الجمهورية الجزائرية الديموقراطية 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. ***/***

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

Licence Académique

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

Thème

Application des méthodes numériques dans le corps Qp

Présenté par :
1- Chelghoum Meriem
2- Rezine Dalila

Dirigé par :
Kecies Mohamed

Année universitaire 2011-2012

*** Remerciements ***

Nous tenons à remercier en premier et avant tout, notre créateur <<ALLAH>>, qui nous aide à réaliser ce travail.

Nos sincères gratitudes et remerciements à notre encadreur Mohamed Kecies pour le grand soutient moral et leur aides précieuses qui nous apportez durant tout ce travail.

Nousadressons, 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.

Meriem et Dalila

Table des matières

Introduction Générale

Les corps $\mathbb{Q}_p$ des nombres p-adiques sont construits par complétion du corps des nombres rationnels $\mathbb{Q}$ lorsque celui-ci est muni d'une norme particulière nommée norme p-adique et notée $||_p$. En un sens, les corps $\mathbb{Q}_p$ sont apparentés au corps $\mathbb{R}$ des nombres réels, qui est également une complétion du corps des nombres rationnels lorsque la norme considérée est la valeur absolue habituelle $||$. Ils sont inventés au début du vingtième siècle par le mathématicien Allemand Kurt Hensel $(1861, 1941)$. 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.

Notre travail consiste à appliquer les méthodes numériques classiques Newton et la sécante dans le cas p-adique. Nous avons étudié les propriétés de chaque méthode dont la vitesse de convergence, le nombre des itérations. Ceci à travers le calcul des racines carrées des nombres p-adiques.

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 l'application des méthodes numériques classiques (Newton, sécante) dans le cas p-adique, pour déterminer la racine carrée d'un nombre $a \in \mathbb{Q}_p$. Ceci 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 la racine carrée de a. 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

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 :
i) $\forall x \in K : \|x\| = 0 \Longleftrightarrow x = 0$.
ii) $\forall x, y \in K : \|x \cdot y\| = \|x\| \cdot \|y\|$.
iii) $\forall x, y \in K : \|x + y\| \leq \|x\| + \|y\|$ *(l'inégalité triangulaire).*
2) On dit que la norme $\|.\|$ est ultramétrique ou non archimédienne si

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

c'est à dire une norme qui vérifie une condition plus forte que l'inégalité triangulaire.

3) Une norme constante $\|.\|$ est dite triviale si est seulement si

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

Remarque 1.1.2
1) On dit parfois valeur absolue au lieu de norme de corps.
2) La norme est une extension de la valeur absolue des nombres aux vecteurs.
3) La norme $\|.\|$ est un morphisme de groupes entre les groupes multiplicatifs $(K^*, .)$ et $(\mathbb{R}_+^*, .)$ et donc que $\|1\| = 1$.

Exemple 1.1.3 *La valeur absolue usuelle $|.|$ est une norme archimédienne sur $\mathbb{R}$. Car*

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

Définition 1.1.4
1) On appelle corps valué, tout couple de la forme $(K, \|.\|)$ ou 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

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

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

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

et la distance induite par cette norme appelée distance ultramétrique.
4) 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 1.1.5 *K est un corps ultramétrique si et seulement si*

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

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

$$\begin{aligned} \|n+1\| &\leq \max\{\|n\|, \|1\|\} = 1 \\ &\Rightarrow \|n+1\| \leq 1 \end{aligned}$$

Pour l'implication réciproque. On suppose que $\forall n \in \mathbb{N} : \|n\| \leq 1$.
Soient $x, y \in K$, alors

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

On sait que

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

Par conséquent

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

On obtient

$$\|x\|^k . \|y\|^{n-k} \leq [\max(\|x\|, \|y\|)]^k . [\max(\|x\|, \|y\|)]^{n-k} = [\max(\|x\|, \|y\|)]^n, \forall K = \overline{0,n}$$

Ce qui donne

$$\begin{aligned} \|(x+y)^n\| &\leq \sum_{k=0}^{n} [\max(\|x\|, \|y\|)]^n \\ &\leq (n+1) . [\max(\|x\|, \|y\|)]^n \end{aligned}$$

$$\Longrightarrow \|x+y\| \leq (n+1)^{\frac{1}{n}} . \max(\|x\|, \|y\|)$$

On sait que $\lim_{n\to\infty} (n+1)^{\frac{1}{n}} = 1$, 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 (non complet) muni d'une norme $\|.\|_K$ et $\hat{K}$ un autre corps normé muni d'une norme $\|.\|_{\hat{K}}$. On dit que $\hat{K}$ est le complété de K si
1) $\hat{K}$ contient K $\left(K \subset \hat{K}\right)$.
2) K est dense dans $\hat{K}$ (i.e : tout élément de $\hat{K}$ est une limite d'une suite d'éléments de K).
3) $\forall x \in K : \|x\|_{\hat{K}} = \|x\|_K$ (Prolongeant la norme définie sur K à tout $\hat{K}$).
4) $\left(\hat{K}, \|.\|_{\hat{K}}\right)$ est complet.

La construction des espaces complets toujours dépend de la norme utilisée. Par exemple si on complète le corps $\mathbb{Q}$ par la valeur absolue usuelle $|.|$, alors on obtient le corps $\mathbb{R}$. Cependant, si on le complète par la norme p-adique notée $|.|_p$ (ou la valeur absolue p-adique), alors on obtient un espace complet que l'on note $\mathbb{Q}_p$. Le role principal dans la procédure de complétion est joué par les suites de Cauchy, tel que les éléments de $\hat{K}$ sont les classes d'équivalences des suites de Cauchy de K.

On note par

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

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

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

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

$$\forall u = (u_n), v = (v_n) \in K : (u_n) \Re (v_n) \Longleftrightarrow \lim_{n \longrightarrow \infty} \|u_n - v_n\|_K = 0$$

On considére l'ensemble quotient

$$\hat{K} = SC(K)/SN(K)$$

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

$$\begin{array}{rccc} \|.\|_{\hat{K}} : & \hat{K} & \longrightarrow & \mathbb{R}^+ \\ & A & \longrightarrow & \|A\|_{\hat{K}} = \lim_{n \to \infty} \|a_n\|_K \end{array}$$

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

Chapitre 2

Corps des nombres p-adiques

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.

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

Dans ce cas x s'écrit

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

tel que (u,p) désigne le pgcd 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 $x \in \mathbb{Q}^*$ est définie par

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

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

Exemple 2.1.3 *Soit $a \in \mathbb{Q}$. Alors*
1) $a = p^2 + p^3 + 2p^4$, $v_p(a) = 2, \forall p \geq 2$
2) $a = 24 = 3 \cdot 8$, $(3,8) = 1$, $v_p(a) = 1$, pour $p = 3$
3) $a = 14 = 2 \cdot 7$, $(2,7) = 1$, $v_p(a) = 1$, pour $p = 2$

Proposition 2.1.4 *La valuation p-adique satisfait les propriétés suivantes :*
1) $\forall x = \frac{a}{b} \in \mathbb{Q}^* : v_p(x) = v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$

2) $\forall x, y \in \mathbb{Q} : v_p(x.y) = v_p(x) + v_p(y)$
3) $\forall x, y \in \mathbb{Q} : v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$

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

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

Ce qui donne

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

Alors

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

2) Soient $x, y \in \mathbb{Q}$, alors il y a trois cas à étudier :
i) Si $x = 0$ ou $y = 0$, on a alors $xy = 0$, donc $v_p(xy) = +\infty$ et $v_p(x) + v_p(y) = +\infty$. D'où l'égalité.
ii) Si $xy = 0$, alors $v_p(xy) = +\infty$. C'est à dire

$$\forall n \in \mathbb{N} : p^n \mid xy$$

$$\Longrightarrow \forall k, m \in \mathbb{N}, k + m = n : \begin{cases} p^k \mid x \\ p^m \mid y \end{cases}$$

$$\Longrightarrow \begin{cases} v_p(x) \geq k, \forall k \in \mathbb{N} \\ v_p(y) \geq m, \forall m \in \mathbb{N} \end{cases}$$

$$\Longrightarrow v_p(x) = +\infty \text{ et } v_p(y) = +\infty$$

Par la convention $(+\infty) + (+\infty) = +\infty$. Donc $v_p(x) + v_p(y) = +\infty$. D'où l'égalité.
iii) Soient $x, y \in \mathbb{Q}^*$ telles que

$$\begin{aligned} x &= c.p^{v_p(x)}, (c, p) = 1 \\ y &= d.p^{v_p(y)}, (d, p) = 1 \end{aligned}$$

On obtient

$$x.y = cd.p^{v_p(x) + v_p(y)}, (cd, p) = 1$$

$$\Longrightarrow v_p(x.y) = v_p(x) + v_p(y)$$

3) Soient $x, y \in \mathbb{Q}$ telles que

$$\begin{aligned} x &= p^r.\frac{a}{b}, v_p(x) = r, (a,p) = (b,p) = 1 \\ y &= p^s.\frac{c}{d}, v_p(y) = s, (c,p) = (d,p) = 1 \end{aligned}$$

On obtient

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

Supposons que $s \geq r$, donc

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

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

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

■

2.2 Norme p-adique

Définition 2.2.1 *Soit p un nombre premier.*
1) On considère l'application $|.|_p$ définie par

$$\begin{array}{rccl} |.|_p : & \mathbb{Q} & \longrightarrow & \mathbb{R}^+ \\ & x & \longrightarrow & |x|_p = \left\{ \begin{array}{ll} p^{-v_p(x)} & , \text{ si } x \neq 0 \\ 0 & , \text{ si } x = 0 \end{array} \right. \end{array}$$

avec $v_p(x)$ représente la valuation p-adique de x. L'application $|.|_p$ 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 est définie par

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

Remarque 2.2.2

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

Proposition 2.2.3 *Pour tout* p *premier l'application* $x \mapsto |x|_p$ *est une norme ultramétrique sur* $\mathbb{Q}$.

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

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

2) Soient $x, y \in \mathbb{Q}$. Alors, si $x = 0$ ou $y = 0$, on a l'égalité.
Si $x \neq 0$ et $y \neq 0$, on trouve

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

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

$$v_p(x+y) \geq \min(v_p(x), v_p(y))$$

$$\Rightarrow -v_p(x+y) \leq -\min(v_p(x), v_p(y)) = \max(-v_p(x), -v_p(y))$$

$$\Rightarrow p^{-v_p(x+y)} \leq p^{-\min(v_p(x), v_p(y))} = p^{\max(-v_p(x), -v_p(y))} = \max\left(p^{-v_p(x)}, p^{-v_p(y)}\right)$$

$$\Rightarrow |x+y|_p \leq \max\left\{|x|_p, |y|_p\right\}$$

■

Exemple 2.2.4
1) Pour $x = \frac{63}{550} = \frac{3^2 \times 7}{2 \times 5^2 \times 11} = 2^{-1} \times 5^{-2} \times 11^{-1} \times 3^2 \times 7 \in \mathbb{Q}$*. Alors*

$$|x|_2 = 2, |x|_3 = \frac{1}{9}, |x|_5 = 25, |x|_7 = \frac{1}{7}, |x|_{11} = 11, |x|_p = 1, \forall p \geq 13$$

2) La distance usuelle de 56 *à* 2 *est* $d(56, 2) = |56 - 2| = 54$*. Par contre, la distance 3-adique de* 56 *à* 2 *que la note* $d_3(56, 2)$ *est*

$$d_3(56, 2) = |56 - 2|_3 = |54|_3 = \left|3^3 \cdot 2\right|_3 = \frac{1}{3^3}$$

Remarque 2.2.5
1) La norme p-adique $|.|_p$ prend ses valeurs dans l'ensemble discret $\{0\} \cup \{p^n : n \in \mathbb{Z}\}$.
2) $\mathbb{Z}$ est un ensemble borné selon cette norme.

$$\forall x \in \mathbb{Z} : |x|_p \leq 1$$

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

Théorème 2.2.6 *(La formule du produit)*
Pour tout a non nul dans $\mathbb{Q}$, on a

$$|a|_\infty \cdot \prod_{p \text{ premier}} |a|_p = 1$$

Autrement dit, pour tout a non nul de $\mathbb{Q}$, $|a|_p$ est égal à 1 sauf pour un nombre fini de valeurs de p.

Preuve. Soit $a \in \mathbb{Q}^*$. Alors la factorisation primaire de a s'écrit $a = \mp \prod_{p \neq \infty} p^{v_{p(a)}}$.
Donc

$$|a|_\infty = \prod_{p \neq \infty} p^{v_{p(a)}}$$

D'autre part,on peut écrire le signe $\mp$ sous la forme $\mp = \frac{a}{|a|_\infty}$. Alors

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

C e qui donne

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

■

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

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

2) Valeur absolue usuelle (ordinaire) $||_\infty$

$$\begin{array}{rcl} \mathbb{Q} & \rightarrow & \mathbb{Q}_\div \\ x & \rightarrow & |x|_\infty = \max(x,-x) = \begin{cases} x, \ si \ \ x \geq 0 \\ -x, \ si \ \ x < 0 \end{cases} \end{array}$$

3) Valeur absolue p-adique $|.|_p$.

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. Soit $(a_n)_n$ 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 obtient

$$\begin{array}{rcl} \forall \varepsilon & > & 0, \exists n_0 \in \mathbb{N}, \forall n \geq n_0 : |a_{n+1} - a_n|_p \leq \varepsilon \\ & \Longrightarrow & \lim_{n \longrightarrow \infty} |a_{n+1} - a_n|_p = 0 \end{array}$$

D'autre part, supposons que $\lim_{n \longrightarrow \infty} |a_{n+1} - a_n|_p = 0$. Alors par définition de la limite, on obtient

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

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

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

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

2.3 Les nombres p-adiques

L'espace métrique associé à la distance p-adique n'est pas un espace complet, tout comme $\mathbb{Q}$ n'est pas complet pour la valeur absolue ordinaire. Lorsqu'on compléte $\mathbb{Q}$ 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 $\mathbb{Q}_p$. L'exemple suivant nous montre que l'espace métrique $\left(\mathbb{Q}, ||_p\right)$ n'est pas complet.

Exemple 2.3.1 *On considère pour $p = 5$ les deux suites $(a_n)_n$et $(x_n)_n$ de $\mathbb{Q}$ définies par*

$$\begin{aligned} a_0 &= 2 \\ x_1 &= a_0 = 2 \\ x_2 &= x_1 + a_1 \cdot 5 = a_0 + a_1 \cdot 5 \\ &\vdots \\ x_n &= a_0 + a_1 \cdot 5 + ... + a_{n-1} \cdot 5^{n-1}, \forall n \geq 1 \end{aligned}$$

$$\Longrightarrow x_{n+1} = x_n + a_n \cdot 5^n$$

$$\Longrightarrow x_{n+1} - x_n \equiv 0 \bmod 5^n$$

On détermine $a_n \in \{0, 1, 2, 3, 4\}$ et x_n par la suite de congruence

$$\forall n \geq 1 : x_n^2 + 1 \equiv 0 \bmod 5^n$$

On obtient la relation de récurrence

$$x_{n+1} \equiv x_n + x_n^2 + 1 \bmod 5^{n+1}$$

La suite $(x_n)_n$est de Cauchy dans $\mathbb{Q}$ car

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

Cependant, elle ne pent converger vers $x \in \mathbb{Q}$, puisque dans ce cas, on aurait $x^2 + 1 = 0$ dans $\mathbb{Q}$. Il n'existe pas d'entier x verifiant cette dernière équation. Ce qui est impossible.

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
Soit $x \in \mathbb{Q}$ avec $|x|_p \leq 1$. Alors pour tout $n \in \mathbb{N}$, il existe un entier unique $\alpha \in \{0, 1, ..., p^n - 1\}$ tel que

$$|\alpha - x|_p \leq p^{-n}$$

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

$$|x|_p = p^{-v_p(x)} \leq 1 \Longrightarrow p^{-v_p(\frac{a}{b})} \leq 1$$

$$\Longrightarrow p^{-v_p(a)+v_p(b)} \leq 1$$

$$\Longrightarrow v_p(b) = 0$$

pour assurer que $|x|_p \leq 1$. Alors

$$\begin{aligned} (p, b) &= 1 \Longrightarrow (p^n, b) = 1, \forall n \in \mathbb{N} \\ &\Longrightarrow \exists m_1, m_2 \in \mathbb{Z} : m_1 b + m_2 . p^n = 1 \end{aligned}$$

Soit

$$a.m_1 \equiv \alpha \bmod p^n \text{ (par la division euclidienne où } 0 \leq \alpha \leq p^n - 1)$$

Alors

$$\begin{aligned} |\alpha - x|_p &= \left|\alpha - \frac{a}{b}\right|_p = \left|a.m_1 - kp^n - \frac{a}{b}\right|_p \\ &= \left|\frac{-a}{b}.(1 - m_1 b) - kp^n\right|_p = \left|\frac{a}{b}.(1 - m_1 b) + kp^n\right|_p \\ &= \left|\frac{a}{b}.(m_2 p^n) + kp^n\right|_p \\ &\leq \max\left\{\left|\frac{a}{b}.(m_2 p^n)\right|_p, |kp^n|_p\right\} = \max\left\{p^{-n}, p^{-n}\right\} = p^{-n} \end{aligned}$$

■

Théorème 2.3.4 *Si la classe d'équivalence $a \in \mathbb{Q}_p$ vérifie la condition $|a|_p \leq 1$, alors elle posséde 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. Voir [9]. ■

Conclusion 2.3.5
1) La suite de Cauchy (λ_n) que vérifie les condition du théorème précédent s'appelle re-

présentant 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* $a = \sum_{k=n}^{\infty} \beta_k \cdot p^k$ *ou* $\beta_k \in \{0, 1, 2, ..., p-1\}, n \in \mathbb{Z}$ *et* $|a|_p = p^{-n}$.
3) On note par $a = \beta_n \beta_{n+1} ... \cdot \beta_0 \beta_1 ...$*la forme canonique de a ou* $\cdot$ *est appelé le point p-adique qui nous permet de déterminer le signe de n, tels que :*
(a) $a = \beta_n \beta_{n+1} ... \beta_{-1} . \beta_0 \beta_1 ...$, *si* $n < 0$.
(b) $a = \cdot \beta_0 \beta_1 \beta_2 ...$, *si* $n = 0$.
(c) $a = \cdot 00...0 \beta_0 \beta_1 ...$, *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) $a_3 = \cdot 01341 = 0 \cdot 5^0 + 1 \cdot 5^1 + 3 \cdot 5^2 + 4 \cdot 5^3 + 1 \cdot 5^4, n = 1$
4) Le développement 5-adique de $b = \frac{1}{3}$

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

2.4 Les entiers p-adiques

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

Définition 2.4.1
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*

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

2) On note par $\mathbb{Z}_p$ *l'ensemble des entier p-adique, 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
1) On dit que le nombre p-adique a est unitaire ou inversible si le développement canonique p-adique de a ne contient que les puissances positives de p et le premier chiffre α_0 *différent de zéro. On écrit*

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

2) Notons par $\mathbb{Z}_p^*$*(ou* U_p*) l'ensemble de nombre p-adique inversibles (unitaires) défini 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

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

Donc

$$\alpha = \frac{a}{b} = \frac{u_1 \cdot p^{m_1}}{u_2 \cdot p^{m_2}} = \frac{u_1}{u_2} \cdot p^{m_1 - m_2} = u \cdot p^n,$$

Où $n = m_1 - m_2, u = \frac{u_1}{u_2} \in \mathbb{Z}_p^*$ (puisque $\mathbb{Z}_p^*$ un corps).
2) Unicité de la représentation : Supposons que α admet deux représentations

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

Alors

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

Or

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

Alors $m^{'} = m^{''}$ et $u^{'} = u^{''}$. ■

Exemple 2.4.5 *Soient $p = 5$ et*

$$\begin{aligned} \alpha^{(1)} &= \cdot 4\overline{13} = 4 + 1 \cdot 5 + 3 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 ... \\ \alpha^{(2)} &= \cdot 4\overline{2} = 4 + 2 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + 2 \cdot 5^4 ... \end{aligned}$$

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

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

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

Lemme 2.4.6 *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

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

■

Proposition 2.4.7 *Soient $x, a \in \mathbb{Q}_p$. Si $|a - x|_p < |a|_p$, alors $|x|_p = |a|_p$. Autrement dit, tout triangle dans l'espace $(\mathbb{Q}_p, |.|_p)$ est isocèle et la longueur de sa base ne dépasse pas les longueurs des côtés.*

$$|a|_p = |x|_p$$

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*

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

Preuve. De la même manière où $||_p$ est définie sur $\mathbb{Q}$. ■

Proposition 2.4.9 *Soit $(a_n)_{n\in\mathbb{N}}$ est une suite dans $\mathbb{Q}_p$ si $\lim_{n\to\infty} a_n = a \neq 0$ dans $\mathbb{Q}_p$, alors $\exists N \in \mathbb{N} : |a_n|_p = |a|_p, \forall n > N$ (la suite $\left(|a_n|_p\right)_n$ est stationnaire à partir d'un rang N). Autrement dit $\exists N \in \mathbb{N} : |a_n|_p = |a_m|_p, \forall n; m > N$.*

Preuve. Soit $(a_n)_{n\in\mathbb{N}}$ est une suite de $\mathbb{Q}_p$ telle que $\lim_{n\to\infty} a_n = a \neq 0$, Alors$(a_n)_n$ est une suite convergente dans $\mathbb{Q}_p$, donc elle est de Cauchy, i.e

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

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

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

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

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

On obtient

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

Donc

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

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

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

Donc, si

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

On obtient

$$\begin{aligned} |a_m|_p &= |a_m - a_n + a_n|_p \quad (\,|a_m - a_n|_p \neq |a_n|_p\,) \\ &= \max(|a_m - a_n|_p\,, |a_n|_p) \qquad (isocèles) \\ &= |a_n|_p \end{aligned}$$

Pour $m \to \infty$, alors $|a|_p = |a_n|_p$. ■

Proposition 2.4.10 *Soit* $a_n \in \mathbb{Q}_p$*, alors la série* $\sum_{n\geq 0} a_n$ *converge dans* $\mathbb{Q}_p$ *si et seulement si* $\lim_{n\to+\infty} a_n = 0$.

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

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

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

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

■

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 par est la série harmonique* $\sum_{i=0} \frac{1}{n}$.

Le lemme de Hensel est un outil puissant qui lie les racines d'un polynôme donné à sa solution modulo un nombre premier. Il existe plusieurs versions. Ce résultat est très probablement le plus important et le plus utile dans toute la théorie des nombres p-adiques.

Théorème 2.4.12 *(Lemme de Hensel)*
Soit $F(x) = c_0 + c_1x + ... + c_nx^n$ *un polynôme dont les cœfficients sont des entiers p-adiques* $(c_i \in \mathbb{Z}_p)$*. Soit*

$$F'(x) = c_1 + 2c_2x + 3c_3x^2 + ... + nc_nx^{n-1}$$

la dérivée de $F(x)$*. Soit* $\bar{a}_0$ *un entier p-adique tel que* $F(\bar{a}_0) \equiv 0 \bmod p$ *et* $F'(\bar{a}_0) \not\equiv 0 \bmod p$*. Alors il existe un entier p-adique unique a tel que* $F(a) = 0$ *et* $a \equiv \bar{a}_0 \bmod p$.

Remarque 2.4.13 *Les hypothèses de ce théorème peuvent s'écrire aussi en utilisant la norme p-adique sous la forme :* $|F(a)|_p < 1$, $|F'(a)|_p = 1$ *et la conclusion* $F(a) = 0$, $|a - \bar{a}_0|_p < 1$.

Preuve. Nous allons montrer l'existence de a en construisant son expansion canonique p-adique $a = \sum_{n=0}^{\infty} b_n p^n$ par récurrence. Pour cela, On va trouver une suite $(a_k)_k$ (de Cauchy) d'entiers p-adiques définie par

$$a_k = b_0 + b_1 p + ... + b_k p^k$$

qui converge vers a. Plus précisément, nous allons montrer la propriété $S(k)$ suivante par récurrence sur k :
$S(k)$: pour tout $n \in \mathbb{N}$ il existe un entier p-adique de la forme

$$a_k = b_0 + b_1 p + ... + b_k p^k, b_i \in \{0, ..., p-1\}$$

telles que

$$\begin{cases} 1) F(a_k) \equiv 0 \bmod p^{k+1} \\ 2) a_k \equiv \bar{a}_0 \bmod p \\ 3) a_k \equiv a_{k-1} \bmod p^k \\ 4) 0 \leq a_k < p^{k+1} \end{cases}$$

Le principe de récurrence est évident :
Choisissons $b_0 \equiv \bar{a}_0 \bmod p$ (égal au premier chiffre p-adique de $\bar{a}_0$). On obtient pour tout $k \geq 1, a_k \equiv \bar{a}_0 \bmod p$ et $F(a_0) = F(b_0) = F(\bar{a}_0) \equiv 0 \bmod p^{0+1=1}$. Alors les conditions (1) et (2) sont satisfaites.
Montrons l'implication $S(k-1) \Longrightarrow S(k)$.
D'après l'hypothèse de récurrence, supposons $b_0, b_1, ..., b_{k-1}$ donnés (c'est à dire $a_0, a_1, ..., a_{k-1}$). Nous devons alors calculer a_k qui doit être de la forme $a_k = a_{k-1} + b_k p^k$ avec $b_k \in \{0, ..., p-1\}$ pour satisfaire les conditions (3) et (4) .
On montre que la condition (1) est satisfaite.
D'après la formule de Taylor, on développe $F(a_k)$ au point a_{k-1}

$$F(a_k) = F(a_{k-1} + b_k p^k) = F(a_{k-1}) + F'(a_{k-1}) b_k p^k$$

$$\Longrightarrow F(a_k) \equiv F(a_{k-1}) + F'(a_{k-1}) b_k p^k \bmod p^{k+1}$$

d'après l'hypothèse de récurrence $F(a_{k-1}) \equiv 0 \bmod p^k$, on peut écrire $F(a_{k-1}) \equiv \lambda p^k \bmod p^{k+1}$ avec p ne divise pas λ et la condition $F(a_k) \equiv 0 \bmod p^{k+1}$ devient donc

$$\lambda p^k + F'(a_{k-1}) b_k p^k \equiv 0 \bmod p^{k+1}$$

c'est à dire

$$\lambda + F'(a_{k-1}) b_k \equiv 0 \bmod p$$

d'après l'hypothèse de récurrence

$$a_{k-1} \equiv a_{k-2} \equiv ... \equiv \bar{a}_0 \equiv 0 \bmod p$$

On a

$$F'(a_{k-1}) \equiv F'(\bar{a}_0) \not\equiv 0 \bmod p$$

et donc, on choisit l'unique b_k tel que

$$b_k \equiv \frac{-\lambda}{F'(a_{k-1})} \bmod p$$

D'où le a_k cherché.
D'autre part, on a la suite (a_k) est de Cauchy dans $\mathbb{Z}_p$ (complet), alors il y a un unique $a \in \mathbb{Z}_p$ tel que

$$\lim_{k \to \infty} a_k = a$$

de plus le polynôme F est continu, on obtient

$$F(a) = F(\lim_{k \to \infty} a_k) = \lim_{k \to \infty} F(a_k) = 0$$

■

Nous allons présenter ici quelques résultats qui découlent du lemme de Hensel. Le théorème suivant nous donne la relation entre les nombres p-adiques et les congruences.

Théorème 2.4.14 *Un polynôme F à coefficients dans $\mathbb{Z}_p$ possède des racines dans $\mathbb{Z}_p$ si et seulement s'il admet des racines modulo p^k pour tout $k \geqslant 1$.*

Preuve. Voir [9]. ■

Nous allons présenter ici une application du lemme de Hensel qui nous permet de déterminer les éléments de $\mathbb{Q}_p$ qui sont des carrés.

Proposition 2.4.15 *1) Supposons que $p \neq 2$. Soit $a = p^{v_p(a)}.u \in \mathbb{Q}_p$ un nombre p-adique non nul avec $u \in \mathbb{Z}_p^*$. Alors a est un carré dans $\mathbb{Q}_p$ si et seulement si $v_p(a)$ est paire et*

l'image de u dans $\mathbb{Z}_p^*$ est un carré. ie $x = p^{2n}y^2$
2) Supposons que $p = 2$, alors pour qu'un élément $a = 2^{v_2(a)}.u \in \mathbb{Q}_2^*$ soit un carré, il faut et il suffit que $v_2(a)$ soit paire et $u \equiv 1 \bmod 8$.

Preuve.
Soit $a \in \mathbb{Q}_p^*$, alors a s'écrit sous la forme

$$a = p^{v_p(a)}.u = p^{v_p(a)}.(a_0 + a_1p + a_2p^2 + ...)$$
$$u = a_0 + a_1p + a_2p^2 + ..., a_0 \neq 0$$

Soit $b = p^{v_p(b)}(x_0 + x_1p + x_2p^2 + ...) \in \mathbb{Q}_p^*$, $x_0 \neq 0$. Alors

$$b^2 = a \Longleftrightarrow p^{2v_p(b)}(x_0 + x_1p + x_2p^2 + ...)^2 = p^{v_p(a)}.u$$

et

$$u = (x_0 + x_1p + x_2p^2 + ...)^2 = a_0 + a_1p + a_2p^2 + ...$$

On distingue deux cas :
1) si $p \neq 2$, donc

$$v_p(a) = 2v_p(b), x_0^2 - a_0 \equiv 0 \bmod p$$

D'autre part, soit le polynôme

$$F(x) = x^2 - u$$

Alors

$$F(x_0) = x_0^2 - u \equiv 0 \bmod p$$

D'autre part, on a

$$F'(x_0) = 2x_0, F'(x_0) \not\equiv 0 \bmod p$$

Donc d'après le lemme de Hensel, u est un carré dans $\mathbb{Q}_p$.
2) Si $p = 2$, alors

$$x_0^2 - a_0 \equiv 0 \bmod 2$$

où $0 < x_0 < 2$. Donc $x_0 = 1, a_0 = 1$.
On obtient

$$b^2 = a \Longleftrightarrow 2^{2v_2(b)}(1 + x_12 + x_22^2 + ...)^2 = 2^{v_2(a)}(1 + a_12 + a_22^2 + ...) = 2^{v_2(a)}.u$$

D'autre part, on a

$$(1 + x_1 2 + x_2 2^2 + ...)^2 = 1 + (\frac{x_1 + x_1^2}{2} + x_2)2^3 + ...$$

Donc

$$2^{2v_2(b)}(1 + (\frac{x_1 + x_1^2}{2} + x_2)2^3 + ...) = 2^{v_p(a)}(1 + a_1 2 + a_2 2^2 + ...)$$

Ce qui donne

$$v_2(a) = 2v_2(b), x_0 = a_0 = 1, a_1 = a_2 = 0$$

Donc la valuation 2-adique de a est paire.
D'autre part, on a

$$u = a_0 + a_1 2 + a_2 2^2 + ...$$
$$a_0 = 1, a_1 = a_2 = 0$$
$$\Longrightarrow u = 1 + a_3 2^3 + a_4 2^4 + ... = 1 + 2^3.(a_3 + a_4 2 + ...)$$

Ce qui donne

$$u \equiv 1 \bmod 8$$

■

Exemple 2.4.16
1) *Ils existent des nombres dans $\mathbb{Q}_3$ qui n'admettent pas des racines carrées par exemple*

$$a = 5 = 2 + 1.3$$

En effet, soit

$$x = \alpha_0 + \alpha_1.3 + ... + \alpha_n.3^n + ... \in \mathbb{Q}_3, \alpha_n \in \{0, 1, 2\}$$

Alors

$$x^2 = a \Longrightarrow (\alpha_0 + \alpha_1.3 + ... + \alpha_n.3^n + ...)^2 = 2 + 1.3$$

Donc

$$\alpha_0^2 = 2 \bmod 3$$

Dans ce cas α_0 n'éxiste pas. Alors x est aussi n'existe pas.
2) *Le nombre 2-adique $y = -1$ n'a pas de racine carrée dans $\mathbb{Q}_2$ car*

$$-1 \not\equiv 1 \bmod 8$$

Chapitre 3

Application des méthodes numériques dans le corps $\mathbb{Q}_p$ (Racine carrée)

L'objet essentiel de ce chapitre est l'approximation des racines d'une fonction définie par

$$f(x) = x^2 - a$$

On a vu que si $(x_n)_n$ est une suite des nombres p-adiques qui converge vers un nombre p-adique $\alpha \neq 0$, alors à partir d'un certain rang

$$|x_n|_p = |\alpha|_p$$

Autrement dit la suite des valeurs absolues est stationnaire.

On sait que s'il existe un nombre p-adique α tel que $\alpha^2 = a$, alors $v_p(a)$ est paire notée $2m$. On obtient

$$|x_n|_p = p^{-m}$$

3.1 La méthode de Newton

La méthode de Newton, ou méthode de Newton-Raphson, est un algorithme pour trouver des approximations d'un zéro (ou racine) d'une fonction f. La suite d'itérations de Newton est définie par

$$\forall n \in \mathbb{N} : x_{n+1} = \frac{x_n^2 + a}{2x_n} \tag{3.1}$$

Remarque 3.1.1 *La détermination de la vitesse de convergence de la méthode de Newton*

consiste à étudier le comportement 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 la racine carrée de* a *d'ordre* r*, alors*
1) Si $p \neq 2$*, alors* x_{n+n_0} *est la racine carrée de* a *d'ordre* γ_n*.*
2) Si $p = 2$*, alors* x_{n+n_0} *est la racine carrée de* a *d'ordre* γ'_n*.*

Preuve.
Soit $(x_n)_n$ la suite définie par (3.1). On a

$$\forall n \in \mathbb{N} : x_{n+1}^2 - a = \frac{(x_n^2 - a)^2}{4x_n^2}$$

Supposons que

$$x_{n_0}^2 - a \equiv 0 \bmod p^r$$

Et comme

$$|4|_p = \begin{cases} \frac{1}{4}, p = 2 \\ 1, p \neq 2 \end{cases}$$

Alors

$$\left|x_{n_0+1}^2 - a\right|_p = \frac{1}{|4|_p} . \frac{\left|(x_{n_0}^2 - a)^2\right|_p}{\left|x_{n_0}^2\right|_p} \Longrightarrow \begin{cases} \left|x_{n_0+1}^2 - a\right|_2 \leq 2^2 . 2^{2m} . 2^{-2r} = 2^{-[2r-2(m+1)]}, \text{ si } p = 2 \\ \\ \left|x_{n_0+1}^2 - a\right|_p \leq p^{2m} . p^{-2r} = p^{-[2r-2m]}, \text{ si } p \neq 2 \end{cases}$$

$$\Longrightarrow \begin{cases} x_{n_0+1}^2 - a \equiv 0 \bmod 2^{2r-2(m+1)}, & p = 2 \\ \\ x_{n_0+1}^2 - a \equiv 0 \bmod p^{2r-2m}, & p \neq 2 \end{cases}$$

De cette manière, on obtient
1- Si $p \neq 2$, alors

$$x_{n_0}^2 - a \equiv 0 \bmod p^r \Longrightarrow \begin{cases} x_{n_0+1}^2 - a \equiv 0 \bmod p^{2r-2m} \\ x_{n_0+2}^2 - a \equiv 0 \bmod p^{4r-6m} \\ x_{n_0+3}^2 - a \equiv 0 \bmod p^{8r-14m} \\ x_{n_0+4}^2 - a \equiv 0 \bmod p^{16r-30m} \\ \vdots \\ \vdots \end{cases}$$

On en déduit que

$$\forall n \in \mathbb{N} : x_{n+n_0}^2 - a \equiv 0 \bmod p^{\gamma_n}$$

La suite $(\gamma_n)_n$ est définie par

$$\forall n \in \mathbb{N} : \gamma_n = 2^n r - C_n.m$$

Où

$$\begin{cases} C_0 = 0 \\ \forall n \in \mathbb{N} : C_{n+1} = 2C_n + 2 \end{cases} \iff \forall n \in \mathbb{N} : C_n = 2(2^n - 1)$$

Donc

$$\forall n \in \mathbb{N} : \gamma_n = 2^n r - 2(2^n - 1)m$$

2- Si $p = 2$, alors

$$x_{n_0}^2 - a \equiv 0 \bmod 2^r \Longrightarrow \begin{cases} x_{n_0+1}^2 - a \equiv 0 \bmod 2^{2r-2(m+1)} \\ x_{n_0+2}^2 - a \equiv 0 \bmod 2^{4r-6(m+1)} \\ x_{n_0+3}^2 - a \equiv 0 \bmod 2^{8r-14(m+1)} \\ x_{n_0+4}^2 - a \equiv 0 \bmod 2^{16r-30(m+1)} \\ \qquad\qquad . \\ \qquad\qquad . \end{cases}$$

Il vient que

$$\forall n \in \mathbb{N} : x_{n+n_0}^2 - a \equiv 0 \bmod 2^{\gamma'_n}$$

Telle que la suite $(\gamma'_n)_n$ est définie par

$$\forall n \in \mathbb{N} : \gamma'_n = 2^n r - C_n(m+1) = 2^n r - 2(2^n - 1)(m+1) = \gamma_n - 2(2^n - 1)$$

D'autre part, on a

$$\forall n \in \mathbb{N} : x_{n+1} - x_n = \frac{a - x_n^2}{2x_n}$$

Et comme

$$|2|_p = \begin{cases} \frac{1}{2}, p = 2 \\ 1, p \neq 2 \end{cases}$$

Alors

$$|x_{n+n_0+1} - x_{n+n_0}|_p = \frac{1}{|2|_p}.\frac{|a - x_{n+n_0}^2|_p}{p^{-m}} \Longrightarrow \begin{cases} |x_{n+n_0+1} - x_{n+n_0}|_2 \leq 2.2^m.2^{-\gamma'_n}, \text{ si } p = 2 \\ \\ |x_{n+n_0+1} - x_{n+n_0}|_p \leq p^m.p^{-\gamma_n} \text{ , si } p \neq 2 \end{cases}$$

$$\Longrightarrow \begin{cases} x_{n+n_0+1} - x_{n+n_0} \equiv 0 \bmod 2^{\gamma'_n-(m+1)}, & \text{si } p = 2 \\ \\ x_{n+n_0+1} - x_{n+n_0} \equiv 0 \bmod p^{\gamma_n-m}, & \text{si } p \neq 2 \end{cases}$$

On obtient

1- Si $p \neq 2$, alors

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

Telle que

$$\forall n \in \mathbb{N} : v_n = \gamma_n - m = 2^n r - (2^{n+1} - 1).m$$

2- Si $p = 2$, alors

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \bmod 2^{v'_n}$$

Telle que

$$\forall n \in \mathbb{N} : v'_n = \gamma'_n - (m+1) = 2^n r - (2^{n+1} - 1)(m+1) = v_n - (2^{n+1} - 1)$$

■

Conclusion 3.1.3

1) ***Si*** $p \neq 2$, *alors*

a) La vitesse de convergence de la suite $(x_n)_n$ *est de l'ordre* v_n .

b) Si $r - 2m > 0$, *alors le nombre des itérations pour* M *chiffres donnés est*

$$\begin{aligned} v_n \quad &\geq \quad M \Longleftrightarrow 2^n r - (2^{n+1} - 1).m \geq M \\ &\Longrightarrow \quad n = \left[\frac{\ln(\frac{M-m}{r-2m})}{\ln 2} \right] \end{aligned}$$

2) ***Si*** $p = 2$, *alors*

a) La vitesse de convergence est de l'ordre v'_n.

b) $n = \left[\frac{\ln\left(\frac{M-(m+1)}{r-2(m+1)}\right)}{\ln 2} \right]$ *représente le nombre nécessaire d'itérations* n *pour* M *chiffres donnés si* $r - 2(m+1) > 0$.

3.2 La méthode de la sécante

La méthode de la sécante est une méthode dérivée de celle de Newton où l'on remplace $f\prime(x_n)$, par

$$\frac{f(x_n) - f(x_{n-1})}{x_n - x_{n-1}}$$

On obtient la relation de récurrence

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

Donc la suite d'itération de la méthode de la sécante est

$$\forall n \in \mathbb{N}^* : x_{n+1} = \frac{x_n.x_{n-1} + a}{x_n + x_{n-1}} \tag{3.2}$$

Théorème 3.2.1 *Si x_{n_0-1} (resp : x_{n_0}) est la racine carrée de a d'ordre α (resp : β), alors :*
1) Si $p \neq 2$, alors x_{n+n_0-1} est la racine carrée de a d'ordre φ_n.
2) Si $p = 2$, alors x_{n+n_0-1} est la racine carrée de a d'ordre φ'_n.

Preuve.
Soit $(x_n)_n$ la suite définie par (3.2). On a

$$\forall n \in \mathbb{N}^* : x_{n+1}^2 - a = \frac{(x_n^2 - a).(x_{n-1}^2 - a)}{(x_n + x_{n-1})^2}$$

Supposons que $x_{n_0-1}^2 \equiv a \bmod p^\alpha, x_{n_0}^2 \equiv a \bmod p^\beta, \alpha$ et $\beta \in \mathbb{N}$. Alors

$$\left|x_{n_0+1}^2 - a\right|_p = \frac{\left|(x_{n_0}^2 - a)(x_{n_0-1}^2 - a)\right|_p}{\left|x_{n_0} + x_{n_0-1}\right|_p^2}$$

$$\Longrightarrow \left|x_{n_0+1}^2 - a\right|_p = \frac{1}{|4|_p}.\frac{\left|x_{n_0}^2 - a\right|_p \left|x_{n_0-1}^2 - a\right|_p}{p^{-2m}}$$

$$\Longrightarrow \begin{cases} \left|x_{n_0+1}^2 - a\right|_2 = 4.2^{2m}.\left|x_{n_0}^2 - a\right|_2 \left|x_{n_0-1}^2 - a\right|_2, & \text{si } p = 2 \\ \left|x_{n_0+1}^2 - a\right|_p = p^{2m}.\left|x_{n_0}^2 - a\right|_p \left|x_{n_0-1}^2 - a\right|_p, & \text{si } p \neq 2 \end{cases}$$

$$\Longrightarrow \begin{cases} \left|x_{n_0+1}^2 - a\right|_2 \leq 2^2.2^{2m}.2^{-\beta}.2^{-\alpha}, & \text{si } p = 2 \\ \left|x_{n_0+1}^2 - a\right|_p \leq p^{2m}.p^{-\beta}.p^{-\alpha}, & \text{si } p \neq 2 \end{cases}$$

$$\Longrightarrow \begin{cases} x_{n_0+1}^2 - a \equiv 0 \bmod 2^{\alpha+\beta-2(m+1)}, & \text{si } p = 2 \\ x_{n_0+1}^2 - a \equiv 0 \bmod p^{\alpha+\beta-2m}, & \text{si } p \neq 2 \end{cases}$$

de cette manière, on obtient
1- Si $p \neq 2$, alors

$$\begin{cases} x_{n_0-1}^2 \equiv a \bmod p^{\alpha} \\ \\ x_{n_0}^2 \equiv a \bmod p^{\beta} \end{cases} \Longrightarrow \begin{cases} x_{n_0+1}^2 - a \equiv 0 \bmod p^{(\alpha+\beta)-2m} \\ x_{n_0+2}^2 - a \equiv \bmod p^{(\alpha+2\beta)-4m} \\ x_{n_0+3}^2 - a \equiv 0 \bmod p^{(2\alpha+3\beta)-8m} \\ x_{n_0+4}^2 - a \equiv 0 \bmod p^{(3\alpha+5\beta)-14m} \\ \vdots \\ \vdots \end{cases}$$

On en déduit que

$$\forall n \in \mathbb{N} : x_{n+n_0-1}^2 - a \equiv 0 \bmod p^{\varphi_n}$$

La suite $(\varphi_n)_n$ est définie par

$$\forall n \in \mathbb{N} : \varphi_n = J_n - mA_n$$

Telles que

$$\begin{cases} J_0 = \alpha \ , \ J_1 = \beta \\ \\ \forall n \in \mathbb{N}^* : J_{n+1} = J_{n-1} + J_n \end{cases} , \begin{cases} A_0 = A_1 = 0 \\ \\ \forall n \in \mathbb{N}^* : A_{n+1} = A_{n-1} + A_n + 2 \end{cases}$$

la suite $(J_n)_n$ est une suite de Fibonacci généralisée dont le terme générale est donnée par

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

Où $\Phi = \frac{1+\sqrt{5}}{2}$.
La suite $(A_n)_n$ est une suite récurrente linéaire d'ordre deux à coefficients constants avec second membre constant s'écrit sous la forme

$$\begin{cases} A_{n+1} = aA_{n-1} + bA_n + c \\ \\ a = b = 1 \ , \ c = 2 \end{cases}$$

La suite $(A_n)_n$ est équivalent à

$$A_{n+1} + 2 = (A_{n-1} + 2) + (A_n + 2)$$

On pose

$$\forall n \in \mathbb{N} : B_n = A_n + 2$$

Ceci est équivalent à

$$\begin{cases} B_0 = B_1 = 2 \\ \forall n \in \mathbb{N} : B_{n+1} = B_{n-1} + B_n \end{cases}$$

Où

$$\forall n \in \mathbb{N} : B_n = 2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1} - (1-\Phi)^{n+1}\right)\right]$$

Donc

$$\forall n \in \mathbb{N} : A_n = B_n - 2 = 2(q_n - 1) = 2(\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1} - (1-\Phi)^{n+1}\right)\right] - 1)$$

La suite $(\varphi_n)_n$ est définie par

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

$$-2(\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1} - (1-\Phi)^{n+1}\right)\right] - 1)m$$

2- Si $p = 2$, alors

$$\begin{cases} x_{n_0-1}^2 \equiv a \bmod 2^{\alpha} \\ \\ x_{n_0}^2 \equiv a \bmod 2^{\beta} \end{cases} \Longrightarrow \begin{cases} x_{n_0+1}^2 - a \equiv 0 \bmod 2^{(\alpha+\beta)-2(m+1)} \\ x_{n_0+2}^2 - a \equiv \bmod 2^{(\alpha+2\beta)-4(m+1)} \\ x_{n_0+3}^2 - a \equiv 0 \bmod 2^{(2\alpha+3\beta)-8(m+1)} \\ x_{n_0+4}^2 - a \equiv 0 \bmod 2^{(3\alpha+5\beta)-14(m+1)} \\ \cdot \\ \cdot \end{cases}$$

Par conséquent

$$\forall n \in \mathbb{N} : x_{n+n_0-1}^2 - a \equiv 0 \bmod 2^{\varphi'_n}$$

Où $(\varphi'_n)_n$ est donnée par

$$\forall n \in \mathbb{N} : \varphi'_n = J_n - (m+1)A_n$$

Donc

$$\forall n \in \mathbb{N} : \varphi'_n = \left[\frac{1}{\sqrt{5}}\left(\beta - \alpha(1-\Phi)\right)\Phi^n + \frac{1}{\sqrt{5}}\left(-\beta + \alpha\Phi\right)(1-\Phi)^n\right] +$$

$$-2(\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1).(m+1)$$

Par conséquent

$$\forall n\in\mathbb{N}:\varphi'_n=\varphi_n-2(\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1)$$

D'autre part, on a

$$\forall n\in\mathbb{N}^*:x_{n+1}-x_n=\frac{a-x_n^2}{x_n+x_{n-1}}$$

On obtient

$$|x_{n+n_0}-x_{n+n_0-1}|_p=\frac{\left|a-x_{n+n_0-1}^2\right|_p}{|x_{n+n_0-1}+x_{n+n_0-2}|_p}$$

$$\Longrightarrow\begin{cases}|x_{n+n_0}-x_{n+n_0-1}|_2=2.2^m.\left|a-x_{n_0-1}^2\right|_2\ ,\ \text{si } p=2\\ \\ |x_{n+n_0}-x_{n+n_0-1}|_p=p^m.\left|a-x_{n_0-1}^2\right|_p\ ,\ \text{si }\ p\neq 2\end{cases}$$

$$\Longrightarrow\begin{cases}|x_{n+n_0}-x_{n+n_0-1}|_2\leq 2.2^m.2^{-\varphi'_n},\ \text{si }\ p=2\\ \\ |x_{n+n_0}-x_{n+n_0-1}|_p\leq p^m.p^{-\varphi_n}\ ,\ \text{si }\ p\neq 2\end{cases}$$

$$\Longrightarrow\begin{cases}x_{n+n_0}-x_{n+n_0-1}\equiv 0\bmod 2^{\varphi'_n-(m+1)}\ ,\ \text{si }\ p=2\\ \\ x_{n+n_0}-x_{n+n_0-1}\equiv 0\bmod p^{\varphi_n-m}\ ,\ \text{si }\ p\neq 2\end{cases}$$

On trouve

1- Si $p\neq 2$, alors

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

Avec

$$\forall n\in\mathbb{N}:\psi_n=\varphi_n-m$$

On obtient

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

$$-(2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1)m$$

2- Si $p=2$, alors

$$\forall n\in\mathbb{N}:x_{n+n_0}-x_{n+n_0-1}\equiv 0\bmod 2^{\psi'_n}$$

La suite$(\psi'_n)_n$ s'écrit sous la forme

$$\forall n \in \mathbb{N} : \psi'_n = \varphi'_n - (m+1)$$

On obtient

$$\forall n \in \mathbb{N} : \psi'_n = \left[\frac{1}{\sqrt{5}}\left(\beta - \alpha(1-\Phi)\right)\Phi^n + \frac{1}{\sqrt{5}}\left(-\beta + \alpha\Phi\right)(1-\Phi)^n\right]$$

$$-(2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1} - (1-\Phi)^{n+1}\right)\right] - 1)(m+1)$$

$$= \psi_n - (2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1} - (1-\Phi)^{n+1}\right)\right] - 1)$$

■

Conclusion 3.2.2

1) ***Si*** $p \neq 2$ ***,*** *alors*

a) La vitesse de convergence de la suite est de l'ordre ψ_n.

b) Comme $|1-\Phi| < 1$, *alors* $(1-\Phi)^n \longrightarrow 0$ *et*

$$\psi_n \simeq \frac{1}{\sqrt{5}}\left(\beta - \alpha(1-\Phi)\right)\Phi^n - \frac{2}{\sqrt{5}}(\Phi^{n+1} - 1)m$$

donc le nombre nécessaire d'itérations n pour M chiffres donnés est

$$n = \left[\frac{\ln\left(\frac{\sqrt{5}(M-m)}{\beta-\alpha(1-\Phi)-2\Phi m}\right)}{\ln\Phi}\right]$$

avec $\beta - \alpha(1-\Phi) - 2\Phi m > 0$.

2) ***Si*** $p = 2$***,*** *alors*

a) La vitesse de convergence de la suite $(x_n)_n$ *est de l'ordre* ψ'_n .

b) $n = \left[\frac{\ln\left(\frac{\sqrt{5}(M-(m+1))}{\beta-\alpha(1-\Phi)-2\Phi(m+1)}\right)}{\ln\Phi}\right]$ *est le nombre des itérations pour une précision donnée M,*
avec $\beta - \alpha(1-\Phi) - 2\Phi(m+1) > 0$.

Conclusion Générale

On considère les ensembles suivant

$$\text{Si } p \neq 2, \begin{cases} S_1 = \left\{a \in \mathbb{Q}_p : |a|_p = 1\right\}, \text{ si } m = 0 \\ S_2 = \left\{a \in \mathbb{Q}_p : |a|_p < 1\right\}, \text{ si } m > 0 \\ S_3 = \left\{a \in \mathbb{Q}_p : |a|_p > 1\right\}, \text{ si } m < 0 \end{cases}$$

$$\text{Si } p = 2, \begin{cases} B_1 = \left\{a \in \mathbb{Q}_2 : |a|_2 = 4\right\}, \text{ si } m = -1 \\ B_2 = \left\{a \in \mathbb{Q}_2 : |a|_2 < 4\right\}, \text{ si } m > -1 \\ B_3 = \left\{a \in \mathbb{Q}_2 : |a|_2 > 4\right\}, \text{ si } m < -1 \end{cases}$$

On conclut

1. **La méthode de Newton :**
   (a) Si $p \neq 2$, alors
      i. La vitesse de convergence est quadratique pour tout nombre p-adique appartient à S_1.
      ii. La vitesse de convergence est plus rapide (quadratique avec un avancement) pour tout nombre p-adique appartient à S_3.
      iii. La vitesse de convergence est moins rapide (quadratique avec un retard) pour tout nombre p-adique appartient à S_2.
   (b) Si $p = 2$ alors
      i. La vitesse de convergence est quadratique pour tout nombre 2-adique appartient à B_1.
      ii. La vitesse de convergence est plus rapide pour tout nombre 2-adique appartient à B_3.
      iii. La vitesse de convergence est moins rapide pour tout nombre 2-adique appartient à B_2.

2. **La méthode de la sécante :**

   (a) Si $p \neq 2$, alors

      i. La vitesse de convergence est superlinéaire pour tout nombre p-adique appartient à S_1.

      ii. La vitesse de convergence est plus rapide (superlinéaire avec un avancement) pour tout nombre p-adique appartient à S_3.

      iii. La vitesse de convergence est moins rapide (superlinéaire avec un retard) pour tout nombre p-adique appartient à S_2.

   (b) Si $p = 2$, alors

      i. La vitesse de convergence est superlinéaire pour tout nombre 2-adique appartient à B_1.

      ii. La vitesse de convergence est plus rapide pour tout nombre 2-adique appartient à B_3.

      iii. La vitesse de convergence est moins rapide pour tout nombre 2-adique appartient à B_2.

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 (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 Bézivin, *Dynamique des fractions rationnelles p-adiques*. Université de Caen (2005).

[8] M. Knapp, C. Xenophotos. *Numerical analysis meets number theory : using rootfinding 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, Mass Program, Fall 2000

(2001).

[10] T. Zerzaihi, M. Kecies, M. Knapp. *Hensel codes of square roots of p-adic numbers*. Appl. Anal. Discrete Math. 32-44, 4. (2010).

[11] W.H. Schiko, *Ultrametric Calculus*, *An Introduction to p-adic Analysis*, Cambridge Studies in Adv. Math. 4, Cambridge University Press, (1984).

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