$, $|a_n t^n|_p = p^{v_p(n)} \geqslant 1$, donc ne peut pas tendre vers 0. On note $\ln_p$ (ou $\log_p$) sa somme, à ne pas confondre avec le logarithme classique en base p. On remarque que le logarithme p-adique a un rayon de convergence plus grand que celui de l'exponentielle ! En fait, ça devient vraiment n'importe quoi quand on apprend qu'il existe un unique prolongement du logarithme p-adique sur la clôture algébrique de $\mathbb{Q}_p$ (qui est plus ou moins un analogue du plan complexe) privée de zéro, alors qu'on a le fameux problème de détermination du logarithme complexe.

2.2 Logarithme et exponentielle

Pour les propositions suivantes, les conditions sur les ensembles de départ sont pour éviter les problèmes de convergence, tandis que les égalités annoncées découlent de ces mêmes égalités pour l'exponentielle et le logarithme formels.

Proposition 2.3. *Le logarithme $1+p\mathbb{Z}_p \to p\mathbb{Z}_p$ (la restriction $1+4\mathbb{Z}_2 \to 4\mathbb{Z}_2$ si $p=2$) et l'exponentielle $p\mathbb{Z}_p \to 1+p\mathbb{Z}_p$ (ou $4\mathbb{Z}_2 \to 1+4\mathbb{Z}_2$ si $p=2$) sont des inverses mutuels.*

La restriction du logarithme dans le cas où $p = 2$ est pour s'assurer que $\exp_2(\ln_2(1+x))$ a un sens, l'exponentielle n'étant définie que sur $4\mathbb{Z}_2$ au lieu de $2\mathbb{Z}_2$.

Proposition 2.4 (L'exponentielle est un morphisme)**.** *Pour tous x et y dans $B\left(0, p^{-1/(p-1)}\right)$, on a $x+y \in B\left(0, p^{-1/(p-1)}\right)$, et :*

$$\exp_p(x+y) = \exp_p(x)\exp_p(y).$$

Proposition 2.5 (Le logarithme est un morphisme)**.** *Pour tous x et y dans $B(0,1)$, on a $(1+x)(1+y) \in B(0,1)$, et :*

$$\ln_p((1+x)(1+y)) = \ln_p(1+x) + \ln_p(1+y).$$

On déduit, par ailleurs, que pour tout entier n, $\ln_p((1+x)^n) = n \cdot \ln_p(1+x)$.

Remarque. Prenons $p = 2$. Comme $|-2|_2 < 1$, le logarithme diadique de -1 est bien défini ! On a $\ln_2(-1) = \ln_2(1-2) = \sum_{n=1}^{+\infty}\frac{2^n}{n}$. Que vaut $\ln_2(-1)$? En fait, grâce à la proposition précédente, on a aisément $\ln_2(1) = 2\ln_2(1)$, donc $\ln_2(1) = 0$ (et ceci vaut pour tout logarithme, puisque c'est un morphisme). Alors, comme $(-1)^2 = 1$, on en déduit que $2\ln_2(-1) = \ln_2(1) = 0$, donc $\ln_2(-1) = 0$. Comme souvent en analyse p-adique, on peut interpréter d'un point de vue arithmétique ce résultat : cette égalité revient à dire que la série qui a pour somme $\ln_2(-1)$ converge, et a pour limite 0. Autrement dit, vue la tête de notre valeur absolue, ça signifie que cette série est divisible par des puissances de 2 arbitrairement grandes (n'oublions pas qu'ici, on est d'autant plus petit qu'on est divisible par 2). Formellement :

$$\forall M \in \mathbb{N},\ \exists N \in \mathbb{N};\ \forall n \geqslant N, \quad 2^M \text{ divise } \sum_{k=1}^{n}\frac{2^k}{k}.$$

Je vous invite à le démontrer par des méthodes élémentaires, pour voir de quoi on fait l'économie avec ce raisonnement analytique. Vu qu'on additionne sans cesse des puissances de

2, on peut penser que c'est évident, mais il n'en est rien. D'ailleurs, le fait de diviser à chaque étape par un entier est crucial : par exemple, la suite $\left(\sum_{k=1}^{n} 2^k\right)_{n\geqslant 1}$, qui ressemble vaguement à notre série, est de valuation constante égale à 1 et ne tend pas du tout vers 0 (mais vers -2).

Une étude plus soignée de la série permet même d'avoir une idée de la rapidité de convergence, qu'on devine de l'ordre de 2^n après le calcul de quelques termes :

$$\begin{array}{lll}
\frac{2}{1}+\frac{4}{2}+\frac{8}{3}+\frac{16}{4}+\frac{32}{5} & = \frac{256}{15} & = \frac{2^8}{3\cdot 5}\\
\frac{2}{1}+\frac{4}{2}+\frac{8}{3}+\frac{16}{4}+\frac{32}{5}+\frac{64}{6} & = \frac{416}{15} & = \frac{13\cdot 2^5}{3\cdot 5}\\
\frac{2}{1}+\frac{4}{2}+\frac{8}{3}+\frac{16}{4}+\frac{32}{5}+\frac{64}{6}+\frac{128}{7} & = \frac{4832}{105} & = \frac{151\cdot 2^5}{3\cdot 5\cdot 7}\\
\frac{2}{1}+\frac{4}{2}+\frac{8}{3}+\frac{16}{4}+\frac{32}{5}+\frac{64}{6}+\frac{128}{7}+\frac{256}{8}+\frac{512}{9}+\frac{1028}{10} & = \frac{74752}{315} & = \frac{73\cdot 2^{10}}{3^2\cdot 5\cdot 7}
\end{array}$$

Une application classique, et relativement aisée, de l'exponentielle p-adique est dans l'étude du groupe multiplicatif de l'anneau $\mathbb{Z}/n\mathbb{Z}$. Par le lemme des restes chinois, on se ramène à l'étude du groupe $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Par un lemme de théorie des groupes qui ne nous intéressera pas ici (puisque ce n'est pas le sujet), on peut montrer que $(\mathbb{Z}/p^n\mathbb{Z})^\times$ est isomorphe au produit direct de $(\mathbb{Z}/p\mathbb{Z})^\times$ (dont on sait qu'il est cyclique, isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$, même si ce n'est pas un résultat trivial) par $(1+p\mathbb{Z}/p^n\mathbb{Z})$ si p est impair, et que $(\mathbb{Z}/2^n\mathbb{Z})^\times$ est isomorphe à $(1+2\mathbb{Z}/2^n\mathbb{Z})$. La structure de ce dernier groupe est donnée par l'exponentielle p-adique, et aboutit au théorème suivant :

Théorème 2.6. *Si p est impair, $(\mathbb{Z}/p^n\mathbb{Z})^\times$ est un groupe cyclique. Si $p=2$, on a $(\mathbb{Z}/2\mathbb{Z})^* = \{1\}$, et si $n\geqslant 2$, on a $(\mathbb{Z}/2^n\mathbb{Z})^\times \simeq \mathbb{Z}/2^{n-2}\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ (qui n'est plus cyclique dès que $n\geqslant 3$).*

Même si on sait que $(p\mathbb{Z}/p^n\mathbb{Z},+)$ est isomorphe à $(\mathbb{Z}/p^{n-1}\mathbb{Z},+)$, ce n'est pas si simple, car ce groupe n'a *a priori* rien à voir avec $(1+p\mathbb{Z}/p^n\mathbb{Z},\times)$ qui est un groupe pour la multiplication.

Démonstration. Soit $\pi_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ le morphisme qui, à un développement p-adique, associe ce développement tronqué à partir de p^n. Si x est un élément de $p\mathbb{Z}/p^n\mathbb{Z}$, on pose :

$$\exp_p(x) = \pi_n(\exp_p(x_1)),$$

où $x_1 \in p\mathbb{Z}_p$ est un relevé p-adique de x (on procède de même en remplaçant p par 4 si $p=2$). On peut montrer que cette définition ne dépend pas du choix du relevé de x. De même, on peut définir le logarithme sur $1+p\mathbb{Z}/p^n\mathbb{Z}$ (ou $1+4\mathbb{Z}/2^n\mathbb{Z}$). Grâce aux propositions précédentes sur l'exponentielle et le logarithme p-adiques, on déduit sans peine que $\exp_p : p\mathbb{Z}/p^n\mathbb{Z} \to 1+p\mathbb{Z}/p^n\mathbb{Z}$ et $\ln_p : 1+p\mathbb{Z}/p^n\mathbb{Z} \to p\mathbb{Z}/p^n\mathbb{Z}$ sont des morphismes réciproques (avec une formulation équivalente si $p=2$). Ce sont en particulier des isomorphismes, donc :

$$1+p\mathbb{Z}/p^n\mathbb{Z} \simeq p\mathbb{Z}/p^n\mathbb{Z},$$

ce qui clôt le cas où p est impair. Si $p=2$, on a dit précédemment que $(\mathbb{Z}/2^n\mathbb{Z})^\times$ est isomorphe à $(1+2\mathbb{Z}/2^n\mathbb{Z})$. Ce groupe a deux sous-groupes particuliers, du moins si $n\geqslant 2$: $(1+4\mathbb{Z}/2^n\mathbb{Z})$ qui est isomorphe à $4\mathbb{Z}/2^n\mathbb{Z} \simeq \mathbb{Z}/2^{n-2}\mathbb{Z}$ grâce au logarithme (donc cyclique), et $\{-1,1\}$ qui est cyclique d'ordre 2. L'intersection de ces deux sous-groupes est triviale, donc votre lemme de théorie des groupes préféré prouve qu'ils sont en somme directe, et $(\mathbb{Z}/2^n\mathbb{Z})^\times \simeq \mathbb{Z}/2^{n-2}\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. □

Exemple. En adaptant la démonstration, on peut trouver des générateurs des $(\mathbb{Z}/p^n\mathbb{Z})^\times$, dans les cas où ils sont cycliques. Par exemple, pour $p = 3$ et $n = 4$, on peut trouver des générateurs de $(\mathbb{Z}/81\mathbb{Z})^\times \simeq \mathbb{Z}/54\mathbb{Z}$ en procédant comme suit : on a

$$(\mathbb{Z}/81\mathbb{Z})^\times \simeq (1 + 3\mathbb{Z}/81\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})^\times.$$

L'exponentielle est un isomorphisme de $3\mathbb{Z}/81\mathbb{Z}$ (qui est engendré par 3) dans $1 + 3\mathbb{Z}/81\mathbb{Z}$, donc $\exp(3)$ engendre $1+3\mathbb{Z}/81\mathbb{Z}$. Comme -1 engendre $(\mathbb{Z}/3\mathbb{Z})^\times$, on en déduit que $-\exp(3)$ engendre $(\mathbb{Z}/81\mathbb{Z})^\times$ qui est produit direct des deux sous-groupes indiqués. Il reste à calculer l'exponentielle triadique de 3. On a

$$\exp(3) = 1 + 3 + \frac{3^2}{2!} + \frac{3^3}{3!} + etc. \mod 81,$$

et on a besoin de trouver à partir de quel rang on peut tronquer l'exponentielle, c'est-à-dire à partir de quel rang n on a $\frac{3^n}{n!}$ divisible par 3^4. Or, on connait la valuation en 3 de $n!$. On a $v_3\left(\frac{3^n}{n!}\right) \geqslant 4$ pour $n - v_3(n!) \geqslant 4$. On sait que $-v_3(n!) \geqslant -\frac{n}{2}$, il suffit donc d'avoir $n - \frac{n}{2} \geqslant 4$, puis $n \geqslant 8$. Reprenons :

$$\exp(3) = 1 + 3 + \frac{3^2}{2!} + \frac{3^3}{3!} + \frac{3^4}{4!} + \frac{3^5}{5!} + \frac{3^6}{6!} + \frac{3^7}{7!} \mod 81.$$

Il va de soi que je ne vais pas me lancer dans ce calcul comme ça. On simplifie par 3 au maximum :

$$\exp(3) = 1 + 3 + \frac{9}{2} + \frac{9}{2} + \frac{27}{8} + \frac{81}{40} + \frac{81}{40} + \frac{243}{280} \mod 81,$$

pour finalement avoir : $\exp(3) = 1 + 3 + 9 + \frac{27}{8}$. Le calcul de $\frac{27}{8}$ peut se faire ainsi :

$$\frac{27}{8} = -27\frac{1}{1-9} = -27(1 + 9 + 9^2 + etc.) \mod 81 = -27 \mod 81,$$

d'où : $\exp(3) = 1 + 3 + 9 - 27 = -14 \mod 81$. Donc 14 engendre $(\mathbb{Z}/81\mathbb{Z})^\times$.

3 Applications

3.1 Résultats de finitude pour les solutions d'une équation

Je rappelle qu'une progression arithmétique est un ensemble de la forme $a + b\mathbb{Z}$, avec a et b des entiers (éventuellement nuls, ici).

Théorème 3.1 (Théorème de Skolem-Mahler-Lech)**.** *Soit $(u_n)_{n\geqslant 0}$ une suite vérifiant une relation de récurrence linéaire à coefficients entiers. L'ensemble des entiers i tels que $u_i = 0$ est une union finie de progressions arithmétiques.*

Ainsi, l'annulation d'une suite linéaire récurrente a des contraintes assez fortes. Il n'est pas possible, par exemple, de trouver une suite qui s'annule en tous les carrés parfaits. L'idée de la preuve est que l'ensemble des termes nuls dans une progression arithmétique peut être vu comme le lieu d'annulation d'une fonction analytique sur $\mathbb{Z}_p$, et une telle fonction définie sur un compact ($\mathbb{Z}_p$ ici) est soit nulle, soit avec un nombre fini de zéros. Si elle est nulle, alors la suite est nulle sur toute une progression arithmétique. Sinon, elle a un nombre fini de zéros, qui correspondent à des progressions arithmétiques de la forme $a + 0\mathbb{Z}$.

Exemple. La suite linéaire récurrente définie par $x_n = x_{n-4} + x_{n-2}$, $x_0 = x_1 = x_3 = 0$, $x_2 = 1$ s'annule pour $n \in \{0\} \cup (2\mathbb{Z} + 1)$: l'ensemble des entiers impairs et 0.

Démonstration. Soit $(u_n)_{n\geqslant 0}$ une suite vérifiant la relation de récurrence linéaire :

$$\forall n \geqslant d, \quad u_n = a_1 u_{n-1} + a_2 u_{n-2} + \cdots + a_d u_{n-d}$$

avec a_d non nul. Alors, un peu d'algèbre linéaire élémentaire permet d'écrire u_n sous la forme ${}^tX {}^tA^n Y = \langle A^n X, Y\rangle$, où X et Y sont des vecteurs colonnes de longueur d, et A une matrice inversible de taille $d \times d$, qui dépendent des a_i et u_0, …, u_{d-1}, et sont donc à coefficients entiers ; leurs formes exactes ne nous importent pas.

Comme A est inversible, son déterminant est non nul. Soit p un nombre premier qui ne divise pas ce déterminant. Alors A est inversible modulo p, et les matrices $A^n \bmod p$ le sont également. Comme l'ensemble $\mathrm{M}_d(\mathbb{Z}/p\mathbb{Z})$ est fini (de cardinal p^{d^2}), il existe deux entiers n et m, avec $n < m$, tels que $A^n \mod p = A^m \bmod p$, puis $A^{m-n} = I_d \bmod p$, où I_d est la matrice identité. Notons $M = m - n > 0$.

Alors, pour tout $r \in [\![0, M-1]\!]$, l'ensemble :

$$\{n \in \mathbb{N}; u_{Mn+r} = 0\}$$

est soit fini, soit égal à tout $\mathbb{N}$; ceci impliquerait le théorème de Skolem-Mahler-Lech (car les progressions arithmétiques $r + M\mathbb{Z}$ partitionnent $\mathbb{Z}$ quand r varie). Pour le prouver, supposons qu'il ne soit pas fini pour un certain r. Alors, $\langle A^{Mn} A^r X, Y\rangle = 0$ pour une infinité de valeurs de n. Par construction de M, on peut écrire :

$$A^M = \mathrm{I}_d + pB$$

pour une certaine matrice B à coefficients entiers. Alors, $P(n) = 0$ pour une infinité d'entiers n, où P est défini sur $\mathbb{Z}$ par la formule :

$$P(n) = \langle (\mathrm{I}_d + pB)^n A^r X, Y\rangle.$$

L'idée de la preuve est de montrer que P peut être étendu en une fonction analytique p-adique, et par le principe des zéros isolés, elle ne peut avoir qu'un nombre fini de zéros dans le compact $\mathbb{Z}_p$ si elle est non nulle. Comme, par hypothèse, elle s'annule une infinité de fois, on a $P = 0$, donc elle s'annule partout, et l'ensemble $\{n \in \mathbb{N}; u_{Mn+r} = 0\}$ est tout $\mathbb{N}$. Mais comme je n'ai pas prouvé que c'était une fonction analytique, et que le principe des zéros isolés était valable dans le cas p-adique, je vais faire tout cela à la main.

En développant l'expression $(\mathrm{I}_d + pB)^n$ à l'aide du binôme de Newton, on remarque que $P(n)$ se met sous la forme d'une série formelle en p, dont les coefficients dépendent de n :

$$P(n) = \sum_{j=0}^{+\infty} p^j P_j(n).$$

Les P_j sont des polynômes en n (essentiellement parce qu'ils dépendent d'un coefficient binomial $\binom{n}{k}$) à coefficients entiers (donc entiers p-adiques). Or, P est limite uniforme, pour la topologie p-adique, des $\sum_{j=0}^{N} p^j P_j(n)$: on a

$$\left| P(n) - \sum_{j=0}^{N} p^j P_j(n) \right|_p \leqslant p^{-N} \to 0,$$

indépendamment de n. Bref, comme P est limite uniforme de polynômes de $\mathbb{Z}_p[X]$, on peut étendre continûment P en une fonction de $\mathbb{Z}_p$ dans $\mathbb{Z}_p$, et $n \mapsto P(n) \mod p^j$ est un polynôme en n pour tout j.

Maintenant, si $P(n_0) = 0$ pour un entier (ou entier p-adique, peu importe) n_0, on peut écrire $P(n) = (n - n_0)Q(n)$ avec $Q(n) = \dfrac{P(n) - P(n_0)}{n - n_0}$, qui est une fonction continue qui, comme P, a une infinité de zéros, est un polynôme modulo p^j pour tout j, et dont le coefficient constant $Q_0(n)$ est soit nul, soit de degré strictement inférieur à celui de $P_0(n)$; toutes ces affirmations se voient en remarquant que n_0 est aussi racine des réductions modulo p^j de P qui sont des polynômes, donc se factorisent en $n - n_0$. En réitérant, on voit que si P a une infinité de zéros, alors il contient un facteur dont le coefficient constant est nul, et donc est divisible par p. En réitérant encore, on obtient que si P a une infinité de zéros, alors il doit être divisible par des puissances arbitrairement grandes de p, donc doit être identiquement nul. D'où le résultat. □

3.2 Résolution effective d'une équation diophantienne

Alors que l'équation de Pell-Fermat $x^2 - dy^2 = 1$, avec $d \geqslant 1$, a une infinité de solutions entières, toutes obtenues à partir d'une solution fondamentale, l'équation sensiblement différente $x^2 - dy^3 = 1$ a un nombre fini de solutions, et même mieux : il n'existe au plus qu'une seule solution avec $y \neq 0$. Je vais me contenter d'ébaucher l'idée de la preuve dans un cas particulier, avec seulement le résultat du finitude :

Proposition 3.2. *L'équation $x^3 - 7y^3 = 1$ n'a qu'un nombre fini de solutions entières.*

À la main, on peut voir que $(x, y) = (1, 0)$ et $(x, y) = (2, 1)$ sont solutions. En fait, ce sont les seules.

Ébauche de démonstration. On peut montrer, par des méthodes algébriques, que si x et y sont des solutions entières de cette équation, alors $x - \sqrt[3]{7}y = (2 - \sqrt[3]{7})^n$ pour un certain entier n [*] ; les solutions $(x, y) = (1, 0)$ et $(2, 1)$ correspondent à $n = 0$ et $n = 1$ respectivement. En développant $(2 - \sqrt[3]{7})^n$ avec la formule du binôme de Newton, on obtient une égalité de la forme

$$x - \sqrt[3]{7}y = a_n + b_n\sqrt[3]{7} + c_n\sqrt[3]{49},$$

où les coefficients a_n, b_n et c_n sont des entiers. Par liberté de la famille $(1, \sqrt[3]{7}, \sqrt[3]{49})$, on doit avoir $c_n = 0$. Voyons ce que cela implique ; on peut écrire c_n explicitement en fonction de n :

$$c_n = \frac{1}{21}\left(\sqrt[3]{7}(2 - \sqrt[3]{7})^n + \omega\sqrt[3]{7}(2 - \omega\sqrt[3]{7})^n + \omega^2\sqrt[3]{7}(2 - \omega^2\sqrt[3]{7}\right)^n,$$

où ω est une racine cubique de l'unité. De la même manière qu'on peut écrire a^x comme une série entière (réelle) quand $a > 0$, on peut écrire c_n comme une série 3-adique entière évaluée en un point de son domaine de convergence, en voyant ω et $\sqrt[3]{7}$ comme des racines cubiques dans les nombres 3-adiques ; rigoureusement, ces quantités n'appartiennent pas forcément à $\mathbb{Q}_3$ mais à une extension finie de $\mathbb{Q}_3$, mais pour alléger cette ébauche de preuve je ne prends pas attention à ceci, en vous demandant d'admettre que le raisonnement qui suit est, en substance, le bon.

Dire que c_n est nul signifie donc que n est une racine entière (donc entière 3-adique) d'une série entière 3-adique. Comme cette série converge sur $\mathbb{Z}_3$ (qui est compact), elle a un nombre fini de racines dans $\mathbb{Z}_3$, par le principe des zéros isolés. Comme $\mathbb{Z}$ est inclus dans $\mathbb{Z}_3$, il y a en particulier un nombre fini d'entiers relatifs tels que $c_n = 0$, donc un nombre fini de solutions (x, y). □

∗. C'est une conséquence du théorème des unités de Dirichlet, car l'anneau des entiers du corps de nombres engendré par $\sqrt[3]{7}$ est de rang 1, et $2 - 3\sqrt[3]{7}$ est une unité fondamentale. Dire que (x, y) est solution revient à dire que la norme de $x - \sqrt[3]{7}$ est de norme 1, donc est une unité.

Références

[B & C] Z.I. Borevitch et Igor Rostilavovich Shafarevich, *Théorie des nombres*, Academic Press Inc, 435 pages, 1996.

[Coh] Henri Cohen, *Number Theory, volume I : Tools and Diophantine Equations*, Springer-Verlag, 680 pages, 2010.

[Kat] Svetlana Katok, *p-adic Analysis Compared With Real*, American Mathematical Society, 152 pages, 2007.

[Kob] Neal Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Springer-Verlag, 184 pages, 1996.