الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Minstère de l'Enseignement Supérieur et de la Recherche Scientifique

CENTRE UNIVERSITAIRE DE MILA
INSTITUT DES SCIENCES ET DE LA TECHNOLOGIE

Réf. ***/11***

Mémoire de fin d'étude
Présenté pour l'obtention du diplôme de

Licence Académique

Domaine : **Mathématiques et Informatique**
Filière : **Mathématiques**
Spécialité : **Mathématiques Fondamentales**

Thème

Calcul de l'inverse d'un nombre p-adique

Présenté par :
Bouchetiba Khadidja
Mehazem Somia

Dirigé par :
Kecies Mohamed

Année universitaire 2010-2011

Remerciements

Mes remerciements vont tout premièrement à Dieu tout puissant pour la volonté, la santé, et la patience qu'il nous a donnée pour terminer ce mémoire.

Nous remercions vivement Monsieur Mohamed. Kecies d'avoir voulu proposer et assurer la direction de ce mémoire, sa disponibilité, son soutien, ses encouragements et ses précieux conseils tout au long de ce travail.

Nous adressons, également, mes remerciements chaleureux aux membres de l'institut des sciences et de la technologie et à tous ceux qui ont pris part de près ou de loin, à la réalisation de ce travail.

Table des matières

Introduction Générale **2**

1 Corps valués ultramétriques complets **3**
1.1 Corps normés 3
1.2 Complétion d'un corps normé 6

2 Corps des nombres p-adique **8**
2.1 Valuation et norme p-adique sur $\mathbb{Q}$ 8
2.2 Norme p-adique 10
2.3 Les nombres p-adiques 13
2.4 Les entiers p-adiques 17

3 Calcul de l'inverse d'un nombre p-adique **24**
3.1 La méthode de Newton 25
3.2 La méthode de la sécante 28
3.3 La méthode du point fixe 31
3.3.1 Cas1 : $s = 2$ 32
3.3.2 Cas 2 : $s = 3$ 33
3.3.3 Généralisation 35

Conclusion Générale **38**

Bibliographie **38**

Introduction Générale

Les nombres p-adiques $\mathbb{Q}_p$ sont des extensions des nombres rationnels. Ils sont inventés au début du vingtième siècle par le mathématicien Allemand Kurt Hensel $(1861, 1941)$. De plus, si $\mathbb{Q}_p$ est muni d'une norme non archimédienne $|.|_p$, alors on obtient une analyse qui se diffère de l'analyse usuelle. On l'appelle analyse p-adique. Les nombres p-adiques n'interviennent pas qu'en mathématiques pures. Ils apparaissent dans plusieurs domaines comme les probabilités et la physique théorique. L'application des nombres p-adique qui nous intéresse dans ce travail est penchée vers l'informatique.

Ce mémoire est réparti sur l'introduction générale, trois chapitres et conclusion générale.

Dans le premier chapitre, nous avons donnés des notions fondamentales sur les corps normés ultramétriques.

Dans le deuxième chapitre nous avons présenté les différents concepts des corps des nombres p-adiques, en particulier celles qui concernent la valuation p-adique, la norme p-adique, le corps des entiers p-adiques, et quelques propriétés des nombres p-adiques.

Dans le dernier chapitre, on s'est intéressé de la détermination de l'inverse d'un nombre p-adique à l'aide de l'étude d'un problème qui consiste à trouver une solution approchée d'une équation de type $f(x) = 0$ qui converge vers l'inverse d'un nombre p-adique selon la norme p-adique par les méthodes numériques élémentaires (Newton, sécante, point fixe) et on a étudié dans ce chapitre la vitesse de convergence, le nombre d'itérations pour chaque méthode.

On a terminé par une conclusion générale.

Chapitre 1

Corps valués ultramétriques complets

1.1 Corps normés

Nous allons dans ce chapitre, donner quelques notions fondamentales concernant les corps normés ultramétrique et le procédé de complétion d'un espace métrique sans démonstration.

On dit qu'un espace métrique E est complet si toute suite de Cauchy de E converge dans E (c'est-à-dire qu'elle a une limite dans E).

On sait que $\mathbb{Q}$ n'est pas complet pour la valeur absolue ordinaire $|.|$, puisque si on considère la suite $(x_n)_n$ définie par

$$\begin{aligned}(x_n)_n &= (1, 1.4, 1.41, 1.414, 1.4142, ...) \\ &= \left(1, \frac{14}{10}, \frac{141}{100}, \frac{1414}{1000}, \frac{14142}{10000}, ...\right)\end{aligned}$$

Alors $(x_n)_n$ est une suite des nombres rationnels, de plus elle est de Cauchy dans $\mathbb{Q}$. Cependant, elle ne converge pas dans $\mathbb{Q}$, puisqu'elle a une limite $\sqrt{2}$ dans le corps complet $\mathbb{R}$.

Définition 1.1.1 *Soit K un corps.*

1. *On appelle une norme sur K toute application $\|.\|$ de K dans $\mathbb{R}^+$ telles que :*

   (a) $\forall x \in K : \|x\| = 0 \Longleftrightarrow x = 0$.

   (b) $\forall x, y \in K : \|x \cdot y\| = \|x\| \cdot \|y\|$.

   (c) $\forall x, y \in K : \|x + y\| \leq \|x\| + \|y\|$ (*l'inégalité triangulaire*).

2. *On dit que la norme $\|.\|$ est ultramétrique ou non archimédienne si*

$$\forall x, y \in K : \|x+y\| \leq \max\left(\|x\|, \|y\|\right) \text{ (}\textit{Inégalité triangulaire forte}\text{)}$$

Définition 1.1.2 *Une norme constante $\|.\|$ est dite triviale si est seulement si*

$$\|x\| = \begin{cases} 1, si\ x \neq 0 \\ \\ 0, si\ x = 0 \end{cases} \tag{1.1}$$

Remarque 1.1.3

1. *On dit parfois valeur absolue au lieu de norme de corps.*
2. *La norme $\|.\|$ est un morphisme de groupes entre les groupes multiplicatifs $(K^*, .)$ et$\left(\mathbb{R}_+^*, .\right)$ et donc que $\|1\| = 1$.*

Exemple 1.1.4 *La valeur absolue usuelle $|.|$ est une norme archimédienne sur $\mathbb{R}$. Car*

$$|(-1) - 4| = 5 > \max\left(|(-1)|, |4|\right) = 4$$

Définition 1.1.5

1. *On appelle corps valué, tout couple de la forme $(K, \|.\|)$ où K est un corps et $\|.\|$ est une norme sur K .*
2. *On appelle la distance induite sur K par $\|.\|$, la distance $d_{\|.\|}$ sur K définie par*

$$\forall x, y \in K : d_{\|.\|}(x, y) = \|x - y\| \tag{1.2}$$

3. *Si $\|.\|$ est une norme ultramétrique, alors*

$$\forall x, y, z \in K : d_{\|.\|}(x, z) \leq \max\left(d_{\|.\|}(x, y), d_{\|.\|}(y, z)\right) \tag{1.3}$$

et la distance induite par cette norme est appelée distance ultramétrique.

Définition 1.1.6 *Lorsque K muni de la distance ultramétrique, on dit que K est un corps valué ultramétrique. Dans le cas contraire, on dit que K est un corps valué archimédien.*

Proposition 1.1.7 *K est un corps ultramétrique si et seulement si*

$$\forall n \in \mathbb{N} : \|n\| \leq 1 \tag{1.4}$$

Autrement dit, $\mathbb{N}$ est borné selon $\|.\|$.

Preuve. Supposons que K est ultramétrique et montrons par récurrence que

$$\forall n \in \mathbb{N} : \|n\| \leq 1$$

pour $n = 1$, on a

$$\|1\| = 1 \leq 1$$

Supposons que $\|i\| \leq 1$ pour tout $i \leq n$ et montrons que $\|n+1\| \leq 1$.

On a

$$\begin{array}{rcl} \|n+1\| & \leq & \max\{\|n\|, \|1\|\} = 1 \\ & \Longrightarrow & \|n+1\| \leq 1 \end{array}$$

D'autre part, supposons que

$$\forall n \in \mathbb{N} : \|n\| \leq 1$$

Soient $x, y \in K$, alors

$$\begin{array}{rcl} \|(x+y)^n\| & = & \left\| \sum_{k=0}^{n} C_n^k \cdot x^k \cdot y^{n-k} \right\| \\ & \leq & \sum_{k=0}^{n} \left\|C_n^k\right\| \cdot \left\|x^k\right\| \cdot \left\|y^{n-k}\right\| \\ & \leq & \sum_{k=0}^{n} \left\|C_n^k\right\| \cdot \|x\|^k \cdot \|y\|^{n-k} \quad \text{, avec } \left\|C_n^k\right\| \leq 1 \end{array}$$

$$\|(x+y)^n\| \leq \sum_{k=0}^{n} \|x\|^k \cdot \|y\|^{n-k}$$

On sait que

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

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

Donc

$$\forall k = \overline{0,n} : \begin{cases} \|x\|^k \leq [\max(\|x\|, \|y\|)]^k \\ \|y\|^{n-k} \leq [\max(\|x\|, \|y\|)]^{n-k} \end{cases}$$

On obtient

$$\begin{aligned} \forall 0 \quad &\leq \quad k \leq n : \|x\|^k \cdot \|y\|^{n-k} \leq [\max(\|x\|, \|y\|)]^k \cdot [\max(\|x\|, \|y\|)]^{n-k} \\ &\leq \quad [\max(\|x\|, \|y\|)]^n \end{aligned}$$

Ce qui donne

$$\begin{aligned} \|(x+y)^n\| \quad &\leq \quad \sum_{k=0}^{n} [\max(\|x\|, \|y\|)]^n \\ &\leq \quad (n+1) \cdot [\max(\|x\|, \|y\|)]^n \\ &\Longrightarrow \quad \|(x+y)\| \leq (n+1)^{\frac{1}{n}} \cdot \max(\|x\|, \|y\|), \forall n \geq 1 \end{aligned}$$

Pour $n \to \infty$, alors

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

Par conséquent $\|.\|$ est une norme ultramétrique. ■

1.2 Complétion d'un corps normé

Définition 1.2.1 *(Définition générale de la complétion)*
Soit K un corps normé arbitraire (non complet) muni d'une norme$\|.\|_K$ et $\widehat{K}$ un autre corps normé muni d'une norme$\|.\|_{\widehat{K}}$. On dit que $\widehat{K}$ est le complété de K si

1. *$\widehat{K}$ contient K $\left(K \subset \widehat{K}\right)$.*
2. *K est dense dans $\widehat{K}$ (i.e : tout élément de $\widehat{K}$ est une limite d'une suite d'éléments de K).*
3. *$\forall x \in K : \|x\|_{\widehat{K}} = \|x\|_K$ $\left(\text{Prolongeant la norme définie sur } K \text{ à tout } \widehat{K}.\right)$.*
4. *$\left(\widehat{K}, \|.\|_{\widehat{K}}\right)$ est complet.*

La construction des espaces complets toujours dépend de la norme utilisée. Par exemple si on complète le corps des nombres rationnels $\mathbb{Q}$ par la valeur absolue usuelle $|.|$, alors on obtient le corps des nombres réels $\mathbb{R}$. Cependant, si on le compléte par la norme p-adique notée $|.|_p$ (où la valeur absolue p-adique), alors on obtient un espace complet que l'on note $\mathbb{Q}_p$.

Le rôle principal dans la procédure de complétion est joué par les suites de Cauchy, tel que les éléments de $\widehat{K}$ sont les classes d'équivalences des suites de Cauchy de K.

On construit $\widehat{K}$ comme suit :

Soit

$$SC(K) = \left\{ A = \{a_n\}_n \in K^{\mathbb{N}} : \lim_{n,m\to\infty} \|a_n - a_m\| = 0 \right\} \tag{1.5}$$

L'ensemble des suites de Cauchy définie dans $(K, \|.\|)$.

On définit l'ensemble des suites nulles de Cauchy

$$SN(K) = \left\{ A = \{a_n\}_n \in K^{\mathbb{N}} : \lim_{n\to\infty} \|a_n\|_K = 0 \right\} \tag{1.6}$$

On définit sur K une relation d'équivalence $\Re$ de la façon suivante :

si $u = (u_n)$ et $v = (v_n)$ sont deux éléments de K, alors $u\Re v$ si et seulement si $\|u_n - v_n\|_K$ tend vers 0 si n tend vers l'infini. Autrement dit la suite $(u_n - v_n)_n$ est une suite nulle $(u_n - v_n)_n \in SN(K)$.

On considère l'ensemble quotient

$$\widehat{K} = SC(K)/SN(K) \tag{1.7}$$

Pour tout $A = (a_n) \in \widehat{K}$, on définit la norme $\|.\|_{\widehat{K}}$ par

$$\begin{array}{rcl} \|.\|_{\widehat{K}} & : & \widehat{K} \longrightarrow \mathbb{R}^+ \\ A & \longrightarrow & \|A\|_{\widehat{K}} = \lim\limits_{n\to+\infty} \|a_n\|_K \end{array} \tag{1.8}$$

On obtient un corps normé complet $\left(\widehat{K}, \|.\|_{\widehat{K}}\right)$.

Chapitre 2

Corps des nombres p-adique

Dans ce chapitre, on va étudier le corps des nombres p-adique $\mathbb{Q}_p$. On commence par la valuation et norme p-adique sur $\mathbb{Q}$. On construit le corps $\mathbb{Q}_p$ et on étudie seulement les propriétés élémentaires analytiques des nombres p-adiques qui concernent la convergence des suites et des séries définies dans $\mathbb{Q}_p$. On donne aussi quelques propriétés topologiques de l'espace $\mathbb{Q}_p$.

2.1 Valuation et norme p-adique sur $\mathbb{Q}$

Définition 2.1.1 *Soit p un nombre premier. Alors*

1. *On appelle valuation p-adique d'un entier rationnel non nul $x \in \mathbb{Z}^*$ notée $v_p(x)$ le plus grand entier positif tel que $p^{v_p(x)}$ divise x .*

$$\begin{array}{rccl} v_p: & \mathbb{Z}^* & \longrightarrow & \mathbb{Z}^+ \\ & x & \longmapsto & v_p(x) = \max\{r \in \mathbb{Z}^+ : p^r \, divise \, x\} \end{array}$$

Dans ce cas x s'écrit

$$x = u \cdot p^{v_p(x)} \ où \ u \in \mathbb{Z}^*, \ (u,p) = 1$$

où (u,p) désigne le $p\,$gcd de u et de p. Autrement dit la valuation p-adique compte le nombre de fois que l'on peut diviser un nombre par p.

2. *La valuation p-adique d'un nombre rationnel non nul $x \in \mathbb{Q}^*$ notée $v_p(x)$ est définie par*

$$\begin{array}{rccl} v_p: & \mathbb{Q}^* & \longrightarrow & \mathbb{Z} \\ & x & \longmapsto & v_p(x) = \max\{r \in \mathbb{Z} : p^r \, divise \, x\} \end{array} \tag{2.1}$$

Remarque 2.1.2 *0 est divisible une infinité de fois par p, alors $v_p(0) = +\infty$.*

Proposition 2.1.3 *La valuation p-adique vérifie les propriétés suivantes :*

1. *si* $x = \frac{a}{b} \in \mathbb{Q}^*$, *alors* $v_p(x) = v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$
2. $v_p(x \cdot y) = v_p(x) + v_p(y), \forall x, y \in \mathbb{Q}$
3. $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}. \forall x, y \in \mathbb{Q}$

Preuve.

1. Soit $x = \frac{a}{b} \in \mathbb{Q}^*$ telles que

$$\begin{cases} a = a_1 \cdot p^{v_p(a)}, (a, a_1) \in \mathbb{Z}^2, (a_1, p) = 1 \\ \\ b = b_1 \cdot p^{v_p(b)}, (b, b_1) \in \mathbb{Z}^{*2}, (b_1, p) = 1 \end{cases}$$

On obtient

$$x = \frac{a}{b} = \frac{a_1 \cdot p^{v_p(a)}}{b_1 \cdot p^{v_p(b)}} = \frac{a_1}{b_1} p^{v_p(a) - v_p(b)}, (a_1, p) = (b_1, p) = 1$$

Alors

$$v_p(x) = v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$$

2. Soient $x, y \in \mathbb{Q}^*$, où

$$\begin{cases} x = c \cdot p^{v_p(x)} \in \mathbb{Q}^*, (c, p) = 1 \\ \\ y = d \cdot p^{v_p(y)} \in \mathbb{Q}^*, (d, p) = 1 \end{cases}$$

Alors

$$\begin{aligned} x \cdot y &= cd \cdot p^{v_p(x) + v_p(y)}, \ (cd, p) = 1 \\ &\Longrightarrow \ v_p(x \cdot y) = v_p(x) + v_p(y) \end{aligned}$$

3. Soient

$$\begin{cases} x = p^r \cdot \frac{a}{b}, v_p(x) = r \\ y = p^s \cdot \frac{c}{d}, v_p(y) = s \end{cases}$$

$$\Longrightarrow v_p(x+y) = v_p\left(p^r \cdot \frac{a}{b} + p^s \cdot \frac{c}{d}\right)$$

Supposons que $s \geq r$, donc

$$\begin{aligned} v_p(x+y) &= v_p\left(p^r \cdot \left(\frac{a}{b} + p^{s-r} \cdot \frac{c}{d}\right)\right) \\ &= v_p\left(p^r \cdot \left(\frac{ad + p^{s-r} \cdot cb}{bd}\right)\right) \end{aligned}$$

$$\begin{aligned} &= v_p\left(p^r\right) + v_p\left(\frac{ad + p^{s-r}\cdot cb}{bd}\right) \\ &= r + v_p\left(ad + p^{s-r}\cdot cb\right) - v_p\left(bd\right) \end{aligned}$$

Tant que $(bd, p) = 1$, alors $v_p(bd) = 0$.
Comme $ad + p^{s-r}\cdot cb \in \mathbb{Z}$, donc $v_p\left(ad + p^{s-r}\cdot cb\right) \geq 0$. On conclut que

$$v_p(x+y) \geq r = \min\left(v_p(x), v_p(y)\right)$$

■

2.2 Norme p-adique

Définition 2.2.1 *Soit p un nombre premier.*

1. *On considère l'application $|.|_p$ définie par*

$$|.|_p : \begin{array}{ccc} \mathbb{Q} & \longrightarrow & \mathbb{R}^+ \\ x & \longrightarrow & |x|_p = \begin{cases} p^{-r} & , \text{ si } x = p^r \cdot \frac{a}{b} \text{ avec } (a,p) = (b,p) = 1,\ r \in \mathbb{Z} \\ 0 & , \text{ si } x = 0 \end{cases} \end{array}$$

avec r représente la valuation p-adique de x.
$|.|_p$ est appelé la norme p-adique (la valeur absolue p-adique) de $\mathbb{Q}$.

2. *La distance sur $\mathbb{Q}$ induite par cette norme notée d_p (la distance p-adique) est définie par*

$$d_p : \begin{array}{ccc} \mathbb{Q}\times\mathbb{Q} & \longrightarrow & \mathbb{R}^+ \\ (x,y) & \longrightarrow & d_p(x,y) = |x-y|_p \end{array}$$

Remarque 2.2.2

1. *0 est divisible une infinité de fois par p, donc on a $|0|_p = \frac{1}{+\infty} = 0$.*
2. *De même, 1 n'est divisible aucune fois par p, donc $|1|_p = \frac{1}{p^0} = 1$.*

Proposition 2.2.3 *L'application $x \longmapsto |x|_p$ est une norme ultramétrique sur $\mathbb{Q}$.*

Preuve.

1. Soit $x \in \mathbb{Q}$, alors

$$|x|_p = 0 \iff p^{-v_p(x)} = 0 \iff -v_p(x) = -\infty \iff v_p(x) = +\infty \iff x = 0$$

2. Soient x,$y \in \mathbb{Q}$. Alors

   (a) Si $x = 0$ ou $y = 0$, alors on a l'égalité.

   (b) Sinon

$$|x \cdot y|_p = p^{-v_p(x \cdot y)} = p^{-v_p(x)-v_p(y)} = p^{-v_p(x)} \cdot p^{-v_p(y)} = |x|_p \cdot |y|_p$$

3. Soient $x, y \in \mathbb{Q}$. Alors

$$\begin{array}{lll} v_p(x+y) \geq \min(v_p(x), v_p(y)) & \Longrightarrow & -v_p(x+y) \leq -\min(v_p(x), v_p(y)) \\ & \Longrightarrow & p^{-v_p(x+y)} \leq p^{-\min(v_p(x),v_p(y))} = p^{\max(-v_p(x),-v_p(y))} \\ & \Longrightarrow & p^{-v_p(x+y)} \leq \max\left\{|x|_p, |y|_p\right\} \end{array}$$

■

Exemple 2.2.4 *La distance usuelle de* 56 *à* 2 *est* $d(56,2) = |56-2| = 54$. *Par contre, on mesure la distance* 3*-adique de* 56 *à* 2 *que la note* $d_3(56,2)$ *comme suit :*

On a

$$56 - 2 = 54 = 3^3 \cdot 2$$

Alors

$$d_3(56,2) = \left|3^3 \cdot 2\right|_3 = \frac{1}{3^3}$$

Remarque 2.2.5

1. *La propriété importante de la norme p-adique est que ses images forment un ensemble discret défini par*

$$|\mathbb{Q}|_p = \{0, p^n : n \in \mathbb{Z}\}$$

2. *Si* p *un nombre premier, tout entier* n *s'écrit sous la forme* $p^r \cdot m$ *où* r *représente la valuation p-adique et* $(m,p) = 1$, *donc*

$$\forall n \in \mathbb{Z} : |n|_p \leq p^{-r} \leq 1$$

ce qui montre que $\mathbb{Z}$ *est un ensemble borné pour toute norme p-adique* $|.|_p$.

Le théorème suivant donne la relation entre les différentes normes p-adiques $|.|_p$:

Théorème 2.2.6 (*La formule du produit*)
Pour tout nombre rationnel non nul $a \in \mathbb{Q}$, *on a* $|a|_\infty \cdot \prod_{p \text{ premier}} |a|_p = 1$. *Autrement dit pour tout* a *non nul dans* $\mathbb{Q}$, $|a|_p$ *est égal à* 1 *sauf pour un nombre fini de valeurs de* p.

Preuve. *La factorisation primaire de a s'écrit*

$$a = \mp \prod_{p \neq \infty} p^{v_p(a)}$$

D'autre part, on peut écrire le signe $\mp$ sous la forme

$$\mp = \frac{a}{|a|_\infty}$$

Alors

$$a = \frac{a}{|a|_\infty} \cdot \prod_{p \neq \infty} \frac{1}{p^{-v_p(a)}} = \frac{a}{|a|_\infty} \cdot \prod_{p \neq \infty} \frac{1}{|a|_p}$$

Donc

$$1 = \frac{1}{|a|_\infty} \cdot \prod_{p \neq \infty} \frac{1}{|a|_p} \Longrightarrow |a|_\infty \cdot \prod_{p \neq \infty} |a|_p = 1$$

■

Exemple 2.2.7 *On a pour tout $p \notin \{2, 3, \infty\}$: $\left|\frac{3}{2}\right|_p = 1$, alors*

$$\left|\frac{3}{2}\right|_\infty \cdot \prod_{p \text{ premier}} \left|\frac{3}{2}\right|_p = \left|\frac{3}{2}\right|_\infty \cdot \left|\frac{3}{2}\right|_2 \cdot \left|\frac{3}{2}\right|_3 = \frac{3}{2} \cdot 2 \cdot \frac{1}{3} = 1$$

Remarque 2.2.8 *On peut définir sur le corps des nombres rationnels $\mathbb{Q}$ trois types de valeurs absolues :*

1. *Valeur absolue triviale :*
$$|x| = \begin{cases} 1 & , \text{ si } x \neq 0 \\ 0 & , \text{ si } x = 0 \end{cases}$$
2. *Valeur absolue usuelle (ordinaire) :*
$$\begin{array}{ccc} \mathbb{Q} & \longrightarrow & \mathbb{Q}_+ \\ x & \longmapsto & |x|_\infty = \max(x, -x) \end{array} = \begin{cases} x & , \text{ si } x \geq 0 \\ -x & , \text{ si } x < 0 \end{cases}$$
3. *Valeur absolue p-adique $|.|_p$.*

On a la propriété remarquable suivante qui n'est pas vraie pour la valeur absolue ordinaire :

Théorème 2.2.9 *Soit $(a_n)_n$suite de $\mathbb{Q}$. Alors $(a_n)_n$ est une suite de Cauchy si et si seulement si*

$$\lim_{n \longrightarrow \infty} |a_{n+1} - a_n|_p = 0$$

Preuve. Si $(a_n)_n$ est une suite de Cauchy. Alors

$$\forall \varepsilon > 0, \exists n_0 \in \mathbb{N}, \forall n, m \geq n_0 : |a_m - a_n|_p \leq \varepsilon$$

En particulier, pour $m = n + 1 \geq n_0$, on a

$$\forall \varepsilon > 0, \exists n_0 \in \mathbb{N}, \forall n \geq n_0 : |a_{n+1} - a_n|_p \leq \varepsilon$$

$$\lim_{n \longrightarrow \infty} |a_{n+1} - a_n|_p = 0$$

D'autre part, supposons que

$$\lim_{n \longrightarrow \infty} |a_{n+1} - a_n|_p = 0$$

Par définition

$$\forall \varepsilon > 0, \exists n_0 \in \mathbb{N}, \forall n \geq n_0 : |a_{n+1} - a_n|_p < \varepsilon$$

Prenons $\varepsilon > 0,\ m > n \geq n_0$ et examinons $|a_m - a_n|_p$.
On a

$$|a_m - a_n|_p = |a_m - a_{m-1} + a_{m-1} - a_{m-2} + ... + a_{n+1} - a_n|_p$$

$$\begin{aligned} &\leq \max\left\{|a_m - a_{m-1}|_p, |a_{m-1} - a_{m-2}|_p, ..., |a_{n+1} - a_n|_p\right\} \\ &\leq \max(\varepsilon, \varepsilon, \varepsilon, ..., \varepsilon) = \varepsilon \end{aligned}$$

Alors $(a_n)_{n \in \mathbb{N}}$ est une suite de Cauchy. ■

2.3 Les nombres p-adiques

On sait que lorsqu'on complète $\mathbb{Q}$ par rapport à la distance associée à la valeur absolue $|.|$, on obtient $\mathbb{R}$. De la même façon, on complète $\mathbb{Q}$ par rapport à la distance associée à la norme p-adique, on obtient un espace complet que l'on note $\mathbb{Q}_p$.
Considérons l'exemple suivant :

Exemple 2.3.1 *Supposons que $p = 5$, $(a_n)_n$ et $(x_n)_n$ deux suites de $\mathbb{Q}$ définies par*

$$\begin{aligned} x_0 &= a_0 = 2 \\ x_1 &= a_0 + a_1 \cdot 5 \end{aligned}$$

$$\vdots$$

$$\begin{aligned} x_{n-1} &= a_0 + a_1 \cdot 5 + \cdots + a_{n-1} \cdot 5^{n-1} \\ x_n &= x_{n-1} + a_n \cdot 5^n \\ &\Longleftrightarrow \quad x_n - x_{n-1} \equiv 0 \bmod 5^n \end{aligned}$$

On détermine $a_n \in \{0,1,2,3,4\}$ *et* x_n *par la congruence* $x_n^2 + 1 \equiv 0 \bmod 5^n$. *La suite* $(x_n)_n$ *est de Cauchy dans* $\mathbb{Q}$ *car*

$$|x_n - x_{n-1}|_p \leq |5^n|_p = \frac{1}{5^n} \longrightarrow 0, n \longrightarrow \infty$$

Cependant, elle ne peut converger vers $x \in \mathbb{Q}$, *puisque dans ce cas, on aurait* $x^2 + 1 = 0$ *dans* $\mathbb{Q}$. *Ce qui est impossible.*

La construction de l'espace complet $\left(\mathbb{Q}_p, |.|_p\right)$ est comme suit :

1) Soit E l'ensemble des suites de Cauchy d'éléments de $\mathbb{Q}$ pour la norme p-adique.

2) On définit sur E une relation d'équivalence $\Re$ de la façon suivante : Si $u = (u_n)$ et $v = (v_n)$ sont deux éléments de E, on a $u\Re v$ si et seulement si $|u_n - v_n|_p$ tend vers zéro si n tend vers l'infini.

3) On considère l'ensemble quotient (l'ensemble des classes d'équivalences des suites de Cauchy des nombres rationnels) $\mathbb{Q}_p = E/\Re$, l'ensemble des nombres p-adiques.

Définition 2.3.2 *Soit* p *un nombre premier.*

1. *Le corps des nombres p-adiques est la complétion de l'espace métrique* $(\mathbb{Q}, d_p)$. *Ses éléments sont les classes d'équivalences des suites de Cauchy des nombres rationnels.*
2. *On prolonge la norme p-adique définie sur* $\mathbb{Q}$ *à tout* $\mathbb{Q}_p$ *par*

$$\forall \alpha \in \mathbb{Q}_p : |\alpha|_p = \lim_{n \longrightarrow \infty} |\alpha_n|_p$$

où (α_n) *est une suite de Cauchy d'éléments de* $\mathbb{Q}$ *qui représente le nombre p-adique* α.

Lemme 2.3.3 *Si* $x \in \mathbb{Q}$ *avec* $|x|_p \leq 1$, *alors*

$$\forall n \in \mathbb{N}, \exists \alpha \in \mathbb{Z} : |\alpha - x|_p \leq p^{-n}$$

Preuve. Soient $x = \frac{a}{b} \in \mathbb{Q}$, p un nombre premier tels que $(a,b) = 1 = (p,b) = (p,a)$. On a

$$\begin{aligned} |x|_p &= p^{-v_p(x)} \leq 1 \Longrightarrow p^{-v_p\left(\frac{a}{b}\right)} \leq 1 \\ &\Longrightarrow p^{-v_p(a)+v_p(b)} \leq 1 \\ &\Longrightarrow \frac{p^{v_p(b)}}{p^{v_p(a)}} \leq 1 \end{aligned}$$

Tant que

$$(p,b) = 1 \Longrightarrow (p^n, b) = 1, \forall n \in \mathbb{N}$$

D'après le théorème de Bézout

$$\exists m_1, m_2 \in \mathbb{Z} : m_1 \cdot b + m_2 \cdot p^n = 1$$

On prend

$$\alpha = a \cdot m_1 \in \mathbb{Z}$$

En effet.
On a

$$\begin{aligned} |\alpha - x|_p &= \left|a \cdot m_1 - \tfrac{a}{b}\right|_p \\ &= \left|\tfrac{a}{b} \cdot (m_1 \cdot b - 1)\right|_p \\ &= \left|\tfrac{a}{b}\right|_p \cdot |(m_1 \cdot b - 1)|_p \\ &\leq |m_1 \cdot b - 1|_p = |m_2 \cdot p^n|_p \leq p^{-n} \end{aligned}$$

■

Théorème 2.3.4 *Si la classe d'équivalence $a \in \mathbb{Q}_p$ vérifie la condition $|a|_p \leq 1$, alors elle possède un seul représentant (λ_n) qui satisfait*

$$\begin{cases} \lambda_n \in \mathbb{Z}, 0 \leq \lambda_n \leq p^n - 1 \\ \\ \lambda_{n+1} \equiv \lambda_n \bmod p^n \end{cases}$$

Preuve. Soit $a \in \mathbb{Q}_p$ tel que $|a|_p \leq 1$, alors d'après le lemme (2.3.3)

$$\exists \alpha_0 \in \mathbb{Z} : |\alpha_0 - a|_p < 1, 0 \leq \alpha_0 \leq p - 1$$

et comme $|a - \alpha_0|_p \leq \frac{1}{p} < 1$, alors $\left|\frac{a-\alpha_0}{p}\right| \leq 1$. D'après le lemme précédent, on obtient

$$\exists \alpha_1 \in \mathbb{Z} : |a - (\alpha_0 + \alpha_1 \cdot p)|_p < p^{-1}, 0 \leq \alpha_1 \leq p - 1$$

On répète cette étape, on obtient une suite des entiers rationnels $\alpha_n \in \mathbb{Z}$ tel que

$$|a - (\alpha_0 + \alpha_1 \cdot p + \ldots + \alpha_n \cdot p^n)|_p < p^{-n}, 0 \leq \alpha_n \leq p-1$$

Soit la suite (λ_n) définie par

$$\lambda_n = \alpha_0 + \alpha_1 \cdot p + \ldots + \alpha_{n-1} \cdot p^{n-1}$$

(λ_n) vérifie

$$\begin{cases} \lambda_n \in \mathbb{Z}, 0 \leq \lambda_n \leq p^n - 1 \\ \\ \lambda_{n+1} \equiv \lambda_n \bmod p^n \\ \\ \lim\limits_{n \longrightarrow \infty} \lambda_n = a \end{cases}$$

Montrons maintenant l'unicité.
Supposons que a possède deux représentants différents (λ_n) et (λ'_n) où

$$\begin{cases} \lambda_n = \alpha_0 + \alpha_1 \cdot p + \ldots + \alpha_{n-1} \cdot p^{n-1} \\ \\ \lambda'_n = \alpha'_0 + \alpha'_1 \cdot p + \ldots + \alpha'_{n-1} \cdot p^{n-1} \end{cases}$$

Soit d le premier entier pour que $\alpha_d \neq \alpha'_d$, alors nous pouvons supposer que $\alpha_d < \alpha'_d$. On trouve

$$1 \leq \alpha'_d - \alpha_d \leq p-1$$

Alors

$$\lambda'_d - \lambda_d = (\alpha'_d - \alpha_d) \cdot p^d$$

Donc

$$|\lambda'_d - \lambda_d|_p = p^{-d}$$

D'autre part, on a

$$\begin{aligned} |\lambda'_d - \lambda_d|_p &= |\lambda'_d - a + a - \lambda_d|_p \\ &\leq \max\left\{|\lambda'_d - a|_p, |a - \lambda_d|_p\right\} \\ &< p^{-d} \end{aligned}$$

Ceci contredit la dernière égalité. ■

Conclusion 2.3.5

1. *La suite de Cauchy* (λ_n) *qui vérifie les conditions du théorème précédent s'appelle représentant canonique de* a.
2. *Tout nombre p-adique* $a \in \mathbb{Q}_p$ *admet un développement p-adique unique sous forme d'une série convergente (série de Hensel) s'écrit sous la forme* $a = \sum_{k=n}^{\infty} \beta_k \cdot p^k$ *où* $\beta_k \in \{0, 1, 2, \ldots, p-1\}, n \in \mathbb{Z}$ *et* $|a|_p = p^{-n}$.
3. *On note par* $a = \beta_n \beta_{n+1} \ldots \cdot \beta_0 \beta_1 \ldots$ *la forme canonique de* a *où* $\cdot$ *est appelé le point p-adique qui nous permet de déterminer le signe de* n, *tels que :*
   (a) $a = \beta_n \beta_{n+1} \ldots \beta_{-1} \cdot \beta_0 \beta_1 \ldots$, *si* $n < 0$.
   (b) $a = \cdot \beta_0 \beta_1 \beta_2 \ldots$, *si* $n = 0$.
   (c) $a = \cdot 00 \ldots 0 \beta_0 \beta_1 \ldots$, *si* $n > 0$.

Exemple 2.3.6

Soient les nombres 5*-adiques suivants :*

1. $a_1 = 13 \cdot 41 = 1 \cdot 5^{-2} + 3 \cdot 5^{-1} + 4 \cdot 5^0 + 1 \cdot 5^1 +$, $n = -2$
2. $a_2 = \cdot 1341 = 1 \cdot 5^0 + 3 \cdot 5^1 + 4 \cdot 5^2 + 1 \cdot 5^3$, $n = 0$
3. $a_3 = \cdot 01341 = 0 \cdot 5^0 + 1 \cdot 5^1 + 3 \cdot 5^2 + 4 \cdot 5^3 + 1 \cdot 5^4$, $n = 1$

Le développement $5-$*adique de* $b = \frac{1}{3}$ *e*

$$\begin{aligned} \frac{1}{3} &= 2 \cdot 5^0 + 3 \cdot 5^1 + 1 \cdot 5^2 + 3 \cdot 5^3 + 1 \cdot 5^4 + \ldots \\ &= \cdot 231313131 \ldots = \cdot 2\overline{31} \ \ (\textit{périodique}) \end{aligned}$$

2.4 Les entiers p-adiques

Une partie intéressante de $\mathbb{Q}_p$ est l'ensemble des éléments de norme p-adique inférieure ou égale à 1, que l'on note $\mathbb{Z}_p$.

Définition 2.4.1 *On dit que le nombre p-adique* $a \in \mathbb{Q}_p$ *est un entier p-adique si le développement canonique de* a *ne contient que les puissances positives de* p. *Autrement dit* $v_p(a) \geq 0$. *On écrit*

$$a = \alpha_0 + \alpha_1 \cdot p + \alpha_2 \cdot p^2 + \ldots + \alpha_n \cdot p^n + \ldots = \sum_{n=0}^{\infty} \alpha_n \cdot p^n, 0 \leq \alpha_n < p$$

On note par $\mathbb{Z}_p$ l'ensemble des entiers p-adiques, où

$$\mathbb{Z}_p = \left\{ a \in \mathbb{Q}_p : a = \sum_{n=0}^{\infty} \alpha_n \cdot p^n \right\} = \{ a \in \mathbb{Q}_p : v_p(a) \geq 0 \}$$

Remarque 2.4.2

1. $\mathbb{Z}_p = \{ a \in \mathbb{Q}_p : v_p(a) \geq 0 \} = \left\{ a \in \mathbb{Q}_p : |a|_p \leq 1 \right\}$. *Autrement dit $\mathbb{Z}_p$ représente le disque de l'unité de rayon 1 et de centre 0.*
2. *Le corps $\mathbb{Q}_p$ est l'ensemble des fractions de $\mathbb{Z}_p$*

$$\mathbb{Q}_p = \left\{ \frac{a}{b} : (a,b) \in \mathbb{Z}_p \times \mathbb{Z}_p^* \right\}$$

Définition 2.4.3 *Soit a un nombre p-adique, on dit que a est inversible ou unitaire si le développement canonique p-adique de a ne contient que les puissances positives de p et le premier chiffre différent de zéro. On écrit*

$$a = \alpha_0 + \alpha_1 \cdot p + \alpha_2 \cdot p^2 + \ldots + \alpha_n \cdot p^n + \ldots = \sum_{n=0}^{\infty} \alpha_n \cdot p^n, 0 < \alpha_n < p$$

Notons par $\mathbb{Z}_p^*$ (ou U_p) l'ensemble de nombres p-adiques inversibles (unitaires) définie par

$$\mathbb{Z}_p^* = \left\{ \sum_{n=0}^{\infty} \alpha_n \cdot p^n : \alpha_0 \neq 0 \right\} = \{ a \in \mathbb{Q}_p : v_p(a) = 0 \} = \left\{ \alpha \in \mathbb{Z}_p : |\alpha|_p = 1 \right\}$$

Proposition 2.4.4 *Tout nombre p-adique $\alpha \in \mathbb{Q}_p$ s'écrit de façon unique sous la forme*

$$\alpha = p^n \cdot u,\ u \in \mathbb{Z}_p^*,\ n \in \mathbb{Z}$$

Preuve.

1. *Existence de la représentation :*

   Soit $\alpha \in \mathbb{Q}_p$, alors α s'écrit sous la forme

   $$\alpha = \frac{a}{b},\ (a,b) \in \mathbb{Z}_p \times \mathbb{Z}_p^*$$

   On sait que

   $$\begin{cases} a = u_1 \cdot p^{m_1}, u_1 \in \mathbb{Z}_p^*, m_1 = v_p(a) \\ \\ b = u_2 \cdot p^{m_2}, u_2 \in \mathbb{Z}_p^*, m_2 = v_p(a) \end{cases}$$

Donc

$$\alpha = \frac{a}{b} = \frac{u_1 \cdot p^{m_1}}{u_2 \cdot p^{m_2}} = \frac{u_1}{u_2} \cdot p^{m_1 - m_2} = u \cdot p^n,\ n = m_1 - m_2,\ u = \frac{u_1}{u_2} \in \mathbb{Z}_p^* \ \left(\textit{puisque } \mathbb{Z}_p^* \textit{ un corps}\right)$$

2. *Unicité de la représentation :*
   Supposons que α admet deux représentations

$$\begin{cases} \alpha = u' \cdot p^{m'}, u' \in \mathbb{Z}_p^*, m' \in \mathbb{Z} \\ \textit{et} \\ \alpha = u'' \cdot p^{m''}, u'' \in \mathbb{Z}_p^*, m'' \in \mathbb{Z} \end{cases}$$

Alors

$$\begin{aligned} u' \cdot p^{m'} &= u'' \cdot p^{m''} \Longrightarrow u' \cdot u''^{-1} = p^{m''-m'} \\ &\Longrightarrow v_p\left(u' \cdot u''^{-1}\right) = m'' - m' \end{aligned}$$

Or

$$v_p\left(u' \cdot u''^{-1}\right) = 0 \ \left(car\ u' \cdot u''^{-1} \in \mathbb{Z}_p^*\right)$$

Alors

$$m' = m''$$

et

$$u' = u''$$

■

Exemple 2.4.5 *Soient*

$$\begin{cases} p = 5 \\ \alpha^{(1)} = \cdot 4\overline{13} = 4 + 1 \cdot 5 + 3 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 \ldots \\ \alpha^{(2)} = \cdot 4\overline{2} = 4 + 2 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + 2 \cdot 5^4 \ldots \end{cases}$$

$\alpha^{(1)}$ et $\alpha^{(2)}$ sont des nombres de $\mathbb{Z}_5^*$. Par contre

$$\begin{cases} \beta^{(1)} = \cdot 01\overline{40} = 0 + 1 \cdot 5 + 4 \cdot 5^2 + 0 \cdot 5^3 + 4 \cdot 5^4 + 0 \cdot 5^5 \ldots \\ \beta^{(2)} = 42 \,.\, 13\overline{31} = 4 \cdot 5^{-2} + 2 \cdot 5^{-1} + 1 + 3 \cdot 5 + 3 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 \ldots \end{cases}$$

$\beta^{(1)} \notin \mathbb{Z}_5^*$ puisque le premier chiffre est nul, $\beta^{(2)} \notin \mathbb{Z}_5^*$ puisque le développement 5-adique de $\beta^{(2)}$ contient des puissances négatives de 5.

Lemme 2.4.6 *Si $x \in \mathbb{Q}_p^*$, alors x est inversible dans $\mathbb{Q}_p$.*

Preuve. On a

$$\forall x \in \mathbb{Q}_p^* : x = p^n \cdot u,\ u \in \mathbb{Z}_p^*,\ n \in \mathbb{Z}$$

On pose

$$u = \sum_{k=0}^{\infty} a_k \cdot p^k, a_0 \neq 0$$

Alors

$$\begin{aligned} u &= a_0 + \sum_{k=1}^{\infty} a_k \cdot p^k = a_0 + p \cdot \sum_{k=1}^{\infty} a_k \cdot p^{k-1} \\ &= a_0 + p \cdot \sum_{k=0}^{\infty} a_{k+1} \cdot p^k = a_0 + p \cdot y \text{ où } y = -\sum_{k=0}^{\infty} a_{k+1} \cdot p^k \in \mathbb{Z}_p \end{aligned}$$

Comme $a_0 \neq 0$, alors on peut prend $a_0 = 1$, on obtient

$$u = 1 - p \cdot y$$

Donc

$$u^{-1} = (1 - p \cdot y)^{-1} = 1 + y \cdot p + y^2 \cdot p^2 + \ldots \in \mathbb{Z}_p^*$$

Ce qui donne

$$x^{-1} = p^{-k} \cdot u^{-1} \in \mathbb{Q}_p^*$$

Puisque $u^{-1} \in \mathbb{Z}_p^*$, $k \in \mathbb{Z}$. Alors x est inversible dans $\mathbb{Q}_p$. ■

Lemme 2.4.7 *Soient $x \in \mathbb{Q}_p$, $k \in \mathbb{Z}$, alors*

$$\left\{ y \in \mathbb{Q}_p : |y - x|_p \leq p^k \right\} = x + p^{-k} \cdot \mathbb{Z}_p$$

Preuve. Nous avons

$$\begin{aligned} x + p^{-k} \cdot \mathbb{Z}_p &= \left\{ x + p^{-k} \cdot z, z \in \mathbb{Z}_p \right\} \\ &= \left\{ x + u,\ |u|_p \leq p^k \right\} \\ &= \left\{ y \in \mathbb{Q}_p,\ |y - x|_p \leq p^k \right\} \end{aligned}$$

■

Théorème 2.4.8 *Une suite $(a_n)_n$ de $\mathbb{Q}_p$ est de Cauchy et par conséquent convergente si et si seulement si*

$$\lim_{n \longrightarrow \infty} |a_{n+1} - a_n|_p = 0$$

Preuve. Si $(a_n)_n$ est une suite de Cauchy. Alors

$$\forall \varepsilon > 0, \exists n_0 \in \mathbb{N}, \forall n, m \geq n_0 : |a_m - a_n|_p \leq \varepsilon$$

En particulier, pour $m = n + 1 \geq n_0$, on a

$$\lim_{n \longrightarrow \infty} |a_{n+1} - a_n|_p = 0$$

D'autre part, supposons que

$$\lim_{n \longrightarrow \infty} |a_{n+1} - a_n|_p = 0$$

Par définition

$$\forall \varepsilon > 0, \exists n_0 \in \mathbb{N} \, ; \forall n \geq n_0 : |a_{n+1} - a_n|_p < \varepsilon$$

Prenons $\varepsilon > 0, \ m > n \geq n_0$ et examinons $|a_m - a_n|_p$.
On a

$$|a_m - a_n|_p = |a_m - a_{m-1} + a_{m-1} - a_{m-2} + ... + a_{n+1} - a_n|_p$$

$$\begin{aligned} &\leq \max\left\{|a_m - a_{m-1}|_p, |a_{m-1} - a_{m-2}|_p, ..., |a_{n+1} - a_n|_p\right\} \\ &\leq \max(\varepsilon, \varepsilon, \varepsilon, ..., \varepsilon) = \varepsilon \end{aligned}$$

Alors $(a_n)_{n \in \mathbb{N}}$ est une suite de Cauchy. ■

Proposition 2.4.9 *Soit $(a_n)_n$ est une suite dans $\mathbb{Q}_p$ si $\lim_{n \longrightarrow \infty} a_n = a \neq 0$ dans $\mathbb{Q}_p$, alors*

$$\exists N \in \mathbb{N} : |a_n|_p = |a|_p, \forall n > N \ \left(\textit{la suite } \left(|a_n|_p\right)_n \textit{ est stationnaire à partir d'un rang } N\right)$$

Preuve. Soit $(a_n)_n$ une suite de $\mathbb{Q}_p$ telle que $\lim_{n \longrightarrow \infty} a_n = a \neq 0$, alors $(a_n)_n$ est une suite convergente dans $\mathbb{Q}_p$, et donc de Cauchy, i.e

$$\forall \varepsilon > 0, \exists n_0 \in \mathbb{N} : \forall m > n > n_0 \Longrightarrow |a_m - a_n|_p < \varepsilon$$

D'autre part, on a

$$\left||a_m|_p - |a_n|_p\right| \leq |a_m - a_n|_p < \varepsilon$$

Donc $\left(|a_n|_p\right)_n$ est une suite de Cauchy dans $\mathbb{R}$ complet, alors $\left(|a_n|_p\right)_n$ est convergente dans $\mathbb{R}$.
Soit l sa limite

$$\lim_{n \longrightarrow +\infty} |a_n|_p = l = |a|_p$$

On a $|a|_p \neq 0$, alors $|a|_p > 0$. Donc pour $\varepsilon = \frac{l}{2} > 0$, on a

$$\exists N_1 \in \mathbb{N} : \forall n \geq N_1 \Longrightarrow \left| |a_n|_p - l \right| < \frac{l}{2}$$

On obtient

$$\begin{aligned} \left| |a_n|_p - l \right| &< \frac{l}{2} \Longrightarrow -\frac{l}{2} < |a_n|_p - l < \frac{l}{2} \\ &\Longrightarrow -\frac{l}{2} + l < |a_n|_p < \frac{l}{2} + l \\ &\Longrightarrow \frac{l}{2} < |a_n|_p < \frac{3l}{2} \end{aligned}$$

Donc

$$\exists N_1 \in \mathbb{N} : \forall n \geq N_1 \Longrightarrow |a_n|_p > \frac{l}{2} \tag{2.2}$$

De même, puisque $(a_n)_n$ est de Cauchy dans $\mathbb{Q}_p$, alors pour $\varepsilon = \frac{l}{2}$, il existe $N_2 \in \mathbb{N}$ tel que

$$\forall m, n \geq N_2 \Longrightarrow |a_m - a_n|_p < \frac{l}{2}$$

Donc, si

$$n \geq N_3 = \max\{N_1, N_2\}$$

On obtient

$$\begin{aligned} |a_m|_p &= |a_m - a_n + a_n|_p \\ &= \max\left(|a_m - a_n|_p , |a_n|_p \right) \\ &= |a_n|_p \end{aligned}$$

Pour $m \longrightarrow \infty$, alors

$$|a|_p = |a_n|_p$$

■

Proposition 2.4.10 *Une série* $\sum_{n\geq 0} a_n$ *avec* $a_n \in \mathbb{Q}_p$ *converge dans* $\mathbb{Q}_p$ *si et seulement si* $\lim_{n\longrightarrow+\infty} a_n = 0$.

Preuve. On note par $\sum_{i=0}^{n} a_i = s_n$ la suite des sommes partielles. Alors

$$\sum_{n\geq 0} a_n \text{converge dans } \mathbb{Q}_p \Longleftrightarrow (s_n)_n = (\sum_{i=0}^{n} a_i)_n \text{ converge dans } \mathbb{Q}_p$$

$$\Longleftrightarrow s_n - s_{n-1} = a_n \text{ converge vers } 0 \text{ dans } \mathbb{Q}_p$$

$$\Longleftrightarrow \lim_{n\longrightarrow\infty} a_n = 0 \text{ dans } \mathbb{Q}_p.$$

■

Remarque 2.4.11 *Cette proposition est fausse dans* $(\mathbb{R}, |.|)$*, L'exemple le plus évident d'une série dans* $(\mathbb{R}, |.|)$ *dont le terme général tend vers* 0*, mais qui ne converge pas, est la série harmonique* $\sum_{n\geq 0} \frac{1}{n}$.

Remarque 2.4.12 *Le corps des nombres p-adiques est analogue au corps des nombres réels* $\mathbb{R}$ *sur plusieurs aspects, mais le corps possède des propriétés différentes de celles du corps des réels, telles que :*

1. *Tout disque* $D(a, r) \subset \mathbb{Q}_p$ *de centre* a *et de rayon* r *est un ensemble à la fois ouvert et fermé.*
2. *Tout point d'un disque est un centre de ce disque.*
3. *Deux disques sont soit disjoints soit l'un est contenu dans l'autre.*
4. *Tout triangle dans l'espace* $(\mathbb{Q}_p, |.|_p)$ *est isocèle et la longueur de sa base ne dépasse pas les longueurs des côtés. C'est-à-dire*

$$\forall x, a \in \mathbb{Q}_p : |a - x|_p < |a|_p \Longrightarrow |x|_p = |a|_p$$

Chapitre 3

Calcul de l'inverse d'un nombre p-adique

Dans cette section, on verra comment utiliser les méthodes numériques de bases (Newton, Sécante, point fixe) pour calculer le zéro d'une fonction f où

$$\begin{cases} f(x) = \frac{1}{x} - a = 0 \\ \\ a \in \mathbb{Q}_p^*, \ p\text{-premier} \end{cases} \tag{3.1}$$

Le but consiste à calculer les développements p-adiques finis (approchés) de l'inverse de $a \in \mathbb{Q}_p^*$, et cela à l'aide de la détermination de la solution de l'équation

$$f(x) = \frac{1}{x} - a = 0 \tag{3.2}$$

par une méthode d'approximation.

La solution de(3.2) est approchée par une suite des nombres p-adiques $(x_n)_n \in \mathbb{Q}_p^*$ construite soit par la méthode de Newton, de la sécante ou par la méthode du point fixe.

Le principe général de calcul

Est le suivant :

Soit a un nombre p-adique non nul tel que

$$\begin{cases} a = p^m \cdot u, \ v_p(a) = m \in \mathbb{Z}, \ u \in \mathbb{Z}_p^* \\ \\ |a|_p = p^{-m}, \ m \in \mathbb{Z} \end{cases}$$

Il est claire que si $b \in \mathbb{Q}_p^*$ est l'inverse de a, alors

$$|b|_p = \left|a^{-1}\right|_p = p^m,\ m \in \mathbb{Z}$$

Donc la suite des nombres p-adiques $(x_n)_n$ devrait tendre vers $b \in \mathbb{Q}_p^*$. Ainsi à partir d'un certain rang, on a

$$|x_n|_p = |b|_p = p^m,\ m \in \mathbb{Z} \tag{3.3}$$

3.1 La méthode de Newton

La méthode de Newton est une méthode basée sur la construction d'une suite de points $(x_n)_n \in \mathbb{Q}_p^*$ qui converge vers le zéro de f. La fonction d'itérations de Newton est définie par

$$g(x) = x - \frac{f(x)}{f'(x)} \tag{3.4}$$

La suite des itérés associée la fonction g est

$$\forall n \in \mathbb{N} : x_{n+1} = g(x_n) = x_n - \frac{f(x_n)}{f'(x_n)} \tag{3.5}$$

Sachant que

$$f(x) = \frac{1}{x} - a,\ f'(x) = \frac{-1}{x^2} \tag{3.6}$$

La suite des itérés de Newton est

$$\forall n \in \mathbb{N} : x_{n+1} = x_n(2 - a \cdot x_n) \tag{3.7}$$

Remarque 3.1.1 *Pour mesurer la vitesse de convergence d'une méthode itérative, on mesure l'évolution de la suite $(e_{n+n_0})_n$ des écarts $e_{n+n_0} = x_{n+n_0} - x_{n+n_0-1}$ entre les itérés de la suite $(x_n)_n$ obtenus à chaque étapes d'itération.*

Théorème 3.1.2 *Si x_{n_0} est l'inverse de a de l'ordre r, alors x_{n+n_0} est l'inverse de a d'ordre $(\eta_n)_n$, tel que la suite $(\eta_n)_n$ est définie par*

$$\forall n \in \mathbb{N} : \eta_n = 2^n \cdot r \tag{3.8}$$

et la suites des écarts est définie par

$$x_{n+n_0+1} - x_{n+n_0} \equiv 0 \bmod p^{\eta'_n}$$

Où la (η'_n) est donnée par

$$\forall n \in \mathbb{N} : \eta'_n = \eta_n - m = 2^n \cdot r - m$$

Preuve. Soit $(x_n)_n$ la suite définie par la formule (3.7). On a x_{n_0} est l'inverse de a d'ordre r, c'est-à-dire

$$a \cdot x_{n_0} - 1 \equiv 0 \bmod p^r$$

Tels que n_0 représente un rang quelconque et $r \in \mathbb{N}^*$. On obtient

$$a \cdot x_{n_0} - 1 \equiv 0 \bmod p^r \implies |a \cdot x_{n_0} - 1|_p \leq p^{-r}$$

D'autre part, on a

$$\forall n \in \mathbb{N} : a \cdot x_{n+1} - 1 = -(ax_n - 1)^2 \tag{3.9}$$

Par conséquent

$$\begin{array}{rcl} |a \cdot x_{n_0+1} - 1|_p & = & |a \cdot x_{n_0} - 1|_p^2 \implies |a \cdot x_{n_0+1} - 1|_p \leq p^{-2r} \\ & \implies & a \cdot x_{n_0+1} - 1 \equiv \bmod p^{2r} \end{array}$$

De cette façon, on obtient

$$a \cdot x_{n_0} - 1 \equiv 0 \bmod p^r \implies \begin{cases} a \cdot x_{n_0+1} - 1 \equiv 0 \bmod p^{2r} \\ a \cdot x_{n_0+2} - 1 \equiv 0 \bmod p^{4r} \\ a \cdot x_{n_0+3} - 1 \equiv 0 \bmod p^{8r} \\ a \cdot x_{n_0+4} - 1 \equiv 0 \bmod p^{16r} \\ \vdots \end{cases}$$

Donc

$$\forall n \in \mathbb{N} : a \cdot x_{n+n_0} - 1 \equiv 0 \bmod p^{\eta_n} \tag{3.10}$$

La suite $(\eta_n)_n$ est définie par

$$\forall n \in \mathbb{N} : \eta_n = 2^n \cdot r \tag{3.11}$$

D'autre part, on a

$$\forall n \in \mathbb{N} : x_{n+1} - x_n = x_n (1 - a \cdot x_n) \tag{3.12}$$

Ce qui donne

$$\begin{aligned} |x_{n+n_0+1} - x_{n+n_0}|_p &= |x_{n+n_0} \cdot (1 - a \cdot x_{n+n_0})|_p \\ &= |x_{n+n_0}|_p \cdot |1 - a \cdot x_{n+n_0}|_p \leq p^m \cdot p^{-\eta_n} \end{aligned}$$

$$\begin{aligned} &\leq \quad p^m \cdot p^{-\eta_n} = p^{-(\eta_n - m)} \\ &\Longrightarrow \quad x_{n+n_0+1} - x_{n+n_0} \equiv 0 \bmod p^{\eta'_n} \end{aligned}$$

Où la suite (η'_n) est définie par

$$\forall n \in \mathbb{N} : \eta'_n = \eta_n - m = 2^n \cdot r - m \tag{3.13}$$

■

Conclusion 3.1.3

1. *La vitesse de convergence de la suite $(x_n)_n$ est de l'ordre $\eta\prime_n$.*
2. *Pour déterminer le nombre des itérations n pour une précision donnée M qui représente le nombre de chiffres p-adiques dans le développement p-adique de a^{-1}, on pose*

$$\eta\prime_n \geq M \Longleftrightarrow 2^n - r \geq M \Longrightarrow n = \left\lceil \frac{\ln \frac{M+m}{r}}{\ln 2} \right\rceil$$

Exemple 3.1.4 *(Application de la méthode de Newton)*

Supposons que

$$p = 5, a = 3, M = 8$$

Alors

$$|a|_5 = |3|_5 = 1 = p^0 \Longleftrightarrow m = 0$$

On prend $x_0 = 2$, car

$$a \cdot x_0 = 2 \cdot 3 = 6 \equiv 1 \bmod 5$$

Ce qui donne $r = 1, n_0 = 0$.
Le nombre des itérations est

$$n = \left\lceil \frac{\ln \frac{M+n}{r}}{\ln 2} \right\rceil = \left\lceil \frac{\ln \frac{8+0}{1}}{\ln 2} \right\rceil = \left\lceil \frac{3 \ln 2}{\ln 2} \right\rceil = 3$$

La suite d'itération de Newton est

$$\forall n \in \mathbb{N} : x_{n+1} = x_n(2 - 3x_n) \tag{3.14}$$

Alors

$$x_1 = 2 \cdot (2 - 2 \cdot 3) = -8 \equiv 17 = 2 + 3 \cdot 5 \bmod 5^2$$

$$x_2 = -8 \cdot (2 - 3 \cdot (-8)) = -208 \equiv 417 = 2 + 3 \cdot 5 + 1 \cdot 5^2 + 3 \cdot 5^3 \bmod 5^4$$

$x_3 = -208\cdot(2-3\cdot(-208)) = -130\,208 \equiv 260417 = 2+3\cdot5+1\cdot5^2+3\cdot5^3+1\cdot5^4+3\cdot5^5+1\cdot5^6+3\cdot5^7 \bmod 5^8$

Donc

$$\begin{cases} \frac{1}{3} \equiv 2+3\cdot5+1\cdot5^2+3\cdot5^3+1\cdot5^4+3\cdot5^5+1\cdot5^6+3\cdot5^7 \bmod 5^8 \\ \frac{1}{3} = \cdot23131313 = \cdot2\overline{31} \end{cases}$$

3.2 La méthode de la sécante

Une méthode élémentaire pour déterminer le zéro d'une fonction est la méthode de la sécante. L'idée de cette méthode consiste à remplacer $f\prime(x_n)$ par $\frac{f(x_n)-f(x_{n-1})}{x_n-x_{n-1}}$ (i.e : dans les cas où on ne peut pas calculer facilement la dérivée de f).

La relation de récurrence est donnée par

$$\forall n \in \mathbb{N}^* : x_{n+1} = x_n - \frac{f(x_n)\cdot(x_n - x_{n-1})}{f(x_n) - f(x_{n-1})} \tag{3.15}$$

La suite des itérés de la sécante est

$$\forall n \in \mathbb{N}^* : x_{n+1} = x_n + x_{n-1} - a x_n x_{n-1} \tag{3.16}$$

Théorème 3.2.1 *Si x_{n_0-1} (resp : x_{n_0}) est l'inverse de a de l'ordre α (resp :β), alors x_{n+n_0-1} est l'inverse de a de l'ordre F_n. Telle que la suite F_n est définie par*

$$\begin{aligned} F_n &= \left[\frac{1}{\sqrt{5}}\left(\beta - \frac{1-\sqrt{5}}{2}\alpha\right)\cdot\left(\frac{1+\sqrt{5}}{2}\right)^n + \frac{1}{\sqrt{5}}\left(-\beta + \frac{1+\sqrt{5}}{2}\alpha\right)\cdot\left(\frac{1-\sqrt{5}}{2}\right)^n\right] \\ &= \left[\frac{1}{\sqrt{5}}\left((\beta - \alpha(1-\Phi))\cdot\Phi^n + (-\beta+\alpha\Phi)\cdot(1-\Phi)^n\right)\right], \forall n \in \mathbb{N} \end{aligned} \tag{3.17}$$

Sachant que $\Phi = \frac{1+\sqrt{5}}{2}$.
Par conséquent

$$\forall n \in \mathbb{N} : x_{n+n_0} - x_{n+n_0-1} = 0 \bmod p^{F_n\prime}$$

Où $(F\prime_n)_n$ est définie par

$$\forall n \in \mathbb{N} : F\prime_n = F_n - m = \left[\frac{1}{\sqrt{5}}\left((\beta - \alpha(1-\Phi))\cdot\Phi^n + (-\beta+\alpha\Phi)\cdot(1-\Phi)^n\right)\right] - m \tag{3.18}$$

et $\alpha, \beta \in \mathbb{N}$.

Preuve. Soit $(x_n)_n$ la suite définie par la formule(3.16). On a x_{n_0-1} (resp : x_{n_0}) est

l'inverse de a d'ordre α (resp :β), alors

$$\begin{cases} ax_{n_0-1}-1\equiv 0 \bmod p^{\alpha} \\ \\ ax_{n_0}-1\equiv 0 \bmod p^{\beta} \end{cases} \Longrightarrow \begin{cases} |ax_{n_0-1}-1|_p \leq p^{-\alpha} \\ \\ |ax_{n_0}-1|_p \leq p^{-\beta} \end{cases}$$

D'autre part, on a

$$\forall n \in \mathbb{N}^* : ax_{n+1}-1 = (ax_n-1)\cdot(1-ax_{n-1}) \tag{3.19}$$

Ce qui donne

$$\begin{array}{rcl} |ax_{n_0+1}-1|_p & = & |ax_{n_0}-1|_p \cdot |1-ax_{n_0-1}|_p \leq p^{-\beta}\cdot p^{-\alpha} = p^{-(\alpha+\beta)} \\ & \Longrightarrow & ax_{n_0+1}-1\equiv 0 \bmod p^{\alpha+\beta} \end{array}$$

De cette manière, on obtient

$$\begin{cases} ax_{n_0-1}-1\equiv 0 \bmod p^{\alpha} \\ \\ ax_{n_0}-1\equiv 0 \bmod p^{\beta} \end{cases} \Longrightarrow \begin{cases} ax_{n_0+1}-1\equiv 0 \bmod p^{\alpha+\beta} \\ ax_{n_0+2}-1\equiv 0 \bmod p^{\alpha+2\beta} \\ ax_{n_0+3}-1\equiv 0 \bmod p^{2\alpha+3\beta} \\ ax_{n_0+4}-1\equiv 0 \bmod p^{3\alpha+5\beta} \\ \vdots \\ \vdots \end{cases}$$

Par conséquent

$$\forall n \in \mathbb{N} : ax_{n+n_0-1}-1\equiv 0 \bmod p^{F_n} \tag{3.20}$$

Où $(F_n)_n$ est une suite linéaire récurrente définie par

$$\begin{cases} \forall n \in \mathbb{N}^* : F_{n+1} = F_{n-1}+F_n \\ F_n = \alpha, F_n = \beta \end{cases} \tag{3.21}$$

dont le terme général est donné par

$$\begin{array}{rcl} \forall n & \in & \mathbb{N} : F_n = \left[\dfrac{1}{\sqrt{5}}\left(\beta-\dfrac{1-\sqrt{5}}{2}\alpha\right)\cdot\left(\dfrac{1+\sqrt{5}}{2}\right)^n + \dfrac{1}{\sqrt{5}}\left(-\beta+\dfrac{1+\sqrt{5}}{2}\alpha\right)\cdot\left(\dfrac{1-\sqrt{5}}{2}\right)^n\right] \\ & = & \left[\dfrac{1}{\sqrt{5}}\left(\beta-\alpha\left(1-\Phi\right)\right)\cdot\Phi^n + \dfrac{1}{\sqrt{5}}\left(-\beta+\alpha\Phi\right)\cdot\left(1-\Phi\right)^n\right] \end{array}$$

Tels que $\Phi = \frac{1+\sqrt{5}}{2}$ est appelé "le nombre d'or".

D'autre part, on a

$$\forall n \in \mathbb{N}^* : x_{n+1} - x_n = x_{n-1}\left(1 - a x_n\right) \tag{3.22}$$

On trouve

$$\begin{aligned} \left|x_{n+n_0} - x_{n+n_0-1}\right|_p &= \left|x_{n+n_0-2}\right|_p \cdot \left|1 - a \cdot x_{n+n_0-1}\right|_p \\ &= p^m \cdot \left|1 - a x_{n+n_0-1}\right|_p \leq p^m \cdot p^{-F_n} = p^{-(F_n - m)} \\ \Longrightarrow \quad & x_{n+n_0} - x_{n+n_0-1} = 0 \bmod p^{F_n - m} \end{aligned}$$

Par conséquent

$$\forall n \in \mathbb{N} : x_{n+n_0} - x_{n+n_0-1} = 0 \bmod p^{F_n \prime}$$

La suite $\left(F\prime_n\right)_n$ est définie par

$$\forall n \in \mathbb{N} : F\prime_n = F_n - m = \left[\frac{1}{\sqrt{5}}\left(\left(\beta - \alpha\left(1 - \Phi\right)\right) \cdot \Phi^n + \left(-\beta + \alpha\Phi\right) \cdot \left(1 - \Phi\right)^n\right)\right] - m$$

■

Conclusion 3.2.2

1. *La vitesse de convergence de la suite* $\left(x_n\right)_n$ *est de l'ordre* $F\prime_n$.
2. *Comme* $|1 - \Phi| < 1$, *alors*

$$F\prime_n \simeq \frac{1}{\sqrt{5}}\left(\beta - \alpha\left(1 - \Phi\right)\right) \cdot \Phi^n - m$$

et le nombre des itérations n *est*

$$n = \left[\frac{\ln \frac{\sqrt{5}(M+n)}{\beta - (1-\Phi)\alpha}}{\ln \Phi}\right]$$

Exemple 3.2.3 *(Application de la méthode de la sécante)*
Soient $p = 5, a = 3, M = 8$. *Alors*

$$|3|_5 = 1 = p^0 \Longrightarrow m = 0$$

On prend $x_0 = x_1 = 2$ *, puisque*

$$a \cdot x_0 = a \cdot x_1 = 3 \cdot 2 = 6 \equiv 1 \bmod 5$$

On obtient $\alpha = \beta = 1$, $n_0 = 0$.
Le nombre des itérations est

$$n = \left[\frac{\ln \frac{\sqrt{5}(8+0)}{1-(1-\Phi)}}{\ln \Phi} \right] = \left[\frac{\ln \frac{8\sqrt{5}}{\Phi}}{\ln \Phi} \right] = 5$$

D'autre part, on a

$$\forall n \in \mathbb{N}^* : x_{n+1} = x_n + x_{n-1} - 3x_n x_{n-1} \tag{3.23}$$

On trouve

$$x_0 \equiv 2 \bmod 5$$

$$x_1 \equiv 2 \bmod 5$$

$$x_2 = 2 + 2 - 3 \cdot 2 \cdot 2 = -8 \equiv 17 = 2 + 3 \cdot 5 \bmod 5^2$$

$$x_3 = -8 + 2 - 3 \cdot (-8) \cdot 2 = 42 \equiv 42 = 2 + 3 \cdot 5 + 1 \cdot 5^2 \bmod 5^3$$

$$x_4 = 42 - 8 - 3 \cdot 42 \cdot (-8) = 1042 \equiv 1042 = 2 + 3 \cdot 5 + 1 \cdot 5^2 + 3 \cdot 5^3 + 1 \cdot 5^4 \bmod 5^5$$

$$x_5 = 1042+42-3\cdot 1042\cdot 42 = -130208 \equiv 260417 = 2+3\cdot 5+1\cdot 5^2+3\cdot 5^3+1\cdot 5^4+3\cdot 5^5+1\cdot 5^6+3\cdot 5^7 \bmod 5^8$$

On écrit

$$\begin{cases} \frac{1}{3} \equiv 2 + 3 \cdot 5 + 1 \cdot 5^2 + 3 \cdot 5^3 + 1 \cdot 5^4 + 3 \cdot 5^5 + 1 \cdot 5^6 + 3 \cdot 5^7 \bmod 5^8 \\ \frac{1}{5} = \cdot 23131313 = \cdot 2\overline{31} \end{cases}$$

3.3 La méthode du point fixe

Une autre classe de méthodes consiste à remplacer la recherche de zéro de l'équation $f(x) = 0$ par une recherche de point fixe de l'équation $x = g(x)$, sous réserve que ces deux formulations soient mathématiquement équivalentes. La méthode du point fixe fournit une suite qui converge rapidement vers la solution.

On sait que si

$$g(\frac{1}{a}) = \frac{1}{a}, g^{(1)}\left(\frac{1}{a}\right) = g^{(2)}\left(\frac{1}{a}\right) = ... = g^{(s-1)}\left(\frac{1}{a}\right) = 0, g^{(s)}\left(\frac{1}{a}\right) \neq 0, s \in \mathbb{N}^* \tag{3.24}$$

Alors, on dit que la vitesse de convergence est de l'ordre s.

Notre but est d'améliorer la vitesse de convergence de la suite $(x_n)_n$. Pour cela, on cherche une fonction g telles que :

1. La fonction g doit être vérifier les conditions de (3.24).
2. La fonction g ne doit pas avoir de l'inverse de a dans ses coefficients.

On choisit g sous la forme

$$g(x) = x + x\gamma(x) = x(1 + \gamma(x)) \tag{3.25}$$

On obtient

$$\begin{cases} g^{(1)}(x) = 1 + \gamma(x) + x\gamma^{(1)}(x) \\ \\ g^{(k)}(x) = k\gamma^{(k-1)}(x) + x\gamma^{(k)}(x), k \geq 2 \end{cases} \tag{3.26}$$

On distingue les cas suivants :

3.3.1 Cas1 : $s = 2$

Si g vérifie la relation

$$g\left(\frac{1}{a}\right) = \frac{1}{a},\ g^{(1)}\left(\frac{1}{a}\right) = 0,\ g^{(2)}\left(\frac{1}{a}\right) \neq 0 \tag{3.27}$$

Alors, la fonction γ vérifie

$$\gamma\left(\frac{1}{a}\right) = 0,\ \gamma^{(1)}\left(\frac{1}{a}\right) = -a \tag{3.28}$$

On cherche la fonction γ de manière à faire disparaître l'inverse de a dans les coefficients de g. Pour cela, on prend

$$\gamma(x) = \alpha_0 + \alpha_1 x \tag{3.29}$$

D'après (3.28), on obtient

$$\begin{cases} \alpha_0 + \alpha_1 \cdot \frac{1}{a} = 0 \\ \alpha_1 = -a \end{cases} \Longrightarrow \begin{cases} \alpha_0 = 1 \\ \alpha_1 = -a \end{cases}$$

Par conséquent

$$\gamma(x) = 1 - ax \tag{3.30}$$

Ce qui donne

$$g(x) = x(1 + (1 - ax))$$

La suite associée à la fonction g est définie par

$$\forall n \in \mathbb{N} : x_{n+1} = x_n(1 + (1 - ax_n)) = x_n \cdot (2 - ax_n) \tag{3.31}$$

Cette suite représente la suite de la méthode de Newton.

Remarque 3.3.1

Dans le cas où $s = 1$, on prend $\gamma(x) = \alpha_0$, on trouve $\alpha_0 = 0$ et $g(x) = x$.

3.3.2 Cas 2 : $s = 3$

Supposons que

$$g\left(\frac{1}{a}\right) = \frac{1}{a},\ g^{(1)}\left(\frac{1}{a}\right) = g^{(2)}\left(\frac{1}{a}\right) = 0,\ g^{(3)}\left(\frac{1}{a}\right) \neq 0 \tag{3.32}$$

Alors

$$\gamma\left(\frac{1}{a}\right) = 0, \gamma^{(1)}\left(\frac{1}{a}\right) = -a, \gamma^{(2)}\left(\frac{1}{a}\right) = 2a^2 \tag{3.33}$$

On prend

$$\gamma(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 \tag{3.34}$$

D'après (3.33), on obtient

$$\begin{cases} \alpha_0 + \alpha_1 \cdot \frac{1}{a} + \alpha_2 \cdot \frac{1}{a^2} = 0 \\ \alpha_1 + 2 \cdot \alpha_2 \cdot \frac{1}{a} + a = 0 \\ 2 \cdot \alpha_2 - 2 \cdot a^2 = 0 \end{cases}$$

On résout ce système, on trouve

$$\alpha_0 = 2, \alpha_1 = -3a, \alpha_2 = a^2 \tag{3.35}$$

Donc

$$\gamma(x) = 2 - 3ax + a^2x^2 = (1 - a \cdot x) + (1 - a \cdot x)^2 \tag{3.36}$$

On écrit

$$g(x) = x\left(1 + (1 - ax) + (1 - ax)^2\right) \tag{3.37}$$

La suite des itérations $(x_n)_n$ associée à g est donnée par

$$\forall n \in \mathbb{N} : x_{n+1} = x_n \cdot \left(1 + (1 - ax_n) + (1 - ax_n)^2\right) \tag{3.38}$$

Théorème 3.3.2 *Si x_{n_0} est l'inverse de a d'ordre r, alors x_{n+n_0} est l'inverse de a d'ordre ω_n, telle que*

$$\forall n \in \mathbb{N} : \omega_n = 3^n \cdot r$$

La suite des écarts est donnée par

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \bmod p^{\omega'_n}$$

Où

$$\forall n \in \mathbb{N} : \omega'_n = \omega_n - m = 3^n \cdot r - m$$

Preuve. Soit $(x_n)_n$ la suite définie par (3.38). On a

$$\forall n \in \mathbb{N} : ax_{n+1} - 1 = (ax_n - 1)^3 \tag{3.39}$$

Supposons que

$$ax_{n_0} - 1 \equiv 0 \bmod p^r$$

Alors

$$a \cdot x_{n_0+1} - 1 \equiv 0 \bmod p^{3r}$$

Par conséquent

$$\forall n \in \mathbb{N} : ax_{n+n_0} - 1 \equiv 0 \bmod p^{\omega_n}$$

Où $(\omega_n)_n$ est définie par

$$\forall n \in \mathbb{N} : \omega_n = 3^n \cdot r$$

D'autre part, on a

$$\forall n \in \mathbb{N} : x_{n+1} - x_n = x_n \left((1 - ax_n) + (1 - ax_n)^2\right) \tag{3.40}$$

On déduit

$$\begin{array}{rcl} |x_{n+n_0+1} - x_{n+n_0}|_p & \leq & |x_{n+n_0}| \cdot \max\left(|1 - ax_{n+n_0}|, |1 - ax_{n+n_0}|^2\right) \\ & \leq & p^m \cdot \max\left\{p^{-\omega_n}, p^{-2\omega_n}\right\} = p^{-(\omega_n - m)} \\ & \Longrightarrow & x_{n+n_0+1} - x_{n+n_0} \equiv 0 \bmod p^{(\omega_n - m)} \end{array}$$

On obtient

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \bmod p^{\omega'_n}$$

Telle que

$$\forall n \in \mathbb{N} : \omega'_n = \omega_n - m = 3^n \cdot r - m$$

■

Conclusion 3.3.3

1. *La vitesse de convergence de la suite $(x_n)_n$ est de l'ordre ω'_n.*
2. $n = \left\lceil \frac{\ln\left(\frac{M+m}{r}\right)}{\ln 3} \right\rceil$ *le nombre nécessaire des itérations.*

Exemple 3.3.4 *Soient $a = 3$, $M = 9$, $p = 5$. On a $|3|_5 = 1$, $m = 0$. On prend $x_0 = 2$ puisque*

$$ax_0 = 2 \cdot 3 = 6 \equiv 1 \bmod 5$$

Alors $n_0 = 0$, $r = 1$.
Le nombre des itérations est

$$n = \left\lceil \frac{\ln\left(\frac{M+m}{r}\right)}{\ln 3} \right\rceil = \left\lceil \frac{\ln 9}{\ln 3} \right\rceil = 2$$

La forme d'itération est

$$\forall n \in \mathbb{N} : x_{n+1} = x_n \left(1 + (1 - 3x_n)\left(2 - 3x_n\right)\right)$$

On obtient

$$x_0 \equiv 2 \bmod 5$$

$$x_1 = 2 \cdot (1 + (1 - 3 \cdot 2) \cdot (2 - 3 \cdot 2)) = 42 \equiv 2 + 3 \cdot 5 + 1 \cdot 5^2 \bmod 5^3$$

$$\begin{aligned} x_2 &= 42 \cdot (1 + (1 - 3 \cdot 42) \cdot (2 - 3 \cdot 42)) \\ &= 651042 \equiv 2 + 3 \cdot 5 + 1 \cdot 5^2 + 3 \cdot 5^3 + 1 \cdot 5^4 + 3 \cdot 5^5 + 1 \cdot 5^6 + 3 \cdot 5^7 + 1 \cdot 5^8 \bmod 5^9 \bmod 5^9 \end{aligned}$$

On écrit

$$\begin{cases} \frac{1}{3} = 2 + 3 \cdot 5 + 1 \cdot 5^2 + 3 \cdot 5^3 + 1 \cdot 5^4 + 3 \cdot 5^5 + 1 \cdot 5^6 + 3 \cdot 5^7 + 1 \cdot 5^8 \bmod 5^9 \\ \frac{1}{3} = \cdot 231313131 = \cdot 2\overline{31} \end{cases}$$

Remarque 3.3.5 *Dans cet exemple, on remarque que cette méthode nécessite seulement deux itérations pour une précision donnée ($M = 9$), ce qui est un grand avantage dans le calcul.*

3.3.3 Généralisation

Généralement, on peut construire une méthode itérative qui converge vers l'inverse de a dans $\mathbb{Q}_p^*$ avec un ordre égal à s suffisamment grand. Pour généraliser la méthode du point fixe, autrement dit pour accéléré la vitesse de convergence de la suite $(x_n)_n$ autant

qu'on veut, on pose

$$\begin{cases} g(x) = x \cdot (1 + \gamma(x)) = x + x\gamma(x) \\ o\grave{u} \\ \gamma(x) = \alpha_0 + \alpha_1 x + ... + \alpha_{s-1} x^{s-1} = \sum_{j=0}^{s-1} \alpha_j x^j = \sum_{j=1}^{s-1} (1 - ax)^j \end{cases} \tag{3.41}$$

On obtient

$$g(x) = x \cdot \sum_{j=0}^{s-1} (1 - ax)^j = x\left(1 + (1 - ax) + (1 - ax)^2 + (1 - ax)^3 + \ldots + (1 - ax)^{s-1}\right) \tag{3.42}$$

La suite associée à g est définie par

$$\forall n \in \mathbb{N} : x_{n+1} = x_n\left(1 + (1 - ax_n) + (1 - ax_n)^2 + (1 - ax_n)^3 + \ldots + (1 - ax_n)^{s-1}\right) \tag{3.43}$$

Théorème 3.3.6 *Si x_{n_0} est l'inverse de a d'ordre r, alors x_{n+n_0} est l'inverse de a d'ordre σ_n, telle que*

$$\forall n \in \mathbb{N} : \sigma_n = s^n \cdot r \tag{3.44}$$

et

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \bmod p^{\sigma'_n} \tag{3.45}$$

Telle que

$$\forall n \in \mathbb{N} : \sigma'_n = \sigma_n - m = s^n \cdot r - m \tag{3.46}$$

Preuve. Soit $(x_n)_n$ la suite définie par la formule (3.43). On a

$$\forall n \in \mathbb{N} : ax_{n+1} - 1 = (-1)^{s+1}(1 - ax_n)^s \tag{3.47}$$

Supposons que

$$ax_{n_0} - 1 \equiv 0 \bmod p^r$$

On obtient

$$\begin{cases} ax_{n_0+1} - 1 \equiv 0 \bmod p^{sr} \\ ax_{n_0+2} - 1 \equiv 0 \bmod p^{s^2 r} \\ ax_{n_0+3} - 1 \equiv 0 \bmod p^{s^3 r} \end{cases}$$

Par conséquent

$$\forall n \in \mathbb{N} : ax_{n+n_0} - 1 \equiv 0 \bmod p^{\sigma_n} \tag{3.48}$$

Où la suite $(\sigma_n)_n$ est définie par

$$\forall n \in \mathbb{N} : \sigma_n = s^n r \tag{3.49}$$

D'autre part, on a

$$\forall n \in \mathbb{N} : x_{n+1} - x_n = x_n \left((1 - ax_n) + (1 - ax_n)^2 + ... + (1 - ax_n)^{s-1}\right)$$

Ce qui donne

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \bmod p^{\sigma'_n} \tag{3.50}$$

Telle que

$$\forall n \in \mathbb{N} : \sigma'_n = \sigma_n - m = s^n r - m \tag{3.51}$$

■

Conclusion 3.3.7

1. *La vitesse de convergence de la suite $(x_n)_n$ est de l'ordre σ'_n.*
2. *le nombre nécessaire d'itérations n pour obtenir M chiffres est $n = \left[\frac{\ln\left(\frac{M+m}{r}\right)}{\ln s}\right]$.*

Conclusion Générale

Soient les ensembles suivants

$$\begin{aligned} S_1 &= \left\{ a \in \mathbb{Q}_p : |a|_p = 1 \right\}, \text{ si } m = 0 \\ S_2 &= \left\{ a \in \mathbb{Q}_p : |a|_p < 1 \right\}, \text{ si } m > 0 \\ S_3 &= \left\{ a \in \mathbb{Q}_p : |a|_p > 1 \right\}, \text{ si } m < 0 \end{aligned}$$

Alors, on conclut que :

1. Si $m < 0$, alors la vitesse de convergence pour tout nombre p-adique appartient à l'ensemble S_3 est plus rapide que celle de S_1.
2. Si $m > 0$, alors la vitesse de convergence pour tout nombre p-adique appartient à l'ensemble S_3est moins rapide que celle de S_1.

Bibliographie

[1] A.J. Baker, *An Introduction to p-adic Numbers and p-adic Analysis*. Department of Mathematics, University of Glasgow, Scotland (2004).

[2] A. Quarteroni, R. Sacco, F. Saleri, *Méthodes Numériques, Algorithmes, analyse et applications.* Springer-Verlag Italia, Milano (2004).

[3] B. Diarra, *Analyse p-adique. Cours DEA- Algèbre Commutative FAST*. Université du Mali. Décembre 1999- Mars (2000).

[4] C. K. Koc, *A Tutorial on P-adic Arithmetic*. Electrical and Computer Engineering. Oregon State University, Corvallis, Oregon 97331. Technical Report, April (2002).

[5] F. B. Vej : *P-adic Numbers*. Aalborg University, Department Of Mathematical Sciences. 7E 9222 Aalborg Øst. Groupe E3-104,(2000).

[6] F.Q. Gouvéa, *P-adic Numbers : An Introduction.* Second Edition. New York : Springer-Verlag, (1997).

[7] J.P CALVI, *Méthodes Numériques*. Université Paul Sabatier 31062 Toulouse CEDEX 4 France (2004) .

[8] M. Knapp, C. Xenophotos, *Numerical analysis meets number theory : using rootfindining methods to calculate inverses mod* p^n. Appl. Anal. Discrete Math. 23–31, 4 (2010).

[9] S. Katok, *Real and p-adic analysis, Course notes for Math 497C.* Department of Mathematics, The Pennsylvania State University, Mass Program, Fall 2000 revised, November (2001).

[10] Y. Amice, *Les nombres p-adiques*. Presses universitaires de France (1975).