REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE
Université De Jijel
FACULTE DES SCIENCES
DEPARTEMENT DE MATHEMATIQUES

N° D'ordre :.....
Série :.....

MEMOIRE

Présenté en vue de l'obtention du diplôme de Magister
En Mathématiques
Option: Analyse

THEME

L'algorithme de calcul de code de Hensel pour les racines des nombres p-adiques

Par

Kecies Mohamed

Devant le jury :

Président	: Aibeche. Aissa	Prof.	Univ. Sétif
Rapporteur	: Zerzaihi. Tahar	MC.	Univ. Jijel
Examinateurs	: Denche. Mohamed	Prof.	Univ. Constantine
	Laouir. Dalila	MC.	Univ. Jijel
	Yarou. Mustapha	MC.	Univ. Jijel

Soutenue le 29/06/2006

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE
Université De Jijel
FACULTE DES SCIENCES
DEPARTEMENT DE MATHEMATIQUES

N° D'ordre :.....
Série :.....

MEMOIRE

Présenté en vue de l'obtention du diplôme de Magister
En Mathématiques
Option: Analyse
THEME

L'algorithme de calcul de code de Hensel pour les racines des nombres p-adiques

Par

Kecies Mohamed

Devant le jury :

Président	: Aibeche. Aissa	Prof.	Univ. Sétif
Rapporteur	: Zerzaihi. Tahar	MC.	Univ. Jijel
Examinateurs	: Denche. Mohamed	Prof.	Univ. Constantine
	Laouir. Dalila	MC.	Univ. Jijel
	Yarou. Mustapha	MC.	Univ. Jijel

Soutenue le 29/06/2006

Remerciements

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

Je remercie vivement Monsieur T.Zerzaihi maître de conférence et vice doyen chargé de la pédagogie à l'université de Jijel, d'avoir voulu proposer et assurer la direction de cette thèse , sa disponibilité , son soutien , ses encouragements et ses précieux conseils tout au long de ce travail .

J'exprime ma profonde reconnaissance à Monsieur A.Aibeche, Professeur à l'université de Sétif, pour avoir accepté de présider le jury de cette thèse et pour son aide précieuse.

J'adresse, également, mes remerciements chaleureux à Mr. M.Denche, professeur à l'institut de mathématiques de l'université de Constantine, pour m'avoir fait l'honneur de participer au jury de ce travail, et pour l'aide qu'il m'a apporté au cours de mon magister.

Je tiens à associer à ces remerciements, Mr. M.Yarrou, Maître de Conférence, et chef de département de mathématiques à l'université de Jijel et Mme D.Azzam-Laouir, Maître de Conférence à l'université de Jijel, qui ont bien voulu prendre la responsabilité d'évaluer ce travail, qu'ils soient vivement remercié.

Je ne saurais oublier l'ensemble des collègues de l'équipe de magister qui ont su installer une joyeuse ambiance de travail, avec une pensée particulière pour Melles N.Fetouci, D.Affane, et Mrs, A.Yagoub, R.Bougecha.

Enfin, je tiens à exprimer ma reconnaissance à Mr.M.Kerada, Mr.B.Diarra, A.Esbelin et M.Boukrouche, aux membres du département de mathématiques de l'université de Jijel et à tous ceux qui ont pris part de près ou de loin, à la réalisation de ce travail.

Dédicace

A mes très chers parents .....

Ames frères :

Mahfoud

Elias

Youcef

Hocine

Abd –rahman

Adel

Ames sœurs:

Fatima

Meriem

Samia

A mes amis :

F. Labrèche

Adlen

Feteh et Son frère, Hocine, ...

Et à tous ceux qui me sont chers.

Table des matières

Introduction Générale

Les nombres p-adiques sont une extension des nombres rationnels qui sont utilisés en théorie des nombres pour calculer modulo une puissance d'un nombre premier p. Il sont des objets curieux, inventés au début du vingtième siècle par le mathématicien Allemand Kurt Hensel (1861,1941). L'objectif étant de rendre disponibles pour la théorie des nombres les méthodes de développement en séries qui jouent un rôle dominant dans la théorie des fonctions.

La principale motivation ayant donné naissance aux corps des nombres p-adiques était de pouvoir utiliser les techniques des séries de puissances dans la théorie des nombres, mais leur utilité dépasse maintenant largement ce cadre. De plus, $\mathbb{Q}_p$ il est muni d'une norme non archimédienne $|.|_p$. On obtient alors une analyse, différente de l'analyse usuelle, que l'on appelle analyse p-aphysique théorique. Une des raisons est que les nombres p-adiques fournissent un exemple simple de structure en arbre (par exemple dans l'études théoriques des propriétés thermodynamiques des verres de spin). Les applications de l'analyse p-adique à la physique pourraient même aller au delà des aspects strictement dique.

Les nombres p-adiques n'interviennent pas qu'en mathématiques pures. On les voit apparaître dans des domaines inattendus comme les probabilités ou la techniques. Des physiciens théoriciens se livrent par exemple à des spéculations sur la structure de l'espace et du temps à très petite échelle. Les lois de la relativité et de la physique quantique semblent indiquer qu'il n'est pas possible de mesurer des longueurs inférieures à une valeur extraordinairement petite, appelée longueur de Plank, et qui est de l'ordre de 10^{-35} mètre. L'existence d'une distance minimale suggère à certains théoriciens qu'à cette échelle, la structure ultime de l'espace - temps pourrait se décrire non pas en terme de nombres réels mais en termes de structure p-adique.

L'application des nombres p-adique et de l'analyse p-adique qui nous intéresse dans ce travail est penchée vers l'informatique. Si l'idée de l'inverse et de la racine carrée d'un nombre réel ne provoque aucun souci de la part d'un mathématicien, alors cette même

question est d'actualité pour l'informatique où l'on doit trouver suffisamment de chiffres après la virgule et avoir des renseignement sur leur nature. Des méthodes existent déjà pour le calcul de l'inverse ou de la racine carrée d'un nombre réel, telles que la méthode de Newton, de la sécante et autres. Dans ce travail, il est question technique de calculer l'inverse et la racine carrée d'un nombre p-adique. Le passage du cas p-adique au cas réel fait partie d'un autre travail qu'on compte réaliser à l'avenir.

Ce mémoire est réparti sur l'introduction générale et trois chapitres ; le premier chapitre est composé de deux parties. Dans la première, on a donné les notions des corps ultramétriques normés, et celles de complétion d'un corps normé. Dans la deuxième partie, on donne des notions fondamentales et des propriétés analytiques des nombres p-adiques, ensuite on définit les codes de Hensel et les opérations arithmétiques avec les codes.

Le deuxième chapitre est réparti aussi sur deux parties. Dans la première partie nous avons présenté les fonctions p-adiques continues et dérivable et on termine cette partie par le lemme de Hensel qui montre l'existence d'une solution p-adiques des équations à variables p-adiques. Dans la deuxième partie, on s'intéresse à la détermination les codes de Hensel de l'inverse des nombres p-adiques à l'aide de l'étude d'un problème qui consiste à trouver une solution approché 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 étudie dans ce chapitre la vitesse de convergence, la détermination du code de Hensel et du nombre d'itération pour chaque méthode, muni par des exemples illustratifs à chaque méthode.

En s'inspirant du cas de l'inverse, on passe au troisième chapitre au calcul de la racine carrée d'un nombre p-adique. Le travail dans ce chapitre consiste à déterminer un algorithme de calcul de codes de Hensel (les premiers chiffres) des racines carrées d'un nombre p-adique engendré par les méthodes numériques précédentes à travers le calcul de la solution approchée d'une équation non linéaire. Nous avons appliqué dans ce chapitre le même travail réalisé dans le deuxième chapitre et enfin, on termine par une conclusion générale.

Chapitre 1

Corps valués ultramétriques complets et nombres p-adiques

Première partie

Corps valués ultramétriques complets

1.1 les corps normés :

Définition 1.1.1 *Soit K un corps . On appelle une norme sur K toute application $\|.\|$ de K dans $\mathbb{R}^+$ telle que*
1)$\forall x \in K : \|x\| = 0 \Longleftrightarrow x = 0$
2) $\forall x, y \in K : \|x.y\| = \|x\| \,.\, \|y\|$
3) $\forall x, y \in K : \|x + y\| = \|x\| + \|y\|$

Exemple 1.1.2 *la valeur absolue usuelle $|.|$ est une norme sur $\mathbb{R}$.*

Définition 1.1.3 *On dit que la norme $\|.\|$ est ultramétrique (non archimédienne) si au lieu de (3) on a*

$$4)\forall x, y \in K : \|x + y\| \leq \max(\|x\|, \|y\|) \text{ (inégalitée triangulaire forte)}$$

et il est claire que 4) $\Rightarrow$ 3)

Définition 1.1.4 *On appelle corps valué, tout couple de la forme $(K, \|.\|)$ où K un corps et $\|.\|$ une norme sur K et on appelle la distance induite sur K par $\|.\|$, la distance $d_{\|.\|}$ sur K définie par*

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

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

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

la distance induite par cette norme est appelée distance ultramétrique.

Définition 1.1.5 *Lorsque K muni de la distance ultramétrique, on dit que K est un corps valué ultramétrique (non archimédien). Dans le cas contraire, on dit que K est un corps valué archimédien.*

Proposition 1.1.6 [11] [24]
K un corps ultramétrique si et seulement si

$$\forall n \in \mathbb{N} : \|n\| \leq 1 \tag{1.1}$$

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

Preuve.
Supposons que

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

alors

$$\begin{aligned}
\forall x, y \quad \in \quad K : \|(x+y)^n\| &= \left\| \sum_{k=0}^{n} c_n^k . x^k . y^{n-k} \right\| \\
&\leq \sum_{k=0}^{n} c_n^k . \left\|x^k\right\| . \left\|y^{n-k}\right\| \\
&\leq \sum_{k=0}^{n} c_n^k . \|x\|^k . \|y\|^{n-k} \quad , \text{avec } c_n^k \leq 1 \\
\|(x+y)^n\| &\leq \sum_{k=0}^{n} \|x\|^k . \|y\|^{n-k}
\end{aligned}$$

d'autre part, on a

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

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

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

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

ce qui donne

$$\begin{aligned}
\forall x, y \quad \in \quad K : \|(x+y)^n\| &\leq \sum_{k=0}^{n} [\max(\|x\| , \|y\|)]^n \\
&\leq (n+1) . [\max(\|x\| , \|y\|)]^n \\
&\Longrightarrow \|(x+y)\| \leq (n+1)^{\frac{1}{n}} . \max(\|x\| , \|y\|), \forall n \geq 1 \\
\text{pour } n \quad &\rightarrow \quad \infty, \ \|(x+y)\| \leq \max(\|x\| , \|y\|)
\end{aligned}$$

alors $\|.\|$ est une norme ultramétrique. ■

Proposition 1.1.7 [18]
Soit K un corps non-archimédien, $a, x \in K$, on a si $\|a - x\| \prec \|a\|$, alors $\|x\| = \|a\|$.

Autrement dit, tout les triangles de $(K, \|.\|)$ sont isocèles.

Preuve.

on a

$$\forall x, a \in K : \|x\| = \|x - a + a\| \leq \max\{\|a\|, \|x - a\|\} = \|a\|$$

d'autre part, on a

$$\|a\| = \|a - x + x\| \leq \max\{\|x - a\|, \|x\|\}$$

si $\|x - a\| \succ \|x\|$, alors

$$\|a\| \leq \|x - a\|$$

contradiction, donc $\|x - a\| \prec \|x\|$, ce qui donne

$$\|a\| \leq \|x\|$$

on déduit que

$$\|a\| = \|x\|$$

■

Définition 1.1.8 *On dit que deux normes $\|.\|_1$ et $\|.\|_2$ sur K sont équivalentes si et seulement si leurs distances associées induisent la même topologie sur K. Autrement dit $\tau_{\|.\|_1} = \tau_{\|.\|_2}$.*

Lemme 1.1.9 [17]
Soit K un corps et $\|.\|_1$ et $\|.\|_2$ deux normes sur K : les normes $\|.\|_1$ et $\|.\|_2$ sont équivalentes si et seulement si

$$\forall x_n \in K : \|x_n\|_1 \underset{n}{\longrightarrow} 0 \Longleftrightarrow \|x_n\|_2 \underset{n}{\longrightarrow} 0$$

Théorème 1.1.10 [2]
Soient $\|.\|_1$ et $\|.\|_2$ deux normes sur K, alors $\|.\|_1$ et $\|.\|_2$ sont équivalentes si et seulement s'il existe un réel positif α tel que

$$\forall x \in K : \|x\|_1 = \|x\|_2^{\alpha}$$

Preuve.

L'implication réciproque est évidente grâce au lemme (1.1.9). Pour l'implication directe Soit x un élément de K tel que $\|x\|_1 \prec 1$. La suite $(x^n)_n$ converge vers 0 dans $(K, d_{\|.\|_1})$ donc elle converge vers 0 dans $(K, d_{\|.\|_2})$ d'ou $\|x\|_2 \prec 1$. En échangeant le rôle joué par les

deux normes, on obtient que

$$\forall x \in K : \|x\|_1 \prec 1 \Longleftrightarrow \|x\|_2 \prec 1$$

Ensuite en remplaçant x par $\frac{1}{x}$ (avec $x \neq 0$), on obtient

$$\forall x \in K : \|x\|_1 \succ 1 \Longleftrightarrow \|x\|_2 \succ 1$$

et par conséquent

$$\forall x \in K : \|x\|_1 = 1 \Longleftrightarrow \|x\|_2 = 1$$

Ainsi si $\|.\|_1$ est une norme triviale, on en déduit que $\|.\|_2$ est également une norme triviale aussi.
Supposons que $\|.\|_1$ ne soit pas triviale, alors

$$\exists x_0 \in K : \|x_0\|_1 \succ 1$$

et

$$\|x_0\|_2 \succ 1$$

ce qui implique qu'il existe $\alpha \in \mathbb{R}^+$ tel que

$$\|x_0\|_1 = \|x_0\|_2^{\alpha}, \alpha = \frac{\ln \|x_0\|_1}{\ln \|x_0\|_2} \succ 0$$

Soit $x \in K$ avec $\|x\|_1 \succ 1$. Considérons le réel β pour lequel

$$\|x\|_1 = \|x_0\|_2^{\beta}$$

Pour tout rationnel $\frac{p}{q} \prec \beta$, on a les équivalences suivantes

$$\|x\|_1 \prec \|x_0\|_1^{\frac{p}{q}} \Longleftrightarrow \|x^q\|_1 \prec \|x_0^p\|_1$$

$$\Longleftrightarrow \left\| \frac{x^q}{x_0^p} \right\|_1 \prec 1$$

$$\Longleftrightarrow \left\| \frac{x^q}{x_0^p} \right\|_2 \prec 1$$

$$\Longleftrightarrow \|x^q\|_2 \prec \|x_0^p\|_2$$

$$\Longleftrightarrow \|x\|_2 \prec \|x_0\|_2^{\frac{p}{q}}$$

En faissant tendre $\frac{p}{q}$ vers β dans $\mathbb{R}$, on obtient que

$$\|x\|_2 \leq \|x_0\|_2^{\beta}$$

En appliquant le même raisonnement à un rationnel $\frac{p}{q} \succ \beta$ puis en passant à la limite, on obtient

$$\|x\|_2 \geq \|x_0\|_2^{\beta}$$

ce qui nous fournit les égalités

$$\begin{aligned} \|x\|_2 &= \|x_0\|_2^{\beta} \\ &= \|x_0\|_1^{\frac{\beta}{\alpha}} \\ &= \|x\|_1^{\frac{1}{\alpha}} \end{aligned}$$

$$\Longrightarrow \|x\|_1 = \|x\|_2^{\alpha}$$

valable pour tout élément $x \in K$ tel que $\|x\|_1 \succ 1$. En remplaçant x par $\frac{1}{x}$ $(x \neq 0)$ et en utilisant la multiplicativitée des normes, on en déduit que

$$\forall x \in K : \|x\|_1 = \|x\|_2^{\alpha}, \text{ pour } \|x\|_1 \neq 1$$

Soit $x \in K$ tel que $\|x\|_1 = 1$. L'élément $\frac{x}{x_0}$ qui vérifie

$$\begin{aligned} \left\|\frac{x}{x_0}\right\|_1 &= \frac{\|x\|_1}{\|x_0\|_1} \\ &= \frac{1}{\|x_0\|_1} \prec 1 \end{aligned}$$

donc on a

$$\left\|\frac{x}{x_0}\right\|_1 = \left\|\frac{x}{x_0}\right\|_1^{\alpha} \Leftrightarrow \|x\|_1 = \|x\|_2^{\alpha}$$

(car $\|x_0\|_1 = \|x_0\|_2^{\alpha}$) ce qui nous permet d'affirmer que

$$\forall x \in K, \exists \alpha \in \mathbb{R}^+ : \|x\|_1 = \|x\|_2^{\alpha}$$

■

1.1.1 Complétion d'un corps normé

Définition 1.1.11 *(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 (construit à partir de K) muni d'une norme $\|.\|_{\widehat{K}}$ .On dit que $\widehat{K}$ est le complété de K si
1) $\widehat{K}$ contient K ($K \subset \widehat{K}$).
2) K est dense dans $\widehat{K}$ par rapport à la topologie associé avec $\|.\|_{\widehat{K}}$.
3) $\forall x \in K : \|x\|_K = \|x\|_{\widehat{K}}$ (la norme $\|.\|_{\widehat{K}}$ est définie à partir de $\|.\|_K$).
4) $(\widehat{K}, \|.\|_{\widehat{K}})$ est complet.

Dans le cas où le corps $\mathbb{Q}$ des nombres rationnels est muni da la norme euclidienne $|.|$ la procédure de complétion donne le corps des nombres réels $\mathbb{R}$. Même procédure sera appliquée plus tard au corps $\mathbb{Q}$ muni d'une autre norme spécifique pour obtenir le corps des nombres p-adiques noté $\mathbb{Q}_p$.
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. Tout d'abord, on commence par une introduction sur les suites de Cauchy dans un corps normé K.
a) 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 $(K, \|.\|)$, cet ensemble est un anneau commutatif, l'élément neutre par rapport à l'addition est la suite

$$\{0\}_{n \in \mathbb{N}} = \{0, 0, 0, ...0, ..\}$$

et l'élément neutre par rapport à la multiplication est la suite

$$\{1\}_{n \in \mathbb{N}} = \{1, 1, 1, ...1, ..\}$$

Il est claire que $SC(K)$ n'est pas un corps puisqu'il contient un diviseur de Zéro.

$$\{1, 0, 0, 0, ...\}.\{0, 1, 0, 0, ...\} = \{0, 0, 0, ..., 0, .\} = \{0\}_{n \in \mathbb{N}^*}$$

b) Maintenant, on définit l'ensemble des suites nulles de Cauchy

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

On a

$$SN(K) \subset SC(K)$$

En effet

$$\forall n, m \in \mathbb{N} : \|a_n - a_m\| \leq \|a_n\| + \|a_m\|$$

donc pour $n, m \longrightarrow \infty$ *alors* $\|a_n - a_m\| \longrightarrow 0$. *ce qui donne* $\{a_n\}_n$ *est une suite de Cauchy*
c) Soit l'ensemble de quotient

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

l'ensemble des classes d'équivalence des suites de Cauchy $\{a_n\}_n$. *Notons que la suite constante*

$$\{a\}_{n\in\mathbb{N}} = \{a, a, a, ...\}, a \in K$$

appartienne à des classes différentes pour différents éléments a. *Et notons par* (a_n) *la classe d'équivalence qui représente la suite de Cauchy* $\{a\}_n$. *Ainsi* $(a_n) \in \widehat{K}$, *et nous allons considérer* K *comme un sous ensemble de* $\widehat{K}$, *et nous identifions* $a \in K$ *avec* $\widehat{a} = (a) \in \widehat{K}$.

Théorème 1.1.12 [4]
L'ensemble de quotient $\widehat{K} = SC(K)/SN(K)$ *est un corps.*

Proposition 1.1.13 [4]
L'application $\|.\|_{\widehat{K}}$ *est une norme sur* $\widehat{K}$, *de plus elle est non archimédienne si* $\|.\|_K$ *est aussi .*

Maintenant, montrons que si $\|.\|_K$ est ultramétrique alors $\|.\|_{\widehat{K}}$ est aussi et pour cela on a le lemme suivant

Lemme 1.1.14 [17]
Soit K *un corps muni de la norme ultramétrique* $\|.\|_K$, $\{a_n\}_n$ *est une suite de Cauchy dans* K *et* $b \in K$ *tel que* $\lim\limits_{n\longrightarrow b} a_n \neq b$, *sous ces conditions on a*

$$\exists N \in \mathbb{N}, \forall n, m \succ N : \|a_n - b\|_K = \|a_m - b\|_K$$

on dit que la suite numérique $(\|a_n - b\|_K)_n$ *est stationnaire à partir d'un rang* $N \in \mathbb{N}$, *de plus si* $\{a_n\}_n$ *n'est pas une suite nulle alors* $(\|a_n\|_K)_n$ *est stationnaire.*

Preuve.
Soit $\{a_n\}_n$ est une suite de Cauchy dans K.

$$\forall \varepsilon \succ 0, \exists N \in \mathbb{N} : \forall n, m \geq N \Longrightarrow \|a_n - a_m\|_K \prec \varepsilon$$

d'autre part

$$\forall n, m \geq N : |\|a_m - b\|_K - \|a_n - b\|_K| \leq \|a_n - a_m\|_K \prec \varepsilon$$

donc la suite $(\|a_n - b\|_k)_n$ est de Cauchy dans $\mathbb{R}^+$, d'où elle est convergente. Soit l sa limite puisque

$$\|a_n - b\|_K \succ 0, \forall n \in \mathbb{N} \text{ et } \lim_n a_n \neq b \Longrightarrow l \succ 0$$

Nous avons d'aprés la définition

$$\exists N_1 \in \mathbb{N}, \forall n \geq N_1 \Longrightarrow \|a_n - b\|_K \succ \frac{1}{2}$$

d'autre part

$$\exists N_2 \in \mathbb{N}, \forall m \geq N_2 \Longrightarrow \|a_m - a_n\|_K \prec \frac{1}{2}$$

posons

$$M = \max(N_1, N_2)$$

donc

$$\begin{aligned} \forall n, m \quad &\geq \quad M \Longrightarrow \|a_m - b\|_K = \|a_n - b + a_m - a_n\|_K \\ &= \quad \max(\|a_n - b\|_K, \|a_m - a_n\|_K) \\ &= \quad \|a_n - b\|_K \end{aligned}$$

donc la suite $(\|a_n - b\|_K)_n$ est stationnaire.

Montrons que $\|.\|_{\widehat{K}}$ est ultramétrique :

Soient $A = (a_n)_n, B = (b_n)_n \in \widehat{K}$ avec $A \neq B$. Supposons que les deux suites ne sont pas nulles, d'aprés le lemme (1.1.14) précédent on a

$$\begin{aligned} \exists N_1 \quad &\in \quad \mathbb{N}, \forall n \succ N_1 \Longrightarrow \|a_n\|_{\widehat{K}} = \|a_n\|_K \\ \exists N_2 \quad &\in \quad \mathbb{N}, \forall n \succ N_2 \Longrightarrow \|b_n\|_{\widehat{K}} = \|b_n\|_K \end{aligned}$$

posons

$$N = \max(N_1, N_2)$$

alors

$$\begin{aligned} \forall n \quad &\succ \quad N : \|a_n - b_n\|_K = \max(\|a_n\|_{\widehat{K}}, \|b_n\|_{\widehat{K}}) \\ &\Longrightarrow \quad \|a_n + b_n\|_{\widehat{K}} = \max(\|a_n\|_{\widehat{K}}, \|b_n\|_{\widehat{K}}) \end{aligned}$$

donc $\|.\|_{\widehat{K}}$ est une norme ultramétrique . ■

Théorème 1.1.15 [4]
$(\widehat{K}, \|.\|_{\widehat{K}})$ est un espace complet, de plus K est un sous ensemble dense dans $\widehat{K}$.

Preuve.

1) Montrons que K est dense dans $\widehat{K}$

Soit $A = (a_n)_n \in \widehat{K}$. Pour tout entier fixé $m \in \mathbb{N}$, considérons la suite constante $\{a_m\}_n$ donc $\{a_n - a_m\}_n$ représente la classe $A - (a_m)$. Tant que $\{a_m\}_m$ est de Cauchy. On peut écrire

$$\lim_{n\longrightarrow\infty} \|A - (a_m)\|_{\widehat{K}} = \lim_{m\longrightarrow\infty} (\lim_{n\longrightarrow\infty} \|a_n - a_m\|_{\widehat{K}}) = 0 \tag{1.2}$$

d'où K est dense dans $\widehat{K}$.

2) Montrons que $(\widehat{K}, \|.\|_{\widehat{K}})$ est complet

c'est à dire toutes les suites de Cauchy de $\widehat{K}$ sont convergentes dans $\widehat{K}$. Soit la suite $\{A_n\}_n$ de Cauchy dans $\widehat{K}$. Alors d'aprés la densité de K dans $\widehat{K}$, on a

$$\forall A_n \in \widehat{K}, \exists a_n \in K : \|A - (a_n)\|_{\widehat{K}} \leq \frac{1}{n} \tag{1.3}$$

donc $\{A - (a_n)\}_n$ est une suite nulle, d'où elle est de Cauchy dans $\widehat{K}$. Nous avons

$$\{(a_n)\}_n = \{A_n\}_n - \{A_n - (a_n)\}_n$$

alors $\{(a_n)\}_n$ est une suite de Cauchy dans $\widehat{K}$ et comme tous ces éléments appartient à K alors $\{a_n\}_n$ est de Cauchy dans K. De (1.2) et (1.3), on déduit que $\{A - (a_n)\}_n$ et $\{A_n - (a_n)\}_n$ sont des suites nulles dans $\widehat{K}$. donc

$$\{A - A_n\}_n = \{A - (a_n)\}_n - \{A_n - (a_n)\}_n$$

est une suite nulle dans $\widehat{K}$, ce qui implique que

$$\lim_{n\longrightarrow\infty} \|A - A_n\|_{\widehat{K}} = 0 \Longrightarrow \lim_{n\longrightarrow\infty} \mathbf{A}_n = \mathbf{A}$$

donc $(\widehat{K}, \|.\|_{\widehat{K}})$ est un espace complet. ■

Proposition 1.1.16 [17]
Les opérations arithmétiques dans $\widehat{K}$ sont prolongé de K par la continuité, si

$$\begin{cases} A = \lim\limits_{n}(a_n) \\ B = \lim\limits_{n}(b_n) \end{cases}$$

alors

$$\begin{cases} A + B = \lim\limits_{n}(a_n + b_n) \\ A.B = \lim\limits_{n}(a_n.b_n) \end{cases}$$

Deuxième partie

Corps Des Nombres P-adiques Et Codes De Hensel

1.2 Corps des nombres p-adiques

Introduction

Nous savons que l'entier 2 n'est pas un carrée rationnel , mais si l'on passe de $\mathbb{Q}$ à $\mathbb{R}$, l'équation $x^2 - 2 = 0$ possède deux solution $\mp\sqrt{2}$ où

$$\sqrt{2} = 1.414213.....$$

cette écriture est l'écriture décimale de $\sqrt{2}$ et tout réel pouvant s'écrit $x = \sum_{k=-\infty}^{n} \alpha_k.10^k$ avec les $\alpha_k \in \{0, 1..., 9\}$. On peut définir les réels de cette manière. Une autre façon de regarder le développement décimal de$\sqrt{2}$ est la suivante :
On considère la suite$(x_n)_n$ définie par

$$x_0 = 1, x_1 = \frac{14}{10}, x_2 = \frac{141}{100}, ...$$

C'est une suite de Cauchy de rationnels qui n'admet pas de limite dans $\mathbb{Q}$ mais converge vers $\sqrt{2}$ dans le corps complet $\mathbb{R}$. La définition moderne des réels passe par les suites de Cauchy : $\mathbb{R}$ est le complété de $\mathbb{Q}$ pour la valeur absolue usuelle $|.|$ (archimédienne). En fin, les rationnels x_n sont des approximations de $\sqrt{2}$ de plus en plus fines :

$$\left|\sqrt{2} - x_n\right| \leq 10^{-n}$$

Considérant maintenant la suite de congruence

$$x^2 \equiv 2 \bmod(7^n), n \geq 1$$

Lorsque $n = 1$,on a deux solutions $x = x_1 \equiv \mp 3 \bmod(7)$. Ce choix fait, les x_n $(n \geq 2)$ sont uniquement déterminés : en effet, supposant x_n construit (et unique modulo7^n), alors x_{n+1} vérifie également

$$x^2 \equiv 2 \bmod(7^n)$$

donc

$$x_{n+1} \equiv x_n \bmod 7^n$$

par unicité. On écrit

$$\begin{cases} x_{n+1} = x_n + c_n 7^n \\ x_n^2 - 2 = d_n 7^n \end{cases}.$$

alors

$$\begin{aligned} x_{n+1}^2 - 2 &\equiv x_n^2 - 2 + 2x_n c_n 7^n \bmod 7^{n+1} \\ &\equiv d_n 7^n + 2x_n c_n 7^n \bmod 7^{n+1} \end{aligned}$$

il faut donc que

$$d_n + 2x_n.c_n \equiv 0 \bmod 7$$

ce qui détermine $c_n \bmod 7$, d'où la formule générale de récurrence est

$$x_{n+1} \equiv x_n^2 + x_n - 2 \bmod 7^{n+1}, n \geq 0$$

que se passe t-il lorsque n tend vers l'infini ? La limite $(x_n)_n$ possède de-t'elle une limite ? D'autre part, il n'existe pas d'entier x vérifiant

$$x^2 \equiv 2 \bmod 7^n, \forall n \geq 1$$

car $x^2 - 2$ serait divisible par 7^n, ce qui n'est pas possible si $x^2 - 2 = 0$. D'autre part la série $\sum_{n\geq 0} c_n 7^n, c_n = \overline{0.6}$ ne converge pas dans $\mathbb{R}$, au sens usuel, pour la distance induite de la valeur absolue archimédienne. Nous allons définir le corps des nombres p-adiques (pour chaque nombre premier p), la valuation p-adique et la normes p-adique pour laquelle la série $\sum_{n\geq 0} c_n 7^n$ converge vers la solution de

$$x^2 \equiv 2 \bmod 7$$

1.2.1 Normes et valuations p-adiques :

La valuation p-adique :

Définition 1.2.1 *Soit p un nombre premier, 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.*

$$\begin{aligned} v_p \quad : \quad & \mathbb{Z}^* \longrightarrow \mathbb{Z}^+ \\ x \quad \longrightarrow \quad & v_p(x) = \max\{r \in \mathbb{Z}^+ : p^r / x\} \end{aligned}$$

donc

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

Remarque 1.2.2

1) On pose par convention que

$$v_p(x) = +\infty \Longleftrightarrow x = 0$$

2) Si

$$x = \frac{a}{b} \in \mathbb{Q}^* \Longrightarrow v_p(x) = v_p(\frac{a}{b}) = v_p(a) - v_p(b)$$

En effet

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

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

alors

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

Proposition 1.2.3 [4]

si $x, y \in \mathbb{Q}$, alors la valuation v_p satisfaite

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

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

Preuve.

1) Soient

$$\begin{cases} x = \frac{a_1}{b_1} \in \mathbb{Q}^* \\ y = \frac{a_2}{b_2} \in \mathbb{Q}^* \end{cases}$$

alors

$$\begin{cases} x = x'.p^{vp(x)}, (x',p) = 1 \\ y = y'.p^{v_p(y)}, (y',p) = 1 \end{cases} \Longrightarrow xy = x'y'.p^{v_p(x)+v_p(y)}, (x'y',p) = 1$$

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

2) Soient

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

Supposons que $s \geq r$ donc $s - r \geq 0$ et

$$\begin{aligned} v_p(x+y) &= v_p(p^r.\frac{a}{b} + p^s.\frac{c}{d}) \\ &= v_p(p^r[\frac{a}{b} + p^{s-r}.\frac{c}{d}]) \\ &= v_p(p^r.[\frac{da + p^{s-r}cb}{bd}]) \ , \ p \not| bd \end{aligned}$$

donc

$$v_p(\frac{da + p^{s-r}cb}{bc}) \geq 0 \Longrightarrow v_p(x+y) = v_p(p^r) + v_p(\frac{da + p^{s-r}cb}{bd})$$

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

■

Exemple 1.2.4 *la valuation p-adique de la suite $a_n = n!$ est*

$$v_p(n!) = \frac{n}{p-1}, \ \textit{quand } n \longrightarrow \infty \tag{1.4}$$

En effet, on a

$$v_p(n!) = \frac{n - S_p(n)}{p-1} = \sum_{k \geq 1} \left[\frac{n}{p^k}\right]$$

Où $S_p(n)$ désigne la somme des chiffres de l'écriture de n en base p et $[x]$ est la partie entière du réel x. Donc

$$\begin{aligned} v_p(n!) &\leq \frac{n}{p}.\sum_{k \geq 0}\frac{1}{p^k} \\ &\leq \frac{n}{p}.\frac{1}{1 - \frac{1}{p}} \\ &\leq \frac{n}{p-1} \end{aligned}$$

Donc

$$v_p(n!) \leq \frac{n}{p-1} \tag{1.5}$$

D'autre part, on a

$$v_p(n!) \geq \sum_{k=0}^{m}\frac{n}{p^k} - m$$

$$\geq \frac{n}{p}.\frac{1 - (\frac{1}{p})^m}{1 - (\frac{1}{p})} - m$$

$$\geq \frac{n}{p-1} - \frac{np^{-m}}{p-1} - m$$

On prend m tel que $p^m \leq n \leq p^{m+1}$, et d'aprés (1.5) on a

$$\begin{aligned} \left|\frac{v_p(n!)}{n} - \frac{1}{p-1}\right| &\leq \frac{p^{-m}}{p-1} + \frac{m}{n} \\ &\leq p^{-m}(\frac{1}{p-1} + m) \longrightarrow 0 \text{ quand } m \longrightarrow +\infty \end{aligned}$$

Or quand $n \longrightarrow +\infty$ et $m \longrightarrow +\infty$, donc

$$\lim_{n\longrightarrow\infty} \frac{v_p(n!)}{n} = \frac{1}{p-1}$$

ce qui donne

$$v_p(n!) = \frac{n}{p-1}, \text{ quand } n \longrightarrow \infty$$

Les normes p-adiques :

Soient x un nombre rationnel, p un nombre premier, en considère la fonction $|.|_p$ définie par

$$\begin{aligned} |.|_p \quad : \quad & \mathbb{Q} \longrightarrow \mathbb{R}^+ \\ x \quad \longmapsto \quad & |x|_p = \begin{cases} p^{-r}, x = p^r.\frac{a}{b}\ , \ (a,p) = (b,p) = 1 \\ 0, \ x = 0 \end{cases} \end{aligned}$$

avec r représente la valuation p-adique de x.

Proposition 1.2.5 [3]
L'application $x \longmapsto |x|_p$ est une norme ultramétrique sur $\mathbb{Q}$.

Définition 1.2.6 *L'application $|.|_p$ est appelée la norme p-adique (la valeur absolue p-adique). La distance sur $\mathbb{Q}$ induite par la norme p-adique $|.|_p$ noté d_p (la distance p-adique) est définie par*

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

Exemple 1.2.7 *Pour la distance usuelle, la distance de 252 à 2 est $d(252,2) = |252-2| = 250$. Voilà comment mesurer la distance $5-$adique de 252 à 2 que le note $d_5(252,2)$: on écrit*

$$252 - 2 = 250 = 5^3.2$$

alors

$$d_5(252,2) = |250|_5 = 5^{-3}$$

de mème pour

$$d_3(252,2) = 1$$

Remarque 1.2.8

- La propriété importante de la norme p-adique est que ses images forment un ensemble discret définie par

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

- Il est claire que l'ensemble des entier rationnels $\mathbb{Z}$ est un ensemble non borné pour la distance usuelle $d_{|.|}$ sur $\mathbb{R}$ induite par la valeur absolue archimédienne $|.|_\infty = |.|$.
- Si p un nombre premier, tout entier n s'écrit sous la forme $p^r.m$ 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 implique que $\mathbb{Z}$ est un ensemble borné pour toute valeur absolue p-adique $|.|_p$.

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

Théorème 1.2.9 [15] ***(la formule du produit)***
pour tout nombre rationnel $a \in \mathbb{Q}$, on a

$$|a|_\infty \cdot \prod_p |a|_p = 1$$

Preuve.
La factorisation canonique 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

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

donc

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

■

Exemple 1.2.10
on a pour tout $p \notin \{2, 3, \infty\}$: $\left|\frac{3}{2}\right|_p = 1$, *alors*

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

Remarque 1.2.11 *On peut définit sur le corps des nombres rationnels* $\mathbb{Q}$ *trois types de valeurs absolues :*
1) Valeur absolue triviale :

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

2) Valeur absolue naturelle (ordinaire) :
On considére l'application de

$$\begin{array}{ccc} \mathbb{Q} & \longrightarrow & \mathbb{Q}_+ \\ x & \longmapsto & |x|_\infty = \max(x, -x) = \begin{cases} x \ , \ si \ x \geq 0 \\ -x \ , \ si \ x \prec 0 \end{cases} \end{array}$$

3) Valeur absolue p-adique définie précédente $|.|_p$.
le théorème d'Ostrowski nous montre que les seuls valeurs absolues sur $\mathbb{Q}$ *sont les valeurs absolues p-adiques et les valeurs absolues* $|x|_\infty^\alpha$ *où* $0 \prec \alpha \leq 1$.

Théorème 1.2.12 [11] ***(Théorème d'Ostrowski)***
Toute valeur absolue non triviale $\|.\|$ *sur* $\mathbb{Q}$ *est équivalente à la valeur absolue archimédienne* $|.|_\infty$ *ou à une certaine valeur absolue p-adique* $|.|_p$.

Corollaire 1.2.13 [17]
Deux valeurs absolues $|.|_{p_1}$ *et* $|.|_{p_2}$ *sont équivalentes si et seulement si* $p_1 = p_2$.

Preuve.
il suffit de considérer la suite $(p_1^n)_n$. Elle converge vers 0 pour $|.|_{p_1}$ car $|p^n|_{p_1} = p^{-n} \underset{n}{\longrightarrow} 0$ et si $p_1 \neq p_2$, elle ne converge pas vers 0 pour $|.|_{p_2}$, cars $|p^n|_{p_2} = 1 \neq 0$. ■

1.2.2 les nombres p-adiques

Définition 1.2.14 *Pour tout p premier, le corps des nombres p-adiques est défini comme la complétion de l'espace métrique $(\mathbb{Q}, d_p)$ suivant la procédure du complétion précédente. Ses éléments sont les classes d'équivalences des suites de Cauchy des nombres rationnels $\{a_n\}_n$, muni de la relation suivante*

$$\{a_n\}\Re\{b_n\} \Longleftrightarrow |\{a_n - b_n\}|_p \underset{n\longrightarrow\infty}{\longrightarrow} 0$$

avec

$$\begin{aligned} \{a_n\}_n + \{b_n\}_n &= \{a_n + b_n\}_n \\ \{a_n\}_n.\{b_n\}_n &= \{a_n.b_n\}_n \\ \frac{1}{\{a_n\}_n} &= \{\frac{1}{a_n}\}_n \\ -\{a_n\}_n &= \{-a_n\}_n \end{aligned}$$

* Nous indiquons comment prolonger la valeur absolue définie sur $\mathbb{Q}$ à tout $\mathbb{Q}_p$.

Soit $x \in \mathbb{Q}_p$ et $(x_n)_n$ une suite de Cauchy des nombres rationnels de limite x pour la distance p-adique $d_{|.|_p}$ alors

$$|x|_p = \lim_{n\longrightarrow\infty} |x_n|_p$$

i.e :

$$\forall x \in \mathbb{Q}_p, \exists x_n \in \mathbb{Q} : x = \lim_{n\longrightarrow\infty} x_n$$

Proposition 1.2.15 [14] [15]
$(\mathbb{Q}_p, |.|_p)$ un corps complet ultramétrique.

Preuve.

1) $\mathbb{Q}_p$ un corps ?

Il est claire que $(\mathbb{Q}_p, +, .)$ est un anneau commutatif. Il nous reste à démontrer que tout $x \in \mathbb{Q}_p$ non nul admet un inverse dans $\mathbb{Q}_p$.

Soit $x_n \in \mathbb{Q}_p$ une suite de limite x. Alors $|x_n|_p$ converge vers $|x|_p$ qui est non nul, donc $|x_n|_p$ est aussi non nul pour n assez grand, et donc la suite $v_p(x_n)$ est une suite convergente dans $\mathbb{R}$. Comme il s'agit d'une suite d'éléments de $\mathbb{Z}$, elle est constante à partir d'un certain rang $N \in \mathbb{N}$.

On définit une suite y_n d'éléments de $\mathbb{Q}$ par

$$y_n = \begin{cases} 0, n \prec N \\ \frac{1}{x_n}, n \geq N \end{cases}$$

Pour tout couple (n,m) avec $n,m \geq N$, on a

$$|y_n - y_m|_p = \frac{|x_n - x_m|_p}{|x_n|_p^2}$$

de sorte que y_n soit une suite de Cauchy dans $\mathbb{Q}_p$, donc elle converge vers $y \in \mathbb{Q}_p$. Comme $x_n.y_n = 1$ pour tout $n \in \mathbb{N}$, on en déduit que $xy = 1$.

2) Soit $(x_n) = ([(x_{1n})], [(x_{2n})], ...)$ une suite des classes d'équivalences des suites de Cauchy dans $\mathbb{Q}$ et $(x_{1n}), (x_{2n}), ...$ des représentants des suites de Cauchy.
Supposons que (x_n) est une suite de Cauchy pour la valeur absolue p-adique $|.|_p$, comme chaque suite $(x_{1n}), (x_{2n}), ...$ est de Cauchy, alors pour chaque (x_{in}) on peut prendre N_i tel que

$$|x_{im} - x_{in}|_p \prec p^{-i}, \forall m, n \geq N_i$$

Soit $(y_n) = (((x_{1N_1}), (x_{2N_2}), ...)$. Alors $(y_n)_n$ est aussi une suite de Cauchy dans $\mathbb{Q}$ (et comme (x_n) est de Cauchy dans $\mathbb{Q}$), alors $(|y_n|_p)$ est de Cauchy dans $\mathbb{Q}$, donc supposons que $y = \lim(|y_n|_p) \in \mathbb{Q}_p$.
Soit $(y'_n) = ([(x_{1N_1})], [(x_{2N_2})], ...)$ une suite des classes d'équivalences des suites constantes (x_{jN_j}). Alors

$$\lim_n (y'_n) = \lim_n |y_n|_p = y \in \mathbb{Q}_p$$

et

$$|x_i - y'_i|_p \prec p^{-i} \longrightarrow 0$$

donc

$$\lim_n (x_n) = y \in \mathbb{Q}_p$$

alors toutes les suites de Cauchy dans $\mathbb{Q}_p$ admet une limite dans $\mathbb{Q}_p$, de plus $|.|_p$ est une norme ultramétrique sur $\mathbb{Q}_p$. Alors $(\mathbb{Q}_p, |.|_p)$ un corps complet ultramétrique. ■

1.2.3 Développement p-adique et series de Hensel

On verra montrer que toute classe d'équivalence de suite de Cauchy $a \in \mathbb{Q}_p$ contient un représentant canonique unique, pour cela, on a le lemme suivant

Lemme 1.2.16 [18]
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

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

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

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

tant que

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

soit

$$\alpha = a.m_1$$

on a

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

■

Théorème 1.2.17 [11] [17]

Si la classe d'équivalence $a \in \mathbb{Q}_p$ vérifier la condition $|a|_p \leq 1$, alors elle possède un seul représentant (λ_n) (suite de Cauchy) qui satisfait

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

Preuve.

Soit $a \in \mathbb{Q}_p$ tel que $|a|_p \leq 1$, alors d'après le lemme (1.2.16)

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

et comme le nombre p-adique $(a-\alpha_0)$ a une norme inférieure à $\frac{1}{p}$, alors le nombre p-adique $(\frac{a-\alpha_0}{p})$ est dans $\mathbb{Q}_p$ et d'après le lemme (1.2.16)

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

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

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

Soit la suite (λ_n) définie par

$$\lambda_n = \alpha_0+\alpha_1 p+ \ldots\ldots + \alpha_n p^n$$

elle satisfait

$$\begin{cases} \lambda_n \in \mathbb{Z}, 0 \leq \lambda_n \leq p^n-1 \\ \lambda_{n+1} \equiv \lambda_n \bmod p^{n+1} \text{ (une suite de Cauchy)} \\ |a-\lambda_n|_p \prec p^{-n} \\ \lim\limits_{n\longrightarrow\infty} \lambda_n = a \text{ (selon } |.|_p) \end{cases}$$

■

Conclusion 1.2.18 *La suite de Cauchy (λ_n) qui vérifier les conditions du théorème précédent s'appelle représentant canonique de a.*

$$\forall a \in \mathbb{Q}_p : |a|_p \leq 1, \exists \lambda_n \in \mathbb{Z} : \begin{cases} \lambda_n = \alpha_0+\alpha_1 p+\alpha_2 p^2+ \ldots\ldots + \alpha_{n-1}p^{n-1} \\ \alpha_j = \overline{0, p-1} \\ a = \lim\limits_{n\longrightarrow\infty} \lambda_n = \sum\limits_{n=0}^{\infty} d_n p^n = \cdot\alpha_0\alpha_1\ldots\ldots\alpha_s\ldots\ldots \end{cases}$$

avec les α_j représentent les chiffres p-adiques et $\sum\limits_{n=0}^{\infty}\alpha_n p^n$ s'appelle la série de Hensel ou le développement p-adique de a. Autrement dit, on peut approché le nombre p-adique a par une série unique convergente définie par $\sum\limits_{n=0}^{\infty}\alpha_n p^n$.
En effet, supposons que a un nombre p-adique développable en deux séries p-adiques

$$\begin{cases} a = \sum\limits_{n=0}^{\infty}\alpha_n p^n = \alpha_0+\alpha_1 p+ \ldots\ldots + \alpha_n p^n + \ldots. \\ a = \sum\limits_{n=0}^{\infty}\alpha'_n p^n = \alpha'_0+\alpha'_1 p+ \ldots\ldots + \alpha'_n p^n + \ldots. \end{cases}$$

et soit d le premier entier pour que $\alpha_d \neq \alpha'_d$, donc on peut supposons que $\alpha_d \prec \alpha'_d$. On a

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

Si

$$\beta'_n = \alpha'_0 + \alpha'_1 p + \ldots\ldots + \alpha'_n p^n$$

alors

$$\beta'_d - \beta_d = (\alpha'_d - \alpha_d)p^d \Longrightarrow |\beta'_d - \beta_d|_p = p^{-d}$$

d'autre part on a

$$\begin{aligned} |\beta'_d - \beta_d|_p &= |\beta'_d - \alpha + \alpha - \beta_d|_p \\ &\leq \max\left\{|\beta'_d - \alpha|_p, |\alpha - \beta_d|_p\right\} \\ &\prec p^{-d} \end{aligned}$$

contradiction. Donc le nombre entier d n'existe pas et en déduit que le développement p-adique est unique.

Remarque 1.2.19

1. *Si $a \in \mathbb{Q}_p$ tel que $|a|_p \succ 1$, alors*

$$|a|_p \succ 1 \Longrightarrow \exists m \in \mathbb{Z}^+ : |a|_p = p^m$$

donc pour ramener au premier cas (i.e. $|a|_p \leq 1$), on multiple a par une puissance de p

$$a' = p^m.a \ , \ a' \in \mathbb{Q}_p$$

d'où

$$a' = p^m.a \Longrightarrow \left|a'\right|_p = |p^m.a|_p$$

$$\Longrightarrow \left|a'\right|_p = |p^m|_p \, . \, |a|_p = p^{-m}.p^m$$

alors

$$\left|a'\right|_p = 1 \leq 1$$

appliquant le théorème (1.2.17) on trouve

$$\begin{aligned} a' &= \sum_{n=0}^{\infty} d_n p^n \Longrightarrow p^m.a = \sum_{n=0}^{\infty} d_n p^n \\ &\Longrightarrow a = \sum_{n=0}^{\infty} d_n p^{n-m} \\ &\Longrightarrow a = \sum_{n=-m}^{\infty} d_{n+m} p^n = \sum_{k=n}^{\infty} \beta_k p^k \end{aligned}$$

ce qui donne tout nombre p-adique $a \in \mathbb{Q}_p$ admet un développement p-adique unique sous forme d'une série convergente s'écrit sous la forme

$$a = \sum_{k=n}^{\infty} \beta_k p^k, \beta_k \in \{0, 1, 2, ..., p-1\}, n \in \mathbb{Z}$$

2. *Si $\beta_n \neq 0$, alors*

$$|a|_p = p^{-n}$$

3. *Le développement p-adique est analogue à le développement décimal d'un nombre réel, tel que tout nombre réel $x \in \mathbb{R}$ s'écrit sous la forme*

$$x = \sum_{k=-\infty}^{n} \theta_k 10^k, \theta_k \in \{0, 1, 2, ..., 9\} \tag{1.6}$$

et comme $\left|10^k\right| = 10^k$, alors 10^k est grand pour tout $k \succ 0$ et converge vers 0 si $k \longrightarrow -\infty$, donc la série (1.6) admet un nombre fini des puissances positives de 10 à droite du point 10-adique et une infinités des puissances négatives à gauche de ce point.

$$\overleftarrow{\text{.....}\theta_{-2}\theta_{-1}}^{\text{infini}} \underbrace{\text{le point 10-adique}} \overrightarrow{\theta_0\theta_1\text{.....}\theta_n}^{\text{fini}} \tag{1.7}$$

par contre si x un nombre p-adique tel que

$$x = \sum_{k=n}^{\infty} \beta_k p^k, \beta_k \in \{0, 1, 2, ..., p-1\} \tag{1.8}$$

Alors $|x|_p = p^{-n}$ est grand si $n \prec 0$ et converge vers 0 si $n \longrightarrow \infty$, donc le développement p-adique de x admet un nombre fini des puissances négatives à gauche du point p-adique et une infinités des puissance positives à droite du point p-adique. Autrement dit (1.8) s'écrit sous la forme

$$\overleftarrow{\beta_n\beta_{n+1}\text{.....}}^{\text{fini}} \overset{\text{point p-adique}}{\longleftrightarrow} \overrightarrow{\beta_0\beta_1\text{.....}\beta_s\text{....}}^{\text{infini}} \tag{1.9}$$

il y a donc une partie "irrégulière" dans le développement p-adique de x si $n \prec 0$ et une partie "régulière" si $n \succ 0$.

4. *On note par $[x]$ la partie entière (régulière) d'un nombre p-adique $x \in \mathbb{Q}_p$, telle que*

$$\forall x \in \mathbb{Q}_p : [x] = \sum_{k=0}^{\infty} \beta_k p^k = \cdot\beta_0\beta_1.....\beta_s.....$$

et on note par $\langle x \rangle$ la partie fractionnel (irrégulière) de x, telle que

$$\forall x \in \mathbb{Q}_p : \langle x \rangle = \sum_{k \prec 0} \beta_k p^k = ...\beta_{-3}\beta_{-2}\beta_{-1}\cdot$$

on obtient

$$\forall x \in \mathbb{Q}_p : x = [x] + \langle x \rangle$$

5. *Le point p-adique nous permet de déterminer le signe de n, tel que*
   i) $a = \beta_n\beta_{n+1}...\beta_{-1} \cdot \beta_0\beta_1..... $, si $n \prec 0$.
   ii) $a = \cdot\beta_0\beta_1\beta_2..... $, si $n = 0$.
   iii) $a = \cdot.....\beta_0\beta_1..... $, si $n \succ 0$.
   Par exemple :

$$\begin{aligned} i)\ a &= 13 \cdot 41 = 1.5^{-2} + 3.5^{-1} + 4.5^0 + 1.5^1 + ..., \ n = -2 \\ ii)\ a &= \cdot 1341 = 1.5^0 + 3.5^1 + 4.5^2 + 1.5^3 \ , \ n = 0 \\ iii)\ a &= \cdot 01341 = 0.5^0 + 1.5^1 + 3.5^2 + 4.5^3 + 1.5^4 \ , \ n = 1 \end{aligned}$$

Théorème 1.2.20 [13] *(développement de Hensel des nombres rationnels)*
le développement p-adique canonique $x = \sum_{n=m}^{\infty} \alpha_n p^n$ représente un nombre rationnel si et seulement si la suite $(\alpha_n)_n$ est périodique (c'est à dire périodique au de la d'un certain rang).

Exemple 1.2.21
1) Soit $x = \frac{1}{3} \in \mathbb{Q}_5$, alors

$$\begin{aligned} \frac{1}{3} &= 2 + 3.5 + 1.5^2 + 3.5^3 + 1.5^4 + 3.5^5 + ... \\ &= \cdot 231313131 \\ &= \cdot 2\overline{31} \end{aligned}$$

le développement 5-adique de $\frac{1}{3}$ est périodique, donc $x = \frac{1}{3} \in \mathbb{Q}$.

1.2.4 Les entiers p-adiques

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

Définition 1.2.22 *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 la valuation p-adique de a doit être positive.*

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

* Notons par $\mathbb{Z}_p$ l'ensemble des entiers p-adiques, avec

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

Théorème 1.2.23 [17]
$\mathbb{Z}_p = \left\{ a \in \mathbb{Q}_p : |a|_p \leq 1 \right\} = \{a \in \mathbb{Q}_p : v_p(a) \geq 0\}$, *autrement dit $\mathbb{Z}_p$ représente le disque de l'unité de rayon 1 et de centre 0.*

Remarque 1.2.24
i) Tout nombre p-adique $\alpha \in \mathbb{Q}_p$ est une limite d'une suite de Cauchy des nombres rationnels $\alpha_n \in \mathbb{Q}$.
ii) Le corps $\mathbb{Q}_p$ est l'ensemble des fractions de $\mathbb{Z}_p$

$$\mathbb{Q}_p = \{\frac{a}{b} : (a, b) \in \mathbb{Z}_p \times \mathbb{Z}_p - \{0\}\}$$

Définition 1.2.25 *Soit a un nombre p-adique, on dit que a est inversible ou unitaire si le développement canonique p-adique ne contient que les puissances positives de p et le premier chiffre différent de zéro.*

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

$$\begin{aligned} \mathbb{Z}_p^* &= \{\sum_{n=0}^{\infty} \alpha_n p^n : \alpha_0 \neq 0\} \\ &= \{\alpha \in \mathbb{Z}_p : \alpha_0 \neq 0\} \end{aligned}$$

Théorème 1.2.26 [11]

$$\mathbb{Z}_p^* = \{\alpha \in \mathbb{Z}_p : |\alpha|_p = 1\}$$

La proposition suivante donne la relation entre les deux ensembles $\mathbb{Z}_p^*$ et $\mathbb{Q}_p$

Proposition 1.2.27 [3]
Tout nombre p-adique $\alpha \in \mathbb{Q}_p$ admet une unique représentation

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

Preuve.
1) Existence de la représentation :
soit $\alpha \in \mathbb{Q}_p$ alors (par définition) α s'écrit sous la forme

$$\alpha = \frac{a}{b} \quad , (a,b) \in \mathbb{Z}_p \times \mathbb{Z}_p - \{0\}$$

On sait que

$$\begin{cases} a = u_1.p^{m_1} \\ \\ b = u_2.p^{m_2} \end{cases}$$

avec

$$\begin{cases} (u_1, u_2) \in (\mathbb{Z}_p^*)^2 \\ \\ m_1 = v_p(a) \ , \ m_2 = v_p(b) \end{cases}$$

donc

$$\begin{aligned} \alpha &= \frac{a}{b} = \frac{u_1.p^{m_1}}{u_2.p^{m_2}} \\ &= \frac{u_1}{u_2}.p^{m_1-m_2} \\ &= u.p^n \ , \ n = m_1 - m_2 \ , \ u = \frac{u_1}{u_2} \in \mathbb{Z}_p^* \text{ (puisque } \mathbb{Z}_p^* \text{ un corps)} \end{aligned}$$

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

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

alors

$$u'.u''^{-1} = p^{m'-m''} \Longrightarrow v_p(u'.u''^{-1}) = m' - m''$$

or

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

ce qui implique

$$m' = m''$$

donc l'unicité de la repésentation. ∎

Exemple 1.2.28
Soient

$$\begin{cases} p = 5 \\ \alpha^{(1)} = \cdot 4\overline{13} = 4 + 1.5 + 3.5^2 + 1.5^3 + 3.5^4 + ... \\ \alpha^{(2)} = \cdot 4\overline{2} = 4 + 2.5 + 2.5^2 + 2.5^3 + 2.5^4 ..... \end{cases}$$

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

$$\begin{cases} \beta^{(1)} = \cdot 01\overline{40} = 0 + 1.5^1 + 4.5^2 + 0.5^3 + 4.5^4 + 0.5^5 + ... \\ \beta^{(2)} = 42 \cdot 13\overline{31} = 4.5^{-2} + 2.5^{-1} + 1 + 3.5^1 + 3.5^2 + 1.5^3 + 3.5^4 + .. \end{cases}$$

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

$$\begin{cases} \beta^{(1)} = \cdot 01\overline{40} = \cdot 1\overline{40}.5^1 & , \cdot 1\overline{40} \in \mathbb{Z}_5^* \\ \beta^{(2)} = 42 \cdot 13\overline{31} = \cdot 4213\overline{31}.5^{-2} & , \cdot 4213\overline{31} \in \mathbb{Z}_5^* \end{cases}$$

Lemme 1.2.29 *Si* $x \in \mathbb{Q}_p^*$, *alors* x *est inversible dans* $\mathbb{Q}_p$.

Preuve.
On a

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

on pose

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

alors

$$\begin{aligned} u &= a_0 + \sum_{k=1}^{\infty} a_k p^k = a_0 + p.\sum_{k=1}^{\infty} a_k p^{k-1} \\ &= a_0 + p.\sum_{k=0}^{\infty} a_{k+1} p^k = a_0 - py \end{aligned}$$

tel que

$$y = -\sum_{k=0}^{\infty} a_{k+1} p^k \in \mathbb{Z}_p$$

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

$$u = 1 - py$$

donc

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

ce qui donne

$$x^{-1} = p^{-k}.u^{-1}, u^{-1} \in \mathbb{Z}_p^*, k \in \mathbb{Z} \Longrightarrow x^{-1} \in \mathbb{Q}_p^*$$

donc x est inversible dans $\mathbb{Q}_p$. ■

Lemme 1.2.30 [11]
Soient $x \in \mathbb{Q}_p$, $k \in \mathbb{Z}$, alors

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

Preuve.
nous avons

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

comme $x \in \mathbb{Q}_p$, $p^{-k}.\mathbb{Z}_p \subset \mathbb{Q}_p$ et $\mathbb{Q}_p$ est un corps, alors

$$\left\{y \in \mathbb{Q}_p, |y - x|_p \leq p^k\right\} \subset \mathbb{Q}_p$$

■

1.3 Les propriétés des nombres p-adiques :

dans cette section, on étudie seulements les propriétés élémentaires analytiques des nombres p-adiques concernant la convergence des suites et des séries définies dans $\mathbb{Q}_p$.

1.3.1 Propriétés Analytiques

Le corps des nombres p-adiques est analogue au corps des nombres réels dans plusieurs cas. Mais le corps $\mathbb{Q}_p$ possède des propriétés intéressantes différentes de celles dans le corps

des réels $\mathbb{R}$. Le point le plus intéressant dans cette partie est la convergence de suites et de séries dans l'espace $(\mathbb{Q}_p, |.|_p)$.

Théorème 1.3.1 [5]
Soit $(a_n)_n$ une suite de $\mathbb{Q}_p$. Alors $(a_n)_n$ est une suite convergente si et seulement si

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

Autrement dit $(a_n)_n$ est une suite de Cauchy.

Maintenant, soit la série

$$\sum_{k=n}^{\infty} a_k, a_k \in \mathbb{Q}_p$$

On sait que la série $\sum_{k=n}^{\infty} a_k$ converge par définition si et seulement si la suite des sommes partielles $s_m = \sum_{k=n}^{m} a_k$ converge dans $\mathbb{Q}_p$.

Proposition 1.3.2 [2]
soit $(a_n)_n$ est une suite dans $\mathbb{Q}_p$, si $\lim_{n\longrightarrow\infty} a_n = a$ dans $\mathbb{Q}_p$, alors on a

$$\begin{cases} \lim_{n\longrightarrow\infty} |a_n - a|_p = 0 \\ \text{ou bien} \\ \exists N \in \mathbb{N} : |a_n|_p = |a|_p \quad \text{(la suite } (|a_n|_p)_n \text{ est stationnaire a partir d'un rang } N) \end{cases}$$

Preuve.
Soit $(a_n)_n \in \mathbb{Q}_p$, telle que $\lim_{n\longrightarrow\infty} a_n = a$. Donc $(a_n)_n$ est une suite convergente dans $\mathbb{Q}_p$

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

d'autre part, on a

$$\Big||a_m|_p - |a_n|_p\Big| \leq |a_m - a_n|_p \prec \varepsilon$$

donc $(|a_n|_p)_n$ est une suite de Cauchy dans $\mathbb{R}$ complét, ce qui donne $(|a_n|_p)_n$ est convergente dans $\mathbb{R}$ et soit l sa limite.

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

si

$$|a|_p \neq 0 \Longrightarrow |a|_p \succ 0$$

alors

$$\forall \epsilon = \frac{l}{2} \succ 0, \exists N_1 \in \mathbb{N} : \forall n \geq N_1 \Longrightarrow |a_n|_p \succ \frac{l}{2} \tag{1.10}$$

en effet, on a

$$\Big|\ |a_n|_p - l\Big| \prec \frac{l}{2} \Longrightarrow \frac{l}{2} \prec |a_n|_p \prec \frac{l}{2} + l$$

de mème, comme $(a_n)_n$ est de Cauchy dans $\mathbb{Q}_p$, alors

$$\forall \varepsilon = \frac{l}{2} \succ 0, \exists N_2 \in \mathbb{N} : \forall m, n \geq N_2 \Longrightarrow |a_m - a_n|_p \prec \frac{l}{2} \tag{1.11}$$

donc

$$\begin{aligned} \forall n \ &\geq \ N_3 = \max(N_1, N_2) \Longrightarrow |a_m| = |a_m - a_n + a_n|_p \\ &= \ \max(|a_m - a_n|_p, |a_n|_p) \\ &= \ |a_n|_p, \forall n \geq N_3 \end{aligned}$$

pour $m \longrightarrow \infty$, alors

$$|a|_p = |a_n|_p, \forall n \geq N_3$$

■

Proposition 1.3.3 [17]
Soit $\sum_{n\geq 0} a_n$ *une série dans* $\mathbb{Q}_p$, *alors*

$$\sum_{n\geq 0} a_n \text{ converge dans } \mathbb{Q}_p \Longleftrightarrow (a_n) \text{converge vers } 0 \text{ dans } \mathbb{Q}_p$$

de plus

$$\left|\sum_{n\geq 0} a_n\right|_p \leq \max(|a_n|_p)$$

1.4 Corps des nombres p-adiques complexes $\mathbb{C}_p$

Définition 1.4.1 *On dit que le corps K est algébriquement clos si chaque polynome $P(x)$ dans $K[x]$ admet des racines dans K. Autrement dit chacun de ces polynômes se divise en facteurs linéaire dans $K[x]$.*

* On note par $\overline{\mathbb{Q}}_p$ la cloture algébrique de $\mathbb{Q}_p$.

Proposition 1.4.2 [14] $\mathbb{Q}_p$ *n'est algébriquement clos pour tout p premier.*

Preuve.
on considere le polynome $P(x) = x^2 - p \in \mathbb{Q}_p[x]$. Supposons que $P(x)$ admet des racines

dans $\mathbb{Q}_p$, donc

$$P(x) = 0 \Longleftrightarrow x^2 = p$$

alors

$$\begin{aligned} |x^2|_p &= |x|_p^2 \\ &= |p|_p = p^{-1} \\ &\Longrightarrow |x|_p = p^{\frac{-1}{2}} \\ &\Longrightarrow v_p(x) = \frac{1}{2} \end{aligned}$$

contradiction, car $v_p(a) \in \mathbb{Z}, \forall a \in \mathbb{Q}_p$. Donc $P(x)$ n'a pas des racines dans $\mathbb{Q}_p$ (i.e :$\sqrt{\pm p} \notin \mathbb{Q}_p$). Ce qui nous prouve que $\mathbb{Q}_p$ n'est algébriquement clos. ■

Le corps $\mathbb{Q}_p$ n'est pas algébriquement clos. Pour faire convenablement de l'analyse, il est donc logique de considérer une clôture algébrique de $\mathbb{Q}_p$, que l'on note en général $\overline{\mathbb{Q}}_p$ et qui n'est pas complet, donc nous avons besoin de le compléter pour former plus grand corps complet algébriquement clos noté $\mathbb{C}_p$ (plus de détail voir [18]).
On peut montré que l'on peut prolonger la valeur absolue à ce corps, qui possède donc aussi une valeur absolue ultramétrique, quel'on note toujours $|.|_p$.

Définition 1.4.3 *Le corps des nombres p-adiques complexes noté $\mathbb{C}_p$ est définie comme le complété de corps $\overline{\mathbb{Q}_p}$ par rapport à la norme p-adique $|.|_p$. De la mème façon lorsqu'on a construit $\mathbb{Q}_p$ en complétant $\mathbb{Q}$.*
On prolonge la norme p-adique de $\overline{\mathbb{Q}_p}$ à $\mathbb{C}_p$, en posant pour tout $x \in \mathbb{C}_p$:

$$|x|_p = \lim_{n \longrightarrow \infty} |x_n|_p$$

avec $(x_n)_n$ est une suite de Cauchy d'éléments de $\overline{\mathbb{Q}_p}$ qui est dans la classe d'équivalence de x.

Proposition 1.4.4 [4] [14]
Le corps des nombres p-adiques complexes $\mathbb{C}_p$ admet les propriétés suivantes :
1) $\mathbb{C}_p$ est agébriquement clos.
2) $\mathbb{C}_p$ n'est pas localement compact.
3) l'ensemble des valeurs de la norme de $\mathbb{C}_p$ est égal

$$\{p^q, q \in \mathbb{Q}\}$$

4) $\mathbb{Q} \subset \mathbb{Q}_p \subset \overline{\mathbb{Q}}_p \subset \mathbb{C}_p$.

1.5 Codes de Hensel :

Les opérations arithmétiques dans le corps des nombres p-adique $\mathbb{Q}_p$ sont faites chiffre à chiffre. On part de la gauche vers la droite comme dans les calculs arithmétiques dans la base p. Donc pour les calculs arithmétiques p-adiques, le problème dépend du nombre (la longueur) de suite des chiffres p-adiques. La solution consiste à introduire une arithmétique p-adique de longueur finie (les codes de Hensel).

Dans cette partie on définit les codes de Hensel sur le corps des nombres rationnels, méthode de calcul les codes, et les opérations arthmétiques dans $H_{p,M}$.

Définition 1.5.1 *Si p un nombre premier, alors le code de Hensel noté $H(p, M, \alpha)$ de longueur M pour tout nombre rationnel*

$$\alpha = p^m.\frac{a}{b} = a_m a_{m+1}..... \cdot a_0 a_1.....$$

est le couple

$$(manto\alpha, \exp_\alpha) = (\cdot a_0 a_1.....a_{M-1}, m)$$

où les chiffres $(a_i)_{i=\overline{0,r-1}}$ (resp : m) sont les mantisses de α (resp :exposant de p), donc

$$\alpha = \sum_{i=0}^{M-1} a_i p^i \in \mathbb{Z}_{p^M}$$

on écrit

$$H(p, M, \alpha) = (manto\alpha, \exp_\alpha) = (\cdot a_0 a_1.....a_{M-1}, m)$$

Autrement dit le code de Hensel est un segment fini (une approximation) de son développement p-adique infini et M un entier positif qui spécifie le nombre de chiffres signéficatifs dans le développement p-adique de α.

$$\begin{cases} \alpha = \sum_{n=m}^{\infty} a_n p^n \xrightarrow{\text{trancature de } M \text{ chiffres premiers}} H(p, M, \alpha) = (a_m a_{m+1}... \cdot a_0 a_1...a_t, m) \\ \\ M = m + t + 1 \end{cases}$$

- Notons par $H_{p,M}$ l'ensemble des codes de Hensel d'un nombre rationnel α.

Exemple 1.5.2

si

$$p = 5,\ M = 4, \alpha = \frac{2}{3} = 0 \cdot 41313 = 0 \cdot 4\overline{13}\ ,\ m = 0$$

alors

$$H(5,4,\frac{2}{3}) = (\cdot 4131, 0)$$

Remarque 1.5.3 *La correspondance entre le corps* $(\mathbb{Q},+,.)$ *et* $(H_{p,M},+,.)$ *n'est pas bijective, puisque chaque code de Hensel de mantisse* $\cdot a_0 a_1 .....a_{M-1}$ $(= \sum_{i=0}^{M-1} a_i p^i)$ *dans* $H_{p,M}$ *est une image d"une infinité de sous ensembles de* $\mathbb{Q}$. *Pour cette raison, on a besoin de définir un sous ensemble convenable de* $\mathbb{Q}$ *tel que la correspondance entre ce sous ensemble et* $H_{p,M}$ *soit bijective. Il s'appelle l'ensemble des fractions de Farey.*

1.5.1 Fractions de Farey

Définition 1.5.4 *L'ensemble de Fractions de Farey d'ordre* N *noté* $F_{p,M,N}$ *est un sous ensemble de* $\mathbb{Q}$ *définie par*

$$\begin{cases} F_{p,M,N} = \left\{ \frac{a}{b} \in \mathbb{Q} / (a,b) = 1, 0 \leq a \leq N \ , \ \ 0 \prec b \leq N \right\} \\ \\ N \leq \sqrt{\frac{p^M - 1}{2}} \end{cases}$$

les dénoménateurs sont inférieurs que N.

Remarque 1.5.5

1) $F_{p,M,N}$ *est un sous ensemble de segment* $[0.1]$.

2) ne calcule pas le développement p-adique infini de α, *il suffit de calculer seulement les* $M-$*chiffres premiers.*

3) l'application

$$f \quad : \quad F_{p,M,N} \longrightarrow H_{p,M}$$

$$x \longmapsto f(x) = H(p,M,x)$$

est une application bijective.

Exemple 1.5.6 *posons*

$$F_N = F_{p,M,N}$$

Si $N = 5$, *alors la suite de fraction de Farey* F_5 *est*

$$F_5 = \left\{ \frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1} \right\}$$

Théorème 1.5.7 [1] [6] [7] [8]
Soit p un nombre premier et M un nombre entier positif. On définit N le plus grand entier positif satisfait l'inégalité

$$N \leq \sqrt{\frac{p^M - 1}{2}}$$

alors tout nombre rationnel α dans F_N peut être représenté uniquement par M chiffres signifécatifs ordonnés p-adique (code de Hensel), chaque chiffres est dans l'intervalle $[0.p-1]$.

1.5.2 Calcul de code de Hensel

on donne une méthode qui nous permet de calculer le code de Hensel d'un nombre rationnel.
soit $\alpha = \frac{a}{b} \in \mathbb{Q}$ un nombre rationnel et p un nombre premier, divisons a et b par le nombre p autant de fois que possible jusqu'à obtenir

$$\alpha = \frac{a}{b} = p^m.\frac{c}{d}, (cd, p) = 1$$

Supposons que le code de Hensel de $\frac{c}{d}$ est

$$H(p, M, \frac{c}{d}) = (\cdot a_0 a_1 .... a_{M-1}, 0)$$

avec $(a_{M-1}.....a_1 a_0)$ est la représentation de $\frac{c}{d} (\mathrm{mod}\, p^M)$ dans la base p.

$$cd^{-1} \equiv a_{M-1}p^{M-1} + ... + a_1 p + a_0 (\mathrm{mod}\, p^M)$$

alors on a les cas suivants :

1) <u>**CAS I** : $m = 0$</u>

Alors, premièrement on écrit le nombre $\frac{c}{d}$ dans la base p, i.e :

$$cd^{-1} \equiv a_{M-1}p^{M-1} + ... + a_1 p + a_0 (\mathrm{mod}\, p^M) = (a_{M-1}....a_1 a_0)_p$$

puis en versant les chiffres $(a_i)_{i=\overline{0,M-1}}$ pour obtenir le code de Hensel de α.

$$H(p, M, \alpha) = (\overleftarrow{(a_{M-1}....a_1 a_0)_p}, 0) = (\cdot a_0 a_1 .... a_{M-1}, 0)$$

Exemple 1.5.8 *soient*

$$\alpha = \frac{2}{3},\ p = 5,\ M = 4,\ p^M = 625$$

on a

$$\begin{aligned} \alpha &= \frac{2}{3} = 5^0.\frac{2}{3},\ m = 0 \\ 2.3^{-1} &= 2.417 \equiv 209 \bmod 625 \end{aligned}$$

exprimons le nombre 209 *dans la base* 5. *On trouve*

$$\begin{aligned} 209 &= 1.5^3 + 3.5^2 + 1.5^1 + 4.5^0 \\ &= (1314)_5 \end{aligned}$$

alors le code de Hensel de $\alpha = \frac{2}{3}$ *est*

$$H(5, 4, \frac{2}{3}) = (\cdot 4131, 0)$$

2) <u>Cas II : $m \prec 0$</u>

Dans ce cas

$$\alpha = p^m.\frac{c}{d}, m \in \mathbb{Z}_-^*$$

pour trouver $H(p, M, \alpha)$ il suffit de trouver $H(p, M, \frac{c}{d})$ comme dans le cas précédent et en suite, en changeant le point p-adique $(-m)$ fois à droite.

$$H(p, M, \alpha) = (\overbrace{\cdot}^{(-m) \text{ fois à droite}} a_0 a_1 .... a_{M-1}, m) = (a_0 a_1 ... a_{m-1} \cdot ... a_{M-1}, m)$$

Exemple 1.5.9

soient

$$\alpha = \frac{2}{15},\ p = 5,\ M = 4$$

alors

$$\alpha = \frac{2}{15} = 5^{-1}.\frac{2}{3},\ m = -1 \prec 0$$

on a

$$H(5, 4, \frac{2}{3}) = (\cdot 4131, 0)$$

alors en change le point p-adique une fois à droite, on obtient

$$H(5, 4, \frac{2}{15}) = (\overbrace{\cdot 4131}^{\textit{une fois à droite}}, 0) = (4 \cdot 131, -1)$$

3) Cas III : $m \succ 0$

dans ce cas

$$\alpha = p^m.\frac{c}{d}, m \in \mathbb{N}$$

donc pour calculer $H(p, M, \alpha)$ il suffit de calculer $H(p, M, \frac{c}{d})$ comme dans le premier cas, en suite en chengeant le point p-adique m fois à gauche.

$$H(p, M, \alpha) = (\overleftarrow{\cdot}^{m \text{ fois à gauche}} a_0 a_1 .... a_{M-1}, m) = (\cdot 0...00000 a_0 a_1 .... a_{M-(m+1)}, m)$$

Exemple 1.5.10 *Soient*

$$\alpha = \frac{10}{3}, p = 5, M = 4$$

on a

$$\alpha = \frac{10}{3} = 5^{+1}.\frac{2}{3},\ m = 1 \succ 0 \quad , \frac{c}{d} = \frac{2}{3}$$

d'aprés le premire cas on a

$$H(5, 4, \frac{2}{3}) = (\cdot 4131, 0)$$

en chenge le point p-adique une fois à gauche, on trouve

$$H(5, 4, \frac{10}{3}) = (\overleftarrow{\cdot 4131}^{\text{une fois à gauche}}, 0) = (\cdot 0413, +1)$$

Remarque 1.5.11 *Les règles pour obtenir les codes de Hensel des nombres négatifs sont les mêmes.*

Exemple 1.5.12

Soit $a = \frac{-2}{3}$, *pour trouver* $H(5, 4, \frac{-2}{3})$, *il suffit de trouver l'expansion de* $\frac{-2}{3} (\mathrm{mod}\, 5^4)$ *dans la base* 5 *comme suit*

$$\begin{aligned} \frac{-2}{3} (\mathrm{mod}\, 5^4) &= -2.3^{-1} (\mathrm{mod}\, 5^4) \\ &= -2.417 \\ &\equiv 416 \,\mathrm{mod}\, 5^4 \\ &= (3131)5 \end{aligned}$$

donc

$$H(5, 4, \frac{-2}{3}) = (\cdot 1313, 0)$$

Théorème 1.5.13 [7]

soient $\alpha = \frac{a}{b}$ *et* $\beta = \frac{c}{d}$ *avec* $(b, p) = (d, p) = 1$, *alors*

$$H(p, M, \alpha) = H(p, M, \beta) \Longleftrightarrow ab^{-1} \equiv cd^{-1} \,\mathrm{mod}\, p^M$$

autrement dit

$$ad \equiv cb \bmod p^M$$

Exemple 1.5.14
soient

$$\alpha = \frac{10}{7}, \beta = \frac{45}{14}, p = 5, M = 4$$

alors

$$\begin{aligned} \alpha &= \frac{10}{7} = 5.\frac{2}{7} \\ \beta &= \frac{45}{14} = 5.\frac{9}{14} \end{aligned}$$

on a

$$10.17^{-1} = 45.14^{-1} \bmod 625 \Leftrightarrow 10.14 = 45.17 \bmod 625$$

1.6 Pseudo codes de Hensel :

Définition 1.6.1 *Le pseudo-code de Hensel d'un nombre rationnel α est un code, tel que*

$$\begin{cases} a_0, a_1, ..., a_k = 0 \ , a_{k+1} \neq 0 \\ 0 \leq k \prec M - 1 \end{cases}$$

Alors le pseudo-code de Hensel est d'ordre k. En écrit

$$PH(p, M, \alpha) = (\cdot 0.....0 a_{k+1} ... a_{M-1}, m)$$

* Notons par $PH_{p,M}$ l'ensemble des pseudo-codes de Hensel et $SH_{p,M}$ le complémentaire de l'ensemble $PH_{p,M}$.

$$H_{p,M} = PH_{p,M} \cup SH_{p,M}$$

1.7 Les opérations arithmétiques avec les codes de Hensel

La possibilité de faire les opérations arithmétiques sur $H_{p,M}$ est assurés par le théorème suivant

Théorème 1.7.1 [6] [23]
Soient p un nombre premier, M un entier positif (une approximation) et Φ_1 un opérateur arithmétique (+,-,.,/) sur $\mathbb{Q}$ et Φ_2 un opérateur arithmétique sur $H_{p,M}$, alors pour tout $\alpha_1, \alpha_2 \in \mathbb{Q}$, si $\alpha_1 \Phi_1 \alpha_2 = \alpha_3$, avec $\alpha_3 \in F_{p,M}$, alors il existe $\beta \in H_{p,M}$ unique tel que

$$H(p, M, \alpha_1)\Phi_2 H(p, M, \alpha_2) = \beta = H(p, M, \alpha_3)$$

i.e

$$\forall \alpha_1, \alpha_2 \in \mathbb{Q} : \alpha_1 \Phi_1 \alpha_2 = \alpha_3 \quad / \alpha_3 \in F_{p,M,N} = F_N$$

$$\Rightarrow \exists! \beta \in H_{p,M} : H(p, M, \alpha_1)\Phi_2 H(p, M, \alpha_2) = \beta \quad = H(p, M, \alpha_3)$$

1.7.1 L' addition :

Soient les codes de Hensel suivants

$$\begin{cases} H(p, M, \alpha) = (mant_\alpha, \exp_\alpha) & = (\cdot a_0 a_1 .....a_{M-1}, \exp_\alpha) \\ \\ H(p, M, \beta) = (mant_\beta, \exp_\beta) & = (\cdot b_0 b_1 .....b_{M-1}, \exp_\beta) \end{cases}$$

pour trouver

$$H(p, M, \alpha) + H(p, M, \beta)$$

on doit :

Premièrement, normaliser le code qui a le plus grand exposant selon les cas I ,II,III précédents pour obtenir $\exp_\beta = \exp_\alpha$

Deuxièmement, en fait l'addition gauche à droite par rapport aux mantisses. Alors

$$\begin{aligned} H(p, M, \alpha) + H(p, M, \beta) &= H(p, M, \gamma) \\ &= (mant_\alpha, \exp_\alpha) + (mant_\beta, \exp_\beta) \\ &= (mant_\beta + mant_\alpha, \exp_\gamma) \end{aligned}$$

donc, si $\alpha = \cdot a_0 a_1 .....a_{M-1}$ et $\beta = \cdot b_0 b_1 .....b_{M-1}$, alors

$$\begin{cases} \gamma = \alpha + \beta = \cdot \gamma_0 \gamma_1 \gamma_2 .....\gamma_{M-1} \\ \\ \gamma_n \equiv a_n + b_n \bmod p \ , \ 0 \leq n \leq M-1 \end{cases}$$

Exemple 1.7.2 *on fait l'addition suivante*

$$\frac{3}{10} + \frac{1}{2} \ , p = 5, M = 4$$

les codes de Hensel de $\frac{3}{10}$ *(resp :* $\frac{1}{2}$*) sont*

$$\begin{cases} H(5,4,\frac{3}{10}) = (\cdot 4222, -1) \\ \\ H(5,4,\frac{1}{2}) = (\cdot 3222, 0) \end{cases}$$

on remarque que les exposants sont différents, donc nous devons normaliser le code qui a le plus grand exposant selon les cas I ,II,III précédents.

$$(\cdot 3222, 0) \longrightarrow (\cdot 0322, -1)$$

on fait l'addition entre les mantisses

$$\begin{array}{rccccccc} + & \cdot & 4 & 2 & 2 & 2 & , & -1 \\ = & \cdot & 0 & 3 & 2 & 2 & , & -1 \\ \hline & \cdot & 4 & 0 & 0 & 0 & , & -1 \end{array}$$

donc le code $(\cdot 4000, -1)$ *représente le nombre rationel* $\frac{4}{5} \in F_{5,4}$.

$$H(5,4,\frac{3}{10}) + H(5,4,\frac{1}{2}) = H(5,4,\frac{4}{5}) = (\cdot 4000, -1)$$

Remarque 1.7.3 *L'addition dans* $H_{p,M}$ *est représentée par le tableau suivant*

$$\begin{bmatrix} + & SH_{p,M} & PH_{p,M} \\ SH_{p,M} & H_{p,M} & SH_{p,M} \\ PH_{p,M} & SH_{p,M} & PH_{p,M} \end{bmatrix}$$

1.7.2 La Soustraction :

Pour faire la soustraction de $H(p, M, \alpha) - H(p, M, \beta)$ en utilisant "l' addition complétée" c'est-à-dire calculons le code $H(p, M, -\beta)$, puis on fait l'addition comme dans le cas précédent.

$$\begin{aligned} H(p, M, \alpha) - H(p, M, \beta) &= H(p, M, \alpha) + H(p, M, -\beta) \\ &= H(p, M, \gamma = \alpha - \beta) \\ &= (mant_\alpha, \exp_\alpha) + (mant_{-\beta}, \exp_{-\beta}) \\ &= (\cdot a_0 a_1 ....a_{M-1}, \exp_\alpha) + (\cdot c_0 c_1 .....c_{M-1}, \exp_{-\beta}) \\ &= (\cdot d_0 d_1 ....d_{M-1}, \exp_\gamma) \end{aligned}$$

donc, si

$$\alpha = \cdot a_0 a_1 .....a_{M-1}$$

$$\beta = \cdot b_0 b_1 .....b_{M-1}$$

alors

$$\begin{cases} \gamma = \alpha - \beta = \cdot \gamma_0 \gamma_1 \gamma_2 .....\gamma_{M-1} \\ \gamma_n \equiv a_n + b'_n \bmod p \ , \ 0 \leq n \leq M-1 \end{cases}$$

tel que

$$b'_n = p - b_n, 0 \leq n \leq M-1$$

Exemple 1.7.4 *on calcul la soustraction suivante*

$$\frac{3}{4} - \frac{3}{2}, p = 5, M = 4$$

on a

$$\begin{aligned} H(5, 4, \frac{3}{4}) &= (\cdot 2111, 0) \\ H(5, 4, \frac{3}{2}) &= (\cdot 4222, 0) \end{aligned}$$

On remarque que les exposants sont égaux. Alors

$$\begin{array}{rcccccc} - & \cdot & 2 & 1 & 1 & 1 & , & 0 \\ = & \cdot & 4 & 2 & 2 & 2 & , & 0 \\ \hline & \cdot & 3 & 4 & 4 & 4 & , & 0 \end{array}$$

Donc le code $(\cdot 3444, 0)$ *représente le nombre rationnel* $\frac{-3}{4}$

$$H(5, 4, \frac{-3}{4}) = (\cdot 3444, 0)$$

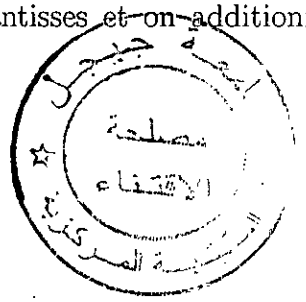
Remarque 1.7.5 *la soustraction dans* $H_{p,M}$ *est représentée par le tableau suivant*

$$\begin{bmatrix} - & SH_{p,M} & PH_{p,M} \\ SH_{p,M} & H_{p,M} & SH_{p,M} \\ PH_{p,M} & SH_{p,M} & PH_{p,M} \end{bmatrix}$$

1.7.3 La multiplication :

Pour faire la multiplication, on multipliant les mantisses et on additionne les exposants. En effet, si

$$\begin{cases} \alpha_1 = p^{m_1}.\frac{c_1}{d_1} \in \mathbb{Q} \\ \alpha_2 = p^{m_2}.\frac{c_2}{d_2} \in \mathbb{Q} \end{cases}$$



alors

$$\begin{aligned} \alpha_1.\alpha_2 &= p^{m_1}.p^{m_2}.(\frac{c_1}{d_1}.\frac{c_2}{d_2}) \\ &= p^{(m_1+m_2)}.\frac{c_3}{d_3} \\ &= \alpha_3 \end{aligned}$$

donc

$$\begin{cases} H(p, M, \alpha_1) = (\cdot a_0 a_1 .... a_{M-1}, m_1) \\ H(p, M, \alpha_2) = (\cdot b_0 b_1 .... b_{M-1}, m_2) \end{cases}$$

$$\Longrightarrow H(p, M, \alpha_1).H(p, M, \alpha_2) = H(p, M, \alpha_3)$$

$$\Longrightarrow H(p, M, \alpha_1).H(p, M, \alpha_2) = (\cdot a_0 a_1 .... a_{M-1}, m_1).(\cdot b_0 b_1 .... b_{M-1}, m_2)$$

$$\Longrightarrow H(p,M,\alpha_1).H(p,M,\alpha_2) = (\cdot s_0 s_1 .... s_{M-1}, m_1 + m_2)$$

Le tableau suivant donne la multiplication dans $H_{p,M}$:

$$\begin{array}{cccccccccccc}
* & \cdot & b_0 & b_1 & b_2 & b_3 & . & . & b_j & . & . & b_{M-1} \\
= & \cdot & a_0 & a_1 & a_2 & a_3 & . & . & a_j & . & . & a_{M-1} \\
 & & P_{0,0} & P_{0,1} & p_{0,2} & P_{0,3} & . & . & P_{0,j} & . & . & P_{0,M-1} \\
 & & & P_{1,0} & P_{1,1} & P_{1,2} & . & . & P_{1,j-1} & . & . & P_{1,M-1} \\
 & & & & P_{2,0} & P_{2,1} & . & . & P_{2,j-2} & . & . & P_{2,M-1} \\
 & & & & & . & . & . & . & . & . & . \\
 & & & & & & . & . & . & . & . & . \\
 & & & & & & & . & . & . & . & . \\
 & & & & & & & & . & . & . & . \\
 & & & & & & & & & . & . & . \\
 & & & & & & & & & & . & . \\
 & & & & & & & & & & & P_{M-1,M-1} \\
= & \cdot & s_0 & s_1 & s_2 & . & . & . & . & . & . & s_{M-1}
\end{array}$$

tels que

$$P_{i,j} = a_i.b_j, 0 \leq i \leq j \leq M-1$$

et

$$\begin{cases}
s_0 = P_{0,0} \\
s_1 = P_{0,1} + P_{1,0} \\
s_2 = P_{0,2} + P_{1,1} + P_{2,0} \\
\cdot \\
\cdot \\
s_j = \sum_{i=0}^{j} P_{i,j-i}
\end{cases}$$

Exemple 1.7.6

trouvons la multiplication suivante

$$\frac{4}{15}.\frac{5}{2}\ ,\ p=5,\ M=4$$

on a

$$H(5,4,\frac{4}{15}) = (\cdot 3313, -1) \quad , \quad H(5,4,\frac{5}{2}) = (\cdot 3222, 1)$$

alors

$$\begin{array}{rccccccc} * & \cdot & 3 & 3 & 1 & 3 & , & -1 \\ = & \cdot & 3 & 2 & 2 & 2 & , & +1 \\ + & & 4 & 0 & 0 & 0 & & \\ & & & 1 & 2 & 3 & & \\ & & & & 1 & 2 & & \\ & & & & & 1 & & \\ = & \cdot & 4 & 1 & 3 & 1 & , & 0 \end{array}$$

le code $(\cdot 4131, 0)$ *représente le nombre rationnel* $\frac{2}{3}$ *(puisque* $\frac{4}{15}.\frac{5}{2} = \frac{2}{3}$*) .i.e :*

$$H(5, 4, \frac{4}{15}.\frac{5}{2}) = H(5, 4, \frac{2}{3}) = (\cdot 4131, 0)$$

Remarque 1.7.7 *La multiplication dans* $H_{p,M}$ *est représentée par le tableau suivant*

$$\begin{bmatrix} * & SH_{p,M} & PH_{p,M} \\ SH_{p,M} & SH_{p,M} & PH_{p,M} \\ PH_{p,M} & PH_{p,M} & PH_{p,M} \end{bmatrix}$$

1.7.4 La Division :

L'opération de division est similaire à l'opération de multiplication tel que pour trouver $H(p, M, \frac{\alpha}{\beta})$ il faut premièrement trouver l'inverse de β modulo p^M, en suite on fait la multiplication $\alpha.\frac{1}{\beta}$ comme dans le cas précédent. Pour faire la division nous devons diviser les mantisses et soustraire les exposants de ces codes. En effet, soient

$$\alpha_1 = p^{m_1}.\frac{c_1}{d_1} \quad , \alpha_2 = p^{m_2}.\frac{c_2}{d_2} \quad , \alpha_3 = \frac{\alpha_1}{\alpha_2}$$

et

$$\begin{cases} H(p, M, \alpha_1) = (\cdot a_0 a_1 ....a_{M-1}, m_1) \\ \\ H(p, M, \alpha_2) = (\cdot b_0 b_1 ....b_{M-1}, m_2) \quad , \ b_0 \neq 0 \end{cases}$$

donc

$$\begin{aligned} \alpha_3 &= \frac{\alpha_1}{\alpha_2} = \frac{p^{m_1}.\frac{c_1}{d_1}}{p^{m_2}.\frac{c_2}{d_2}} \\ &= p^{(m_1 - m_2)}.\frac{x}{y} \end{aligned}$$

ce qui donne

$$\begin{cases} H(p, M, \alpha_3) = (\cdot t_0 t_1 .... t_{M-1}, m_1 - m_2) \\ \\ \cdot t_0 t_1 .... t_{M-1} = \frac{\cdot a_0 a_1 .... a_{M-1}}{\cdot b_0 b_1 .... b_{M-1}} \end{cases}$$

d'autre part, on a

$$\alpha_3 = \frac{\alpha_1}{\alpha_2} = \alpha_1 . \alpha_2^{-1}$$

donc pour déterminer α_3 il suffit de trouver α_2^{-1} comme suit :
supposons que

$$\alpha_2^{-1} = \cdot b'_0 b'_1 .... b'_{M-1}$$

alors

$$\alpha_2 . \alpha_2^{-1} \quad = \quad 1 \Longleftrightarrow \cdot 100..... 0 = (\cdot b_0 b_1 .... b_{M-1}) . (\cdot b'_0 b'_1 .... b'_{M-1})$$

$$\Longleftrightarrow \begin{cases} b_0 b'_0 \equiv 1 \bmod p \\ (b_0 b'_1 + b_1 b'_0) p \equiv 0 \bmod p^2 \\ (b_0 b'_2 + b_1 b'_1 + b_2 b'_0) p^2 \equiv 0 \bmod p^3 \\ (b_0 b'_3 + b_1 b'_2 + b_2 b'_1 + b_3 b'_0) p^3 \equiv 0 \bmod p^4 \\ \\ \\ (\sum_{i=0}^{j} b_i b'_{j-i}) p^j \equiv 0 \bmod p^{j+1} \end{cases}$$

$$\Longleftrightarrow \begin{cases} b_0 b'_0 \equiv 1 \bmod p \\ b_0 b'_1 + b_1 b'_0 \equiv 0 \bmod p \\ b_0 b'_2 + b_1 b'_1 + b_2 b'_0 \equiv 0 \bmod p \\ b_0 b'_3 + b_1 b'_2 + b_2 b'_1 + b_3 b'_0 \equiv 0 \bmod p \\ . \\ \sum_{i=0}^{j} b_i b'_{j-i} \equiv 0 \bmod p \\ . \end{cases}$$

avec $0 \leq b_i, b'_i \leq p-1$, les donnés sont p, b_i et les inconnus sont b'_i. En suite on trouve $\alpha_3 = \frac{\alpha_1}{\alpha_2} = \alpha_1 . \alpha_2^{-1}$.

Exemple 1.7.8 *Trouvons la division suivante*

$$\frac{\frac{3}{4}}{\frac{6}{5}}, p = 5, M = 4$$

on a

$$\begin{cases} H(5,4,\frac{3}{4}) = (\cdot 2111, 0) \\ H(5,4,\frac{6}{5}) = (\cdot 1100, -1) \\ F_{5,4} = 17 \end{cases}$$

Pour faire la division, il faut trouver l'inverse du déviseur $(\frac{1}{\frac{6}{5}} \bmod p^M)$*, puis on le multiplie par* $(\frac{3}{4})$.

$$\begin{array}{cccccccccc} 2 & 1 & 1 & 1 & \div & 1 & 0 & 0 & 0 \\ \\ 3 & 2 & 4 & 4 & & 2 & 4 & 1 & 3 \\ & 4 & 0 & 0 & & & & & \\ & 1 & 0 & 4 & & & & & \\ & & 1 & 4 & & & & & \\ & & 4 & 3 & & & & & \\ & & & 3 & & & & & \end{array}$$

alors le code $(\cdot 2413, 1)$ *représente le nombre rationnel* $\frac{5}{8}$.

$$H(5,4,\frac{3}{4}).H(5,4,\frac{6}{5}) = H(5,4,\frac{5}{8}) = (\cdot 2413, 1)$$

Remarque 1.7.9 *La division dans* $H_{p,M}$ *est représentée par le tableau suivant*

$$\begin{bmatrix} / & SH_{p,M} & PH_{p,M} \\ SH_{p,M} & SH_{p,M} & PH_{p,M} \\ PH_{p,M} & PH_{p,M} & PH_{p,M} \end{bmatrix}$$

Chapitre 2

Algorithme de calcul du code de Hensel de l'inverse d'un nombre p-adique

Première partie

Fonctions p-adiques et Lemme de Hensel

2.1 Les fonctions p-adiques

Dans cette partie nous étudierons les fonctions à variables p-adique. En commençant par les fonctions p-adiques continues.

2.1.1 Les fonctions p-adiques continues

Définition 2.1.1
1) une fonction p-adique $f : X \longrightarrow \mathbb{Q}_p \ \ (X \subset \mathbb{Q}_p)$ *est dite continue au point* $x_0 \in X$ *si*

$$\forall \varepsilon \succ 0, \exists \delta \succ 0 : |x - x_0|_p \prec \delta \Longrightarrow |f(x) - f(x_0)|_p \prec \varepsilon \tag{2.1}$$

autrement dit

$$\forall \varepsilon \succ 0, \exists \delta \succ 0, \forall x \in B(x_0, \delta) \Longrightarrow f(x) \in B(f(x_0), \varepsilon)$$

2) une fonction p-adique $f : X \longrightarrow \mathbb{Q}_p$ *est dite continue sur* X *si elle est continue en tout point de* X.

Notons par $C(\mathbb{Q}_p)$ l'ensemble des fonctions p-adiques continues à variable dans $\mathbb{Q}_p$.

Définition 2.1.2 *une fonction p-adique* $f : X \longrightarrow \mathbb{Q}_p$ *est dite uniformément continue sur* X *si*

$$\forall \varepsilon \succ 0, \exists \delta \succ 0 : |x - y|_p \prec \delta \Longrightarrow |f(x) - f(y)|_p \prec \varepsilon, \forall x, y \in X$$

Exemple 2.1.3
1) Soit

$$f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + ... + \alpha_n x^n, \alpha_k \in \mathbb{Q}_p$$

une fonction polynomiale, la fonction f *est continue sur* $\mathbb{Q}_p$. *En effet*
Soit $y \in \mathbb{Q}_p$, *montrons que* f *est continue au point* y.
on a

$$\begin{aligned} |f(x) - f(y)|_p &= \left| \sum_{k=0}^{n} \alpha_k x^k - \sum_{k=0}^{n} \alpha_k y^k \right|_p \\ &= |x - y|_p \cdot \left| \sum_{k=1}^{n} \alpha_k \cdot (x^{n-1} + x^{n-2} y + ... + y^{n-1}) \right|_p \end{aligned}$$

supposons que

$$|x|_p \prec |y|_p$$

alors

$$\begin{aligned} |f(x)-f(y)|_p &\leq |x-y|_p . \max\left\{\left|y^{k-1}\alpha_k\right|_p, 1 \leq k \leq n\right\} \\ &\leq r.|x-y|_p \end{aligned}$$

dans ce cas nous pouvons prendre

$$\delta = \frac{\varepsilon}{r}$$

pour que

$$|x-y|_p \prec \delta \Longrightarrow |f(x)-f(y)|_p \leq \varepsilon$$

2) Soient $\sum_{n\geq 0}\alpha_n x^n$ *est une série p-adique de puissance et r son rayon de convergence. alors la fonction p-adique*

$$\begin{aligned} f &: B(0,r) \longrightarrow \mathbb{Q}_p \\ x &\longmapsto f(x) = \sum_{n\geq 0}\alpha_n x^n \end{aligned}$$

est continue.

Théorème 2.1.4 [17]
Soient $X \subset \mathbb{Z}_p$ *et* $f, g : X \longrightarrow \mathbb{Q}_p$ *des fonctions p-adiques. Alors*
1) f *est continue au point* $x_0 \in X \Longleftrightarrow \forall x_n \in X, \lim_n x_n = \alpha \Longrightarrow \lim_n f(x_n) = f(\alpha)$
2) si f, g *sont continues en* x_0 *alors* $f+g$, $f-g$, $f.g$ *et* $\frac{f}{g}$ $(g(x_0) \neq 0)$ *sont continues en* x_0.

Définition 2.1.5 *Soit* $f : X \longrightarrow \mathbb{Q}_p, X \subset \mathbb{Q}_p$ *une fonction p-adique, on dit que* f *est localement constante sur* X*,si pour tout* $x \in X$ *il existe un voisinage* V_x *de* x *telle que* f *soit constante sur* V_x.

Exemple 2.1.6
Soit $X = \mathbb{Z}_p$. *Alors*

$$\forall x \in \mathbb{Z}_p, \exists \alpha_n = \overline{0.p-1} : x = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + ... + \alpha_n p^n .....$$

considérons la fonction f_n *définie par :*

$$\begin{aligned} f_n &: \mathbb{Z}_p \longrightarrow \mathbb{Z}_p \\ x &\longmapsto f_n(x) = \alpha_n, n \geq 0 \end{aligned}$$

On a f_n est une fonction localement constante sur $\mathbb{Z}_p$. En effet, on remarque que f_n prendre la même valeur si nous remplaçons x par tout y satisfait $|x-y|_p \prec p^{-n}$ pour tout $n \geq 0$, c'est à dire il existe un voisinage $V_x = B(x, p^{-n})$ telle que f soit constante sur V_x. Nous pouvons prolonger cet exemple à la fonction f_n, telle que

$$\begin{aligned} f_n &: \mathbb{Q}_p \longrightarrow \mathbb{Q}_p \\ x &= \sum_{k=n}^{\infty} \alpha_k p^k \longmapsto f_n(x) = \alpha_n \end{aligned}$$

les fonctions $(f_n)_{n\in\mathbb{Z}}$ sont localements constantes sur $\mathbb{Q}_p$.

Proposition 2.1.7 [17]
Si $f : X \longrightarrow \mathbb{Q}_p$ une fonction localement constante sur X, alors f est continue sur X.

Preuve.
Dans ce cas il suffit de remplacer $\delta = p^{-m}$ dans (2.1). ■

Exemple 2.1.8
Soit $X = B(0.1) \subset \mathbb{Z}_p$. On définit la fonction caractéristique χ_X de X par

$$\begin{aligned} \chi_X &: \mathbb{Z}_p \longrightarrow \mathbb{Q}_p \\ x &\longmapsto \chi_X(x) = \begin{cases} 1, x \in X \\ 0, x \notin X \end{cases} \end{aligned}$$

la fonction χ_X est localement constante sur $\mathbb{Z}_p$, donc elle est constante aussi sur toute boule $B(k,1)$ tel que $0 \leq k \leq p-1$, par conséquence elle est continue sur toute boule $B(x,\delta)$ avec $\delta \succ 0$.

Corollaire 2.1.9 [17]
Toute fonction localement constante sur $\mathbb{Z}_p$ est uniformément continue.

Preuve.
Soient f une fonction localement constante sur $\mathbb{Z}_p$, p^{-m_i} les rayons de $(V_{x_i})_{i=\overline{1,n}}$ voisinages de x_i et $m = \max_{1\leq i\leq n} m_i$.
Soit

$$x, y \in \mathbb{Z}_p : |x-y|_p \prec p^{-m}$$

Montrons que $\delta = p^{-m}$
Soit $x \in V_{x_i}$, et comme tout point de la boule est son centre, alors on peut écrire $x = x_i$ donc

$$|x_i - y|_p \leq p^{-m_i} \leq p^{-m}$$

alors

$$f(y) = f(x_i) = f(x)$$

ce qui donne f est uniformément continue. ■

2.1.2 Les fonctions p-adiques dérivables

Définition 2.1.10

a) Soit X un sous ensemble de $\mathbb{Q}_p$ et $a \in X$. La fonction $f : X \longrightarrow \mathbb{Q}_p$ est dite dérivable au point a si le nombre $f'(a) = \lim\limits_{x \longrightarrow a} \frac{f(x)-f(a)}{x-a}$ existe.

b) On dit que f est dérivable sur X si $f'(a)$ existe pour tout $a \in X$.

Remarque 2.1.11

1) Les règles de la dérivation (la somme, le produit, quotient ,composition ...) sur le corps $\mathbb{R}$ restent valables sur le cors $\mathbb{Q}_p$, et par conséquence la dérivée du polynome $p(x) = \sum\limits_{k=0}^{n} \alpha_k x^k \in \mathbb{Q}_p$ est $p'(x) = \sum\limits_{k=1}^{n} k\alpha_k x^{k-1}$.

2) Sur les nombres réels, les seules fonctions dont les dérivées sont nulles sont les fonctions constantes. Ceci n'est pas vrai sur les nombres p-adiques. Par exemple, la fonction

$$\begin{array}{rcl} f & : & \mathbb{Q}_p \longrightarrow \mathbb{Q}_p \\ x & \longmapsto & f(x) = \begin{cases} \left(\frac{1}{|x|_p}\right)^2, x \neq 0 \\ 0, x = 0 \end{cases} \end{array}$$

possède une dérivée nulle en tous points, mais n'est même pas constante localement en 0.

Définition 2.1.12 *Soit $E \subset \mathbb{Z}_p$ et $\alpha \succ 0$. Une fonction $f : E \longrightarrow \mathbb{Q}_p$ est Lipchitzienne d'ordre α, s'il existe une constante $M \succ 0$ (s'appelle constante de Lipchitz), tel que*

$$|f(x) - f(y)|_p \leq M.|x - y|_p^{\alpha}, \forall x, y \in E$$

Remarque 2.1.13 *Dans l'analyse réelle, le théorème de Rolle dit que si $f : [a, b] \longrightarrow \mathbb{R}$ est continue , dérivable sur (a, b) et $f(a) = f(b)$, alors il existe un réel $\delta \in (a, b)$, tel que $f'(\delta) = 0$. Par contre le théorème de Rolle est faux dans le cas p-adique.*

Exemple 2.1.14

Soit $f : \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ definie par

$$f(x) = x^p - x$$

on a

$$\begin{cases} f(0) = 0 \\ f(1) = 0 \\ f'(x) = px^{p-1} - 1 \end{cases}$$

et

$$|f'(x) + 1|_p = \left|px^{p-1}\right|_p \leq p^{-1}$$

donc

$$f'(x) \in -1 + p\mathbb{Z}_p$$

alors

$$f'(x) \neq 0, \forall x \in \mathbb{Z}_p$$

2.2 Lemme de Hensel

Le lemme de Hensel que nous prouvons ci dessous nous permettre de donner une description précise de l'ensemble des zéros de f, et de traiter dans certains cas les problèmes de divisibilité.

Lemme 2.2.1 [5] [11]
Soient n un entier ≥ 1, $f \in \mathbb{Z}_p[x]$ et $a \in \mathbb{Z}_p$ tels que $f(a) \equiv 0 \bmod p^n$: ie. $|f(a)|_p \leq p^{-n}$. Soit f' la dérivée de f. S'il on a $|f'(a)|_p = p^{-k}$ où $0 \leq 2k \prec n$;alors $b = a - \frac{f(a)}{f'(a)} \in \mathbb{Z}_p$ est tel que
i) $b \equiv a \bmod p^{n-k}$
ii) $f(b) \equiv 0 \bmod p^{n+1}$
iii) $|f'(b)|_p = |f'(a)|_p = p^{-k}$

Lemme de Hensel nous montre l'existence de la solutions d'une équation à variables p-adiques, et nous approche cette solution par une suite des nombres p-adiques qui satisfaisant les conditiond *i*), *ii*), *iii*).

Preuve.
Soit

$$f(x) = \sum_{j=0}^{m} \frac{f^{(j)}(a)}{j!}(x-a)^j$$

le développement de Taylor de f. On a

$$f(x) = f(a) + f'(a)(x-a) + (x-a)^2 g(x) \ , \ g(x) \in \mathbb{Z}_p[x]$$

Considérant $b = a - \frac{f(a)}{f'(a)}$, on obtient

$$f(b) = f(a) - \frac{f(a)}{f'(a)} f'(a) + \left(\frac{f(a)}{f'(a)}\right)^2 g(b) = \left(\frac{f(a)}{f'(a)}\right)^2 g(b)$$

On a

$$|f(b)|_p = \frac{|f(a)|_p^2}{|f'(a)|_p^2} |g(b)|_p \leq \frac{|f(a)|_p^2}{|f'(a)|_p^2} = \frac{|f(a)|_p^2}{p^{-2k}} \leq \frac{p^{-2n}}{p^{-2k}} = p^{-n-(n-2k)}$$

Mais par hypothèse $0 \leq 2k \prec n$, donc $n - 2k \geq 1$ et

$$|f(b)|_p \leq p^{-n}.p^{-(n-2k)} \leq p^{-(n+1)}$$

i.e.

$$f(b) \equiv 0 \bmod p^{n+1}$$

Il est claire que

$$|b - a|_p = \frac{|f(a)|_p}{|f'(a)|_p} \leq p^{-n+k} = p^{-(n-k)}$$

i.e.

$$b \equiv a \bmod p^{p-k}$$

Considérant le développement de Taylor

$$f'(x) = f'(a) + f''(a)(x - a) + (x - a)^2 h(x) \ , \ h(x) \in \mathbb{Z}_p$$

On a

$$f'(b) = f'(a) + f''(a)(b - a) + (b - a)^2 h(b)$$

$$\Longleftrightarrow f'(b) = f'(a) - \frac{f(a)}{f'(a)} f''(a) + \left(\frac{f(a)}{f'(a)}\right)^2 h(b)$$

De plus

$$\begin{cases} \left|\frac{f(a)}{f'(a)} f''(a)\right|_p \leq \frac{|f(a)|_p}{|f'(a)|_p} \leq p^{-(n-k)} \\ \left|\left(\frac{f(a)}{f'(a)}\right)^2 h(b)\right|_p \leq \frac{|f(a)|_p^2}{|f'(a)|^2} \leq p^{-2(n-k)} \end{cases}$$

Ainsi

$$\left|-\frac{f(a)}{f'(a)} f''(a) + \left(\frac{f(a)}{f'(a)}\right)^2 h(b)\right|_p \leq \max\left\{p^{-(n-k)}, p^{-2(n-k)}\right\} = p^{-(n-k)} \prec p^{-k} = |f'(a)|_p$$

D'où l'on déduit

$$|f'(b)|_p = \left| f'(a) - \frac{f(a)}{f'(a)} f''(a) + \left(\frac{f(a)}{f'(a)}\right)^2 h(b) \right|_p = |f'(a)|_p = p^{-k}$$

■

Corollaire 2.2.2 [11]
Soit $f \in \mathbb{Z}_p[x]$, $x \in \mathbb{Z}_p$, et $N, k \in \mathbb{Z}$ tels que$0 \leq 2k \prec N$, $f(x) \equiv 0 \bmod p^N$ et $|f'(x)|_p = p^{-k}$. Alors il existe $z \in \mathbb{Z}_p$ tels que $f(z) = 0$ et $z \equiv x \bmod p^{N-k}$.

Preuve.
on pose $x_0 = x_1$, alors d'aprés le lemme de Hensel, on trouve

$$\begin{cases} x_1 \equiv x_0 \bmod^{N-k} \\ f(x_1) \equiv 0 \bmod p^{N+1} \\ |f'(x_1)|_p = p^{-k}, \\ 2k \prec N \prec N+1 \end{cases}$$

en répétant cette procédure, on obtient une suite $(x_n)_n$ telle que

$$\begin{cases} f(x_n) \equiv 0 \bmod p^{N+n} \\ x_{n+1} \equiv x_n \bmod p^{N+n-k} \end{cases}$$

par conséquent $|x_{n+1} - x_n| \leq p^{k-n-N}$, alors $(|x_{n+1} - x_n|_p)_n$ converge vers 0. Donc $(x_n)_n$ est une suite de Cauchy, elle converge vers $z \in \mathbb{Z}_p$ et comme f est continue, alors

$$|f(z)|_p = \left| f(\lim_{n \longrightarrow \infty} x_n) \right|_p = \lim_{n \longrightarrow \infty} |f(x_n)|_p = 0$$

et

$$|x_n - x|_p \prec p^{-N+k}, \forall n \in \mathbb{N}$$

donc

$$\begin{aligned} |z - x|_p &= \left| \lim_{n \longrightarrow \infty} (x_n) - x \right|_p = \left| \lim_{n \longrightarrow \infty} (x_n - x) \right|_p = \lim_{n \longrightarrow \infty} |x_n - x|_p \leq p^{-N+k} \\ &\Longrightarrow |z - x|_p \leq p^{-N+k} \end{aligned}$$

alors

$$z \equiv x \bmod p^{N-k}$$

■

2.2.1 Applications de lemme de Hensel :

les racines $(p-1)$ ièmes de l'unité

Théorème 2.2.3 [11] [17]
le corps des nombres p-adiques $\mathbb{Q}_p$ contient les racines $(p-1)$ ièmes de l'unité.

Preuve.
En appliquant le lemme de Hensel sur la fonction

$$f(x) = x^{p-1} - 1$$

on a

$$\forall t = \overline{1.p-1} : \begin{cases} f(t) \equiv 0 \bmod p \\ f'(t) \equiv 1 \bmod p \end{cases}$$

en effet , on a

$$\forall t = \overline{1.p-1} : |t|_p = 1$$

alors

$$\begin{aligned} \left|t^{p-1} - 1\right|_p &\leq \max\left\{\left|t^{p-1}\right|_p, |1|_1\right\} \\ &\leq \max\left\{|t|_p^{p-1}, |1|_1\right\} \\ &\leq 1 \end{aligned}$$

donc

$$\left|t^{p-1} - 1\right|_p \leq p^{-1}$$

d'autre part

$$\begin{aligned} f'(x) &= (p-1)x^{p-2} \Longrightarrow \left|f'(s)\right|_p = \left|(p-1)s^{p-2}\right|_p \\ &\Longrightarrow \left|f'(s)\right|_p = \left|ps^{p-2} - s^{p-2}\right|_p \\ &\Longrightarrow \left|f'(s)\right|_p \leq \max\left\{|p|\,.\,|s|_p^{p-2}, |s|_p^{p-2}\right\} \\ &\Longrightarrow \left|f'(s)\right|_p \leq \max\left\{p^{-1}; 1\right\} \\ &\Longrightarrow \left|f'(s)\right|_p \leq 1 \\ &\Longrightarrow f'(s) \not\equiv 0 \bmod p \end{aligned}$$

alors, d'aprés le lemme de Hensel pour les nombres $s = \overline{1.p-1}$, on trouve $(p-1)$ racines de f dans $\mathbb{Z}_p$, on les notés $r_1, r_2, ..., r_{p-1}$ telle que $f(r_s) \equiv 0 \bmod p$, $s = \overline{1.p-1}$. ■

Les racines carrées dans $\mathbb{Q}_p$

Proposition 2.2.4 [25] [26]

1) Supposons que $p \neq 2$, et soit $a = p^{v_p(a)}.u \in \mathbb{Q}_p^*$, $u \in \mathbb{Z}_p^*$ un nombre p-adique unitaire. Alors pour que a soit un carré, il faut et il suffit que $v_p(a)$ soit pair et que l'image de u dans $\mathbb{Z}_p^*$ soit un carré.

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 pair et $u \equiv 1 \bmod 8$.

Preuve.

Soit a un carré dans $\mathbb{Q}_p^*$ s'écrit sous la forme

$$a = p^{v_p(a)}(a_0 + a_1 p + a_2 p^2 + ...) = p^{v_p(a)}.u \quad , a_0 \neq 0 \ , \ u \in \mathbb{Z}_p^*$$

et

$$x = p^{v_p(x)}(x_0 + x_1 p + x_2 p^2 + ...) \in \mathbb{Q}_p^* \ , \ x_0 \neq 0$$

on a

$$x^2 = a \Longleftrightarrow p^{2v_p(x)}(x_0 + x_1 p + x_2 p^2 + ...)^2 = p^{v_p(a)}(a_0 + a_1 p + a_2 p^2 + ...)$$

on distingue deux cas :
1) si $p \neq 2$, alors

$$\begin{cases} v_p(a) = 2v_p(x) \\ \\ x_0^2 - a_0 \equiv \mod p \end{cases}$$

donc la valuation p-adique de a est un nombre paire. D'autre part on a

$$x_0^2 - a_0 \equiv \mod p$$

on applique le lemme de Hensel sur la fonction

$$f(x_0) = x_0^2 - a_0$$

telle que

$$\begin{cases} f'(x_0) = 2x_0 \\ \\ |f'(x_0)|_p = |2x_0|_p = 1 \end{cases}$$

donc d'aprés le lemme de Hensel, a est une racine carrée dans $\mathbb{Q}_p$.
2) Si $p = 2$, alors on a

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

avec

$$0 \prec x_0 \prec 2$$

donc

$$x_0 = 1 \Longrightarrow a_0 = 1$$

on obtient

$$\begin{aligned} x^2 &= a \Longleftrightarrow 2^{2v_2(x)}(1 + x_1 2 + x_2 2^2 + ...)^2 = 2^{v_2(a)}(1 + a_1 2 + a_2 2^2 + ...) = 2^{v_2(a)}.u \\ &\Longleftrightarrow 2^{2v_2(x)}(1 + x_1 2 + x_2 2^2 + ...)^2 = 2^{2v_2(x)}(1 + (\frac{x_1 + x_1^2}{2} + x_2)2^3 + ...) \\ &= 2^{v_p(a)}(1 + a_1 2 + a_2 2^2 + ...) \end{aligned}$$

donc

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

ce qui donne

$$\begin{cases} v_2(a) = 2v_2(x) \\ x_0 = a_0 = 1, a_1 = a_2 = 0 \end{cases}$$

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

$$\begin{cases} u = a_0 + a_1 2 + a_2 2^2 + ... \\ a_0 = 1, a_1 = a_2 = 0 \end{cases}$$

$$\Longrightarrow u = 1 + a_3 2^3 + a_4 2^4 + ... = 1 + 2^3.(a_3 + a_4 2^4 + ...)$$

ce qui donne

$$u \equiv 1 \bmod 8$$

■

Exemple 2.2.5

a) *Il existent des nombres dans $\mathbb{Q}_3$ qui n'admettent pas des racines carrées par exemple*

$$a = 5 = 2 + 1.3$$

en effet, soit

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

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.

b) *Le nombre 2-adique $y = -1$ n'a pas de racine carrée dans $\mathbb{Q}_2$ car*

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

Deuxième partie

Algorithme de calcul de code de Hensel de l'inverse d'un nombre p-adique

Introduction

La connaissance des propriétés arithmétiques et algébriques des nombres p-adiques est utile à l'étude de leurs propriétés diophantiennes et des problèmes d'approximation. Il s'agit, dans cette section, d'une une application intéressante des outils de l'analyse numérique à la théorie des nombres. On verra comment utiliser les méthodes numériques de bases (Newton, sécante, point fixe) pour calculer le zéro d'une fonction f où

$$\begin{array}{rcl} f & : & \mathbb{Z}_p(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p \\ x & \longrightarrow & f(x) \end{array}$$

Est une fonction p-adique continue et dérivable sur un domaine $D \subset \mathbb{Q}_p$, p est un nombre premier. Pour calculer l'inverse d'un nombre p-adique, on se propose d'étudie le problème suivant

$$\begin{cases} f(x) = \frac{1}{x} - a = 0 \\ \\ a \in \mathbb{Q}_p^* \ \text{, } p\text{-premier} \end{cases} \tag{2.2}$$

Notre but est de calculer les développements finis p-adiques approchés (c'est-à-dire déterminer les premiers chiffres du développement p-adique) de l'inverse de $a \in \mathbb{Q}_p^*$ à l'aide à de détermination de la solution de l'équation

$$f(x) = \frac{1}{x} - a = 0 \tag{2.3}$$

par une méthode d'approximation. La solution de (2.3) 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.

Etude du problème :

On considère la fonction d'itération $g(x)$ continue et dérivable sur un domaine $D \subset \mathbb{Q}_p$. alors l'étude du problème comprend quatre étapes :

Etape 1 : Choisir une méthode itérative :

$$x_{n+1} = g(x_n), n \in \mathbb{N}$$

Etape 2 : Trouver un point de départ x_0 suffisamment proche de zéro de (2.3) pour que $(x_n)_n$ converge.

Il n'existe pas une méthode générale permettant de choisir un point de départ x_0 faisant converger la suite $(x_n)_n$, mais si x_0 et la fonction $g(x)$ sont bien choisies, alors la suite $(x_n)_n$ doit converger vers la solution de (2.3).

Etape 3 : Déterminer un critère d'arrêt.

C'est-à-dire $(x_n)_n$ proche de la solution de l'équation (2.3) et

$$|e_n|_p = |x_n - x_{n-1}|_p \leq p^{-M}$$

avec M une précision donnée qui représente le nombre de chiffres p-adiques (la longueur de la série de solution ou la longueur de code de Hensel). Donc, il est quéstion de trouver n tel que

$$|e_n|_p = |x_n - x_{n-1}|_p \leq p^{-M}$$

Etape 4 : Déterminer la vitesse de convergence de la suite $(x_n)_n$.
La détermination de la vitesse de convergence d'une méthode itérative 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 de l'itération avec n_0 représente un rang quelconque. Exemple convergence linéaire, quadratique, cubique.....
a) Si la vitesse de convergence est par exempe d'ordre 2 alors
- dans la première itération, on obtient 2 chiffres p-adiques dans le développement p-adique de zéro de (2.3).
- dans la deuxième itération, on obtient 4 chiffres p-adiques dans le développement p-adique de zéro de (2.3), et ainsi de suite.

Le principe générale de calcul :
Est le suivant
Soit a un nombre p-adique non nul ($a \in \mathbb{Q}_p^*$) tel que

$$|a|_p = p^{-v_p(a)} = p^{-m}, m \in \mathbb{Z} \tag{2.4}$$

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

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

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

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

d'où il suffit de trouvé une suite de nombres p-adiques qui satisfait les conditions

$$\begin{cases} x_n = \sum_{k=-m}^{z_n-1} \alpha_k . p^k, \ 0 \leq \alpha_k \leq p-1, z_n \leq M \\ |x_n|_p = p^m \\ |x_{n+1} - x_n|_p \longrightarrow 0 \end{cases} \tag{2.5}$$

2.3 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 un zéro de f. On remplace pour cela l'équation $f(x) = 0$ dans $\mathbb{Q}_p^*$ par une équation du point fixe $g(x) = x$ toujours dans $\mathbb{Q}_p^*$. On considère donc la suite des itérés de la fonction g. la fonction d'itérations de Newton est définie par

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

la suite des itérés de la fonction $g(x)$ est

$$\forall n \in \mathbb{N} : x_{n+1} = g(x_n) = x_n - \frac{f(x_n)}{f'(x_n)} \tag{2.6}$$

où

$$\begin{cases} f(x) = \frac{1}{x} - a \\ \\ f'(x) = \frac{-1}{x^2} \end{cases}$$

la suite des itérés de Newton est

$$\forall n \in \mathbb{N} : x_{n+1} = x_n(2 - ax_n) \tag{2.7}$$

donc

$$\forall n, k \in \mathbb{N} : x_{n+k+1} = x_{n+k}(2 - ax_{n+k}) \tag{2.8}$$

2.3.1 La vitesse de convergence de la méthode de Newton

On rappelle que 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.

Soit $(x_n)_n$ la suite définie par (2.7). Supposons que

$$ax_{n_0} - 1 \equiv 0 \bmod p^r \iff x_{n_0} \text{ est l'inverse de } a \text{ d'ordre } r$$

tels que n_0 représente un rang quelconque et $r \in \mathbb{N}$. D'aprés la définition de la norme p-adique, on a

$$|ax_{n_0} - 1|_p \leq p^{-r}$$

d'autre part on a

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

$$\Longrightarrow \quad ax_{n+1} - 1 = ax_n(2 - ax_n) - 1$$
$$\Longrightarrow \quad ax_{n+1} - 1 = -(1 - ax_n)^2$$

donc

$$\forall n, k \in \mathbb{N} : ax_{n+k+1} - 1 = -(1 - ax_{n+k})^2 \tag{2.9}$$

par conséquent

1.
$$ax_{n_0+1} - 1 = -(1 - ax_{n_0})^2 \Longrightarrow |ax_{n_0+1} - 1|_p = |ax_{n_0} - 1|_p^2$$
$$\Longrightarrow |ax_{n_0+1} - 1|_p \leq p^{-2r}$$
$$\Longrightarrow ax_{n_0+1} - 1 \equiv \mod p^{2r}$$

2.
$$ax_{n_0+2} - 1 = -(1 - ax_{n_0+1})^2 \Longrightarrow |ax_{n_0+2} - 1|_p = |ax_{n_0+1} - 1|_p^2$$
$$\Longrightarrow |ax_{n_0+2} - 1|_p \leq p^{-4r}$$
$$\Longrightarrow ax_{n_0+2} - 1 \equiv 0 \mod p^{4r}$$

de cette façon, on obtient

$$ax_{n_0} - 1 \equiv 0 \mod p^r \Longrightarrow \begin{cases} ax_{n_0+1} - 1 \equiv 0 \mod p^{2r} \\ ax_{n_0+2} - 1 \equiv 0 \mod p^{4r} \\ ax_{n_0+3} - 1 \equiv 0 \mod p^{8r} \\ ax_{n_0+4} - 1 \equiv 0 \mod p^{16r} \\ \vdots \end{cases} \tag{2.10}$$

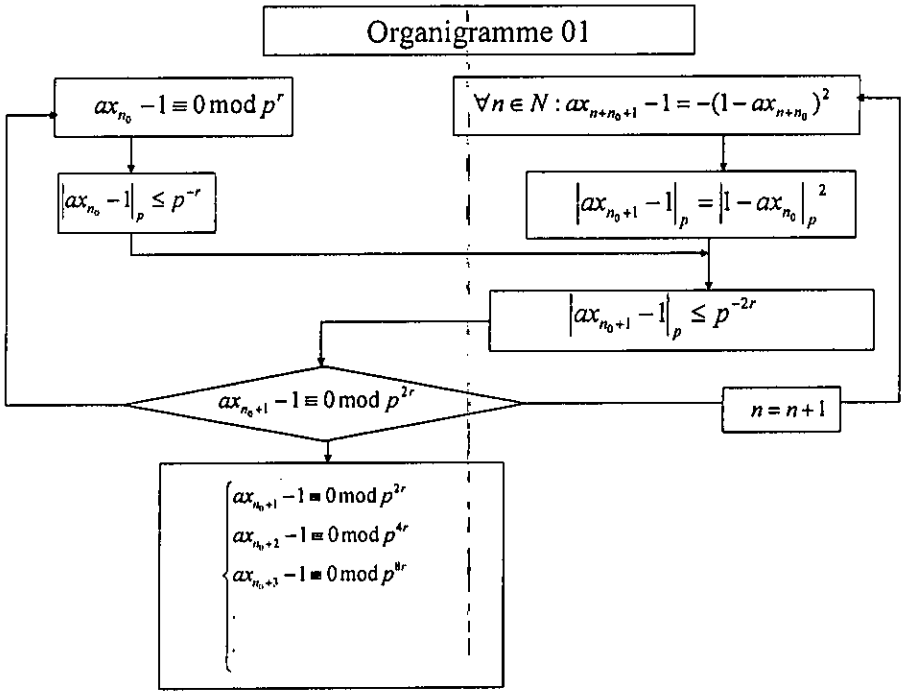
donc

$$\forall n \in \mathbb{N} : ax_{n+n_0} - 1 \equiv 0 \mod p^{\eta_n} \tag{2.11}$$

la suite $(\eta_n)_n$ est définie par

$$\forall n \in \mathbb{N} : \eta_n = 2^n r \tag{2.12}$$

on a l'organigramme suivant



d'autre part, on a

$$\begin{aligned}\forall n,k \in \mathbb{N} : x_{n+k+1} &= x_{n+k}(2-ax_{n+k}) \\ &= x_{n+k}+x_{n+k}(1-ax_{n+k})\end{aligned}$$

alors

$$\forall n,k \in \mathbb{N} : x_{n+k+1}-x_{n+k} = x_{n+k}(1-ax_{n+k}) \tag{2.13}$$

ce qui donne

1.

$$|x_{n_0+1}-x_{n_0}|_p = |x_{n_0}(1-ax_{n_0})|_p \Longrightarrow |x_{n_0+1}-x_{n_0}|_p = |x_{n_0}|_p \cdot |1-ax_{n_0}|_p$$

$$\Longrightarrow |x_{n_0+1}-x_{n_0}|_p = p^m |1-ax_{n_0}|_p$$

$$\Longrightarrow |x_{n_0+1}-x_{n_0}|_p \le p^m p^{-r}$$

$$\Longrightarrow |x_{n_0+1}-x_{n_0}|_p \le p^{-(r-m)}$$

$$\Longrightarrow x_{n_0+1} - x_{n_0} \equiv 0 \bmod p^{r-m}$$

2.

$$|x_{n_0+2} - x_{n_0+1}|_p = |x_{n_0+1}|_p \,.\, |1 - ax_{n_0+1}|_p \Longrightarrow |x_{n_0+2} - x_{n+1}|_p = p^m.\, |1 - ax_{n_0+1}|_p$$

$$\Longrightarrow |x_{n_0+2} - x_{n_0+1}|_p \leq p^m.p^{-2r}$$

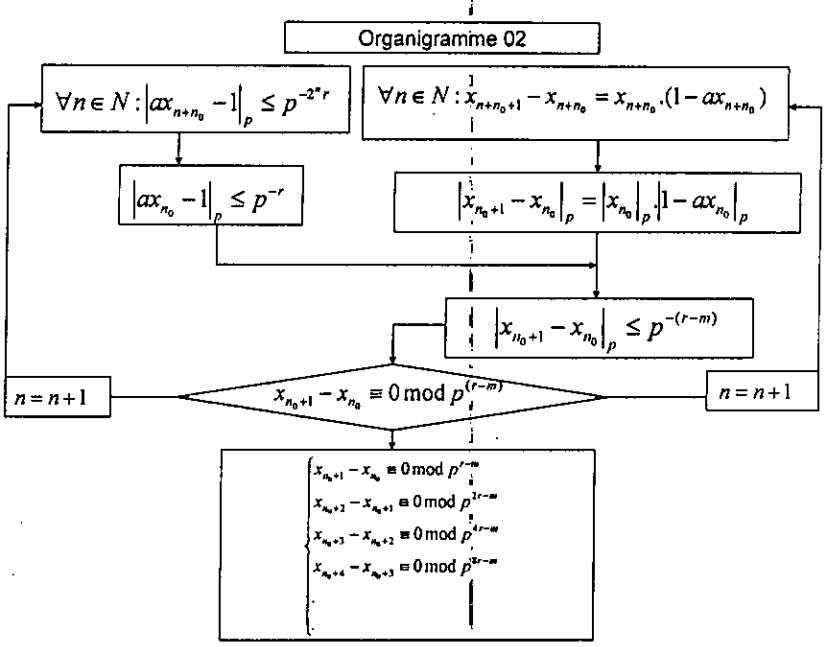
$$\Longrightarrow |x_{n_0+2} - x_{n_0+1}|_p \leq p^{-(2r-m)}$$

$$\Longrightarrow x_{n_0+2} - x_{n_0+1} \equiv 0 \bmod p^{2r-m}$$

de cette manière, on obtient

$$\begin{cases} x_{n_0+1} - x_{n_0} \equiv 0 \bmod p^{r-m} \\ x_{n_0+2} - x_{n_0+1} \equiv 0 \bmod p^{2r-m} \\ x_{n_0+3} - x_{n_0+2} \equiv 0 \bmod p^{4r-m} \\ x_{n_0+4} - x_{n_0+4} \equiv 0 \bmod p^{8r-m} \\ \cdot \\ \cdot \end{cases} \tag{2.14}$$

on a l'organigramme suivant :



Conclusion 2.3.1

1. *La suite $(e_{n+n_0})_n$ des écarts $e_{n+n_0+1} = x_{n+n_0+1} - x_{n+n_0}$ entre les itérés de la suite $(x_n)_n$ obtenus à chaque pas d'itération est donnée par*

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

Autrement dit la vitesse de convergence de la méthode de Newton est d'ordre η'_n, lequel est définie par

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

et on dit que la suite x_{n+n_0+1} est une approximation de a^{-1} avec environs $|2^n r - m|$ chiffres significatifs.

2. *Pour déterminer le nombre d'itération n pour M chiffres (donnés), on pose*

$$|\eta'_n| \geq M \Longleftrightarrow |2^n r - m| \geq M \Longrightarrow n = \left\lceil \frac{\ln \left| \frac{M+m}{r} \right|}{\ln 2} \right\rceil \tag{2.15}$$

3. *Avec les codes de Hensel, on peut écrire la formule (2.7) sous la forme*

$$H(p, 2^n r - m, x) = H(p, 2^{n-1} r - m, x).\left(2 - H(p, \infty, x^{-1}).H(p, 2^{n-1} r - m, x)\right)$$

Où $H(p, \infty, x^{-1})$ est le développement p-adique infini de $a = x^{-1}$.

4. *Les chiffres significatifs α_n et les longueurs de code de Hensel augmentent $|2^n r - m|$ fois à chaque itération, par exemple si $m = 0$ alors ils augmentent de façon quadratique.*

Exemple 2.3.2 *(Application de la méthode de Newton)*
soient

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

on a

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

et

$$2.3 \equiv 1 \bmod 5 \Longleftrightarrow a x_0 \equiv 1 \bmod p^1$$

donc on prend

$$x_0 = 2$$

la suite d'itération de Newton est

$$x_{n+1} = x_n(2 - ax_n)$$

on a

$$\begin{cases} n_0 = 0 \\ r = 1 \\ M = 8 \end{cases} \Longrightarrow n = \left[\frac{\ln\left|\frac{8+0}{1}\right|}{\ln 2}\right] = \left[\frac{3\ln 2}{\ln 2}\right] = 3$$

donc le nombre des itérations est $n = 3$. *En effet*

1)

$$x_1 = 2.(2 - 2.3) = -8 \equiv 17 = 2 + 3.5 \bmod 5^2$$

2)

$$x_2 = 17.(2 - 3.17) \equiv 417 = 2 + 3.5 + 1.5^2 + 3.5^3 \bmod 5^4$$

3)

$$\begin{aligned} x_3 &= 417.(2 - 3.417) \equiv 260417 \\ &= 2 + 3.5 + 1.5^2 + 3.5^3 + 1.5^4 + 3.5^5 + 1.5^6 + 3.5^7 \bmod 5^8 \end{aligned}$$

donc

$$\begin{cases} \frac{1}{3} \equiv 2 + 3.5 + 1.5^2 + 3.5^3 + 1.5^4 + 3.5^5 + 1.5^6 + 3.5^7 \bmod 5^8 \\ H(5, 8, \frac{1}{3}) = \cdot 23131313 = \cdot 2\overline{31} \end{cases}$$

2.4 La méthode de la sécante

Une autre méthode élémentaire pour déterminer le zéro d'une fonction est la méthode de la sécante. Cette méthode permet de pallier les cas où l'on ne peut pas calculer facilement la dérivée de f. Dans ce cas, on remplace $f'(x_n)$ dans Newton par le taux d'accroissement de f entre x_n et x_{n-1}. i.e :

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

la suite des itérés associée à $g(x)$ est donnée par

$$\forall n \in \mathbb{N}^* : x_{n+1} = x_n - \frac{f(x_n)(x_n - x_{n-1})}{f(x_n) - f(x_{n-1})} \tag{2.16}$$

et comme

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

la suite des itérations de la méthode de la sécante est

$$\forall n \in \mathbb{N}^* : x_{n+1} = x_n + x_{n-1} - a x_n . x_{n-1} \tag{2.17}$$

donc

$$\forall (n,k) \in \mathbb{N}^* \times \mathbb{N} : x_{n+k+1} = x_{n+k} + x_{n+k-1} - a x_{n+k} . x_{n+k-1} \tag{2.18}$$

2.4.1 La vitesse de convergence de la méthode de sécante

Soit $(x_n)_n$ la suite définie par la formule (2.17). Supposons que

$$\begin{cases} a x_{n_0-1} - 1 \equiv 0 \bmod p^{\alpha} \\ a x_{n_0} - 1 \equiv 0 \bmod p^{\beta} \end{cases} , \alpha \, , \beta \in \mathbb{N}$$

alors

$$\begin{cases} |a x_{n_0-1} - 1|_p \leq p^{-\alpha} \\ |a x_{n_0} - 1|_p \leq p^{-\beta} \end{cases}$$

on a

$$x_{n+1} = x_n + x_{n-1} - a x_n . x_{n-1} \Longrightarrow a x_{n+1} - 1 = (a x_n - 1).(1 - a x_{n-1})$$

on obtient

$$\forall (n,k) \in \mathbb{N}^* \times \mathbb{N} : a x_{n+k+1} - 1 = (a x_{n+k} - 1).(1 - a x_{n+k-1})$$

on a

1.

$$ax_{n_0+1}-1=(ax_{n_0}-1).(1-ax_{n_0-1}) \Longrightarrow |ax_{n_0+1}-1|_p=|(ax_{n_0}-1)|_p.|(1-ax_{n_0-1})|_p$$

$$\Longrightarrow |ax_{n_0+1}-1|_p \leq p^{-\beta}.p^{-\alpha}$$

$$\Longrightarrow |ax_{n_0+1}-1|_p \leq p^{-(\alpha+\beta)}$$

$$\Longrightarrow ax_{n_0+1}-1 \equiv 0 \bmod p^{\alpha+\beta}$$

2.

$$ax_{n_0+2}-1=(ax_{n_0+1}-1).(1-ax_{n_0}) \Longrightarrow |ax_{n+2}-1|_p=|ax_{n_0+1}-1|_p.|1-ax_{n_0}|_p$$

$$\Longrightarrow |ax_{n_0+2}-1|_p \leq p^{-(\alpha+\beta)}.p^{-\beta}$$

$$\Longrightarrow |ax_{n_0+2}-1|_p \leq p^{-(\alpha+2\beta)}$$

$$\Longrightarrow ax_{n_0+2}-1 \equiv 0 \bmod p^{\alpha+2\beta}$$

de cette manière, on obtient

$$\begin{cases} ax_{n_0-1}-1 \equiv 0 \bmod p^{\alpha} \\ ax_{n_0}-1 \equiv 0 \bmod p^{\beta} \end{cases} \Longrightarrow \begin{cases} ax_{n_0+1}-1 \equiv 0 \bmod p^{\alpha+\beta} \\ ax_{n_0+2}-1 \equiv 0 \bmod p^{\alpha+2\beta} \\ ax_{n_0+2}-1 \equiv 0 \bmod p^{2\alpha+3\beta} \\ ax_{n_0+2}-1 \equiv 0 \bmod p^{3\alpha+5\beta} \\ \vdots \\ \vdots \end{cases} \tag{2.19}$$

donc

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

où $(F_n)_n$ est une suite définie par

$$\begin{cases} \forall n \in \mathbb{N}^* : F_{n+1}=F_{n-1}+F_n \\ F_0=\alpha \\ F_1=\beta \end{cases}$$

La suite $(F_n)_n$ est une suite récurrente linéaire d'ordre 2 appelée la suite de Fibonacci généralisée et le terme général est définie par

$$F_n \simeq \lambda r_1^n + \mu r_2^n \tag{2.20}$$

avec $r_1$et r_2 sont les racines de l'équation caractéristique

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

λ et μ sont déterminés à partir des conditions initiales

$$F_0 = \alpha, F_0 = \beta$$

il est claire que

$$\begin{cases} r_1 = \frac{1+\sqrt{5}}{2} = \Phi \\ r_2 = \frac{1-\sqrt{5}}{2} = (1-\Phi) \end{cases}$$

et

$$F_n \simeq \lambda \left(\frac{1+\sqrt{5}}{2}\right)^n + \mu \left(\frac{1-\sqrt{5}}{2}\right)^n = \lambda \Phi^n + \mu (1-\Phi)^n$$

$\Phi = \frac{1+\sqrt{5}}{2}$ est appelé le nombre d'or. D'autre part, on a

$$\begin{cases} F_0 = \alpha \\ F_1 = \beta \end{cases} \Longrightarrow \begin{cases} \lambda + \mu = \alpha \\ \lambda \left(\frac{1+\sqrt{5}}{2}\right) + \mu \left(\frac{1-\sqrt{5}}{2}\right) = \beta \end{cases} \Longrightarrow \begin{cases} \lambda = \frac{1}{\sqrt{5}} \left(\beta - \frac{1-\sqrt{5}}{2}\alpha\right) \\ \mu = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\alpha - \beta\right) \end{cases}$$

donc

$$\begin{aligned} \forall n \in \quad & F_n \simeq \frac{1}{\sqrt{5}} \left(\beta - \frac{1-\sqrt{5}}{2}\alpha\right) \left(\frac{1+\sqrt{5}}{2}\right)^n + \frac{1}{\sqrt{5}} \left(-\beta + \frac{1+\sqrt{5}}{2}\alpha\right) \left(\frac{1-\sqrt{5}}{2}\right)^n \\ \simeq \quad & \frac{1}{\sqrt{5}} \left(\beta - \alpha (1-\Phi)\right) \Phi^n + \frac{1}{\sqrt{5}} \left(-\beta + \alpha\Phi\right) (1-\Phi)^n \end{aligned}$$

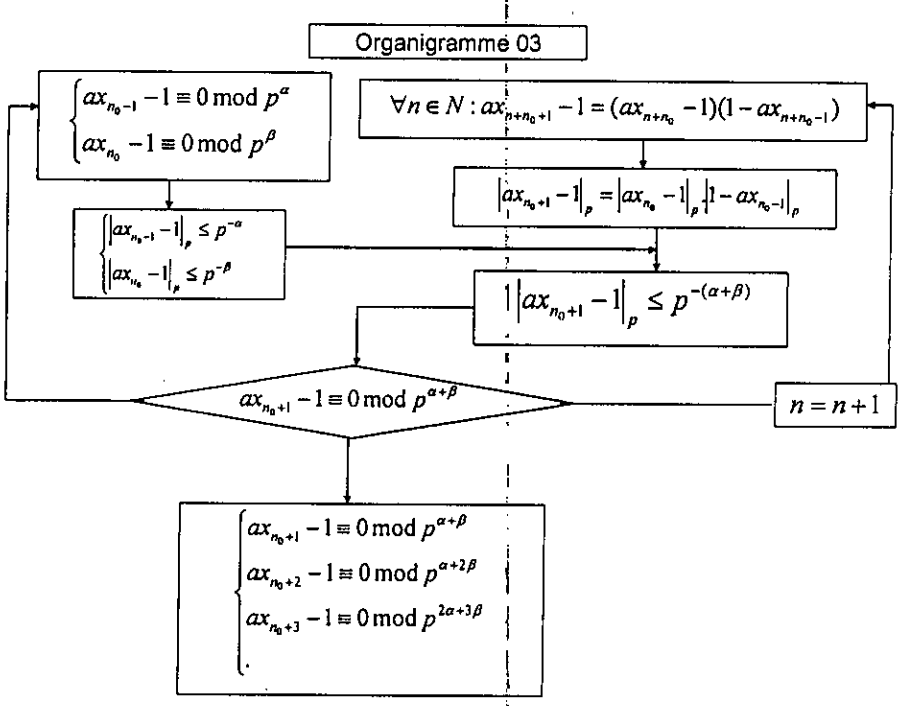
on trouve

$$\begin{aligned} \forall n \in \mathbb{N} : F_n &= \left[\frac{1}{\sqrt{5}} \left(\beta - \frac{1-\sqrt{5}}{2}\alpha\right) \left(\frac{1+\sqrt{5}}{2}\right)^n + \frac{1}{\sqrt{5}} \left(-\beta + \frac{1+\sqrt{5}}{2}\alpha\right) \left(\frac{1-\sqrt{5}}{2}\right)^n\right] \\ &= \left[\frac{1}{\sqrt{5}} \left(\left(\beta - \alpha(1-\Phi)\right) \Phi^n + \left(-\beta + \alpha\Phi\right) (1-\Phi)^n\right)\right] \end{aligned} \tag{2.21}$$

cette dèrnière expréssion est la partie entière de

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

on a l'organigramme suivant



d'autre part, on a

$$x_{n+1}=x_n+x_{n-1}-ax_n.x_{n-1}\Longleftrightarrow x_{n+1}-x_n=x_{n-1}(1-ax_n)$$

alors

$$\forall(n,k)\in\mathbb{N}^*\times\mathbb{N}: x_{n+k+1}-x_{n+k}=x_{n+k-1}(1-ax_{n+k}) \tag{2.22}$$

ce qui donne

1.

$$x_{n_0}-x_{n_0-1}=x_{n_0-2}(1-ax_{n_0-1})\Longrightarrow |x_{n_0}-x_{n_0-1}|_p=\left|x_{n_0-2}.(1-ax_{n_0-1})\right|_p$$

$$\Longrightarrow |x_{n_0}-x_{n_0-1}|_p=|x_{n_0-2}|_p.|1-ax_{n_0-1}|_p$$

$$\Longrightarrow |x_{n_0}-x_{n_0-1}|_p=p^m.|1-ax_{n_0-1}|_p$$

$$\Longrightarrow |x_{n_0}-x_{n_0-1}|_p\le p^m.p^{-\alpha}$$

$$\Longrightarrow |x_{n_0}-x_{n_0-1}|_p\le p^{-(\alpha-m)}$$

$$\Longrightarrow x_{n_0}-x_{n_0-1}\equiv 0 \bmod p^{\alpha-m}$$

2.

$$x_{n_0+1}-x_{n_0}=x_{n_0-1}(1-ax_{n_0})\Longrightarrow |x_{n+1}-x_n|_p=|x_{n_0-1}|_p.|1-ax_{n_0}|_p$$

$$\Longrightarrow |x_{n_0+1}-x_n|_p=p^m.|1-ax_{n_0}|_p$$

$$\Longrightarrow |x_{n_0+1} - x_{n_0}|_p \leq p^m.p^{-\beta}$$

$$\Longrightarrow |x_{n_0+1} - x_{n_0}|_p \leq p^{-(\beta-m)}$$

$$\Longrightarrow x_{n_0+1} - x_{n_0} \equiv 0 \bmod p^{\beta-m}$$

on trouve

$$\begin{cases} x_{n_0} - x_{n_0-1} \equiv 0 \bmod p^{\alpha-m} \\ x_{n_0+1} - x_{n_0} \equiv 0 \bmod p^{\beta-m} \\ x_{n_0+2} - x_{n_0+1} \equiv 0 \bmod p^{\alpha+\beta-m} \\ x_{n_0+3} - x_{n_0+2} \equiv 0 \bmod p^{\alpha+2\beta-m} \\ x_{n_0+4} - x_{n_0+3} \equiv 0 \bmod p^{2\alpha+3\beta-m} \\ \cdot \\ \cdot \end{cases} \tag{2.23}$$

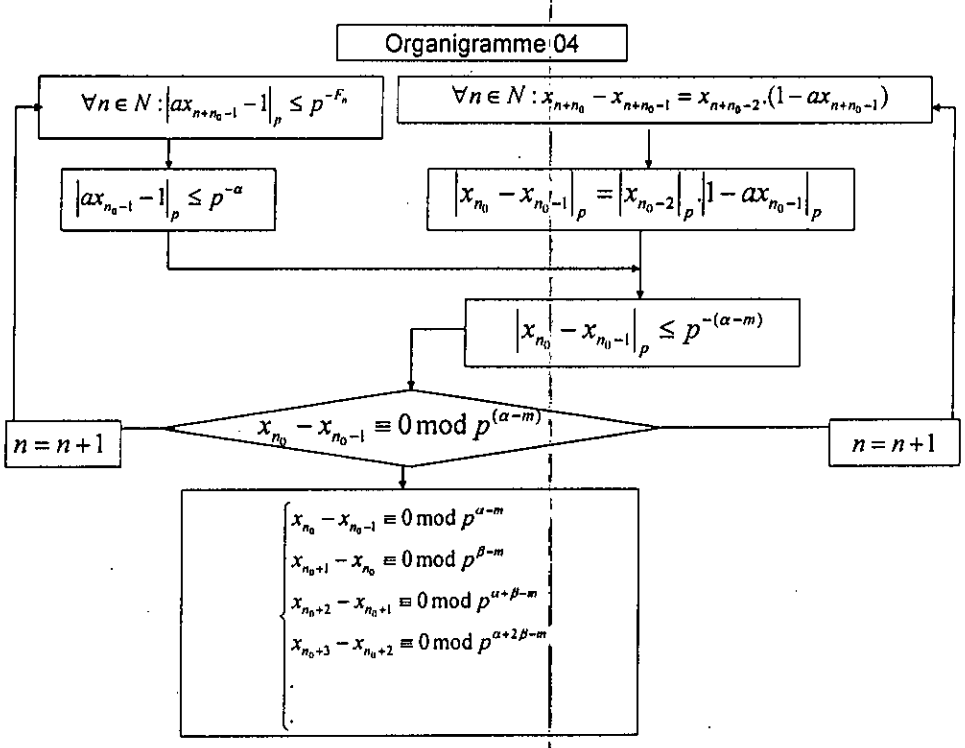
donc

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

telle que la suite $(F'_n)_n$ est définie par

$$\forall n \in \mathbb{N} : F'_n = F_n - m = \left[\frac{1}{\sqrt{5}}\left(\left(\beta - \alpha(1-\Phi)\right)\Phi^n + \left(-\beta + \alpha\Phi\right)(1-\Phi)^n\right)\right] - m \tag{2.24}$$

on a l'organigramme suivant



Conclusion 2.4.1

1. *La suite des écarts entre les itérés de la suite* $(x_n)_n$ *est donnée par*

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

signifie que la vitesse de convergence de la méthode de sécante est de l'ordre F'_n*, lequel définie par*

$$\begin{aligned} \forall n \in \mathbb{N} : F'_n &= F_n - m \\ &= \left[\frac{1}{\sqrt{5}}\left(\left(\beta - \alpha(1-\Phi)\right)\Phi^n + \left(-\beta + \alpha\Phi\right)(1-\Phi)^n\right)\right] - m \end{aligned}$$

et on dit que la suite x_{n+n_0+1} *est une approximation de* a^{-1} *avec environs* $|F_n - m|$ *chiffres significatifs.*

2. *Comme* $|1-\Phi| \prec 1$*, alors* $(1-\Phi)^n \to 0$ *, pour* n *est assez grand et*

$$\forall n \in \mathbb{N} : F'_n \simeq \frac{1}{\sqrt{5}}\left(\beta - \alpha(1-\Phi)\right)\Phi^n - m$$

et on peut déterminer le nombre des'itérations n *pour* M *chiffres donnés comme suit*

$$|F'_n| \geq M \Longleftrightarrow \left|\frac{1}{\sqrt{5}}\left(\beta - \alpha(1-\Phi)\right)\Phi^n - m\right| \geq M \Longrightarrow n = \left[\frac{\ln\left|\frac{\sqrt{5}(M+m)}{\beta-(1-\Phi)\alpha}\right|}{\ln\Phi}\right] \quad (2.25)$$

3. *Les normes p-adiques des erreurs s'écrivent sous la forme*

$$p^{-(\alpha-m)}, p^{-(\beta-m)}, p^{-(\alpha+\beta-m)}, \ldots\ldots, p^{-\left(\left[\frac{1}{\sqrt{5}}\left(\left(\beta-\alpha(1-\Phi)\right)\Phi^n+\left(-\beta+\alpha\Phi\right)(1-\Phi)^n\right)\right]-m\right)}, \ldots.$$

4. *Avec les codes de Hensel la formule (2.17) s'écrit sous la forme*

$$H(p, \left[\frac{1}{\sqrt{5}}\left(\left(\beta - \alpha(1-\Phi)\right)\Phi^{n+1} + \left(-\beta + \alpha\Phi\right)(1-\Phi)^{n+1}\right)\right] - m, x) =$$

$$\begin{aligned} = \; & H(p, \left[\frac{1}{\sqrt{5}}\left(\left(\beta - \alpha(1-\Phi)\right)\Phi^n + \left(-\beta + \alpha\Phi\right)(1-\Phi)^n\right)\right] - m, x) + \\ & + H(p, \left[\frac{1}{\sqrt{5}}\left(\left(\beta - \alpha(1-\Phi)\right)\Phi^{n-1} + \left(-\beta + \alpha\Phi\right)(1-\Phi)^{n-1}\right)\right] - m, x) + \end{aligned}$$

$$-H(p,\infty,x^{-1})H(p,\left[\frac{1}{\sqrt{5}}\left(\left(\beta-\alpha(1-\Phi)\right)\Phi^{n}+\left(-\beta+\alpha\Phi\right)(1-\Phi)^{n}\right)\right]-m,x).$$
$$H(p,\left[\frac{1}{\sqrt{5}}\left(\left(\beta-\alpha(1-\Phi)\right)\Phi^{n-1}+\left(-\beta+\alpha\Phi\right)(1-\Phi)^{n-1}\right)\right]-m,x)$$

5. *Les chiffres significatifs α_n et les longueurs de code de Hensel augmentent $|F_n'|$ fois à chaque pas d'itération.*

Exemple 2.4.2 *(Application de la méthode de sécante) :*
soient

$$p=7,a=5,M=8$$

on a

$$|5|_7=1,m=0$$

la formule d'itération de sécante est

$$x_{n+1}=x_n+x_{n-1}-5x_n.x_{n-1}$$

on prend

$$x_0=x_1=3$$

en effet

$$3.5\equiv 1 \bmod 7$$

on obtient

$$\begin{cases}\alpha=\beta=1\\ \\ n_0=0\end{cases}$$

donc le nombre des itérations est

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

en effet

$$x_0\equiv 3 \bmod 7$$
$$x_1\equiv 3 \bmod 7$$
$$x_2=3+3-5.3.3\equiv 10=3+1.7 \bmod 7^2$$
$$x_3=10+3-5.10.3\equiv 206=3+1.7+4.7^2 \bmod 7^3$$
$$x_4\equiv 6723=3+1.7+4.7^2+5.7^3+2.7^4 \bmod 7^5$$
$$x_5\equiv 4611841=3+1.7+4.7^2+5.7^3+2.7^4+1.7^5+4.7^6+5.7^7 \bmod 7^8$$

alors

$$\begin{cases} \frac{1}{5} \equiv 3 + 1.7 + 4.7^2 + 5.7^3 + 2.7^4 + 1.7^5 + 4.7^6 + 5.7^7 \bmod 7^8 \\ H(7, 8, \frac{1}{5}) = \cdot 31452145 = \cdot 3\overline{1452} \end{cases}$$

2.5 La méthode du point fixe (accélération de convergence)

Soit à résoudre l'équation $f(x) = 0$ dans $\mathbb{Q}_p^*$ où f est une fonction continue sur un domaine $D \subset \mathbb{Q}_p$. On suppose que cette équation est équivalente à une équation du type

$$g(x) = x \tag{2.26}$$

Où $g(x)$ est une fonction devant vérifier certaines hypothèses, cette dernière l'équation (2.26) est dite problème du point fixe. À partir de $x_0 \in D$, on construit la suite $(x_n)_n \subset D$ telle que

$$\forall n \in \mathbb{N} : x_{n+1} = g(x_n) \tag{2.27}$$

cette méthode est basée sur le théorème du point fixe suivant

Théorème 2.5.1 [12] [15]
Soit $D \subset \mathbb{Q}_p$ un domaine et $g : D \longrightarrow D$ une fonction contractante, c'est-à-dire

$$\exists L \in [0, 1] \text{ et } |g(x) - g(y)|_p \leq L\,|x - y|_p, \forall x, y \in D$$

on a pout tout $x_0 \in D$, la suite des itérés $(x_n)_n$ des nombres p-adiques définie par

$$x_n = g(x_{n-1})$$

converge vers la solution de l'équation

$$g(x) = x$$

Preuve.
pour $n \geq 1$, on a

$$|x_{n+1} - x_n|_p = |g(x_n) - g(x_{n-1})|_p \leq L.\,|x_n - x_{n-1}|_p$$

par récurence on trouve

$$\begin{aligned} |x_{n+1} - x_n|_p &\leq L.\,|x_n - x_{n-1}|_p \\ &\leq L^2.\,|x_{n-1} - x_{n-2}|_p \end{aligned}$$

$$\leq L^3 . |x_{n-2} - x_{n-3}|_p$$

$$\leq L^n . |x_1 - x_0|_p$$

donc

$$\lim_{n\to\infty} |x_{n+1} - x_n|_p \leq \lim_{n\to\infty} L^n . |x_1 - x_0|_p = 0 \Longrightarrow \lim_{n\to\infty} |x_{n+1} - x_n|_p = 0$$

par conséquent $(x_n)_n$ est une suite de Cauchy dans $\mathbb{Q}_p^*$ qui est complet par construction. La suite $(x_n)_n$ converge vers $x \in D$. Par passage à la limite

$$\lim_{n\to\infty} x_{n+1} = \lim_{n\longrightarrow\infty} g(x_n) \Longrightarrow x = g(x)$$

on note que $g(x)$ est une fonction continue car contractante.Montrons l'unicité du point fixe de $g(x)$.
on a, s'il existait deux différents, qu'on note t_1 et t_2 on aurait

$$\begin{cases} t_1 = g(t_1) \\ \\ t_2 = g(t_2) \end{cases} \Longrightarrow |t_1 - t_2|_p = |g(t_1) - g(t_2)|_p \leq |L|_p . |t_1 - t_2|_p \prec |t_1 - t_2|_p$$

ce qui est absurde, donc on a $t_1 = t_2$. ■

On s'intéresse à la rapidité de convergence de la suite (x_n). Le théorème précédent nous montre que plus la constante de contraction L est petite par rapport à 1, plus la convergence est rapide. Toutefois il y a une autre technique pour améliorer la rapidité de la convergence; il s'agit l'ordre de convergence.

Proposition 2.5.2 *(ordre de convergence)*
Soient D un domaine de $\mathbb{Q}_p$ et $\alpha \in D$. Si $g(x) \in C^s(D)$, $g^{(k)}(x) = 0, k = \overline{1, s-1}$, et $g^{(s)}(x) \neq 0$. Alors la vitesse de convergence de la méthode du point fixe est de l'ordre s. On en déduit que, plus s est grand plus la convergence est plus rapide.

La démonstration est similaire à celle dans le cas réel.

Exemple 2.5.3 *On trouve la solution dans $\mathbb{Q}_3$ de l'équation*

$$y = 1 + 3y$$

en appliquant la méthode du point fixe. On prend $y_0 = 1$. La suite (y_n) est définie par

$$\forall n \in \mathbb{N} : y_{n+1} = 1 + 3y_n$$

donc

$$\begin{aligned} y_1 &= 1+3y_0 = 1+3 = y_0+3 \\ y_2 &= 1+3y_1 = 1+3+3^2 = y_1+3^2 \\ y_3 &= 1+3x_2 = 1+3+3^2+3^3 = y_2+3^3 \end{aligned}$$

$$y_n = 1+3+3^2+3^3+.....+3^n = \sum_{k=0}^{n} 3^k = y_{n-1}+3^n$$

il est claire que la suite (y_n) est divergente dans $\mathbb{R}$. Par contre elle converge dans $\mathbb{Q}_3$ vers $\frac{-1}{2}$. On écrit

$$\lim_{n\longrightarrow\infty} y_n = \sum_{n=0}^{\infty} 3^n = \frac{-1}{2} \in \mathbb{Q}_3$$

d'autre part, on a

$$\begin{aligned} y_3 - y_2 &= 3^3 = 3(y_2-y_1) = 3^2(y_1-y_0) \\ &\Longrightarrow |y_3-y_2|_3 = \left|3^2\right|_3 |y_1-y_0|_3 \\ &\Longrightarrow |y_3-y_2|_3 = 3^{-2}\,|y_1-y_0|_3 \end{aligned}$$

donc

$$\begin{aligned} |y_{n+1}-y_n|_3 &= 3^{-n}\,|y_1-y_0|_3 = 3^{-n}.3^{-1} = 3^{-(n+1)} \\ &\Longrightarrow \lim_{n\longrightarrow\infty} y_{n+1}-y_n = \lim_{n\longrightarrow\infty} 3^{-(n+1)} = 0 \end{aligned}$$

Le but est d'améliorer la vitesse de convergence de la suite $(x_n)_n$. Pour elever l'ordre de convergence, on définit une suite qui converge plus vite vers la solution de l'équation proposée. Les conditions qui permettent la détermination de la fonction $g(x)$ sont que les deux premières dérivées au point $x = \frac{1}{a}$ sont nulles est la dérivées d'ordre 3 au point $\frac{1}{a}$ différente de zéro, de plus la fonction polynôme $g(x)$ ne doit pas avoir de l'inverse de a dans ses coefficients. Alors pour accélérer la convergence de la suite $(x_n)_n$, on pose

$$g(x) = x(1+\gamma(x))$$

on obtient

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

Cas 1 :

on sait que si g est une fonction telle que

$$\begin{cases} g(\frac{1}{a}) = \frac{1}{a} \\ g^{(1)}(\frac{1}{a}) = 0 \\ g^{(2)}(\frac{1}{a}) \neq 0 \end{cases} \tag{2.28}$$

donc

$$\begin{cases} \gamma(\frac{1}{a}) = 0 \\ \gamma^{(1)}(\frac{1}{a}) = -a \end{cases} \tag{2.29}$$

on cherche une fonction $\gamma(x)$ de manière à faire disparaître l'inverse de a dans les coefficients de $g(x)$. Pour cela on prend

$$\gamma(x) = \alpha_0 + \alpha_1 x$$

donc, d'aprés (2.29), on obtient

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

par conséquent

$$\gamma(x) = 1 - ax.$$

ce qui donne

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

la suite associée à la fonction $g(x)$ est définie par

$$\forall n \in \mathbb{N} : x_{n+1} = x_n(1 + (1 - ax_n)) = x_n(2 - ax_n) \tag{2.30}$$

on remarque que la suite définie par la formule (2.30) représente la suite de a méthode de Newton qui nous avons étudier précédemment.

Cas 2 :

dans ce cas, on a si

$$\begin{cases} g(\frac{1}{a}) = \frac{1}{a} \\ g^{(1)}(\frac{1}{a}) = 0 \\ g^{(2)}(\frac{1}{a}) = 0 \\ g^{(3)}(\frac{1}{a}) \neq 0 \end{cases}$$

on obtient

$$\begin{cases} \gamma(\frac{1}{a}) = 0 \\ \gamma^{(1)}(\frac{1}{a}) = -a \\ \gamma^{(2)}(\frac{1}{a}) = 2a^2 \end{cases}$$

on prend

$$\gamma(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2$$

ce qui donne

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

on trouve

$$\alpha_0 = 2, \alpha_1 = -3a, \alpha_2 = a^2$$

donc

$$\gamma(x) = 2 - 3ax + a^2x^2 = (1 - ax) + (1 - ax)^2$$

alors

$$g(x) = x\left(1 + y(x) + y(x)^2\right) = x\left(1 + (1 - ax) + (1 - ax)^2\right) \tag{2.31}$$

on remarque que la fonction $g(x)$ ne contient pas de l'inverse de a dans ses coefficientson. La suite des itérations $(x_n)_n$ associée à $g(x)$ est donnée par

$$\forall n \in \mathbb{N} : x_{n+1} = x_n\left(1 + (1 - ax_n) + (1 - ax_n)^2\right) \tag{2.32}$$

par conséquent

$$\forall n, k \in \mathbb{N} : x_{n+k+1} = x_{n+k}\left(1 + (1 - ax_{n+k}) + (1 - ax_{n+k})^2\right) \tag{2.33}$$

2.5.1 la vitesse de convergence

Soit $(x_n)_n$ la suite définie par (2.32). Supposons que

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

alors

$$|ax_{n_0} - 1|_p \leq p^{-r}$$

on a

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

on obtient

$$\forall n, k \in \mathbb{N} : ax_{n+k+1} - 1 = -(1 - ax_{n+k})^3 \tag{2.34}$$

ce qui donne

1.

$$ax_{n_0+1} - 1 = -(1 - ax_{n_0})^3 \Longrightarrow |ax_{n_0+1} - 1|_p = |1 - ax_{n_0}|_p^3$$
$$\Longrightarrow |ax_{n_0+1} - 1|_p \leq p^{-3r}$$
$$\Longrightarrow ax_{n_0+1} - 1 \equiv 0 \bmod p^{3r}$$

2.

$$ax_{n_0+2} - 1 = -(1 - ax_{n_0+1})^3 \Longrightarrow |ax_{n_0+2} - 1|_p = |1 - ax_{n_0+1}|_p^3$$
$$\Longrightarrow |ax_{n_0+2} - 1|_p \leq p^{-9r}$$
$$\Longrightarrow ax_{n_0+2} - 1 \equiv 0 \bmod p^{9r}$$

de cette façon, on obtient

$$ax_{n_0} - 1 \equiv 0 \bmod p^r \Longrightarrow \begin{cases} ax_{n_0+1} - 1 \equiv 0 \bmod p^{3r} \\ ax_{n_0+2} - 1 \equiv 0 \bmod p^{9r} \\ ax_{n_0+3} - 1 \equiv 0 \bmod p^{27r} \\ \cdot \\ \cdot \end{cases}$$

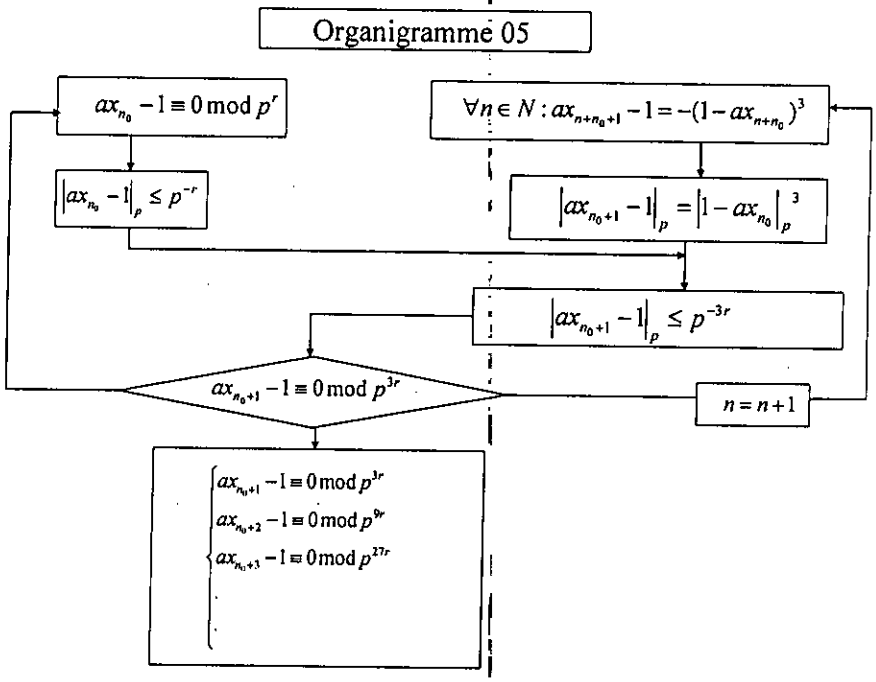
ce qui donne

$$\forall n \in \mathbb{N} : ax_{n+n_0} - 1 \equiv 0 \bmod p^{\omega_n} \tag{2.35}$$

où $(\omega_n)_n$ est définie par

$$\forall n \in \mathbb{N} : \omega_n = 3^n r \tag{2.36}$$

on a l'organigramme suivant



d'autre part, on a

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

$$\Longrightarrow x_{n+1} - x_n = x_n(1 - ax_n) + x_n(1 - ax_n)^2$$

$$\Longrightarrow x_{n+1} - x_n = x_n\left((1 - ax_n) + (1 - ax_n)^2\right)$$

on déduit

$$\forall n, k \in \mathbb{N} : x_{n+k+1} - x_{n+k} = x_{n+k}\left((1 - ax_{n+k}) + (1 - ax_{n+k})^2\right) \tag{2.37}$$

ce qui donne

1.

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

$$\Longrightarrow |x_{n_0+1} - x_{n_0}|_p \le p^m \cdot \max\left\{|1 - ax_{n_0}|_p, |1 - ax_{n_0}|_p^2\right\}$$

$$\Longrightarrow |x_{n_0+1} - x_{n_0}|_p \le p^m \cdot \max\left\{p^{-r}, p^{-2r}\right\}$$

$$\Longrightarrow |x_{n_0+1} - x_{n_0}|_p \le p^m . p^{-r}$$

$$\Longrightarrow |x_{n_0+1} - x_n|_p \le p^{-(r-m)}$$

$$\Longrightarrow x_{n_0+1} - x_{n_0} \equiv 0 \bmod p^{r-m}$$

2.

$$x_{n_0+2} - x_{n_0+1} = x_{n_0+1}.\left((1 - ax_{n_0+1}) + (1 - ax_{n_0+1})^2\right)$$

$$\Longrightarrow |x_{n_0+2} - x_{n_0+1}|_p = |x_{n_0+1}|_p . \left|(1 - ax_{n_0+1}) + (1 - ax_{n_0+1})^2\right|_p$$

$$\Longrightarrow |x_{n_0+2} - x_{n_0+1}|_p \leq p^m . \max\left\{|1 - ax_{n_0+1}|_p , |1 - ax_{n_0+1}|_p^2\right\}$$

$$\Longrightarrow |x_{n_0+2} - x_{n_0+1}|_p \leq p^m . \max\left\{p^{-3r}, p^{-6r}\right\}$$

$$\Longrightarrow |x_{n_0+2} - x_{n+1}|_p \leq p^m . p^{-3r}$$

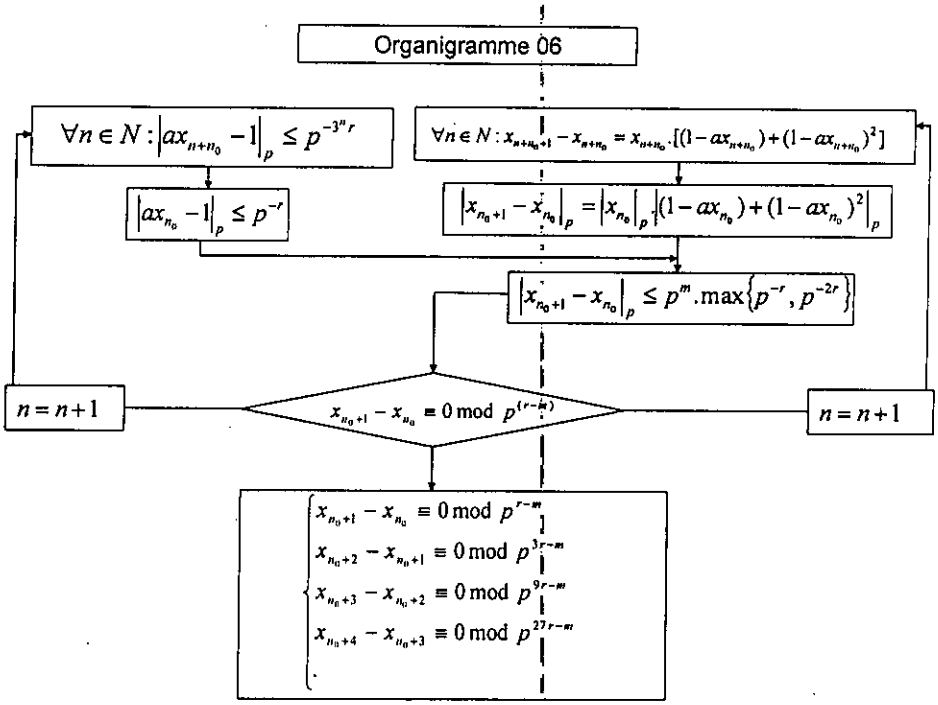
$$\Longrightarrow |x_{n_0+2} - x_{n_0+1}|_p \leq p^{-(3r-m)}$$

$$\Longrightarrow x_{n_0+2} - x_{n_0+1} \equiv 0 \bmod p^{3r-m}$$

et ainsi de suite, on obtient

$$\begin{cases} x_{n_0+1} - x_{n_0} = 0 \bmod p^{r-m} \\ x_{n_0+2} - x_{n_0+1} = 0 \bmod p^{3r-m} \\ x_{n_0+3} - x_{n_0+2} = 0 \bmod p^{9r-m} \\ x_{n_0+4} - x_{n_0+3} = 0 \bmod p^{27r-m} \\ \cdots \end{cases} \tag{2.38}$$

On a l'organigramme suivant



Conclusion 2.5.4

1. *La suite des écarts entre les itérés de $(x_n)_n$ obtenus à chaque itération est donnée par*

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

Signifie que la vitesse de convergence de la méthode du point fixe est de l'ordre ω'_n telle que

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

et on dit que la suite x_{n+n_0+1} est une approximation de a^{-1} avec environs $|3^n r - m|$ chiffres significatifs p-adiques.

2. *Le nombre nécessaire d'itérations n pour obtenir M chiffres, on pose*

$$|\omega'_n| \geq M \Longleftrightarrow |3^k r - m| \geq M \Longrightarrow n = \left\lceil \frac{\ln(|\frac{M+m}{r}|)}{\ln 3} \right\rceil \tag{2.39}$$

3. *Les normes p-adiques des erreurs s'écrivent sous la forme*

$$p^{-(r-m)}, p^{-(3r-m)}, p^{-(9r-m)}, \ldots\ldots, p^{-(3^n r-m)}, \ldots\ldots$$

4. *Avec les codes de Hensel, l'égalité (2.32) s'écrit sous la forme*

$$\begin{aligned} H(p, 3^n r - m, x) &= H(p, 3^{n-1} r - m, x)\big(1 + (1 - H(p, \infty, x^{-1}).H(p, 3^{n-1} r - m, x)) + \\ &\quad (1 - H(p, \infty, x^{-1}).H^2(p, 3^{n-1} r - m, x)\big) \end{aligned}$$

5. *Les chiffres significatifs α_n et les longueurs de code de Hensel augmentent $|3^n r - m|$ fois à chaque itération, en particulier si $m = 0$ alors ils augmentent de façon cubique à chaque itération.*

Exemple 2.5.5 *(Application de la méthode du point fixe)*
Soient

$$a = 3, M = 9, p = 5$$

on a

$$|a|_5 = |3|_5 = 1, m = 0$$

et

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

supponsons que

$$x_0 = 2$$

en effet

$$2.3 \equiv 1 \bmod 5 \Longleftrightarrow ax_0 \equiv 1 \bmod p$$

ce qui nous donne

$$\begin{cases} n_0 = 0 \\ \\ r = 1 \end{cases}$$

donc le nombre des itérations est

$$n = \left[\frac{\ln(\left|\frac{M+m}{r}\right|)}{\ln 3}\right] = \left[\frac{\ln 9}{\ln 3}\right] = 2$$

en effet

$$\begin{cases} x_0 \equiv 2 \bmod 5 \\ x_1 = 2\,(1 + (1 - 3.2).(2 - 3.2)) \equiv 42 \bmod 5^3 \\ x_2 = 42\,(1 + (1 - 3.42).(2 - 3.42)) = 651042 \bmod 5^9 \end{cases}$$

$$\Longrightarrow \begin{cases} x_1 \equiv 2 + 3.5 + 1.5^2 \bmod 5^3 \\ x_2 \equiv 2 + 3.5 + 1.5^2 + 3.5^3 + 1.5^4 + 3.5^5 + 1.5^6 + 3.5^7 + 1.5^8 \bmod 5^9 \end{cases}$$

donc

$$\begin{cases} \frac{1}{3} = 2 + 3.5 + 1.5^2 + 3.5^3 + 1.5^4 + 3.5^5 + 1.5^6 + 3.5^7 + 1.5^8 \bmod 5^9 \\ H(5, 9, \frac{1}{3}) = \cdot 231313131 = \cdot \overline{231} \end{cases}$$

Remarque 2.5.6 *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.*

2.6 Généralisation

Généralement, on peut construire une méthode itérative $x_{n+1} = g(x_n)$ suffisamment hyper accélérée qui converge vers l'inverse de a dans $\mathbb{Q}_p^*$ avec un ordre égal à s suffisamment grand.
on a, si g est une fonction telle que

$$\begin{cases} g(\frac{1}{a}) = \frac{1}{a} \\ g^{(1)}(\frac{1}{a}) = 0 \\ g^{(2)}(\frac{1}{a}) = 0 \\ g^{(3)}(\frac{1}{a}) = 0 \\ g^{(4)}(\frac{1}{a}) \neq 0 \end{cases}$$

alors

$$\begin{cases} \gamma(\frac{1}{a}) = 0 \\ \gamma^{(1)}(\frac{1}{a}) = -a \\ \gamma^{(2)}(\frac{1}{a}) = 2a^2 \\ \gamma^{(3)}(\frac{1}{a}) = -6a^3 \end{cases}$$

dans ce cas, on prend

$$\gamma(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3$$

donc

$$\begin{cases} \alpha_0 + \alpha_1 \frac{1}{a} + \alpha_2 (\frac{1}{a})^2 + \alpha_3 (\frac{1}{a})^3 = 0 \\ \alpha_1 + 2\alpha_2 \frac{1}{a} + 3\alpha_3 (\frac{1}{a})^2 + a = 0 \\ 2\alpha_2 + 6\alpha_3 \frac{1}{a} - 2a^2 = 0 \\ 6\alpha_3 + 6a^3 = 0 \end{cases}$$

on obtient

$$\alpha_0 = 3, \alpha_1 = -6a, \alpha_2 = 4a^2, \alpha_3 = -a^3$$

la fonction $\gamma(x)$ est définie par

$$\gamma(x) = 3 - 6ax + 4a^2x^2 - a^3x^3 = (1 - ax) + (1 - ax)^2 + (1 - ax)^3$$

ce qui donne

$$g(x) = x(1 + (1 - ax) + (1 - ax)^2 + (1 - ax)^3)$$

la suite associée à la fonction $g(x)$ est définie par

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

de cette manière, on obtient si

$$\begin{cases} g(\frac{1}{a}) = \frac{1}{a} \\ g^{(1)}(\frac{1}{a}) = 0 \\ g^{(2)}(\frac{1}{a}) = 0 \\ g^{(3)}(\frac{1}{a}) = 0 \\ \vdots \\ \vdots \\ g^{(s)}(\frac{1}{a}) \neq 0 \end{cases}$$

alors

$$\gamma(x) = \sum_{j=0}^{s-1} \alpha_j x^j = \sum_{j=1}^{s-1} (1 - ax)^j$$

donc

$$g(x) = x\sum_{j=0}^{s-1}(1-ax)^j \tag{2.40}$$

ce qui donne

$$g(x) = x(1+(1-ax)+(1-ax)^2+(1-ax)^3+.....+(1-ax)^{s-1}) \tag{2.41}$$

la fonction $g(x)$ n'a pas de l'inverse de a dans ses coefficients.
la suite des itérées associée à $g(x)$ est définie par

$$\forall n \in \mathbb{N} : x_{n+1} = x_n\left(1+(1-ax_n)+(1-ax_n)^2+.....+(1-ax_n)^{s-1}\right) \tag{2.42}$$

donc

$$\forall n,k \in \mathbb{N} : x_{n+k+1} = x_{n+k}\left(1+(1-ax_{n+k})+(1-ax_{n+k})^2+....+(1-ax_{n+k})^{s-1}\right) \tag{2.43}$$

2.6.1 la vitesse de convergence

Soit $(x_n)_n$ la suite définie par la formule (2.42). Supposons que

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

on a par récurrence

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

donc

$$\forall n,k \in \mathbb{N} : ax_{n+k+1}-1 = -(1-ax_{n+k})^s \tag{2.44}$$

on trouve

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

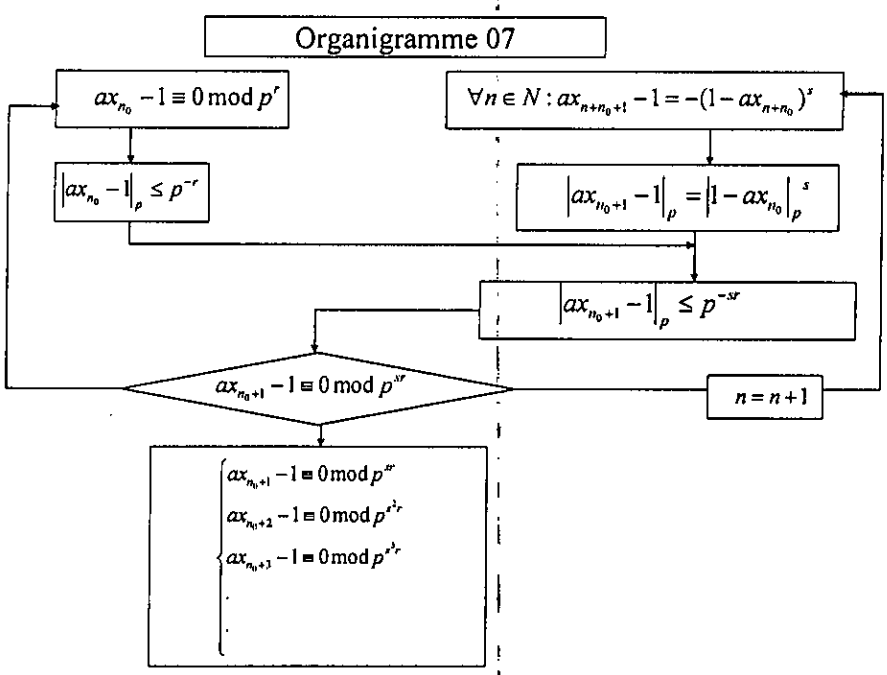
on déduit

$$\forall n \in \mathbb{N} : ax_{n+n_0}-1 \equiv 0 \bmod p^{\sigma_n} \tag{2.45}$$

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

$$\forall n \in \mathbb{N} : \sigma_n = s^n r \tag{2.46}$$

on a l'organigramme suivant



d'autre part on a

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

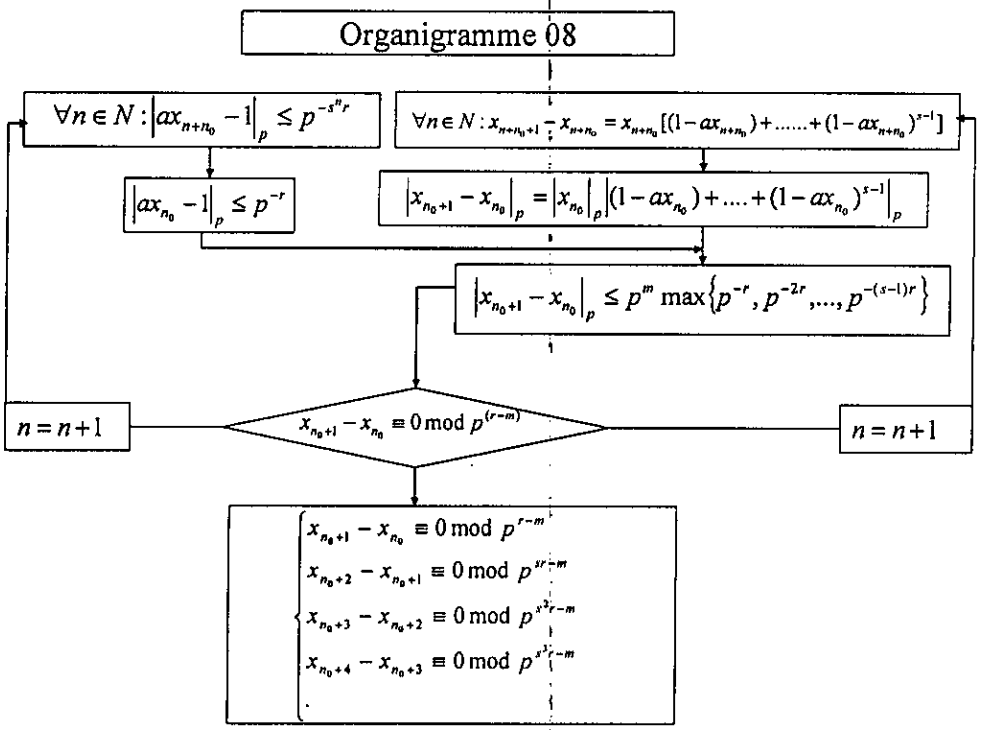
donc

$$\forall n, k \in \mathbb{N} : x_{n+k+1} - x_{n+k} = x_{n+k} \left((1 - ax_{n+k}) + (1 - ax_{n+k})^2 + \ldots\ldots + (1 - ax_{n+k})^{s-1}\right)$$

on obtient

$$\begin{cases} x_{n_0+1} - x_{n_0} \equiv 0 \bmod p^{r-m} \\ x_{n_0+2} - x_{n_0+1} \equiv 0 \bmod p^{sr-m} \\ x_{n_0+3} - x_{n_0+2} \equiv 0 \bmod p^{s^2 r-m} \\ x_{n_0+4} - x_{n_0+3} \equiv 0 \bmod p^{s^3 r-m} \\ \vdots \end{cases} \tag{2.47}$$

on a l'organigramme suivant



Conclusion 2.6.1

1. *La suite $(e_n)_n$ des écarts s'écrit sous la forme*

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

Autrement dit la vitesse de convergence de la méthode du point fixe est de l'ordre σ'_n telle que

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

et on dit que la suite x_{n+n_0+1} est une approximation de a^{-1} avec environs $|s^n r - m|$ chiffres p-adiques significatifs.

2. *Le nombre nécessaire d'itérations n pour obtenir M chiffres, on pose*

$$\begin{aligned} |\sigma'_n| \quad &\geq \quad M \Longleftrightarrow |s^n r - m| \geq M \\ &\Longrightarrow \quad n = \left[\frac{\ln(\left|\frac{M+m}{r}\right|)}{\ln s}\right] \end{aligned}$$

3. *Les normes p-adiques des erreurs s'écrivent sous la forme*

$$p^{-(r-m)}, p^{-(sr-m)}, p^{-(s^2r-m)}, \ldots\ldots, p^{-(s^n r-m)}, \ldots.$$

4. *Avec les codes de Hensel la formule (2.42) s'écrit sous la forme*

$$H(p, s^n r - m, x) = H(p, s^{n-1} r - m, x)\left(1 + (1 - H(p, \infty, x^{-1})H(p, s^{n-1} r - m, x)) + \right.$$

$$\left.(1 - H(p, \infty, x^{-1})H^2(p, s^{n-1} r - m, x)) + \ldots + (1 - H(p, \infty, x^{-1})H^{s-1}(p, s^{n-1} r - m, x))\right)$$

5. *Les chiffres significatifs α_n et les longueurs de code de Hensel augmentent $|s^n r - m|$ fois à chaque étape d'itération.*

d'après les résultats précédents, on conclut que :

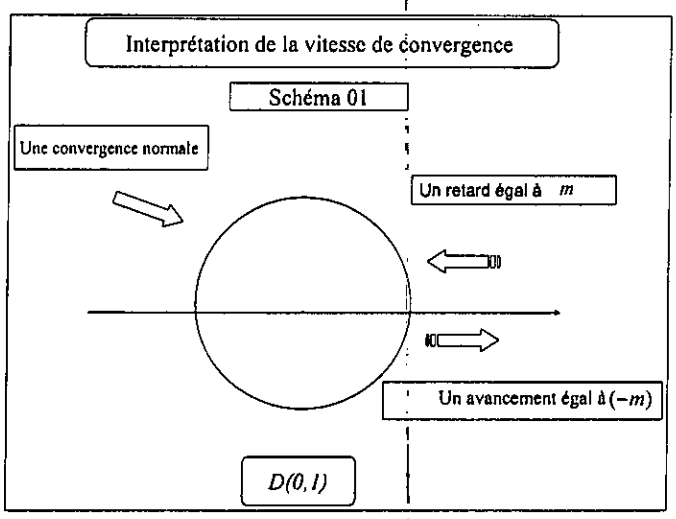
Corollaire 2.6.2

1. *Si $m = 0$, il' y a une convergence normale sur la frontière de $D(0,1)$ (par exemple convergence quadratique par rapport à la méthode de Newton).*

2. *Si $m \succ 0$, il 'y a un retard égal m à l'intérieur du $D(0,1)$.*

3. *Si $m \prec 0$ alors, il y a un avancement égal $(-m)$ par rapport à la vitesse de convergence à l'extérieure du disque de l'unité $D(0,1)$.*
4. *La relation entre le retard, l'avancement et les de codes de Hensel est comme suit :*
   (a) *Le retard représente le déplacement du point p-adique m fois à gauche.*
   (b) *L'avancement représente le déplacement du point p-adique $(-m)$ fois vers l'adroite.*

Le schéma suivant interprète ses résultats



Chapitre 3

Algorithme de calcul de code de Hensel de la racine carrée d'un nombre p-adique

Dans cette partrie, on utilise les méthodes numériques classiques pour calculer la solution approchée, dans le corps $\mathbb{Q}_p$, du problème :

$$\begin{cases} f(x) = x^2 - a = 0 \\ a \in \mathbb{Q}_p^*, \ p\text{- premier} \end{cases} \tag{3.1}$$

Et cela par une suite de nombres p-adiques $(x_n)_n \subset \mathbb{Q}_p^*$ construite par la méthode de Newton, sécante et le point fixe. On note que le but est de calculer les développements finis p-adiques approchés (c'est-à-dire déterminer les premiers chiffres du développement p-adique) de la racine carrée d'un nombre p-adique $a \in \mathbb{Q}_p^*$ à l'aide de la recherche de la solution du problème précédent par une méthode approximative.

Principe générale de calcul :

Soit a un carré dans $\mathbb{Q}_p^*$, alors la valuation p-adique de a est paire.

$$|a|_p = p^{-v_p(a)} = p^{-2m}, m \in \mathbb{Z}$$

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 on a

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

Autrement dit la suite des valeurs absolues est stationnaire, et nous savons aussi que s'il

existe un nombre p-adique α tel que

$$\alpha^2 = a$$

alors, on a

$$|\alpha|_p^2 = |a|_p = p^{-2m}$$

donc

$$|\alpha|_p = p^{-m}$$

alors la suite $(x_n)_n$ devrait tendre vers α, ainsi à partir d'un certain rang on a

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

dans ce cas, on cherche suite de nombres p-adiques qui satisfait les conditions

$$\begin{cases} |x_n|_p = p^{-m} \\ x_n = \sum_{k=m}^{l_n-1} \beta_k . p^k, 0 \leq \beta_k \leq p-1, l_n \leq M \\ |x_{n+1} - x_n|_p \longrightarrow 0 \end{cases} \tag{3.2}$$

3.1 La méthode de Newton

Soit

$$a \in \mathbb{Q}_p^* : |a|_p = p^{-2m}, m \in \mathbb{Z}$$

la fonction d'itération de Newton est

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

avec

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

donc

$$x_{n+1} = g(x_n) \Longleftrightarrow x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$$

$$\Longleftrightarrow x_{n+1} = x_n - \frac{(x_n^2 - a)}{2x_n}$$

$$\Longleftrightarrow x_{n+1} = \frac{x_n^2 + a}{2x_n}$$

la formule des itérations de Newton est

$$\forall n \in \mathbb{N} : x_{n+1} = \frac{x_n^2 + a}{2x_n} \tag{3.3}$$

donc

$$\forall n, k \in \mathbb{N} : x_{n+k+1} = \frac{x_{n+k}^2 + a}{2x_{n+k}} \tag{3.4}$$

3.1.1 La vitesse de convergence

Soit $(x_n)_n$ la suite définie par (3.3).

On a

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

alors

$$\begin{aligned} x_{n+1}^2 - a &= \frac{x_n^4 + 2ax_n^2 + a^2}{4x_n^2} - a = \frac{x_n^4 - 2ax_n^2 + a^2}{4x_n^2} \\ &= \frac{(x_n^2 - a)^2}{4x_n^2} \end{aligned}$$

on déduit

$$\forall n, k \in \mathbb{N} : x_{n+k+1}^2 - a = \frac{(x_{n+k}^2 - a)^2}{4x_{n+k}^2} \tag{3.5}$$

supposons que

$$x_{n_0}^2 - a \equiv 0 \bmod p^r \ , \ n_0 \in \mathbb{N}$$

donc

$$\left|x_{n_0}^2 - a\right|_p \leq p^{-r}$$

d'autre part on a

1.

$$x_{n_0+1}^2 - a = \frac{(x_{n_0}^2 - a)^2}{4x_{n_0}^2} \Longrightarrow \left|x_{n_0+1}^2 - a\right|_p = \frac{1}{|4|_p} \cdot \frac{\left|(x_{n_0}^2 - a)^2\right|_p}{\left|x_{n_0}^2\right|_p}$$

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

et comme

$$|4|_p = \begin{cases} \frac{1}{4}, p = 2 \\ 0, p \neq 2 \end{cases}$$

ce qui donne

$$\left|x_{n_0+1}^2-a\right|_p=\frac{1}{|4|_p}.\frac{\left|x_{n_0}^2-a\right|_p^2}{\left|x_{n_0}^2\right|_p}\Longrightarrow\begin{cases}\left|x_{n_0+1}^2-a\right|_2=2^2.2^{2m}.\left|x_{n_0}^2-a\right|_2^2 & ,\ p=2\\ \left|x_{n_0+1}^2-a\right|_p=p^{2m}.\left|x_{n_0}^2-a\right|_p^2 & ,\ p\neq 2\end{cases}$$

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

$$\Longrightarrow\begin{cases}\left|x_{n_0+1}^2-a\right|_2\leq 2^{-(2r-2m-2)} & ,\ p=2\\ \left|x_{n_0+1}^2-a\right|_p\leq p^{-(2r-2m)} & ,\ p\neq 2\end{cases}$$

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

2.

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

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

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

$$\Longrightarrow\begin{cases}\left|x_{n_0+2}^2-a\right|_2\leq 2^2.2^{2m}.2^{-(4r-4m-4)} & ,\ p=2\\ \left|x_{n_0+2}^2-a\right|_p\leq p^{2m}.p^{-(4r-4m)} & ,\ p\neq 2\end{cases}$$

$$\Longrightarrow\begin{cases}\left|x_{n_0+2}^2-a\right|_2\leq 2^{-(4r-6m-6)} & ,\ p=2\\ \left|x_{n_0+2}^2-a\right|_p\leq p^{-(4r-6m)} & ,\ p\neq 2\end{cases}$$

$$\Longrightarrow\begin{cases}x_{n_0+2}^2-a\equiv 0\bmod 2^{(4r-6m-6)} & ,\ p=2\\ x_{n_0+2}^2-a\equiv 0\bmod p^{(4r-6m)} & ,\ p\neq 2\end{cases}$$

de cette manière, on obtient

1. **Si $p \neq 2$:**

$$x_{n_0}^2 - a \equiv 0 \bmod p^r \Longrightarrow \begin{cases} x_{n_0+1}^2 - a \equiv 0 \bmod p^{2r-2m} \\ x_{n_0+2}^2 - a \equiv 0 \bmod p^{4r-6m} \\ x_{n_0+3}^2 - a \equiv 0 \bmod p^{8r-14m} \\ x_{n_0+4}^2 - a \equiv 0 \bmod p^{16r-30m} \\ \cdot \\ \cdot \end{cases} \tag{3.6}$$

on déduit

$$\forall n \in \mathbb{N} : x_{n+n_0}^2 - a \equiv 0 \bmod p^{\gamma_n} \tag{3.7}$$

où la suite $(\gamma_n)_n$ est définie par

$$\forall n \in \mathbb{N} : \gamma_n = 2^n r - C_n.m \tag{3.8}$$

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

il est claire que la suite $(C_n)_n$ est une suite récurrente linéaire d'ordre 1 s'écrit sous la forme

$$\begin{cases} C_{n+1} = aC_n + b \\ a = b = 2 \end{cases}$$

et le terme générale est donné par la formule

$$\forall n \in \mathbb{N} : C_n = a^n.C_0 + b(\frac{1-a^n}{1-a})$$

donc

$$\begin{aligned} \forall n \in \mathbb{N} : C_n &= b(\frac{1-a^n}{1-a}) \\ &= 2(\frac{1-2^n}{1-2}) = 2(2^n - 1) \end{aligned}$$

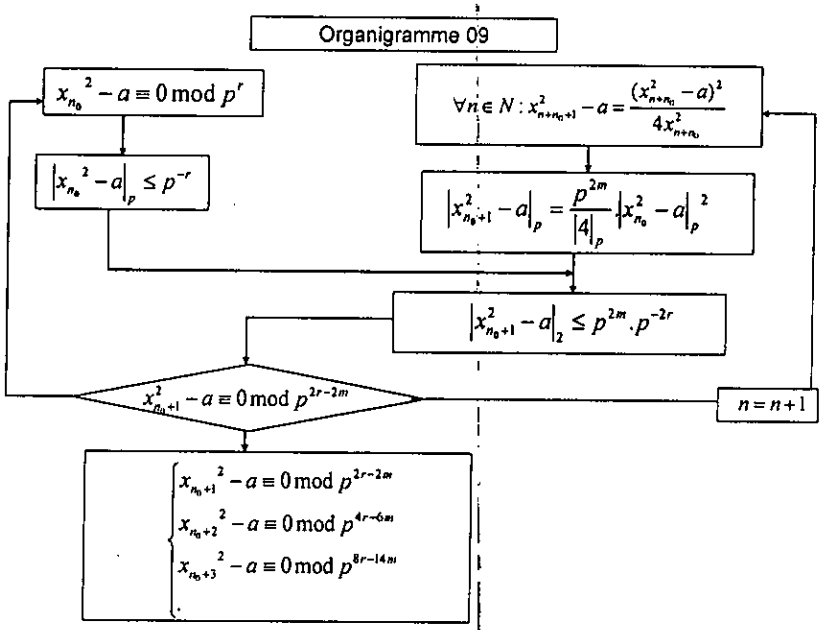
ce qui donne

$$\forall n \in \mathbb{N} : C_n = 2(2^n - 1) \tag{3.9}$$

donc

$$\forall n \in \mathbb{N} : \gamma_n = 2^n r - 2(2^n - 1)m \tag{3.10}$$

On a l'organigramme suivant



2. <u>Si $p = 2$:</u>

$$x_{n_0}^2 - a \equiv 0 \bmod 2^r \Longrightarrow \begin{cases} x_{n_0+1}^2 - a \equiv 0 \bmod 2^{2r-2(m+1)} \\ x_{n_0+2}^2 - a \equiv 0 \bmod 2^{4r-6(m+1)} \\ x_{n_0+3}^2 - a \equiv 0 \bmod 2^{8r-14(m+1)} \\ x_{n_0+4}^2 - a \equiv 0 \bmod 2^{16r-30(m+1)} \\ \cdots \end{cases} \tag{3.11}$$

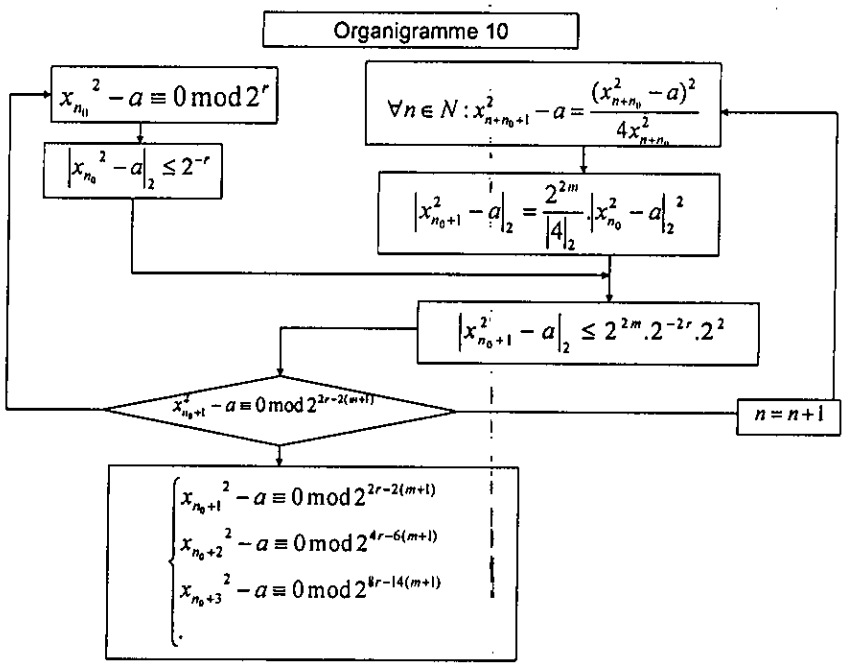
on obtient

$$\forall n \in \mathbb{N} : x_{n+n_0}^2 - a \equiv 0 \bmod 2^{\gamma'_n} \tag{3.12}$$

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

$$\begin{aligned} \forall n \in \mathbb{N} : \gamma'_n &= 2^n r - C_n(m+1) \\ &= 2^n r - 2(2^n - 1)(m+1) \\ &= \gamma_n - 2(2^n - 1) \end{aligned} \tag{3.13}$$

On a l'organigramme suivant



d'autre part, on a

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

alors

$$\begin{aligned} x_{n+1} - x_n &= \frac{x_n^2 + a}{2x_n} - x_n \\ &= \frac{a - x_n^2}{2x_n} \end{aligned}$$

donc

$$\forall n, k \in \mathbb{N} : x_{n+k+1} - x_{n+k} = \frac{a - x_{n+k}^2}{2x_{n+k}} \tag{3.14}$$

on a

$$x_{n_0+1} - x_{n_0} = \frac{a - x_{n_0}^2}{2x_{n_0}} \Longrightarrow |x_{n_0+1} - x_{n_0}|_p = \frac{1}{|2|_p}.\frac{|a - x_{n_0}^2|_p}{|x_{n_0}|_p}$$

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

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

et comme

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

alors

$$|x_{n_0+1} - x_{n_0}|_p = \frac{p^m}{|2|_p} . |a - x_{n_0}^2|_p \Longrightarrow \begin{cases} |x_{n+1} - x_n|_2 = 2.2^m |a - x_{n_0}^2|_2 & , \quad p = 2 \\ |x_{n+1} - x_n|_p = p^m . |a - x_{n_0}^2|_p & , \quad p \neq 2 \end{cases}$$

$$\Longrightarrow \begin{cases} |x_{n_0+1} - x_{n_0}|_2 \leq 2.2^m.2^{-r} & , \quad p = 2 \\ |x_{n_0+1} - x_{n_0}|_p \leq p^m.p^{-r} & , \quad p \neq 2 \end{cases}$$

$$\Longrightarrow \begin{cases} |x_{n_0+1} - x_{n_0}|_2 \leq 2^{-(r-m-1)} & , \quad p = 2 \\ |x_{n_0+1} - x_{n_0}|_p \leq p^{-(r-m)} & , \quad p \neq 2 \end{cases}$$

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

de cette manière, on obtient

1. <u>Si $p \neq 2$:</u>

$$\begin{cases} x_{n_0+1} - x_{n_0} \equiv 0 \bmod p^{r-m} \\ x_{n_0+2} - x_{n_0+1} \equiv 0 \bmod p^{2r-3m} \\ x_{n_0+3} - x_{n_0+2} \equiv 0 \bmod p^{4r-7m} \\ x_{n_0+4} - x_{n_0+3} \equiv 0 \bmod p^{8r-15m} \\ x_{n_0+5} - x_{n_0+4} \equiv 0 \bmod p^{16r-31m} \\ \cdots \end{cases} \tag{3.15}$$

alors la suite des écarts s'écrit sous la forme

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

avec

$$\forall n \in \mathbb{N} : v_n = 2^n r - T_n m \tag{3.16}$$

et

$$\begin{cases} T_0 = 1 \\ \forall n \in \mathbb{N} : T_{n+1} = 2T_n + 1 \end{cases}$$

on a aussi $(T_n)_n$ est une suite récurrente linéaire d'ordre 1, dont le terme général est donné par

$$\forall n \in \mathbb{N} : T_n = 2^n T_0 + 1.(\frac{1-2^n}{1-2}) = 2^n - (1-2^n) = 2^{n+1} - 1$$

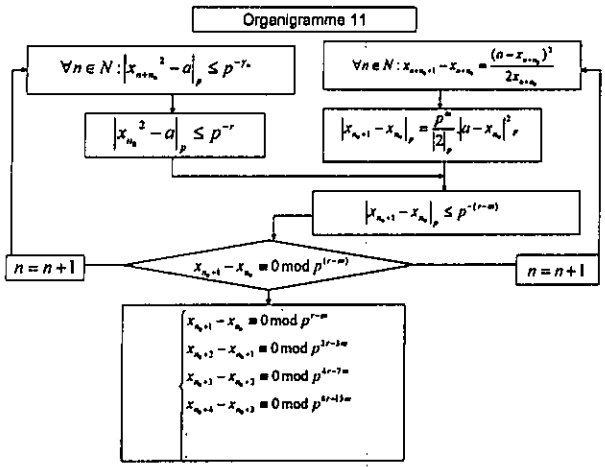
on écrit

$$\forall n \in \mathbb{N} : T_n = 2^{n+1} - 1 \tag{3.17}$$

ce qui donne

$$\forall n \in \mathbb{N} : v_n = 2^n r - (2^{n+1} - 1).m \tag{3.18}$$

on a l'organigramme suivant



2. <u>Si $p = 2$:</u>

$$\begin{cases} x_{n_0+1} - x_{n_0} \equiv 0 \bmod 2^{r-(m+1)} \\ x_{n_0+2} - x_{n_0+1} \equiv 0 \bmod 2^{2r-3(m+1)} \\ x_{n_0+3} - x_{n_0+2} = 0 \bmod 2^{4r-7(m+1)} \\ x_{n_0+4} - x_{n_0+3} \equiv 0 \bmod 2^{8r-15(m+1)} \\ x_{n_0+5} - x_{n_0+4} \equiv 0 \bmod 2^{16r-31(m+1)} \\ \cdot \\ \cdot \end{cases} \tag{3.19}$$

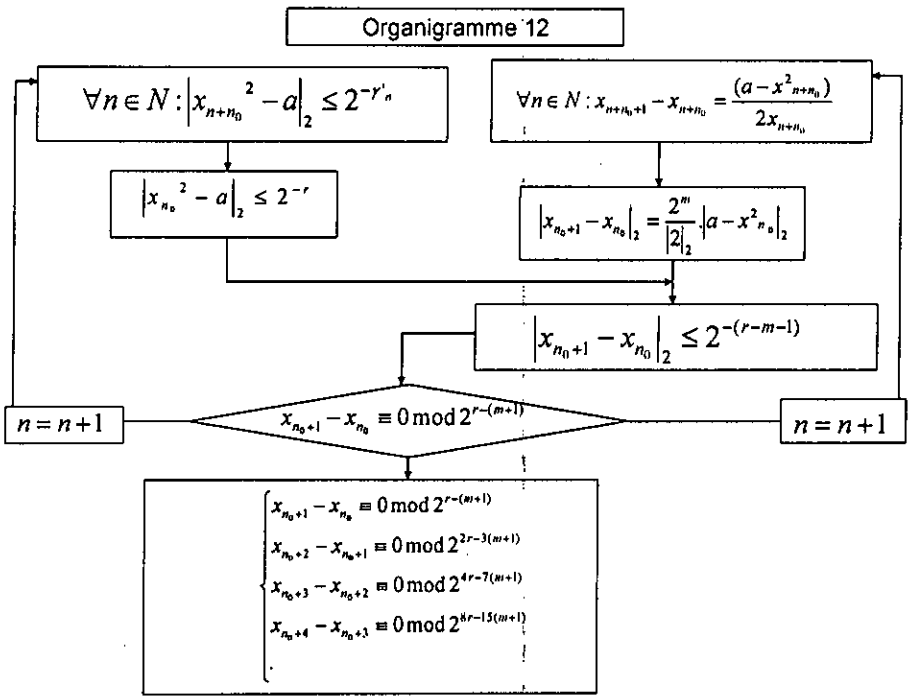
donc

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \bmod 2^{v'_n} \tag{3.20}$$

telle que

$$\begin{aligned} \forall n \in \mathbb{N} : v'_n &= 2^n r - (m+1)T_n \\ &= 2^n r - (2^{n+1}-1)(m+1) \\ &= v_n - (2^{n+1}-1) \end{aligned} \tag{3.21}$$

on a l'organigramme suivant



Conclusion 3.1.1

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

   (a) *La suite des écarts entre les itérés de la suite* $(x_n)_n$ *obtenus à chaque pas de l'itération est donnée par*

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

   autrement dit la vitesse de convergence de la méthode de Newton est de l'ordre v_n *telle que*

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

   et on dit que la suite x_{n+n_0+1} *est une approximation de* $\sqrt{a}$ *avec environs* $|2^n r - (2^{n+1}-1).m|$ *chiffres p-adiques significatifs.*

(b) *Pour détreminer le nombre des itérations pour M chiffres donnés, on pose*

$$|v_n| \quad \geq \quad M \Longleftrightarrow \left|2^n r - (2^{n+1}-1).m\right| \geq M$$

$$\Longrightarrow \quad n = \left[\frac{\ln(\left|\frac{M-m}{r-2m}\right|)}{\ln 2}\right]$$

(c) *Avec les codes de Hensel on peut écrit l'égalité de la formule (3.3) sous la forme*

$$H(p, 2^n r - (2^{n+1}-1).m, x) = \frac{H^2(p, 2^{n-1}r - (2^n-1).m, x)^2 + H^2(p, \infty, x)}{2.H(p, 2^{n-1}r - (2^n-1).m, x)}$$

(d) *Les chiffres significatifs β_n et les longueurs de code de Hensel augmentent $|2^n r - (2^{n+1}-1)|$ fois à chaque itération.*

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

(a) *La suite des écarts entre les itérés de la suite $(x_n)_n$ est*

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

autrement dit la vitesse de convergence est de l'ordre v'_n telle que

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

et on dit que la suite x_{n+n_0+1} est une approximation de $\sqrt{a}$ avec environs $|2^n r - (2^{n+1}-1)(m+1)|$ chiffres 2-adiques significatifs.

(b) *On peut déterminer le nombre nécessaire d'itérations n pour M chiffres donnés comme suit*

$$|v'_n| \quad \geq \quad M \Longleftrightarrow \left|2^n r - (2^{n+1}-1)(m+1)\right| \geq M$$

$$\Longrightarrow \quad n = \left[\frac{\ln\left(\left|\frac{M-(m+1)}{r-2(m+1)}\right|\right)}{\ln 2}\right]$$

(c) *Avec les codes de Hensel, l'équation de la formule (3.3) s'écrit sous la forme*

$$H(2, 2^n r - (2^{n+1}-1)(m+1), x) = \frac{H^2(2, 2^{n-1}r - (2^n-1)(m+1), x) + H^2(2, \infty, x)}{2.H(2, 2^{n-1}r - (2^n-1)(m+1), x)}$$

(d) *Les chiffres significatifs β_n et les longueurs de code de Hensel augmentent $|2^n r - (2^{n+1}-1)(m+1)|$ fois à chaque itération.*

d'aprés les conclusions précédentes, on peut dire que :

Corollaire 3.1.2

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

   (a) *Si $m = 0$, alors on a une convergence normale sur le bord du $D(0,1)$.*

   (b) *Si $m \succ 0$, alors on a un retard égal $(2^{n+1}-1)m$ à l'intérieur du disque de l'unité $D(0,1)$.*

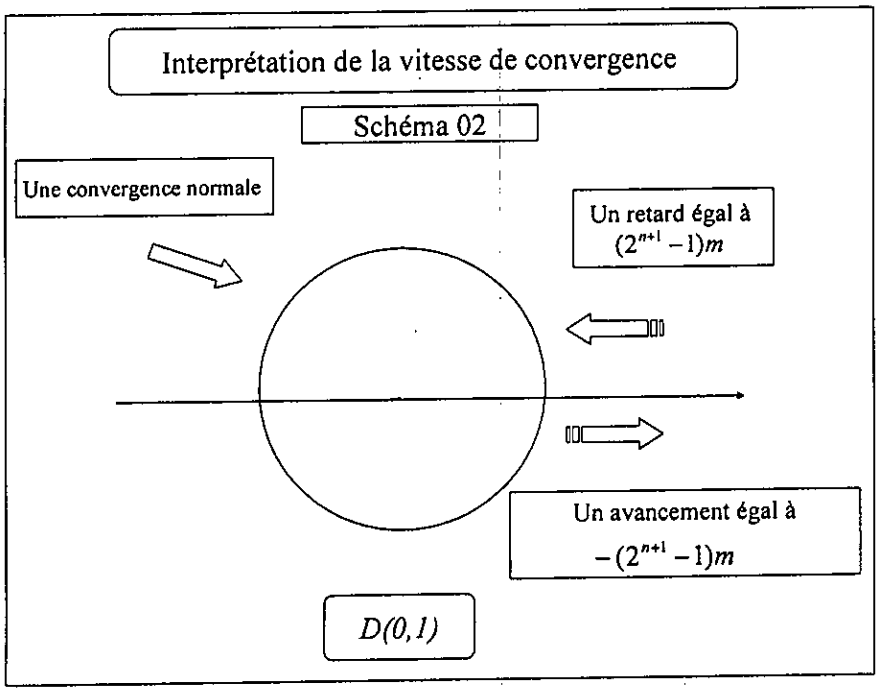
   (c) *Si $m \prec 0$, alors on a un avancement égal $(-(2^{n+1}-1)m)$, à l'extérieur du $D(0.1)$).*

   (d) *La relation entre le retard, l'avancement et les codes de Hensel est comme suit :*

      i. *Le retard représente le déplacement du point p-adique $(2^{n+1}-1)m$ fois à gauche.*

      ii. *L'avancement représente le déplacement du point p-adique $(-(2^{n+1}-1)m)$ fois vers l'adroite*

On a le schéma suivant



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

   (a) *Si* $m = -1$, *alors on a aussi une convergence normale sur la frontière du* $D(0,4)$*(ie : sur* $S(0,4)$*).*

   (b) *Si* $m \succ -1$, *alors il 'y a un retard égal* $(m+1)(2^{n+1}-1)$ *à l'intérieur du* $D(0,4)$.

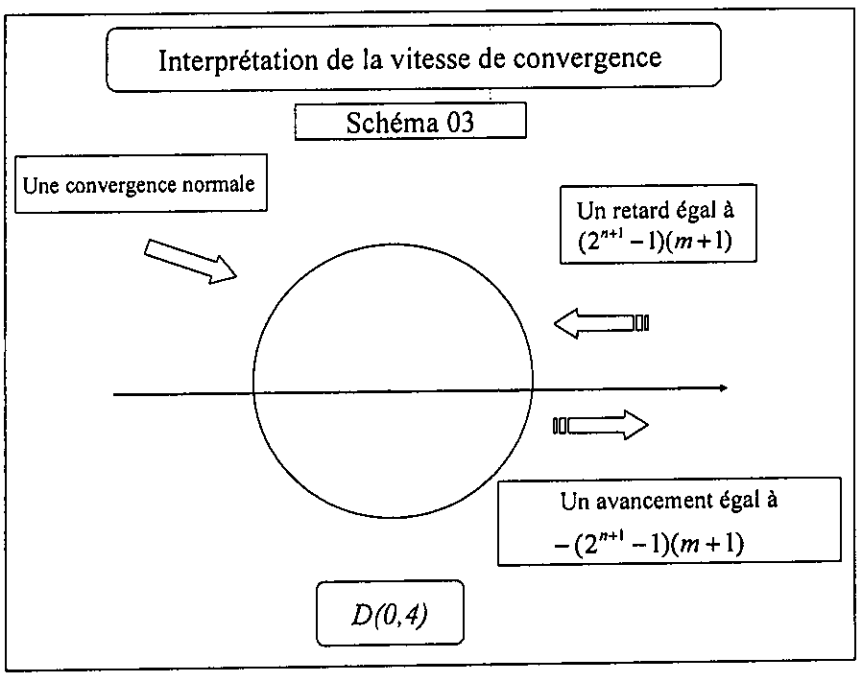
   (c) *Si* $m \prec -1$, *alors il y a un avancement égal* $-(m+1)(2^{n+1}-1)$ *à l'extérieur du disque* $D(0.2)$.

   (d) *La relation entre le retard, l'avancement et les codes de Hensel est comme suit :*

      i. *Le retard représente le déplacement du point 2-adique* $(m+1)(2^{n+1}-1)$ *fois à gauche.*

      ii. *L'avancement représente le déplacement du point 2-adique* $-(m+1)(2^{n+1}-1)$ *fois vers l'adroite.*

On a le schéma suivant



3.2 La méthode de la sécante

La suite d'itération de la méthode de sécante est

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

et comme

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

donc

$$\begin{aligned} x_{n+1} &= x_n - (x_n - x_{n-1}).\frac{x_n^2 - a}{x_n^2 - x_{n-1}^2} \\ &= x_n - \frac{x_n^2 - a}{x_n + x_{n-1}} \\ &= \frac{x_n.x_{n-1} + a}{x_n + x_{n-1}} \end{aligned}$$

On obtient la formule d'itération de la méthode de sécante

$$\forall n \in \mathbb{N}^* : x_{n+1} = \frac{x_n.x_{n-1} + a}{x_n + x_{n-1}} \tag{3.22}$$

donc

$$\forall (n,k) \in \mathbb{N}^* \times \mathbb{N} : x_{n+k+1} = \frac{x_{n+k}.x_{n+k-1} + a}{x_{n+k} + x_{n+k-1}} \tag{3.23}$$

3.2.1 la vitesse de convergence

On a

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

donc

$$x_{n+1} = \frac{x_n.x_{n-1} + a}{x_n + x_{n-1}} \Longrightarrow x_{n+1}^2 - a = \left(\frac{x_n.x_{n-1} + a}{x_n + x_{n-1}}\right)^2 - a$$

$$\Longrightarrow x_{n+1}^2 - a = \frac{(x_n^2 - a).(x_{n-1}^2 - a)}{(x_n + x_{n-1})^2}$$

on obtient

$$\forall (n,k) \in \mathbb{N}^* \times \mathbb{N} : x_{n+k+1}^2 - a = \frac{(x_{n+k}^2 - a)(x_{n+k-1}^2 - a)}{(x_{n+k} + x_{n+k-1})^2} \tag{3.24}$$

Supposons que

$$\begin{cases} x_{n_0-1}^2 \equiv a \bmod p^{\alpha} \\ x_{n_0}^2 \equiv a \bmod p^{\beta} \end{cases}$$

alors

$$\begin{cases} \left|x_{n_0-1}^2 - a\right|_p \leq p^{-\alpha} \\ \left|x_{n_0}^2 - a\right|_p \leq p^{-\beta} \end{cases}$$

on a

1.

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

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

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

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

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

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

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

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

2.

$$x_{n_0+2}^2 - a = \frac{(x_{n_0+1}^2 - a).(x_{n_0}^2 - a)}{(x_{n_0+1} + x_{n_0})^2}$$

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

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

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

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

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

$$\Longrightarrow \begin{cases} \left|x_{n_0+2}^2 - a\right|_2 \leq 2^{-(\alpha+2\beta-4m-4)} & , \quad p = 2 \\ \\ \left|x_{n_0+2}^2 - a\right|_p \leq p^{-(\alpha+2\beta-4m)} & , \quad p \neq 2 \end{cases}$$

$$\Longrightarrow \begin{cases} x_{n_0+2}^2 - a \equiv 0 \bmod 2^{(\alpha+2\beta-4m-4)} & , \quad p = 2 \\ \\ x_{n_0+2}^2 - a \equiv 0 \bmod p^{(\alpha+2\beta-4m)} & , \quad p \neq 2 \end{cases}$$

de cette manière, on obtient

1. <u>Si $p \neq 2$:</u>

$$\begin{cases} x_{n_0-1}^2 \equiv a \bmod p^{\alpha} \\ \\ x_{n_0}^2 \equiv a \bmod p^{\beta} \end{cases} \Longrightarrow \begin{cases} x_{n_0+1}^2 - a \equiv 0 \bmod p^{(\alpha+\beta)-2m} \\ x_{n_0+2}^2 - a \equiv \bmod p^{(\alpha+2\beta)-4m} \\ x_{n_0+3}^2 - a \equiv 0 \bmod p^{(2\alpha+3\beta)-8m} \\ x_{n_0+4}^2 - a \equiv 0 \bmod p^{(3\alpha+5\beta)-14m} \\ \\ \\ \end{cases} \tag{3.25}$$

on déduit

$$\forall n \in \mathbb{N} : x_{n+n_0-1}^2 - a \equiv 0 \bmod p^{\varphi_n} \tag{3.26}$$

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

$$\forall n \in \mathbb{N} : \varphi_n = J_n - mA_n \tag{3.27}$$

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

$$\begin{cases} A_0 = A_1 = 0 \\ \forall n \in \mathbb{N}^* : A_{n+1} = A_{n-1} + A_n + 2 \end{cases}$$

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

$$\forall n \in \mathbb{N} : J_n = \left[\frac{1}{\sqrt{5}} \left(\beta - \alpha(1-\Phi) \right) \Phi^n + \frac{1}{\sqrt{5}} \left(-\beta + \alpha\Phi \right) (1-\Phi)^n \right] \tag{3.28}$$

la suite $(A_n)_n$ est une suite récurrente linéaire du second ordre à coefficients canstants 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

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

donc

$$A_{n+1} + 2 = (A_{n-1} + 2) + (A_n + 2) \Longleftrightarrow \begin{cases} B_{n+1} = B_{n-1} + B_n \\ B_0 = A_0 + 2 = 2 \\ B_1 = A_1 + 2 = 2 \end{cases}$$

on a

$$\begin{cases} B_0 = 2 = 2.1 = 2q_0 \ , q_0 = 1 \\ B_1 = 2 = 2.1 = 2q_1 \ , q_1 = 1 \end{cases}$$

et

$$\begin{cases} B_2 = B_0 + B_1 = 4 = 2.(q_0 + q_1) = 2q_2 \quad , \; q_2 = q_0 + q_1 = 2 \\ \\ B_3 = B_1 + B_2 = 6 = 2.3 = 2q_3 \quad , \; q_3 = q_1 + q_2 = 3 \end{cases}$$

et ainsi de suite on obtient

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

où $(q_n)_n$ est une suite définie par

$$\begin{cases} q_0 = q_1 = 1 \\ \\ \forall n \in \mathbb{N}^* : q_{n+1} = q_{n-1} + q_n \end{cases} \tag{3.29}$$

la suite $(q_n)_n$ est une suite de Fibonacci dont le terme général est donné par

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

ce qui donne

$$\forall n \in \mathbb{N} : B_n = 2q_n = 2 \left[\frac{1}{\sqrt{5}} \left(\Phi^{n+1} - (1-\Phi)^{n+1} \right) \right] \tag{3.30}$$

donc

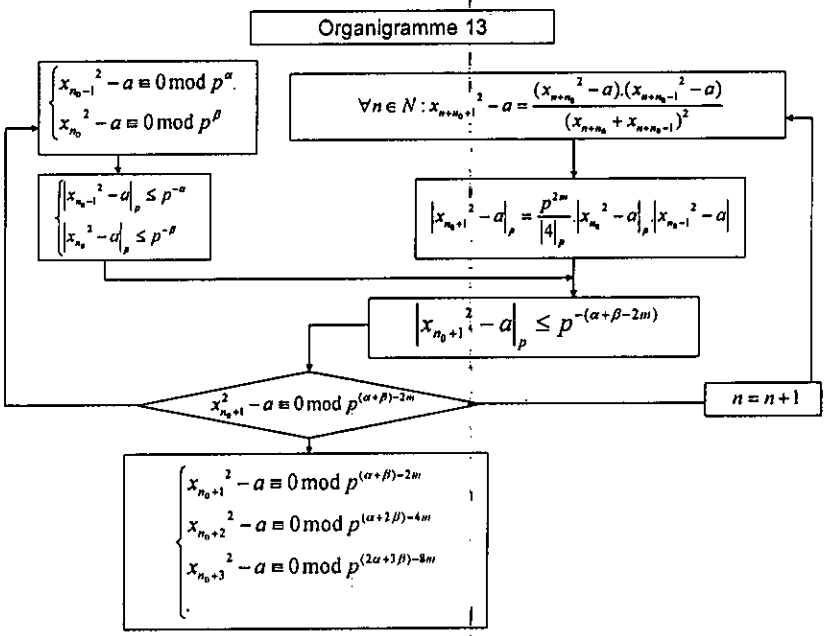
$$\begin{aligned} \forall n \; \in \; & \mathbb{N} : A_n = B_n - 2 = 2(q_n - 1) \\ = \; & 2(\left[\frac{1}{\sqrt{5}} \left(\Phi^{n+1} - (1-\Phi)^{n+1} \right) \right] - 1) \end{aligned}$$

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

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

$$-2(\left[\frac{1}{\sqrt{5}} \left(\Phi^{n+1} - (1-\Phi)^{n+1} \right) \right] - 1)m \tag{3.31}$$

on a l'organigramme suivant



2. <u>Si $p = 2$:</u>

$$\begin{cases} x_{n_0-1}^2 \equiv a \bmod 2^{\alpha} \\ x_{n_0}^2 \equiv a \bmod 2^{\beta} \end{cases} \Longrightarrow \begin{cases} x_{n_0+1}^2 - a \equiv 0 \bmod 2^{(\alpha+\beta)-2(m+1)} \\ x_{n_0+2}^2 - a \equiv \bmod 2^{(\alpha+2\beta)-4(m+1)} \\ x_{n_0+3}^2 - a \equiv 0 \bmod 2^{(2\alpha+3\beta)-8(m+1)} \\ x_{n_0+4}^2 - a \equiv 0 \bmod 2^{(3\alpha+5\beta)-14(m+1)} \\ \cdots \end{cases} \tag{3.32}$$

donc

$$\forall n \in \mathbb{N} : x_{n+n_0-1}^2 - a \equiv 0 \bmod 2^{\varphi'_n} \tag{3.33}$$

la suite $(\varphi'_n)_n$ est donnée par

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

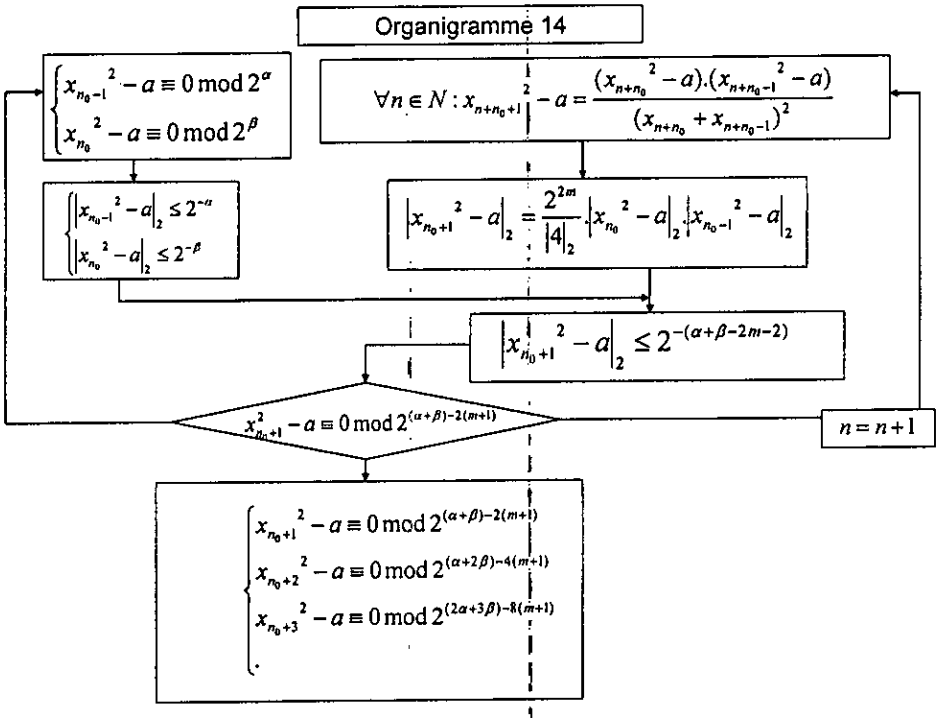
donc

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

donc

$$\forall n \in \mathbb{N} : \varphi'_n = \varphi_n - 2(\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1} - (1-\Phi)^{n+1}\right)\right] - 1) \tag{3.34}$$

On a l'organigramme suivant



d'autre part, on a

$$x_{n+1} = \frac{x_n.x_{n-1} + a}{x_n + x_{n-1}} \Longrightarrow x_{n+1} - x_n = \frac{x_n.x_{n-1} + a}{x_n + x_{n-1}} - x_n$$

$$\Longrightarrow x_{n+1} - x_n = \frac{a - x_n^2}{x_n + x_{n-1}}$$

donc

$$\forall (n,k) \in \mathbb{N}^* \times \mathbb{N} : x_{n+k+1} - x_{n+k} = \frac{a - x_{n+k}^2}{x_{n+k} + x_{n+k-1}} \tag{3.35}$$

on a

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

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

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

$$\Longrightarrow \begin{cases} |x_{n_0} - x_{n_0-1}|_2 \leq 2.2^m.2^{-\alpha} & , \quad p = 2 \\ |x_{n_0} - x_{n_0-1}|_p \leq p^m.p^{-\alpha} & , \quad p \neq 2 \end{cases}$$

$$\Longrightarrow \begin{cases} |x_{n_0} - x_{n_0-1}|_2 \leq 2^{-(\alpha-m-1)} & , \quad p = 2 \\ |x_{n_0} - x_{n_0-1}|_p \leq p^{-(\alpha-m)} & , \quad p \neq 2 \end{cases}$$

$$\Longrightarrow \begin{cases} x_{n_0} - x_{n_0-1} \equiv 0 \bmod 2^{\alpha-m-1} & , \quad p = 2 \\ x_{n_0} - x_{n_0-1} \equiv 0 \bmod p^{\alpha-m} & , \quad p \neq 2 \end{cases}$$

d'autre part, on a

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

$$\Longrightarrow |x_{n_0+1} - x_{n_0}|_p = \frac{1}{|2|_p} \cdot \frac{|a - x_{n_0}^2|_p}{p^{-m}}$$

$$\Longrightarrow \begin{cases} |x_{n_0+1} - x_{n_0}|_2 = 2.2^m.|a - x_{n_0}^2|_2 & , \quad p = 2 \\ |x_{n_0+1} - x_{n_0}|_p = p^m.|a - x_{n_0}^2|_p & , \quad p \neq 2 \end{cases}$$

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

$$\Longrightarrow \begin{cases} |x_{n_0+1} - x_{n_0}|_2 \leq 2^{-(\beta-m-1)} & , \quad p = 2 \\ |x_{n_0+1} - x_{n_0}|_p \leq p^{-(\beta-m)} & , \quad p \neq 2 \end{cases}$$

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

de cette manière, on trouve

1. Si $p \neq 2$:

$$\begin{cases} x_{n_0} - x_{n_0-1} \equiv 0 \bmod p^{\alpha-m} \\ x_{n_0+1} - x_{n_0} \equiv 0 \bmod p^{\beta-m} \\ x_{n_0+2} - x_{n_0+1} \equiv 0 \bmod p^{(\alpha+\beta)-3m} \\ x_{n_0+3} - x_{n_0+2} \equiv 0 \bmod p^{(\alpha+2\beta)-5m} \\ x_{n_0+4} - x_{n_0+3} \equiv 0 \bmod p^{(2\alpha+3\beta)-9m} \\ \cdots \end{cases} \tag{3.36}$$

alors la suite des écarts est donnée par

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

avec

$$\forall n \in \mathbb{N} : \psi_n = J_n - S_n m \tag{3.37}$$

et

$$\begin{cases} S_0 = S_1 = 1 \\ \forall n \in \mathbb{N}^* : S_{n+1} = S_{n-1} + S_n + 1 \end{cases} \tag{3.38}$$

$(S_n)_n$ est une suite récurrente linéaire du second ordre à coefficients canstants avec second membre constant s'écrit sous la forme

$$\begin{cases} a = b = c = 1 \\ \forall n \in \mathbb{N}^* : S_{n+1} = aS_{n-1} + bS_n + c \end{cases}$$

la suite $(S_n)_n$ est équivalent à

$$S_{n+1} + 1 = (S_{n-1} + 1) + (S_n + 1)$$

on pose

$$\forall n \in \mathbb{N} : B'_n = S_n + 1$$

donc

$$S_{n+1} + 1 = (S_{n-1} + 1) + (S_n + 1) \Longleftrightarrow \begin{cases} B'_{n+1} = B'_{n-1} + B'_n \\ B'_0 = S_0 + 1 = 2 \\ B'_1 = S_1 + 1 = 2 \end{cases}$$

on a

$$\begin{cases} B'_0 = 2 = 2.1 = 2q_0 & , q_0 = 1 \\ B'_1 = 2 = 2.1 = 2q_1 & , q_1 = 1 \end{cases}$$

et

$$\begin{cases} B'_2 = B'_0 + B'_1 = 4 = 2(q_0 + q_1) = 2q_2 & , q_2 = q_0 + q_1 = 2 \\ B'_3 = B'_1 + B'_2 = 6 = 2.3 = 2q_3 & , q_3 = q_1 + q_2 = 3 \end{cases}$$

et ainsi de suite on obtient

$$\forall n \in \mathbb{N} : B'_n = 2q_n$$

avec $(q_n)_n$ est une suite de Fibonacci définie par

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

ce qui donne

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

donc

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

alors

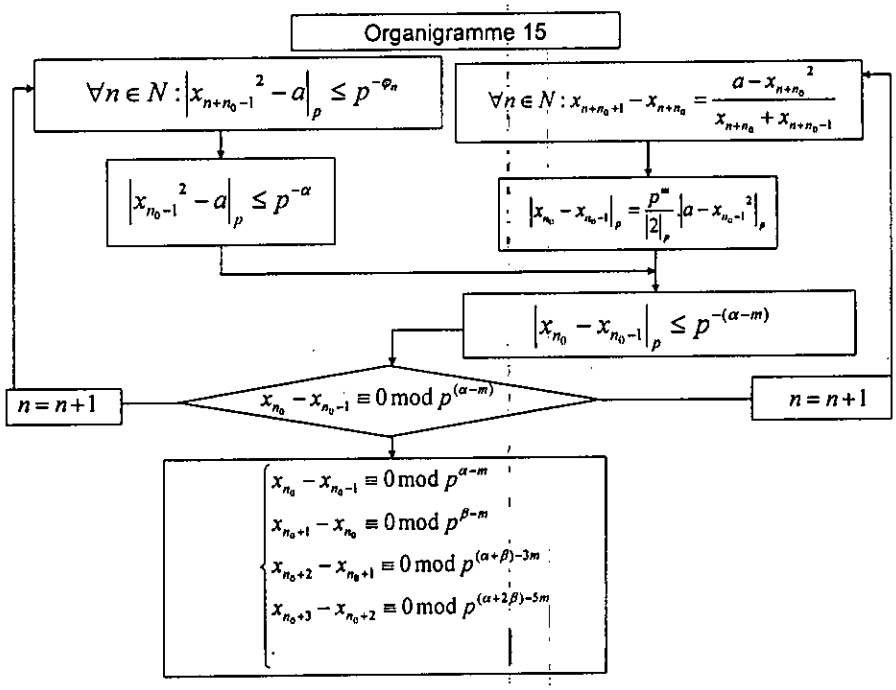
$$\forall n \in \mathbb{N} : \psi_n = J_n - (2q_n - 1)m$$

on obtient

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

$$-(2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1} - (1-\Phi)^{n+1}\right)\right] - 1)m \qquad (3.39)$$

on a l'organigramme suivant



2. Si $p = 2$:

$$\begin{cases} x_{n_0} - x_{n_0-1} \equiv 0 \bmod 2^{\alpha-(m+1)} \\ x_{n_0+1} - x_{n_0} \equiv 0 \bmod 2^{\beta-(m+1)} \\ x_{n_0+2} - x_{n_0+1} \equiv 0 \bmod 2^{(\alpha+\beta)-3(m+1)} \\ x_{n_0+3} - x_{n_0+2} \equiv 0 \bmod 2^{(\alpha+2\beta)-5(m+1)} \\ x_{n_0+4} - x_{n_0+3} \equiv 0 \bmod 2^{(2\alpha+3\beta)-9(m+1)} \\ \cdots \end{cases} \tag{3.40}$$

alors la suite des écarts est définie par

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

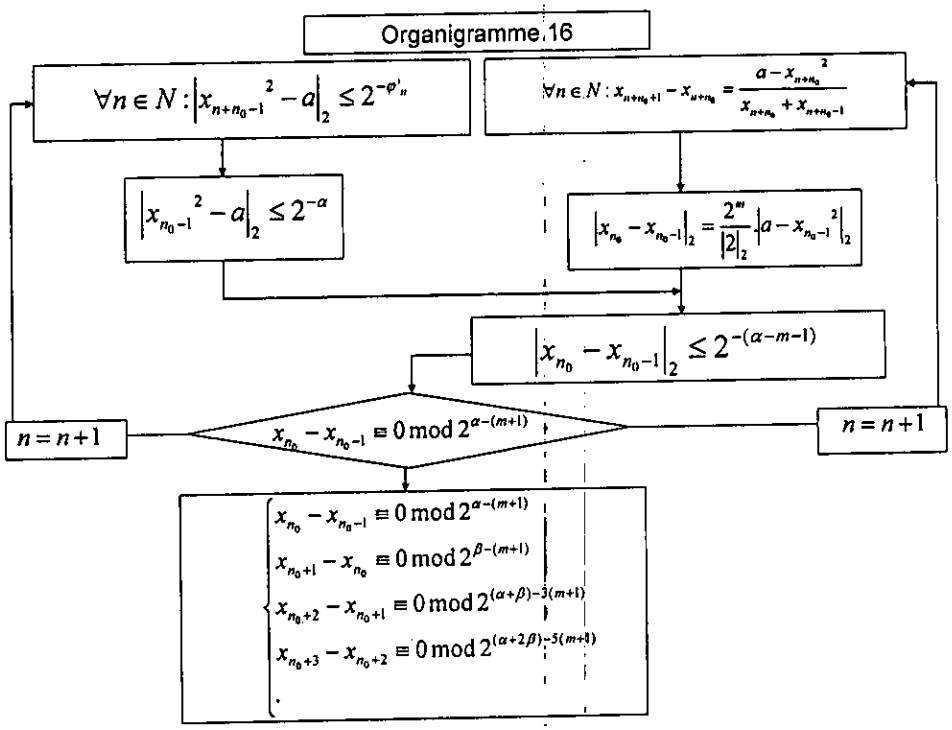
la suite$(\psi'_n)_n$ s'écrit sous la forme

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

on obtient

$$\begin{aligned}\forall n \in \mathbb{N} : \psi'_n &= \left[\frac{1}{\sqrt{5}}\left(\beta - \alpha(1-\Phi)\right)\Phi^n + \frac{1}{\sqrt{5}}\left(-\beta + \alpha\Phi\right)(1-\Phi)^n\right] \\ &-(2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1} - (1-\Phi)^{n+1}\right)\right] - 1)(m+1) \\ &= \psi_n - (2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1} - (1-\Phi)^{n+1}\right)\right] - 1)\end{aligned} \tag{3.41}$$

On a l'organigramme suivant



Conclusion 3.2.1

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

   (a) *La suite des écarts entre les itérés de la suite* $(x_n)_n$ *obtenus à chaque étapes de l'itération est donnée par*

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

   autrement dit la vitesse de convergence de la méthode de sécante est de l'ordre ψ_n *telle que*

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

$$-(2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1)m \tag{3.42}$$

et on dit que la suite x_{n+n_0+1} est une approximation de $\sqrt{a}$ avec environs $|\psi_n|$ chiffres p-adiques significatifs.

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

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

et pour déterminer le nombre nécessaire d'itérations n pour M chiffres donné on pose

$$|\psi_n| \geq M \Longleftrightarrow \left|\frac{1}{\sqrt{5}}\left(\beta-\alpha\left(1-\Phi\right)\right)\Phi^n-(\frac{2}{\sqrt{5}}\Phi^{n+1}-1)m\right| \geq M \tag{3.43}$$

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

(c) Avec les codes de Hensel l'équation de la formule (3.22) s'écrit sous la forme :

$$H(p,\psi_{n+1},x)=\frac{H(p,\psi_n,x)H(p,\psi_{n-1},x)+H^2(p,\infty,x)}{H(p,\psi_n,x)+H(p,\psi_{n-1},x)} \tag{3.44}$$

(d) Les chiffres significatifs β_n et les longueurs de code de Hensel augmentent

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

fois à chaque itération.

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

(a) La suite des écarts entre les itérés de la suite $(x_n)_n$ est définie par

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

autrement dit la vitesse de convergence de la méthode de sécante est de l'ordre ψ'_n avec

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

$$-(2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1)(m+1) \tag{3.45}$$

et on dit que la suite x_{n+n_0+1} est une approximation de $\sqrt{a}$ avec environs $|\psi'_n|$ chiffres 2-adiques significatifs.

(b) Comme $|(1-\Phi)| \prec 1$, alors

$$\forall n \in \mathbb{N} : \psi'_n \simeq \frac{1}{\sqrt{5}}\left(\beta-\alpha\left(1-\Phi\right)\right)\Phi^n-(\frac{2}{\sqrt{5}}\Phi^{n+1}-1)(m+1)$$

et pour déterminer le nombre des itérations n pour une précision donnée M, on pose

$$|\psi'_n| \geq M \Longleftrightarrow \left|\frac{1}{\sqrt{5}}\left(\beta-\alpha\left(1-\Phi\right)\right)\Phi^n-(\frac{2}{\sqrt{5}}\Phi^{n+1}-1)(m+1)\right| \geq \tag{3.46}$$

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

(c) Avec les codes de Hensel on peut écrire la formule (3.22) sous la forme

$$H(2,\psi'_{n+1},x)=\frac{H(2,\psi'_n,x)H(2,\psi'_{n-1},x)+H^2(2,\infty,x)}{H(2,\psi'_n,x)+H(2,\psi'_{n-1},x)} \tag{3.47}$$

(d) Les chiffres significatifs β_n et les longueurs de code de Hensel augmentent ψ'_n fois à chaque itération .

Corollaire 3.2.2

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

   (a) Si $m=0$, alors on a une convergence normale sur le bord du $D(0,1)$.

   (b) Si $m \succ 0$, alors on a un retard égale $(2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1)m$ à l'intérieur du disque de l'unité $D(0,1)$.

   (c) Si $m \prec 0$, alors on a un avancement égal $-(2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1)m)$ à l'extérieur du $D(0.1)$.

   (d) La relation entre le retard, l'avancement et les codes de Hensel est comme suit :

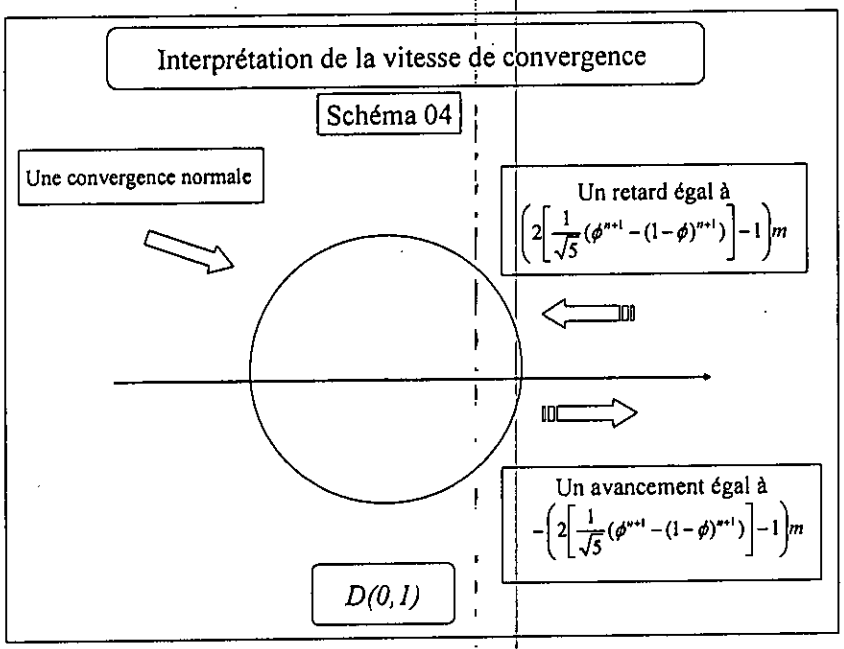
      i. Le retard représente le déplacement du point p-adique

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

      fois à gauche.

ii. L'avancement représente le déplacement du point p-adique $-(2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+}\right.\right.$ $1)m$ *fois vers l'adroite.*

On a le schéma suivant



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

   (a) *Si* $m=-1$, *alors on a aussi une convergence normale sur la frontière du* $D(0,4)$

   (b) *Si* $m \succ -1$, *alors il y a un retard égal* $(m+1)(2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1)$ *à l'intérieur du ce disque.*

   (c) *Si* $m \prec -1$, *alors il y a un avancement égal* $-(m+1)(2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-$ $1)$ *à l'extérieur du* $D(0.4)$.

   (d) *La relation entre le retard, l'avancement et les codes de Hensel est comme suit :*

      i. Le retard représente le déplacement du point 2-adique

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

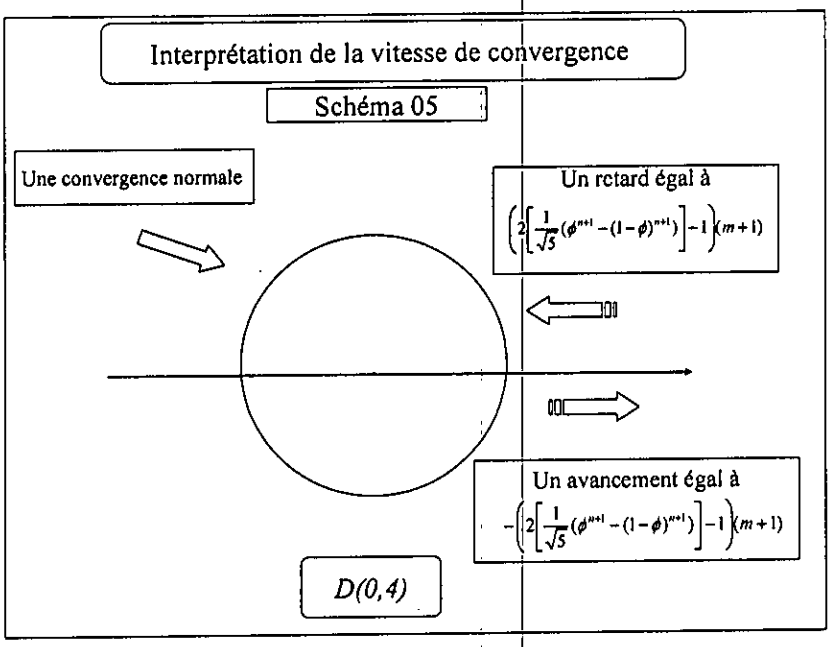
      fois à gauche.

      ii. L'avancement représente le déplacement du point 2-adique

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

fois vers l'adroite.

On a le schémas suivant



3.3 La méthode du point fixe (accélération de convergence)

Le but est d'améliorer la vitesse de convergence de la suite $(x_n)_n$. Pour augmenter l'ordre de convergence on va définir une suite qui converge plus vite vers la solution de l'équation proposée.
La technique qui nous permet d'accélérer l'ordre de convergence est comme suit :

1. Le choix de la fonction $g(x)$:

   On sait que si g est une fonction telle que

$$\begin{cases} g(\sqrt{a}) = \sqrt{a} \\ g^{(1)}(\sqrt{a}) \neq 0 \end{cases}$$

équivaut à $\sqrt{a}$ est une racine simple de $g(x) - \sqrt{a}$ autrement dit, il existe un polynôme Q_1 tel que

$$g(x) = \sqrt{a} + (x - \sqrt{a})Q_1(x)$$

g est une fonction telle que

$$\begin{cases} g(\sqrt{a}) = \sqrt{a} \\ g^{(1)}(\sqrt{a}) = 0 \\ g^{(2)}(\sqrt{a}) \neq 0 \end{cases}$$

donc $\sqrt{a}$ est la racine double de $g(x) - \sqrt{a}$ équivaut à, il existe un polynôme Q_2 tel que

$$g(x) = \sqrt{a} + (x - \sqrt{a})^2 Q_2(x)$$

g est une fonction qui vérifier

$$\begin{cases} g(\sqrt{a}) = \sqrt{a} \\ g^{(1)}(\sqrt{a}) = 0 \\ g^{(2)}(\sqrt{a}) = 0 \\ g^{(3)}(\sqrt{a}) \neq 0 \end{cases}$$

donc $\sqrt{a}$ est la racine triple de $g(x) - \sqrt{a}$ autrement dit, il existe un polynôme Q_3 tel que

$$g(x) = \sqrt{a} + (x - \sqrt{a})^3 Q_3(x)$$

de cette manière, il existe un polynôme $h(x)$ tel que

$$\begin{cases} g(x) = \sqrt{a} + (x - \sqrt{a})^s h(x) \\ g(\sqrt{a}) = \sqrt{a}, g^{(k)}(\sqrt{a}) = 0, k = \overline{1, s-1}, g^{(s)}(\sqrt{a}) \neq 0 \end{cases}$$

par conséquent le choix de la fonction $g(x)$ est comme suit

$$g(x) = \sqrt{a} + (x - \sqrt{a})^s h(x) \tag{3.48}$$

pour trouver la formule de la fonction $g(x)$, il faut déterminer l'expression de $h(x)$.

2. Le choix de la fonction $h(x)$:

les conditions qui permettent la détermination de $h(x)$ sont :
i) la fonction polynôme $g(x)$ ne doit pas avoir de $\sqrt{a}$ dans ses coefficients.
ii) $h(x)$ dépend de nombre entier rationnel s.
Pour savoir la formule exacte de $h(x)$, il suffit de travailler avec des coefficients indéterminés et d'écrire les conditions voulues. Alors pour accélérer la vitesse de convergence de la suite $(x_n)_n$, on écrit $g(x)$ sous la forme

$$g(x) = \sqrt{a} + (x - \sqrt{a})^s h(x) \tag{3.49}$$

et on distingue les cas suivants :

3.3.1 Cas 1 : $S = 1$

dans ce cas $g(x)$ s'écrit sous la forme

$$g(x) = \sqrt{a} + (x - \sqrt{a})h(x)$$

on prend la fonction $h(x)$ de manière à faire disparaître les $\sqrt{a}$ dans les coefficients de $g(x)$. Pour cela, on pose

$$h(x) = \alpha_0$$

donc

$$g(x) = \sqrt{a} + \alpha_0(x - \sqrt{a}) = \sqrt{a}(1 - \alpha_0) + \alpha_0 x$$

soient

$$c_0 = \sqrt{a}(1 - \alpha_0) \ , \ c_1 = \alpha_0$$

pour que $g(x)$ n'a pas de $\sqrt{a}$ dans ses coefficients c_0, c_1, il faut que ces derniers ne contient pas de $\sqrt{a}$, en particulier α_0 ne contient pas de $\sqrt{a}$. Il est claire qu'il n'existe pas α_0 pour rendre c_0 ne contient pas $\sqrt{a}$.
donc

$$c_0 = \sqrt{a}(1 - \alpha_0) = 0 \Longrightarrow \alpha_0 = 1$$

alors

$$c_1 = 1 \qquad \text{(ne contient de } \sqrt{a}\text{)}$$

ce qui donne

$$g(x) = x$$

la suite associée à $g(x)$ est définie par

$$\forall n \in \mathbb{N} : x_{n+1} = g(x_n) = x_n$$

dans ce cas, on a une convergence linéaire.

3.3.2 Cas 2 : $S = 2$

dans ce cas la fonction $g(x)$ s'écrit sous la forme

$$g(x) = \sqrt{a} + (x - \sqrt{a})^2 h(x)$$

on prend la fonction $h(x)$ de manière à faire disparaître les $\sqrt{a}$ aussi.
on pose

$$h(x) = \alpha_0 + \alpha_1 x$$

on obtient

$$\begin{aligned} g(x) &= \sqrt{a} + (x - \sqrt{a})^2(\alpha_0 + \alpha_1 x) \\ &= \left(a\alpha_0 + \sqrt{a}\right) + x\left(a\alpha_1 - 2\sqrt{a}\alpha_0\right) + x^2\left(\alpha_0 - 2\sqrt{a}\alpha_1\right) + \alpha_1 x^3 \\ &= c_0 + c_1 x + c_2 x^2 + c_3 x^3 \end{aligned}$$

tels que

$$\begin{cases} c_0 = a\alpha_0 + \sqrt{a} \\ c_1 = a\alpha_1 - 2\sqrt{a}\alpha_0 \\ c_2 = \alpha_0 - 2\sqrt{a}\alpha_1 \\ c_3 = \alpha_1 \end{cases}$$

pour que $g(x)$ n'a pas de $\sqrt{a}$, il faut que les coefficients $(c_k)_{0\leq k\leq 3}$ ne contient de $\sqrt{a}$, en particulier

$$\begin{cases} c_0 = a\alpha_0 + \sqrt{a} = 0 \\ \\ c_3 = \alpha_1 \text{ ne contient de } \sqrt{a} \end{cases}$$

donc

$$a\alpha_0 + \sqrt{a} = 0 \Longrightarrow \alpha_0 = \frac{-\sqrt{a}}{a}$$

si

$$c_1 = a\alpha_1 - 2\sqrt{a}\alpha_0 = 0$$

alors

$$\alpha_1 = -\frac{2}{a}$$

donc

$$c_2 = \frac{-\sqrt{a}}{a} - 2\sqrt{a}(-\frac{2}{a}) = \frac{3\sqrt{a}}{a} \quad \text{(contient de racine de } a)$$

par conséquent, il faut que

$$\begin{cases} c_2 = \alpha_0 - 2\sqrt{a}\alpha_1 = 0 \\ \text{et} \\ c_1 = a\alpha_1 - 2\sqrt{a}\alpha_0 \neq 0 \end{cases} \Longrightarrow \frac{-\sqrt{a}}{a} - 2\sqrt{a}\alpha_1 = 0$$

$$\Longrightarrow \alpha_1 = \frac{-1}{2a}$$

donc

$$c_1 = a\alpha - 2\sqrt{a}\beta = a(\frac{-1}{2a}) - 2\sqrt{a}(\frac{-\sqrt{a}}{a}) = \frac{3}{2} \text{ (ne contient pas de } \sqrt{a})$$

les coefficients de la fonction $h(x)$ sont

$$\alpha_0 = -\frac{1}{a^{\frac{1}{2}}} \quad , \quad \alpha_1 = \frac{-1}{2a}$$

et les coefficients de $g(x)$ sont

$$\begin{cases} c_0 = a(\frac{-\sqrt{a}}{a}) + \sqrt{a} = 0 \\ c_1 = a(\frac{-1}{2a}) - 2\sqrt{a}(\frac{-\sqrt{a}}{a}) = \frac{3}{2} \\ c_2 = (\frac{-\sqrt{a}}{a}) - 2\sqrt{a}(\frac{-1}{2a}) = 0 \\ c_3 = \frac{-1}{2a} \end{cases}$$

on obtient

$$\begin{aligned} h(x) &= -\frac{1}{2a}(x+2\sqrt{a}) \\ g(x) &= \frac{3}{2}x - \frac{1}{2a}x^3 \end{aligned}$$

on remarque que la fonction $g(x)$ n'a pas de $\sqrt{a}$ dans ses coefficient. D'autre part, la fonction $g(x)$ vérifiée

$$g(\sqrt{a}) = \sqrt{a}, g^{(1)}(\sqrt{a}) = 0, g^{(2)}(\sqrt{a}) \neq 0$$

la suite associée à $g(x)$ est définie par

$$\forall n \in \mathbb{N} : x_{n+1} = \frac{-1}{2a}x_n^3 + \frac{3}{2}x_n \tag{3.50}$$

Remarque 3.3.1
il est claire que la suite $(x_n)_n$ définie par la formule (3.50) représente la suite de la méthode de Newton (ce cas est traité précédement).

3.3.3 Cas 3 : $S = 3$

la fonction $g(x)$ est définie par

$$g(x) = \sqrt{a} + (x - \sqrt{a})^3 h(x)$$

tel que

$$h(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2$$

donc

$$\begin{aligned} g(x) &= \sqrt{a} + (x-\sqrt{a})^3(\alpha_0 + \alpha_1 x + \alpha_2 x^2) \\ &= \left(\sqrt{a} - a^{\frac{3}{2}}\alpha_0\right) + x\left(3a\alpha_0 - a^{\frac{3}{2}}\alpha_1\right) + x^2\left(3a\alpha_1 - 3\sqrt{a}\alpha_0 - a^{\frac{3}{2}}\alpha_2\right) + \\ &\quad x^3\left(\alpha_0 + 3a\alpha_2 - 3\sqrt{a}\alpha_1\right) + x^4\left(\alpha_1 - 3\sqrt{a}\alpha_2\right) + \alpha_2 x^5 \end{aligned}$$

on pose

$$\begin{cases} c_0 = \sqrt{a} - a^{\frac{3}{2}}\alpha_0 \\ c_1 = 3a\alpha_0 - a^{\frac{3}{2}}\alpha_1 \\ c_2 = 3a\alpha_1 - 3\sqrt{a}\alpha_0 - a^{\frac{3}{2}}\alpha_2 \\ c_3 = \alpha_0 + 3a\alpha_2 - 3\sqrt{a}\alpha_1 \\ c_4 = \alpha_1 - 3\sqrt{a}\alpha_2 \\ c_5 = \alpha_2 \end{cases}$$

pour que $g(x)$ n'a pas de $\sqrt{a}$ dans ses coefficients, il faut qu'au moins

$$\begin{cases} c_0 = \sqrt{a} - a^{\frac{3}{2}}\alpha_0 = 0 \\ \\ c_5 = \alpha_2 \text{ ne contient de } \sqrt{a} \end{cases}$$

alors

$$\begin{aligned} c_0 = \sqrt{a} - a^{\frac{3}{2}}\alpha_0 = 0 \\ \Longrightarrow \alpha_0 = \frac{1}{a} \end{aligned}$$

supposons que

$$c_1 = 3a\alpha_0 - a^{\frac{3}{2}}\alpha_1 = 0$$

donc

$$3 - a^{\frac{3}{2}}\alpha_1 = 0 \Longrightarrow \alpha_1 = \frac{3}{a\sqrt{a}}$$

on obtient

$$c_4 = \alpha_1 - 3\sqrt{a}\alpha_2 = \frac{3}{a\sqrt{a}} - 3\sqrt{a}\alpha_2 = \frac{3}{a\sqrt{a}}(1 - a^2\alpha_2)$$

et comme α_2 ne contient pas de $\sqrt{a}$, donc α_2 n'existe pas pour que c_4 ne contient pas de $\sqrt{a}$. par conséquent

$$\begin{cases} c_1 \neq 0 \\ \text{et} \\ c_4 = \alpha_1 - 3\sqrt{a}\alpha_2 = 0 \end{cases}$$
$$\Longrightarrow \alpha_1 = 3\sqrt{a}\alpha_2$$

ce qui donne

$$\begin{cases} \alpha_0 = \frac{1}{a} \\ \\ \alpha_1 = 3\sqrt{a}\alpha_2 \end{cases} \Longrightarrow \begin{cases} c_1 = 3a\alpha_0 - a^{\frac{3}{2}}\alpha_1 = 3 - a^{\frac{3}{2}}\alpha_1 \\ \\ c_3 = \alpha_0 + 3a\alpha_2 - 3\sqrt{a}\alpha_1 = \frac{1}{a} - 6a\alpha_2 \end{cases}$$

et comme α_2 ne contient pas de $\sqrt{a}$, alors c_3 ne contient pas de $\sqrt{a}$ aussi.
D'autre part, on a

$$c_2 = 3a\alpha_1 - 3\sqrt{a}\alpha_0 - a^{\frac{3}{2}}\alpha_2 \Longrightarrow c_2 = 8a\sqrt{a}\alpha_2 - \frac{3}{\sqrt{a}} = \frac{1}{\sqrt{a}}(8a^2\alpha_2 - 3)$$

il est claire qu'il n'existe pas α_2 pour que c_2 ne contient pas de $\sqrt{a}$.
par conséquent

$$c_2 = 3a\alpha_1 - 3\sqrt{a}\alpha_0 - a^{\frac{3}{2}}\alpha_2 = 0 \Longrightarrow \frac{1}{\sqrt{a}}(8a^2\alpha_2 - 3) = 0$$

$$\Longrightarrow \alpha_2 = \frac{3}{8a^2}$$

$$\Longrightarrow \quad \alpha_1 = 3\sqrt{a}\alpha_2 = \frac{9\sqrt{a}}{8a^2} = \frac{9}{8a^{\frac{3}{2}}}$$

$$\Longrightarrow \quad c_1 = 3 - a^{\frac{3}{2}}\alpha_1 = \frac{15}{8}$$

enfin, on obtient

$$\alpha_0 = \frac{1}{a}, \alpha_1 = \frac{9}{8a^{\frac{3}{2}}}, \alpha_2 = \frac{3}{8a^2}$$

et

$$\begin{cases} c_0 = \sqrt{a} - a^{\frac{3}{2}}(\frac{1}{a}) = 0 \\ c_1 = 3a(\frac{1}{a}) - a^{\frac{3}{2}}(\frac{9}{8a\sqrt{a}}) = \frac{15}{8} \\ c_2 = 3a(\frac{9}{8a\sqrt{a}}) - 3\sqrt{a}\frac{1}{a} - a^{\frac{3}{2}}\frac{3}{8a^2} = 0 \\ c_3 = \frac{1}{a} + 3a\frac{3}{8a^2} - 3\sqrt{a}\frac{9}{8a\sqrt{a}} = -\frac{5}{4a} \\ c_4 = \frac{9}{8a\sqrt{a}} - 3\sqrt{a}\frac{3}{8a^2} = 0 \\ c_5 = \frac{3}{8a^2} \end{cases}$$

on trouve

$$h(x) = \frac{1}{a} + \frac{9}{8a\sqrt{a}}x + \frac{3}{8a^2}x^2$$

et

$$g(x) = \frac{15}{8}x - \frac{5}{4a}x^3 + \frac{3}{8a^2}x^5$$

la fonction polynôme $g(x)$ n'a pas de $\sqrt{a}$ dans ses coefficients et elle a deux dérivées successives nulles.

$$g(\sqrt{a}) = \sqrt{a}, g^{(1)}(\sqrt{a}) = 0, g^{(2)}(\sqrt{a}) = 0, g^{(3)}(\sqrt{a}) \neq 0$$

la suite associée à $g(x)$ est définie par

$$\forall n \in \mathbb{N} : x_{n+1} = \frac{3}{8a^2}x_n^5 - \frac{5}{4a}x_n^3 + \frac{15}{8}x_n \tag{3.51}$$

la vitesse de convergence

pour trouver la vitesse de convergence de la suite $(x_n)_n$, il suffit étudier le comportement de la suite $(x_{n+n_0+1} - x_{n+n_0})_n$.
On a

$$\forall n \in \mathbb{N} : x_{n+1} = \frac{3}{8a^2}x_n^5 - \frac{10}{8a}x_n^3 + \frac{15}{8}x_n$$

donc

$$x_{n+1}^2 - a = \left(\frac{3}{8a^2}x_n^5 - \frac{10}{8a}x_n^3 + \frac{15}{8}x_n\right)^2 - a$$

$$\Longrightarrow x_{n+1}^2 - a = \left(a - x_n^2\right)^3 \left(-\frac{1}{a^2} + \frac{33}{64a^3}x_n^2 - \frac{9}{64a^4}x_n^4\right)$$

on trouve

$$\forall n \in \mathbb{N} : x_{n+1}^2 - a = \left(a - x_n^2\right)^3 . F_1(x_n)$$

telle que

$$F_1(x_n) = -\frac{1}{a^2} + \frac{33}{64a^3}x_n^2 - \frac{9}{64a^4}x_n^4 \tag{3.52}$$

supposon que

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

donc

$$\left|x_{n_0}^2 - a\right|_p \leq p^{-r}$$

ce qui donne

$$\left|x_{n+1}^2 - a\right|_p = \left|a - x_n^2\right|_p^3 . \left|F_1(x_n)\right|_p \leq p^{-3r} . \left|F_1(x_n)\right|_p$$

d'autre part, on a

$$\left|F_1(x_{n_0})\right|_p = \left|-\frac{1}{a^2} + \frac{33}{64a^3}x_{n_0}^2 - \frac{9}{64a^4}x_{n_0}^4\right|_p \leq \max\left\{\left|-\frac{1}{a^2}\right|_p, \left|\frac{33}{64a^3}\right| . \left|x_{n_0}^2\right|_p, \left|-\frac{9}{64a^4}\right|_p . \left|x_{n_0}^4\right|_p\right\}$$

$$\Longrightarrow \begin{cases} \left|F_1(x_{n_0})\right|_p \leq \max\left\{p^{4m}, p^{6m}.p^{-2m}, p^{8m}.p^{-4m}\right\} & , \text{si } p \neq 2 \\ \left|F_1(x_{n_0})\right|_2 \leq \max\left\{2^{4m}, 2^6.2^{6m}.2^{-2m}, 2^6.2^{8m}.2^{-4m}\right\} & , \text{si } p = 2 \end{cases}$$

$$\Longrightarrow \begin{cases} |F_1(x_{n_0})|_p \leq \max\{p^{4m}, p^{4m}, p^{4m}\} & , \text{si } p \neq 2 \\ |F_1(x_{n_0})|_2 \leq \max\{2^{4m}, 2^{4m+6}, 2^{4m+6}\} & , \text{si } p = 2 \end{cases}$$

$$\Longrightarrow \begin{cases} |F_1(x_{n_0})|_p \leq p^{4m} & , \text{si } p \neq 2 \\ |F_1(x_{n_0})|_2 \leq 2^{4m+6} & , \text{si } p = 2 \end{cases}$$

on déduit que

$$\forall n \in \mathbb{N} : \begin{cases} |F_1(x_{n+n_0})|_p \leq p^{4m} & , \text{si } p \neq 2 \\ |F_1(x_{n+n_0})|_2 \leq 2^{4m+6} & , \text{si } p = 2 \end{cases}$$

alors

1.

$$|x_{n_0+1}^2 - a|_p = |a - x_{n_0}^2|_p^3 . |F_1(x_{n_0})|_p \leq p^{-3r} . |F_1(x_{n_0})|_p$$

$$\Longrightarrow \begin{cases} |x_{n_0+1}^2 - a|_p \leq p^{-3r} . p^{4m} & , \text{si } p \neq 2 \\ |x_{n_0+1}^2 - a|_2 \leq 2^{-3r} . 2^{4m+6} & , \text{si } p = 2 \end{cases}$$

$$\Longrightarrow \begin{cases} |x_{n_0+1}^2 - a|_p \leq p^{-(3r-4m)} & , \text{si } p \neq 2 \\ |x_{n_0+1}^2 - a|_2 \leq 2^{-(3r-4m-6)} & , \text{si } p = 2 \end{cases}$$

on obtient

$$\begin{cases} x_{n_0+1}^2 - a \equiv 0 \bmod p^{(3r-4m)} & , \text{si } p = 2 \\ x_{n_0+1}^2 - a \equiv 0 \bmod 2^{(3r-4m-6)} & , \text{si } p = 2 \end{cases}$$

2.

$$|x_{n_0+2}^2 - a|_p = |a - x_{n_0+1}^2|_p^3 . |F_1(x_{n_0+1})|_p$$

$$\Longrightarrow \begin{cases} |x_{n_0+2}^2 - a|_p \leq p^{-9r+12m} . p^{4m} \\ |x_{n_0+2}^2 - a|_2 \leq 2^{-9r+12m+18} . 2^{4m+6} \end{cases}$$

$$\Longrightarrow \begin{cases} |x_{n_0+2}^2 - a|_p \leq p^{-(9r-16m)} \\ |x_{n_0+2}^2 - a|_2 \leq 2^{-(9r-16m-24)} \end{cases}$$

alors

$$\begin{cases} x_{n_0+2}^2 - a \equiv 0 \bmod p^{(9r-16m)} \\ x_{n_0+2}^2 - a \equiv 0 \bmod 2^{(9r-16m-24)} \end{cases}$$

de cette façon, on obtient

1. Si $p \neq 2$, alors

$$x_{n_0}^2 - a \equiv 0 \bmod p^r \Longrightarrow \begin{cases} x_{n_0+1}^2 - a \equiv 0 \bmod p^{3r-4m} \\ x_{n_0+2}^2 - a \equiv 0 \bmod p^{3^2r-16m} \\ x_{n_0+3}^2 - a \equiv 0 \bmod p^{3^3r-52m} \\ \vdots \end{cases}$$

donc

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

telle que la suite (π_n) est définie par

$$\forall n \in \mathbb{N} : \pi_n = 3^n r - \rho_n m$$

la suite $(\rho_n)_n$ représente les termes $0, 4, 16, 52, ...$ s'écrit sous la forme

$$\begin{cases} \rho_0 = 0 \\ \forall n \in \mathbb{N} : \rho_{n+1} = 3\rho_n + 4 \end{cases}$$

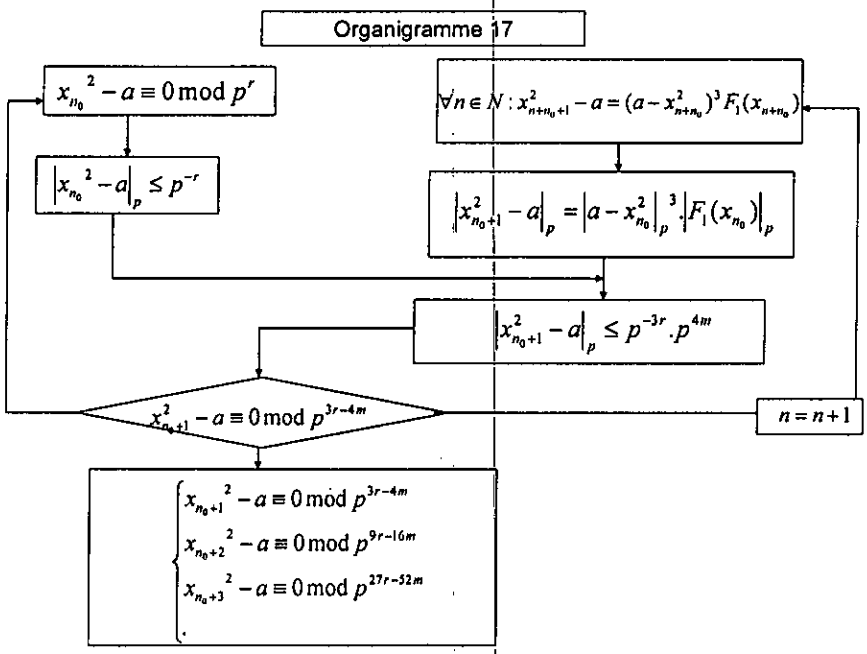
(ρ_n) est une suite récurrente linéaire d'ordre 1, dont le terme générale est définie par

$$\forall n \in \mathbb{N} : \rho_n = 2(3^n - 1)$$

donc

$$\forall n \in \mathbb{N} : \pi_n = 3^n r - 2.(3^n - 1)m \tag{3.53}$$

on a l'organigramme suivant



2. Si $p = 2$, alors

$$x_{n_0}^2 - a \equiv 0 \bmod 2^r \Longrightarrow \begin{cases} x_{n_0+1}^2 - a \equiv 0 \bmod 2^{3r-4m-6} \\ x_{n_0+2}^2 - a \equiv 0 \bmod 2^{3^2 r-16m-24} \\ x_{n_0+3}^2 - a \equiv 0 \bmod 2^{3^3 r-52m-78} \\ \cdot \\ \cdot \end{cases}$$

donc

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

telle que la suite (π'_n) est donnée par

$$\forall n \in \mathbb{N} : \pi'_n = \pi_n - \rho'_n = 3^n r - 2.(3^n - 1)m - \rho'_n$$

et la suite (ρ'_n) représente les termes $0, 6, 24, 78, ...$, s'écrit sous la forme

$$\begin{cases} \rho'_0 = 0 \\ \forall n \in \mathbb{N} : \rho'_{n+1} = 3\rho'_n + 6 \end{cases}$$

il est claire que $(\rho'_n)_n$ est une suite récurrente linéaire d'ordre 1, dont le terme

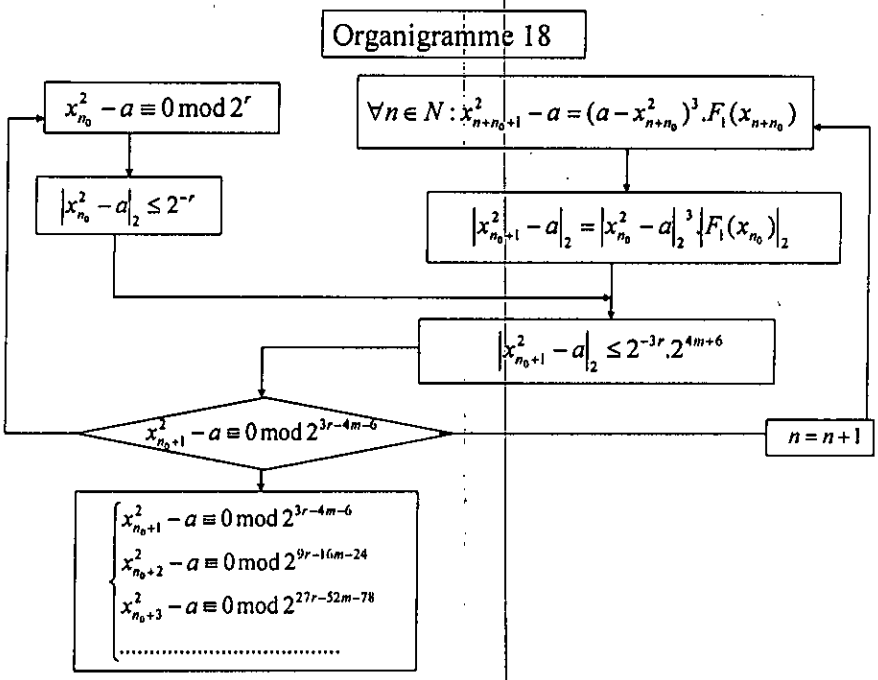
générale est donnée par

$$\forall n \in \mathbb{N} : \rho'_n = 3(3^n - 1)$$

donc

$$\forall n \in \mathbb{N} : \pi'_n = 3^n r - (3^n - 1)(2m + 3) \tag{3.54}$$

on a l'organigramme suivant



d'autre part, on a

$$\forall n \in \mathbb{N} : x_{n+1} = \frac{3}{8a^2}x_n^5 - \frac{5}{4a}x_n^3 + \frac{15}{8}x_n$$

alors

$$\begin{aligned} x_{n+1} - x_n &= \frac{3}{8a^2}x_n^5 - \frac{10}{8a}x_n^3 + \frac{15}{8}x_n - x_n \\ &= \frac{x_n}{8a^2}\left(a - x_n^2\right)\left(7a - 3x_n^2\right) \\ &= \left(a - x_n^2\right).\left(\frac{7}{8a}x_n - \frac{3}{8a^2}x_n^3\right) \end{aligned}$$

donc

$$\forall n \in \mathbb{N} : x_{n+1} - x_n = \left(a - x_n^2\right).C_1(x_n)$$

telle que

$$C_1(x_n) = \frac{7}{8a}x_n - \frac{3}{8a^2}x_n^3$$

ce qui donne

$$|x_{n_0+1} - x_{n_0}|_p = |a - x_{n_0}^2|_p \cdot |C_1(x_{n_0})|_p$$

on a

$$|C_1(x_{n_0})|_p = \left|\frac{7}{8a}x_{n_0} - \frac{3}{8a^2}x_{n_0}^3\right|_p$$

$$\Longrightarrow |C_1(x_{n_0})|_p \leq \max\left\{\left|\frac{7}{8a}\right|_p \cdot |x_{n_0}|_p, \left|-\frac{3}{8a^2}\right|_p \cdot |x_{n_0}^3|_p\right\}$$

$$\Longrightarrow \begin{cases} |C_1(x_{n_0})|_p \leq \max\{p^{2m}.p^{-m}, p^{4m}.p^{-3m}\} & , \text{si } p \neq 2 \\ |C_1(x_{n_0})|_2 \leq \max\{2^3.2^{2m}.2^{-m}, 2^3.2^{4m}.2^{-3m}\} & , \text{si } p = 2 \end{cases}$$

$$\Longrightarrow \begin{cases} |C_1(x_{n_0})|_p \leq \max\{p^m, p^m\} & , \text{si } p \neq 2 \\ |C_1(x_{n_0})|_2 \leq \max\{2^{3+m}, 2^{3+m}\} & , \text{si } p = 2 \end{cases}$$

donc

$$\begin{cases} |C_1(x_{n_0})|_p \leq p^m & , \text{si } p \neq 2 \\ |C_1(x_{n_0})|_2 \leq 2^{m+3} & , \text{si } p = 2 \end{cases}$$

et on déduit

$$\forall n \in \mathbb{N} : \begin{cases} |C_1(x_{n+n_0})|_p \leq p^m & , \text{si } p \neq 2 \\ |C_1(x_{n+n_0})|_2 \leq 2^{m+3} & , \text{si } p = 2 \end{cases} \tag{3.55}$$

donc

1.

$$|x_{n_0+1} - x_{n_0}|_p = |a - x_{n_0}^2|_p \cdot |C_1(x_{n_0})|_p$$

$$\Longrightarrow \begin{cases} |x_{n_0+1} - x_{n_0}|_p \leq p^{-r}.p^m & , \text{si } p \neq 2 \\ |x_{n_0+1} - x_{n_0}|_2 \leq 2^{-r}.2^{m+3} & , \text{si } p = 2 \end{cases}$$

$$\Longrightarrow \begin{cases} |x_{n_0+1} - x_{n_0}|_p \leq p^{-(r-m)} & , \text{si } p \neq 2 \\ |x_{n_0+1} - x_{n_0}|_2 \leq 2^{-(r-m-3)} & , \text{si } p = 2 \end{cases}$$

donc

$$\begin{cases} x_{n_0+1} - x_{n_0} \equiv 0 \bmod p^{(r-m)} & , \text{si } p \neq 2 \\ x_{n_0+1} - x_{n_0} \equiv 0 \bmod 2^{(r-m-3)} & , \text{si } p = 2 \end{cases}$$

2.

$$|x_{n_0+2} - x_{n_0+1}|_p = \left|a - x_{n_0+1}^2\right|_p \cdot |C_1(x_{n_0+1})|_p$$

$$\Longrightarrow \begin{cases} |x_{n_0+2} - x_{n_0+1}|_p \leq p^{-3r+4m}.p^m & , \text{si } p \neq 2 \\ |x_{n_0+2} - x_{n_0+1}|_2 \leq 2^{-3r+4m+6}.2^{m+3} & , \text{si } p = 2 \end{cases}$$

$$\Longrightarrow \begin{cases} |x_{n_0+2} - x_{n_0+1}|_p \leq p^{-(3r-5m)} & , \text{si } p \neq 2 \\ |x_{n_0+2} - x_{n_0+1}|_2 \leq 2^{-(3r-5m-9)} & , \text{si } p = 2 \end{cases}$$

donc

$$\begin{cases} x_{n_0+2} - x_{n_0+1} \equiv 0 \bmod p^{(3r-5m)} & , \text{si } p \neq 2 \\ x_{n_0+2} - x_{n_0+1} \equiv 0 \bmod 2^{(3r-5m-9)} & , \text{si } p = 2 \end{cases}$$

de cette manière, on obtient

1. Si $p \neq 2$, alors

$$\begin{cases} x_{n_0+1} - x_{n_0} \equiv 0 \bmod p^{r-m} \\ x_{n_0+2} - x_{n_0+1} \equiv 0 \bmod p^{3r-5m} \\ x_{n_0+3} - x_{n_0+2} \equiv 0 \bmod p^{9r-17m} \\ x_{n_0+4} - x_{n_0+3} \equiv 0 \bmod p^{27r-53m} \\ \cdot \\ \cdot \end{cases} \iff \begin{cases} x_{n_0+1} - x_{n_0} \equiv 0 \bmod p^{r-m} \\ x_{n_0+2} - x_{n_0+1} \equiv 0 \bmod p^{(3r-4m)-m} \\ x_{n_0+3} - x_{n_0+2} \equiv 0 \bmod p^{(9r-16m)-m} \\ x_{n_0+4} - x_{n_0+3} \equiv 0 \bmod p^{(27r-52m)-m} \\ \cdot \\ \cdot \end{cases} \tag{3.56}$$

donc

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

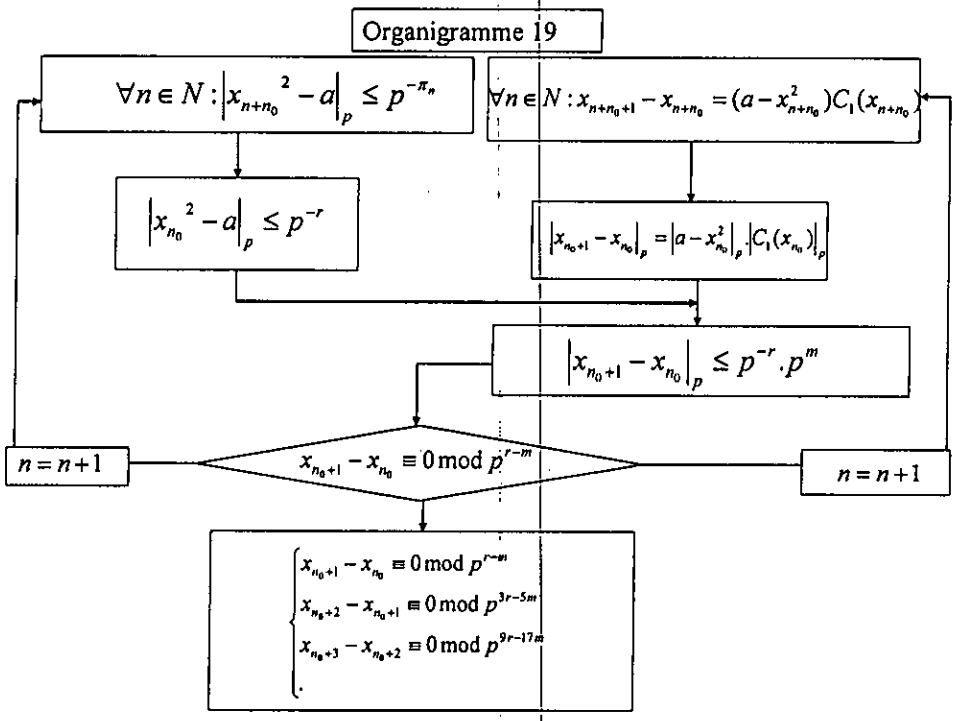
la suite $(\Sigma_n)_n$ est définie par

$$\forall n \in \mathbb{N} : \Sigma_n = \pi_n - m = 3^n r - 2(3^n - 1)m - m = 3^n r - (2.3^n - 1)m$$

par conséquent

$$\forall n \in \mathbb{N} : \Sigma_n = 3^n r - (2.3^n - 1)m \tag{3.57}$$

on a l'organigramme suivant



2. Si $p = 2$, alors

$$\begin{cases} x_{n_0+1} - x_{n_0} \equiv 0 \bmod 2^{r-m-3} \\ x_{n_0+2} - x_{n_0+1} \equiv 0 \bmod 2^{3r-5m-9} \\ x_{n_0+3} - x_{n_0+2} \equiv 0 \bmod 2^{9r-17m-27} \\ x_{n_0+4} - x_{n_0+3} \equiv 0 \bmod 2^{27r-53m-81} \\ \cdot \\ \cdot \end{cases} \Longleftrightarrow \begin{cases} x_{n_0+1} - x_{n_0} \equiv 0 \bmod 2^{r-(m+3)} \\ x_{n_0+2} - x_{n_0+1} \equiv 0 \bmod 2^{3r-4m-6-(m+3)} \\ x_{n_0+3} - x_{n_0+2} \equiv 0 \bmod 2^{9r-16m-24-(m+3)} \\ x_{n_0+4} - x_{n_0+3} \equiv 0 \bmod 2^{27r-52m-78-(m+3)} \\ \cdot \\ \cdot \end{cases} \tag{3.58}$$

donc

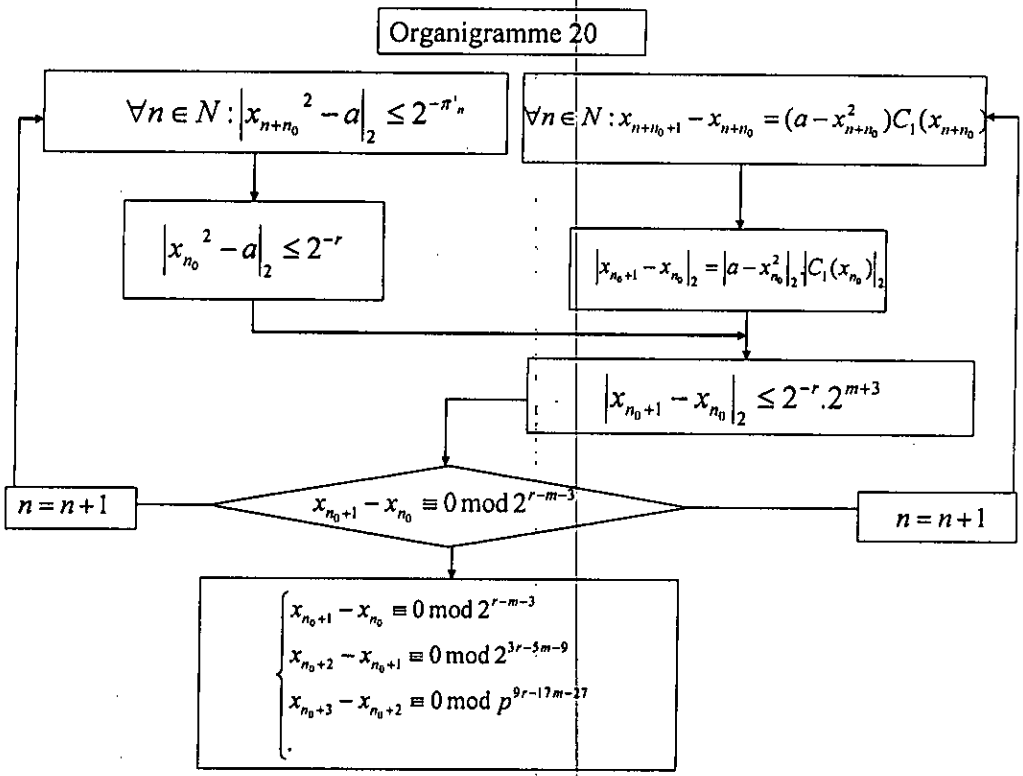
$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \bmod 2^{\Sigma'_n}$$

$$\forall n \in \mathbb{N} : \Sigma'_n = \pi'_n - (m+3) = 3^n r - ((3^n - 1)(2m+3) + m + 3)$$

par conséquent

$$\forall n \in \mathbb{N} : \Sigma'_n = 3^n r - \left((2.3^n - 1)m + 3^{n+1}\right)$$

on a l'oganigramme suivant



Conclusion 3.3.2

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

   (a) *La suite des écarts entre les itérés de la suite $(x_n)_n$ obtenus pour chaque pas de l'itération est donnée par*

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

   autrement dit la vitesse de convergence de la méthode du point fixe est d'ordre Σ_n, lequel est définie par

   $$\forall n \in \mathbb{N} : \Sigma_n = 3^n r - (2.3^n - 1)m$$

   et on dit que la suite x_{n+n_0+1} est une approximation de $\sqrt{a}$ avec environs $|3^n r - (2.3^n - 1)m|$ chiffres p-adiques significatifs.

(b) Pour déterminer le nombre des itérations pour M chiffres donnés, on pose

$$|\Sigma_n| \geq M \Longleftrightarrow |3^n r - (2.3^n - 1)m| \geq M$$

$$\Longrightarrow n = \left\lceil \frac{\ln(|\frac{M-m}{r-2m}|)}{\ln 3} \right\rceil$$

(c) Avec les codes de Hensel on peut écrit l'égualité de la formule (3.51) sous la forme

$$H(p, 3^n r - (2.3^n - 1).m, x) = H(p, \infty, \frac{3}{8}).\frac{H^5(p, 3^{n-1} r - (2.3^{n-1} - 1).m, x)}{H^4(p, \infty, x)} +$$

$$+H(p, \infty, \frac{-5}{4})\frac{H^3(p, 3^{n-1} r - (2.3^{n-1} - 1).m, x)}{H^2(p, \infty, x)} +$$

$$H(p, \infty, \frac{15}{8})H(p, 3^{n-1} r - (2.3^{n-1} - 1)m, x)$$

(d) Les chiffres significatifs β_n et les longueurs de code de Hensel augmentent $|3^n r - (2.3^n - 1)m|$ fois à chaque itération.

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

(a) La suite des écarts entre les itérés de la suite $(x_n)_n$ est donnée par

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

la vitesse de convergence de la méthode du point fixe est d'ordre Σ'_n, lequel est définie par

$$\forall n \in \mathbb{N} : \Sigma'_n = 3^n r - \left((2.3^n - 1)m + 3^{n+1}\right)$$

et on dit que la suite x_{n+n_0+1} est une approximation de $\sqrt{a}$ avec environs $|3^n r - ((2.3^n - 1)m + 3^{n+1})|$ chiffres 2-adiques significatifs.

(b) Pour détreminer le nombre des itérations pour M chiffres donnés, on pose

$$|\Sigma'_n| \geq M \Longleftrightarrow \left|3^n r - \left((2.3^n - 1)m + 3^{n+1}\right)\right| \geq M$$

$$\Longrightarrow n = \left\lceil \frac{\ln(|\frac{M-m}{r-2m-3}|)}{\ln 3} \right\rceil$$

(c) Avec les codes de Hensel on peut écrit l'égalité de la formule (3.51) sous la

forme

$$H(2,3^n r-\left((2.3^n-1)m+3^{n+1}\right),x)=H(2,\infty,\frac{3}{8})\frac{H^5(2,3^{n-1}r-((2.3^{n-1}-1)m+3^n),x)}{H^4(2,\infty,x)}$$

$$+H(2,\infty,\frac{-5}{4})\frac{H^3(2,3^{n-1}r-((2.3^{n-1}-1)m+3^n),x)}{H^2(2,\infty,x)}+$$
$$H(2,\infty,\frac{15}{8})H(2,3^{n-1}r-\left((2.3^{n-1}-1)m+3^n\right),x)$$

(d) Les chiffres significatifs β_n et les longueurs de code de Hensel augmentent $|3^n r-((2.3^n-1)m+3^{n+1})|$ fois à chaque itération.

Corollaire 3.3.3

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

   (a) Si $m=0$, alors on a une convergence cubique sur le bord du $D(0,1)$.

   (b) Si $m\succ 0$, alors on a un retard égal $(2.3^n-1)m$ à l'intérieur du disque de l'unité $D(0,1)$ (convergence cubique avec un retard).

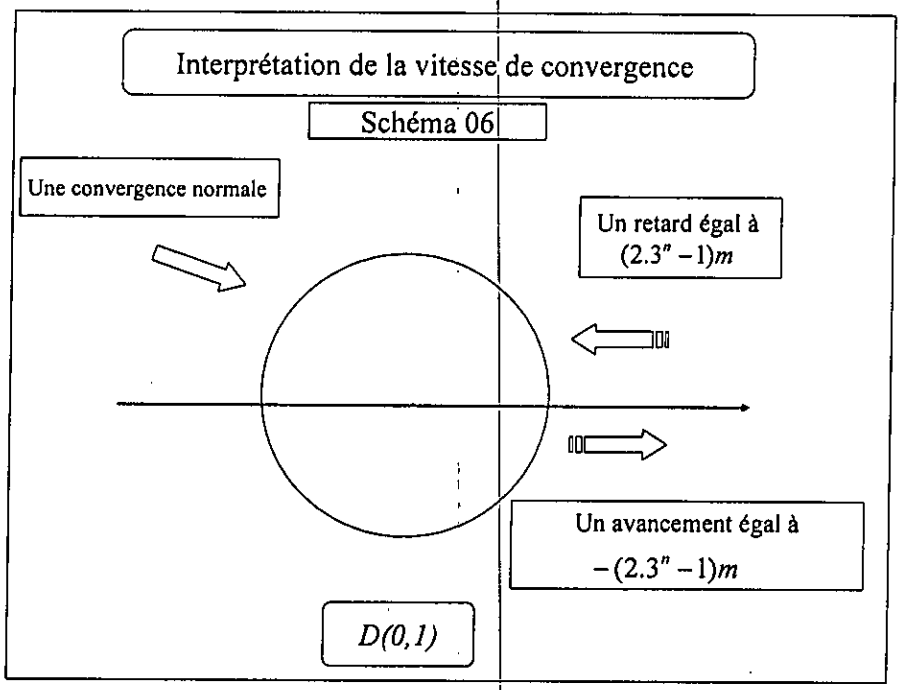
   (c) Si $m\prec 0$, alors on a un avancement égal $(-(2.3^n-1)m)$, à l'extérieur du $D(0.1)$ (convergence cubique avec un avancement).

   (d) La relation entre le retard, l'avancement et les codes de Hensel est comme suit :

      i. Le retard représente le déplacement du point p-adique $(2.3^n-1)m$ fois à gauche.

      ii. L'avancement représente le déplacement du point p-adique $(-(2.3^n-1)m)$ fois vers l'adroite.

on a le schéma suivant



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

   (a) *Si* $m \geq -1$, *alors on a un retard égal* $((2.3^n - 1)m + 3^{n+1})$ *à l'intérieur du disque de* $D(0, 4)$ *(convergence cubique avec un retard).*

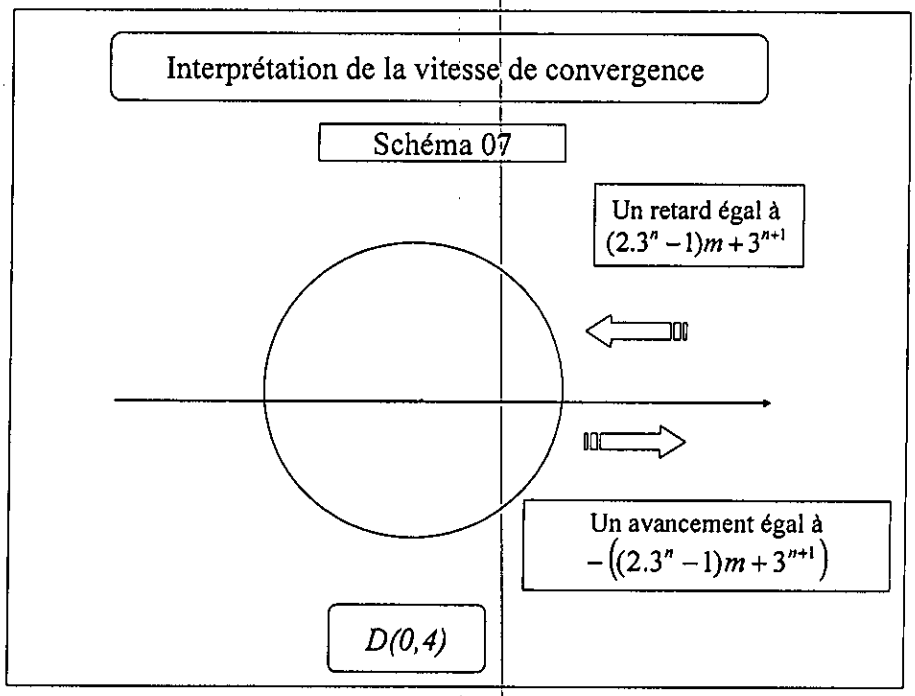
   (b) *Si* $m \leq -1$, *alors on a un avancement égal* $(-((2.3^n - 1)m + 3^{n+1}))$, *à l'extérieur du* $D(0.4)$ *(convergence cubique avec un avancement).*

   (c) *La relation entre le retard, l'avancement et les codes de Hensel est comme suit :*

      i. *Le retard représente le déplacement du point 2-adique* $(2.3^n - 1)m + 3^{n+1}$ *fois à gauche.*

      ii. *L'avancement représente le déplacement du point 2-adique* $(-(2.3^n-1)m+3^{n+1})$ *fois vers l'adroite.*

on a le schéma suivant



3.3.4 Cas 4 : $S = 4$

Pour augmenter encore l'ordre de convergence de la suite $(x_n)_n$, on pose

$$g(x) = \sqrt{a} + (x - \sqrt{a})^4 h(x)$$

telle que

$$h(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3$$

donc

$$g(x) = \sqrt{a} + (x - \sqrt{a})^4 (\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3)$$

on obtient

$$\begin{aligned} g(x) \;=\; & a^2\alpha_0 + \sqrt{a} + (a^2\alpha_1 - 4a^{\frac{3}{2}}\alpha_0)x + (6a\alpha_0 + a^2\alpha_2 - 4a^{\frac{3}{2}}\alpha_1)x^2 + \\ & (6a\alpha_1 + a^2\alpha_3 - 4\sqrt{a}\alpha_0 - 4a^{\frac{3}{2}}\alpha_2)x^3 + (\alpha_0 + 6a\alpha_2 - 4\sqrt{a}\alpha_1 - 4a^{\frac{3}{2}}\alpha_3)x^4 \\ & + (\alpha_1 + 6a\alpha_3 - 4\sqrt{a}\alpha_2)x^5 + (\alpha_2 - 4\sqrt{a}\alpha_3)x^6 + x^7\alpha_3 \end{aligned}$$

pour déterminer les coefficients de la fonction $h(x)$ on utilise la méthode que nous avons appliqué dans les cas 1, 2 et 3.

on pose

$$\begin{cases} c_0 = a^2\alpha_0 + \sqrt{a} \\ c_1 = a^2\alpha_1 - 4a^{\frac{3}{2}}\alpha_0 \\ c_2 = 6a\alpha_0 + a^2\alpha_2 - 4a^{\frac{3}{2}}\alpha_1 \\ c_3 = 6a\alpha_1 + a^2\alpha_3 - 4\sqrt{a}\alpha_0 - 4a^{\frac{3}{2}}\alpha_2 \\ c_4 = \alpha_0 + 6a\alpha_2 - 4\sqrt{a}\alpha_1 - 4a^{\frac{3}{2}}\alpha_3 \\ c_5 = \alpha_1 + 6a\alpha_3 - 4\sqrt{a}\alpha_2 \\ c_6 = \alpha_2 - 4\sqrt{a}\alpha_3 \\ c_7 = \alpha_3 \end{cases}$$

donc, on a les conditions suivantes

$$\begin{cases} c_0 = a^2\alpha_0 + \sqrt{a} = 0 \\ \\ c_i \text{ ne contient pas de } \sqrt{a}\ , 1 \leq i \leq 7 \end{cases}$$

d'après les cas précédents, on obtient le système linéaire suivant

$$\begin{cases} c_0 = a^2\alpha_0 + \sqrt{a} = 0 \\ \\ c_2 = 6a\alpha_0 + a^2\alpha_2 - 4a^{\frac{3}{2}}\alpha_1 = 0 \\ \\ c_4 = \alpha_0 + 6a\alpha_2 - 4\sqrt{a}\alpha_1 - 4a^{\frac{3}{2}}\alpha_3 = 0 \\ \\ c_6 = \alpha_2 - 4\sqrt{a}\alpha_3 = 0 \end{cases}$$

les solutions sont

$$\alpha_0 = -\frac{1}{a^{\frac{3}{2}}}\ ,\ \alpha_1 = -\frac{29}{16a^2}\ ,\ \alpha_2 = -\frac{5}{4a^{\frac{5}{2}}}\ ,\ \alpha_3 = -\frac{5}{16a^3}$$

donc

$$\begin{cases} c_1 = a^2\alpha_1 - 4a^{\frac{3}{2}}\alpha_0 = \frac{35}{16} \\ c_3 = 6a\alpha_1 + a^2\alpha_3 - 4\sqrt{a}\alpha_0 - 4a^{\frac{3}{2}}\alpha_2 = -\frac{35}{16a} \\ c_5 = \alpha_1 + 6a\alpha_3 - 4\sqrt{a}\alpha_2 = \frac{21}{16a^2} \\ c_7 = \alpha_3 = -\frac{5}{16a^3} \end{cases}$$

$h(x)$ et $g(x)$ s'écrivent alors sous la forme

$$\begin{aligned} h(x) &= -(\frac{1}{a^{\frac{3}{2}}} + \frac{29}{16a^2}x + \frac{5}{4a^{\frac{5}{2}}}x^2 + \frac{5}{16a^3}x^3) \\ g(x) &= \frac{35}{16}x - \frac{35}{16a}x^3 + \frac{21}{16a^2}x^5 - \frac{5}{16a^3}x^7 \end{aligned}$$

la fonction polynôme $g(x)$ n'a pas de$\sqrt{a}$ dans ses coefficients et possède trois dérivées successives nulles

$$g(\sqrt{a}) = \sqrt{a}, g^{(1)}(\sqrt{a}) = 0, g^{(2)}(\sqrt{a}) = 0, g^{(3)}(\sqrt{a}) = 0, g^{(4)}(\sqrt{a}) \neq 0$$

la suite associée à la fonction $g(x)$ est donnée par

$$\forall n \in \mathbb{N} : x_{n+1} = -\frac{5}{16a^3}x_n^7 + \frac{21}{16a^2}x_n^5 - \frac{35}{16a}x_n^3 + \frac{35}{16}x_n \tag{3.59}$$

donc

$$x_{n+1}^2 - a = \left(a - x_n^2\right)^4 \left(-\frac{1}{a^3} + \frac{201}{256a^4}x_n^2 - \frac{55}{128a^5}x_n^4 + \frac{25}{256a^6}x_n^6\right)$$

on obtient

$$\forall n \in \mathbb{N} : x_{n+1}^2 - a = \left(a - x_n^2\right)^4 . F_2(x_n)$$

telle que

$$F_2(x_n) = -\frac{1}{a^3} + \frac{201}{256a^4}x_n^2 - \frac{55}{128a^5}x_n^4 + \frac{25}{256a^6}x_n^6$$

la suite des écarts est définie par

$$\begin{aligned} x_{n+1} - x_n &= -\frac{5}{16a^3}x_n^7 + \frac{21}{16a^2}x_n^5 - \frac{35}{16a}x_n^3 + \frac{35}{16}x_n - x_n \\ &= \left(a - x_n^2\right)\left(\frac{19}{16a}x_n - \frac{1}{a^2}x_n^3 + \frac{5}{16a^3}x_n^5\right) \end{aligned}$$

donc

$$\forall n \in \mathbb{N} : x_{n+1} - x_n = \left(a - x_n^2\right) C_2(x_n)$$

telle que

$$C_2(x_n) = \frac{19}{16a}x_n - \frac{1}{a^2}x_n^3 + \frac{5}{16a^3}x_n^5$$

3.3.5 Cas 5 : $S = 5$

La fonction $g(x)$ s'écrit sous la forme

$$g(x) = \sqrt{a} + (x - \sqrt{a})^5 h(x)$$

avec

$$h(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3 + \alpha_4 x^4$$

on obtient

$$\begin{aligned}
g(x) &= \sqrt{a} + (x - \sqrt{a})^5(\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3 + \alpha_4 x^4) \\
&= (\sqrt{a} - a^{\frac{5}{2}}\alpha_0) + (5a^2\alpha_0 - a^{\frac{5}{2}}\alpha_1)x + (5a^2\alpha_1 - 10a^{\frac{3}{2}}\alpha_0 - a^{\frac{5}{2}}\alpha_2)x^2 + \\
&\quad (10a\alpha_0 + 5a^2\alpha_2 - 10a^{\frac{3}{2}}\alpha_1 - a^{\frac{5}{2}}\alpha_3)x^3 + \\
&\quad (10a\alpha_1 + 5a^2\alpha_3 - 5\sqrt{a}\alpha_0 - 10a^{\frac{3}{2}}\alpha_2 - a^{\frac{5}{2}}\alpha_4)x^4 + \\
&\quad (\alpha_0 + 10a\alpha_2 + 5a^2\alpha_4 - 5\sqrt{a}\alpha_1 - 10a^{\frac{3}{2}}\alpha_3)x^5 + (\alpha_1 + 10a\alpha_3 - 5\sqrt{a}\alpha_2 - 10a^{\frac{3}{2}}\alpha_4)x^6 + \\
&\quad (\alpha_2 + 10a\alpha_4 - 5\sqrt{a}\alpha_3)x^7 + (\alpha_3 - 5\sqrt{a}\alpha_4)x^8 + \alpha_4 x^9 \\
&= \sum_{k=0}^{9} c_k x^k
\end{aligned}$$

on rappelle que les conditions qui nous permettent de trouver l'expression de $g(x)$ sont tels que les coefficients $(c_i)_{0\leq i\leq 9}$ n'ont pas de racine de a.
Avant de déterminer les c_i, on a la remarque suivante

Remarque 3.3.4
d'après les cas 1,2,3,4 précédents, on remarque que pour déterminer les coefficients de la fonction $h(x)$ il faut que les coefficients des puissances paires dans $g(x)$ soient nuls. Autrement dit

$$\begin{cases} c_0(\alpha_j, \sqrt{a}) = 0 \\ c_2(\alpha_j, \sqrt{a}) = 0 \\ c_4(\alpha_j, \sqrt{a}) = 0 \\ c_6(\alpha_j, \sqrt{a}) = 0 \\ c_8(\alpha_j, \sqrt{a}) = 0 \end{cases} \iff c_{2i}(\alpha_j, \sqrt{a}) = 0 \ , \ 0 \leq i \leq 4 \ , \ 0 \leq j \leq 4$$

donc on fait la résolution du système linéaire suivant

$$\begin{cases} c_0 = \sqrt{a} - a^{\frac{5}{2}}\alpha_0 = 0 \\ c_2 = 5a^2\alpha_1 - 10a^{\frac{3}{2}}\alpha_0 - a^{\frac{5}{2}}\alpha_2 = 0 \\ c_4 = 10a\alpha_1 + 5a^2\alpha_3 - 5\sqrt{a}\alpha_0 - 10a^{\frac{3}{2}}\alpha_2 - a^{\frac{5}{2}}\alpha_4 = 0 \\ c_6 = \alpha_1 + 10a\alpha_3 - 5\sqrt{a}\alpha_2 - 10a^{\frac{3}{2}}\alpha_4 = 0 \\ c_8 = \alpha_3 - 5\sqrt{a}\alpha_4 = 0 \end{cases}$$

on obtient les solutions suivantes

$$\alpha_0 = \frac{1}{a^2}\ ,\ \alpha_1 = \frac{325}{128a^{\frac{5}{2}}}\ ,\ \alpha_2 = \frac{345}{128a^3}\ ,\ \alpha_3 = \frac{175}{128a^{\frac{7}{2}}}\ ,\ \alpha_4 = \frac{35}{128a^4}$$

ce qui donne

$$\begin{cases} c_1 = 5a^2\alpha_0 - a^{\frac{5}{2}}\alpha_1 = \frac{315}{128} \\ c_3 = 10a\alpha_0 + 5a^2\alpha_2 - 10a^{\frac{3}{2}}\alpha_1 - a^{\frac{5}{2}}\alpha_3 = -\frac{105}{32a} \\ c_5 = \alpha_0 + 10a\alpha_2 + 5a^2\alpha_4 - 5\sqrt{a}\alpha_1 - 10a^{\frac{3}{2}}\alpha_3 = \frac{189}{64a^2} \\ c_7 = \alpha_2 + 10a\alpha_4 - 5\sqrt{a}\alpha_3 = -\frac{45}{32a^3} \\ c_9 = \alpha_4 = \frac{35}{128a^4} \end{cases}$$

par conséquent

$$\begin{aligned} h(x) &= \frac{1}{a^2} + \frac{325}{128a^{\frac{5}{2}}}x + \frac{345}{128a^3}x^2 + \frac{175}{128a^{\frac{7}{2}}}x^3 + \frac{35}{128a^4}x^4 \\ g(x) &= \frac{315}{128}x - \frac{105}{32a}x^3 + \frac{189}{64a^2}x^5 - \frac{45}{32a^3}x^7 + \frac{35}{128a^4}x^9 \end{aligned}$$

la fonction $g(x)$ n'a pas de $\sqrt{a}$ dans ses coefficients, de plus

$$g(\sqrt{a}) = \sqrt{a}\ ,\ g^{(k)}(\sqrt{a}) = 0\ ,\ 0 \leq k \leq 4\ ,\ g^{(5)}(\sqrt{a}) \neq 0$$

la suite associée à $g(x)$ est définie par

$$\forall n \in \mathbb{N} : x_{n+1} = \frac{315}{128}x_n - \frac{105}{32a}x_n^3 + \frac{189}{64a^2}x_n^5 - \frac{45}{32a^3}x_n^7 + \frac{35}{128a^4}x_n^9 \qquad (3.60)$$

ce qui donne

$$\forall n \in \mathbb{N} : x_{n+1}^2 - a = \left(a - x_n^2\right)^5 F_3(x_n)$$

telle que

$$\forall n \in \mathbb{N} : F_3(x_n) = -\frac{1}{a^4} + \frac{17305}{16384a^5}x_n^2 - \frac{14\,235}{16384a^6}x_n^4 + \frac{6475}{16384a^7}x_n^6 - \frac{1225}{16384a^8}x_n^8$$

la suite des écarts est définie par

$$\forall n \in \mathbb{N} : x_{n+1} - x_n = \left(a - x_n^2\right) C_3(x_n)$$

telle que

$$\forall n \in \mathbb{N} : C_3(x_n) = \frac{187}{128a}x_n - \frac{233}{128a^2}x_n^3 + \frac{145}{128a^3}x_n^5 - \frac{35}{128a^4}x_n^7$$

on a le tableaux suivant

Ordre de convergence S	Les coefficients de $h(x)$	Les coefficients de $g(x)$
$S=1$	$\alpha_0 = 1$	$c_1 = 1$
$S=2$	$\alpha_0 = \frac{-\sqrt{a}}{a}, \alpha_1 = \frac{-1}{2a}$	$c_1 = \frac{3}{2}, c_3 = \frac{-1}{2a}$
$S=3$	$\alpha_0 = \frac{1}{a}, \alpha_1 = \frac{9}{8a\sqrt{a}}, \alpha_2 = \frac{3}{8a^2}$	$c_1 = \frac{15}{8}, c_3 = -\frac{5}{4a}$ $c_5 = \frac{3}{8a^2}$
$S=4$	$\alpha_0 = -\frac{1}{a^{\frac{3}{2}}}, \alpha_1 = -\frac{29}{16a^2}$ $\alpha_2 = -\frac{5}{4a^{\frac{5}{2}}}, \alpha_3 = -\frac{5}{16a^3}$	$c_1 = \frac{35}{16}, c_3 = -\frac{35}{16a}$ $c_5 = \frac{21}{16a^2}, c_7 = -\frac{5}{16a^3}$
$S=5$	$\alpha_0 = \frac{1}{a^2}, \alpha_1 = \frac{325}{128a^{\frac{5}{2}}}, \alpha_2 = \frac{345}{128a^3}$ $\alpha_3 = \frac{175}{128a^{\frac{7}{2}}}, \alpha_4 = \frac{35}{128a^4}$	$c_1 = \frac{315}{128}, c_3 = -\frac{105}{32a}$ $c_5 = \frac{189}{64a^2}, c_7 = -\frac{45}{32a^3}$ $c_9 = \frac{35}{128a^4}$
$S=6$	$\alpha_0 = -\frac{1}{a^{\frac{5}{2}}}, \alpha_1 = -\frac{843}{256a^3}$ $\alpha_2 = -\frac{609}{128a^{\frac{7}{2}}}, \alpha_3 = -\frac{469}{128a^4}$ $\alpha_4 = -\frac{189}{128a^{\frac{9}{2}}}, \alpha_5 = -\frac{63}{256a^5}$	$c_1 = \frac{693}{256}, c_3 = -\frac{1155}{256a}$ $c_5 = \frac{693}{128a^2}, c_7 = -\frac{495}{128a^3}$ $c_9 = \frac{385}{256a^4}, c_{11} = -\frac{63}{256a^5}$
$S=7$	$\alpha_0 = \frac{1}{a^3}, \alpha_1 = \frac{4165}{1024a^{\frac{7}{2}}},$ $\alpha_2 = \frac{7651}{1024a^4}, \alpha_3 = \frac{3969}{512a^{\frac{9}{2}}}$ $\alpha_4 = \frac{2415}{512a^5}, \alpha_5 = \frac{1617}{1024a^{\frac{11}{2}}}$ $\alpha_6 = \frac{231}{1024a^6}$	$c_1 = \frac{3003}{1024}, c_3 = -\frac{3003}{512a}$ $c_5 = \frac{9009}{1024a^2}, c_7 = -\frac{2145}{256a^3}$ $c_9 = \frac{5005}{1024a^4}, c_{11} = -\frac{819}{512a^5}$ $c_{13} = \frac{231}{1024a^6}$

$S=8$	$\alpha_0=-\frac{1}{a^{\frac{7}{2}}},\alpha_1=-\frac{9949}{2048a^4}$ $\alpha_2=-\frac{2781}{256a^{\frac{9}{2}}},\alpha_3=-\frac{29115}{2048a^5}$ $\alpha_4=-\frac{1485}{128a^{\frac{11}{2}}},\alpha_5=-\frac{11979}{2048a^6}$ $\alpha_6=-\frac{429}{256a^{\frac{13}{2}}},\alpha_7=-\frac{429}{2048a^7}$	$c_1=\frac{6435}{2048},c_3=-\frac{15015}{2048a}$ $c_5=\frac{27027}{2048a^2},c_7=-\frac{32175}{2048a^3}$ $c_9=\frac{25025}{2048a^4},c_{11}=-\frac{12285}{2048a^5}$ $c_{13}=\frac{3465}{2048a^6},c_{15}=-\frac{429}{2048a^7}$
$S=9$	$\alpha_0=\frac{1}{a^4},\alpha_1=\frac{185517}{32768a^{\frac{9}{2}}}$ $\alpha_2=\frac{490005}{32768a^5},\alpha_3=\frac{775665}{32768a^{\frac{11}{2}}}$ $\alpha_4=\frac{795465}{32768a^6},\alpha_5=\frac{536679}{32768a^{\frac{13}{2}}}$ $\alpha_6=\frac{231231}{32768a^7},\alpha_7=\frac{57915}{32768a^{\frac{15}{2}}}$ $\alpha_8=\frac{6435}{32768a^8}$	$c_1=\frac{109395}{32768},c_3=-\frac{36465}{4096a}$ $c_5=\frac{153153}{8192a^2},c_7=-\frac{109395}{4096a^3}$ $c_9=\frac{425425}{16384a^4},c_{11}=-\frac{69615}{4096a^5}$ $c_{13}=\frac{58905}{8192a^6},c_{15}=-\frac{7293}{4096a^7}$ $c_{17}=\frac{6435}{32768a^8}$
$S=10$	$\alpha_0=-\frac{1}{a^{\frac{9}{2}}},\alpha_1=-\frac{424415}{65536a^5}$ $\alpha_2=-\frac{647515}{32768a^{\frac{11}{2}}},\alpha_3=-\frac{602195}{16384a^6}$ $\alpha_4=-\frac{1489345}{32768a^{\frac{13}{2}}},\alpha_5=-\frac{1260259}{32768a^7}$ $\alpha_6=-\frac{725725}{32768a^{\frac{15}{2}}},\alpha_7=-\frac{136565}{16384a^8}$ $\alpha_8=-\frac{60775}{32768a^{\frac{17}{2}}},\alpha_9=-\frac{12155}{65536a^9}$	$c_1=\frac{230945}{65536},c_3=-\frac{692835}{65536a}$ $c_5=\frac{415701}{16384a^2},c_7=-\frac{692835}{16384a^3}$ $c_9=\frac{1616615}{32768a^4},c_{11}=-\frac{1322685}{32768a^5}$ $c_{13}=\frac{373065}{16384a^6},c_{15}=-\frac{138567}{16384a^7}$ $c_{17}=\frac{122265}{65536a^8},c_{19}-\frac{12155}{65536a^9}$
$S=11$	$\alpha_0=\frac{1}{a^5},\alpha_1=\frac{1913615}{262144a^{\frac{11}{2}}}$ $\alpha_2=\frac{6631845}{262144a^6}\alpha_3=\frac{3547115}{65536a^{\frac{13}{2}}}$ $\alpha_4=\frac{5140135}{65536a^7},\alpha_5=\frac{10471461}{131072a^{\frac{15}{2}}}$ $\alpha_6=\frac{7554547}{131072a^8},\alpha_7=\frac{1898611}{65536a^{\frac{17}{2}}}$ $\alpha_8=\frac{634491}{65536a^9},\alpha_9=\frac{508079}{262144a^{\frac{19}{2}}}$ $\alpha_{10}=\frac{46189}{262144a^{10}}$	$c_1=\frac{969969}{262144},c_3=-\frac{1616615}{131072a}$ $c_5=\frac{8729721}{262144a^2},c_7=-\frac{2078505}{32768a^3}$ $c_9==\frac{11316305}{131072a^4},c_{11}=-\frac{5555277}{65536a^5}$ $c_{13}=\frac{7834365}{131072a^6},c_{15}=-\frac{969969}{32768a^7}$ $c_{17}=\frac{2567565}{262144a^8},c_{19}=-\frac{255255}{131072a^9}$ $c_{21}=\frac{46189}{262144a^{10}}$
$S=12$	$\alpha_0=-\frac{1}{a^{\frac{11}{2}}},\alpha_1=-\frac{4263339}{524288a^6}$ $\alpha_2=-\frac{4139265}{131072a^{\frac{13}{2}}},\alpha_3=-\frac{40084135}{524288a^7}$ $\alpha_4=-\frac{1041495}{8192a^{\frac{15}{2}}},\alpha_5=-\frac{39721227}{262144a^8}$ $\alpha_6=-\frac{8615243}{65536a^{\frac{17}{2}}},\alpha_7=-\frac{21686067}{262144a^9}$ $\alpha_8=-\frac{37791}{1024a^{\frac{19}{2}}},\alpha_9=-\frac{5815615}{524288a^{10}}$ $\alpha_{10}=-\frac{264537}{131072a^{\frac{21}{2}}},\alpha_{11}=-\frac{88179}{524288a^{11}}$	$c_1=\frac{2028117}{524288},c_3=-\frac{7436429}{524288a}$ $c_5=\frac{22309287}{524288a^2},c_7=-\frac{47805615}{524288a^3}$ $c_9=\frac{37182145}{262144a^4},c_{11}=-\frac{42590457}{262144a^5}$ $c_{13}=\frac{36038079}{262144a^6},c_{15}=-\frac{22309287}{262144a^7}$ $c_{17}=\frac{19684665}{524288a^8},c_{19}=-\frac{5870865}{524288a^9}$ $c_{21}=\frac{1062347}{524288a^{10}},c_{23}=-\frac{88179}{524288a^{11}}$

$S=13$	$\alpha_0=\frac{1}{a^6},\alpha_1=\frac{37\,624\,977}{4194\,304a^{\frac{13}{2}}}$ $\alpha_2=\frac{161\,968\,989}{4194\,304a^7},\alpha_3=\frac{438\,023\,495}{4194\,304a^{\frac{15}{2}}}$ $\alpha_4=\frac{822\,540\,355}{4194\,304a^8},\alpha_5=\frac{561\,720\,341}{2097\,152a^{\frac{17}{2}}}$ $\alpha_6=\frac{569\,696\,673}{2097\,152a^9},\alpha_7=\frac{430\,855\,191}{2097\,152a^{\frac{19}{2}}}$ $\alpha_8=\frac{240\,539\,715}{2097\,152a^{10}},\alpha_9=\frac{192\,965\,045}{4194\,304a^{\frac{21}{2}}}$ $\alpha_{10}=\frac{52\,701\,649}{4194\,304a^{11}},\alpha_{11}=\frac{8788\,507}{4194\,304a^{\frac{23}{2}}}$ $\alpha_{12}=\frac{676\,039}{4194\,304a^{12}}$	$c_1=\frac{16\,900\,975}{4194\,304},c_3=-\frac{16\,900\,975}{1048\,576a}$ $c_5=\frac{111\,546\,435}{2097\,152a^2},c_7=-\frac{132\,793\,375}{1048\,576a^3}$ $c_9=\frac{929\,553\,625}{4194\,304a^4},c_{11}=-\frac{152\,108\,775}{524\,288a^5}$ $c_{13}=\frac{300\,317\,325}{1048\,576a^6},c_{15}=-\frac{111\,546\,435}{524\,288a^7}$ $c_{17}=\frac{492\,116\,625}{4194\,304a^8},c_{19}=-\frac{48\,923\,875}{1048\,576a^9}$ $c_{21}=\frac{26\,558\,675}{2097\,152a^{10}},c_{23}=-\frac{2204\,475}{1048\,576a^{11}}$ $c_{25}=\frac{676\,039}{4194\,304a^{12}}$
$S=14$	$\alpha_0=-\frac{1}{a^{\frac{13}{2}}},\alpha_1=-\frac{82\,338\,487}{8388\,608a^7}$ $\alpha_2=-\frac{194\,687\,745}{4194\,304a^{\frac{15}{2}}},\alpha_3=-\frac{582\,008\,315}{4194\,304a^8}$ $\alpha_4=-\frac{1218\,637\,945}{4194\,304a^{\frac{17}{2}}},\alpha_5=-\frac{3754\,603\,629}{8388\,608a^9}$ $\alpha_6=-\frac{1090\,048\,449}{2097\,152a^{\frac{19}{2}}},\alpha_7=-\frac{963\,171\,465}{2097\,152a^{10}}$ $\alpha_8=-\frac{645\,979\,005}{2097\,152a^{\frac{21}{2}}},\alpha_9=-\frac{1296\,649\,585}{8388\,608a^{11}}$ $\alpha_{10}=-\frac{236\,249\,629}{4194\,304a^{\frac{23}{2}}},\alpha_{11}=-\frac{59\,127\,411}{4194\,304a^{12}}$ $\alpha_{12}=-\frac{9100\,525}{4194\,304a^{\frac{25}{2}}},\alpha_{13}=-\frac{1300\,075}{8388\,608a^{13}}$	$c_1=\frac{35\,102\,025}{8388\,608},c_3=-\frac{152\,108\,775}{8388\,608a}$ $c_5=\frac{273\,795\,795}{4194\,304a^2},c_7=-\frac{717\,084\,225}{4194\,304a^3}$ $c_9=\frac{2788\,660\,875}{8388\,608a^4},c_{11}=-\frac{4106\,936\,925}{8388\,608a^5}$ $c_{13}=\frac{1158\,366\,825}{2097\,152a^6},c_{15}=-\frac{1003\,917\,915}{2097\,152a^7}$ $c_{17}=\frac{2657\,429\,775}{8388\,608a^8},c_{19}=-\frac{1320\,944\,625}{8388\,608a^9}$ $c_{21}=\frac{239\,028\,075}{4194\,304a^{10}},c_{23}=-\frac{59\,520\,825}{4194\,304a^{11}}$ $c_{25}=\frac{18\,253\,053}{8388\,608a^{12}},c_{27}=-\frac{1300\,075}{8388\,608a^{13}}$
$S=15$	$\alpha_0=\frac{1}{a^7},\alpha_1=\frac{357\,893\,805}{33\,554\,432a^{\frac{15}{2}}}$ $\alpha_2=\frac{1845\,191\,715}{33\,554\,432a^8},\alpha_3=\frac{3022\,465\,955}{16\,777\,216a^{\frac{17}{2}}}$ $\alpha_4=\frac{6984\,365\,085}{16\,777\,216a^9},\alpha_5=\frac{23\,967\,555\,111}{33\,554\,432a^{\frac{19}{2}}}$ $\alpha_6=\frac{31\,369\,151\,145}{33\,554\,432a^{10}},\alpha_7=\frac{7930\,281\,465}{8388\,608a^{\frac{21}{2}}}$ $\alpha_8=\frac{6211\,692\,135}{8388\,608a^{11}},\alpha_9=\frac{14\,974\,598\,155}{33\,554\,432a^{\frac{23}{2}}}$ $\alpha_{10}=\frac{6825\,416\,037}{33\,554\,432a^{12}},\alpha_{11}=\frac{1139\,422\,875}{16\,777\,216a^{\frac{25}{2}}}$ $\alpha_{12}=\frac{263\,172\,325}{16\,777\,216a^{13}},\alpha_{13}=\frac{75\,218\,625}{33\,554\,432a^{\frac{27}{2}}}$ $\alpha_{14}=\frac{5014\,575}{33\,554\,432a^{14}}$	$c_1=\frac{145\,422\,675}{33\,554\,432},c_3=-\frac{339\,319\,575}{16\,777\,216a}$ $c_5=\frac{2646\,692\,685}{33\,554\,432a^2},c_7=-\frac{1890\,494\,775}{8388\,608a^3}$ $c_9=\frac{16\,174\,233\,075}{33\,554\,432a^4},c_{11}=-\frac{13\,233\,463\,425}{16\,777\,216a^5}$ $c_{13}=\frac{33\,592\,637\,925}{33\,554\,432a^6},c_{15}=-\frac{4159\,088\,505}{4194\,304a^7}$ $c_{17}=\frac{25\,688\,487\,825}{33\,554\,432a^8},c_{19}=-\frac{7661\,478\,825}{16\,777\,216a^9}$ $c_{21}=\frac{6931\,814\,175}{33\,554\,432a^{10}},c_{23}=-\frac{575\,367\,975}{8388\,608a^{11}}$ $c_{25}=\frac{529\,338\,537}{33\,554\,432a^{12}},c_{27}=-\frac{37\,702\,175}{16\,777\,216a^{13}}$ $c_{29}=\frac{5014\,575}{33\,554\,432a^{14}}$
$S=16$	$\alpha_0=-\frac{1}{a^{\frac{15}{2}}},\alpha_1=-\frac{773\,201\,629}{67\,108\,864a^8}$ $\alpha_2=-\frac{269\,885\,149}{4194\,304a^{\frac{17}{2}}},\alpha_3=-\frac{15\,390\,067\,479}{67\,108\,864a^9}$ $\alpha_4=-\frac{1216\,136\,667}{2097\,152a^{\frac{19}{2}}},\alpha_5=-\frac{73\,618\,020\,141}{67\,108\,864a^{10}}$ $\alpha_6=-\frac{6702\,668\,931}{4194\,304a^{\frac{21}{2}}},\alpha_7=-\frac{122\,162\,255\,391}{67\,108\,864a^{11}}$ $\alpha_8=-\frac{1710\,460\,389}{1048\,576a^{\frac{23}{2}}},\alpha_9=-\frac{77\,032\,333\,631}{67\,108\,864a^{12}}$ $\alpha_{10}=-\frac{2635\,029\,155}{4194\,304a^{\frac{25}{2}}},\alpha_{11}=-\frac{17\,604\,538\,445}{67\,108\,864a^{13}}$ $\alpha_{12}=-\frac{169\,492\,635}{2097\,152a^{\frac{27}{2}}},\alpha_{13}=-\frac{1163\,047\,095}{67\,108\,864a^{14}}$ $\alpha_{14}=-\frac{9694\,845}{4194\,304a^{\frac{29}{2}}},\alpha_{15}=-\frac{9694\,845}{67\,108\,864a^{15}}$	$c_1=\frac{300\,540\,195}{67\,108\,864},c_3=-\frac{1502\,700\,975}{67\,108\,864a}$ $c_5=\frac{6311\,344\,095}{67\,108\,864a^2},c_7=-\frac{19\,535\,112\,675}{67\,108\,864a^3}$ $c_9=\frac{45\,581\,929\,575}{67\,108\,864a^4},c_{11}=-\frac{82\,047\,473\,235}{67\,108\,864a^5}$ $c_{13}=\frac{115\,707\,975\,075}{67\,108\,864a^6},c_{15}=\frac{128\,931\,743\,655}{67\,108\,864a^7}$ $c_{17}=\frac{113\,763\,303\,225}{67\,108\,864a^8},c_{19}=-\frac{79\,168\,614\,525}{67\,108\,864a^9}$ $c_{21}=\frac{42\,977\,247\,885}{67\,108\,864a^{10}},c_{23}=-\frac{17\,836\,407\,225}{67\,108\,864a^{11}}$ $c_{25}=\frac{5469\,831\,549}{67\,108\,864a^{12}},c_{27}=-\frac{1168\,767\,425}{67\,108\,864a^{13}}$ $c_{29}=\frac{155\,451\,825}{67\,108\,864a^{14}},c_{31}=-\frac{9694\,845}{67\,108\,864a^{15}}$

$S=17$	$\alpha_0=\frac{1}{a^8},\alpha_1=\frac{26\,589\,395\,581}{2147\,483\,648a^{\frac{17}{2}}}$ $\alpha_2=\frac{159\,961\,948\,749}{2147\,483\,648a^9},\alpha_3=\frac{616\,379\,284\,677}{2147\,483\,648a^{\frac{19}{2}}}$ $\alpha_4=\frac{1693\,400\,722\,485}{2147\,483\,648a^{10}},\alpha_5=\frac{3502\,194\,212\,097}{2147\,483\,648a^{\frac{21}{2}}}$ $\alpha_6=\frac{5621\,201\,133\,009}{2147\,483\,648a^{11}},\alpha_7=\frac{7123\,667\,423\,961}{2147\,483\,648a^{\frac{23}{2}}}$ $\alpha_8=\frac{7188\,510\,469\,833}{2147\,483\,648a^{12}},\alpha_9=\frac{5785\,592\,836\,375}{2147\,483\,648a^{\frac{25}{2}}}$ $\alpha_{10}=\frac{3696\,547\,932\,935}{2147\,483\,648a^{13}},\alpha_{11}=\frac{1853\,167\,281\,615}{2147\,483\,648a^{\frac{27}{2}}}$ $\alpha_{12}=\frac{713\,968\,168\,095}{2147\,483\,648a^{14}},\alpha_{13}=\frac{204\,202\,520\,235}{2147\,483\,648a^{\frac{29}{2}}}$ $\alpha_{14}=\frac{40\,863\,771\,675}{2147\,483\,648a^{15}},\alpha_{15}=\frac{5109\,183\,315}{2147\,483\,648a^{\frac{31}{2}}}$ $\alpha_{16}=\frac{300\,540\,195}{2147\,483\,648a^{16}}$	$c_1=\frac{9917\,826\,435}{2147\,483\,648},c_3=-\frac{3305\,942\,145}{134\,217\,728a}$ $c_5=\frac{29\,753\,479\,305}{268\,435\,456a^2},c_7=-\frac{49\,589\,132\,175}{134\,217\,728a^3}$ $c_9=\frac{501\,401\,225\,325}{536\,870\,912a^4},c_{11}=-\frac{246\,142\,419\,705}{134\,217\,728a^5}$ $c_{13}=\frac{763\,672\,635\,495}{268\,435\,456a^6},c_{15}=-\frac{472\,749\,726\,735}{134\,217\,728a^7}$ $c_{17}=\frac{3754\,189\,006\,425}{1073\,741\,824a^8},c_{19}=-\frac{373\,223\,468\,475}{134\,217\,728a^9}$ $c_{21}=\frac{472\,749\,726\,735}{268\,435\,456a^{10}},c_{23}=-\frac{117\,720\,287\,685}{134\,217\,728a^{11}}$ $c_{25}=\frac{180\,504\,441\,117}{536\,870\,912a^{12}},c_{27}=-\frac{12\,856\,441\,675}{134\,217\,728a^{13}}$ $c_{29}=\frac{5129\,910\,225}{268\,435\,456a^{14}},c_{31}=-\frac{319\,929\,885}{134\,217\,728a^{15}}$ $c_{33}=\frac{300\,540\,195}{2147\,483\,648a^{16}}$
$S=18$	$\alpha_0=-\frac{1}{a^{\frac{13}{2}}},\alpha_1=-\frac{82\,338\,487}{8388\,608a^7}$ $\alpha_2=-\frac{194\,687\,745}{4194\,304a^{\frac{15}{2}}},\alpha_3=-\frac{582\,008\,315}{4194\,304a^8}$ $\alpha_4=-\frac{1218\,637\,945}{4194\,304a^{\frac{17}{2}}},\alpha_5=-\frac{3754\,603\,629}{8388\,608a^9}$ $\alpha_6=-\frac{1090\,048\,449}{2097\,152a^{\frac{19}{2}}},\alpha_7=-\frac{963\,171\,465}{2097\,152a^{10}}$ $\alpha_8=-\frac{645\,979\,005}{2097\,152a^{\frac{21}{2}}},\alpha_9=-\frac{1296\,649\,585}{8388\,608a^{11}}$ $\alpha_{10}=-\frac{236\,249\,629}{4194\,304a^{\frac{23}{2}}},\alpha_{11}=-\frac{59\,127\,411}{4194\,304a^{12}}$ $\alpha_{12}=-\frac{9100\,525}{4194\,304a^{\frac{25}{2}}},\alpha_{13}=-\frac{1300\,075}{8388\,608a^{13}}$	$c_1=\frac{35\,102\,025}{8388\,608},c_3=-\frac{152\,108\,775}{8388\,608a}$ $c_5=\frac{273\,795\,795}{4194\,304a^2},c_7=-\frac{717\,084\,225}{4194\,304a^3}$ $c_9=\frac{2788\,660\,875}{8388\,608a^4},c_{11}=-\frac{4106\,936\,925}{8388\,608a^5}$ $c_{13}=\frac{1158\,366\,825}{2097\,152a^6},c_{15}=-\frac{1003\,917\,915}{2097\,152a^7}$ $c_{17}=\frac{2657\,429\,775}{8388\,608a^8},c_{19}=-\frac{1320\,944\,625}{8388\,608a^9}$ $c_{21}=\frac{239\,028\,075}{4194\,304a^{10}},c_{23}=-\frac{59\,520\,825}{4194\,304a^{11}}$ $c_{25}=\frac{18\,253\,053}{8388\,608a^{12}},c_{27}=-\frac{1300\,075}{8388\,608a^{13}}$
$S=19$	$\alpha_0=\frac{1}{a^9},\alpha_1=\frac{242\,472\,512\,971}{17\,179\,869\,184a^{\frac{19}{2}}}$ $\alpha_2=\frac{1669\,220\,115\,985}{17\,179\,869\,184a^{10}},\alpha_3=\frac{925\,418\,216\,765}{2147\,483\,648a^{\frac{21}{2}}}$ $\alpha_4=\frac{368\,650\,331\,665}{268\,435\,456a^{11}},\alpha_5=\frac{14\,289\,079\,177\,219}{4294\,967\,296a^{\frac{23}{2}}}$ $\alpha_6=\frac{27\,187\,951\,164\,451}{4294\,967\,296a^{12}},\alpha_7=\frac{20\,722\,144\,788\,125}{2147\,483\,648a^{\frac{25}{2}}}$ $\alpha_8=\frac{6401\,329\,638\,275}{536\,870\,912a^{13}},\alpha_9=\frac{103\,193\,523\,929\,925}{8589\,934\,592a^{\frac{27}{2}}}$ $\alpha_{10}=\frac{84\,871\,568\,296\,515}{8589\,934\,592a^{14}},\alpha_{11}=\frac{14\,196\,427\,096\,215}{2147\,483\,648a^{\frac{29}{2}}}$ $\alpha_{12}=\frac{957\,912\,466\,875}{268\,435\,456a^{15}},\alpha_{13}=\frac{6579\,679\,345\,575}{4294\,967\,296a^{\frac{31}{2}}}$ $\alpha_{14}=\frac{2195\,681\,842\,275}{4294\,967\,296a^{16}},\alpha_{15}=\frac{274\,652\,487\,615}{2147\,483\,648a^{\frac{33}{2}}}$ $\alpha_{16}=\frac{12\,121\,787\,865}{536\,870\,912a^{17}},\alpha_{17}=\frac{43\,106\,892\,675}{17\,179\,869\,184a^{\frac{35}{2}}}$ $\alpha_{18}=\frac{2268\,783\,825}{17\,179\,869\,184a^{18}}$	$c_1=\frac{83\,945\,001\,525}{17\,179\,869\,184}$ $c_3=-\frac{251\,835\,004\,575}{8589\,934\,592a}$ $c_5=\frac{2568\,717\,046\,665}{17\,179\,869\,184a^2}$ $c_7=-\frac{611\,599\,296\,825}{1073\,741\,824a^3}$ $c_9=\frac{7135\,325\,129\,625}{4294\,967\,296a^4}$ $c_{11}=-\frac{8173\,190\,603\,025}{2147\,483\,648a^5}$ $c_{13}=\frac{29\,968\,365\,544\,425}{4294\,967\,296a^6}$ $c_{15}=-\frac{11\,131\,107\,202\,215}{1073\,741\,824a^7}$ $c_{17}=\frac{108\,037\,216\,962\,675}{8589\,934\,592a^8}$ $c_{19}=-\frac{53\,702\,710\,186\,125}{4294\,967\,296a^9}$ $c_{21}=\frac{87\,458\,699\,445\,975}{8589\,934\,592a^{10}}$ $c_{23}=-\frac{7259\,417\,740\,575}{1073\,741\,824a^{11}}$ $c_{25}=\frac{15\,583\,550\,083\,101}{4294\,967\,296a^{12}}$ $c_{27}=-\frac{3329\,818\,393\,825}{2147\,483\,648a^{13}}$ $c_{29}=\frac{2214\,411\,247\,125}{4294\,967\,296a^{14}}$ $c_{31}=-\frac{138\,103\,067\,025}{1073\,741\,824a^{15}}$ $c_{33}=\frac{389\,199\,552\,525}{17\,179\,869\,184a^{16}}$ $c_{35}=-\frac{21\,585\,857\,535}{8589\,934\,592a^{17}}$ $c_{37}=\frac{2268\,783\,825}{17\,179\,869\,184a^{18}}$

$S = 20$

$$\alpha_0 = -\frac{1}{a^{\frac{19}{2}}}$$

$$\alpha_1 = -\frac{514\,886\,606\,335}{34\,359\,738\,368a^{10}}$$

$$\alpha_2 = -\frac{942\,345\,459\,195}{8589\,934\,592a^{\frac{21}{2}}}$$

$$\alpha_3 = -\frac{17\,820\,568\,291\,295}{34\,359\,738\,368a^{11}}$$

$$\alpha_4 = -\frac{3795\,413\,479\,165}{2147\,483\,648a^{\frac{23}{2}}}$$

$$\alpha_5 = -\frac{39\,478\,617\,193\,323}{8589\,934\,592a^{12}}$$

$$\alpha_6 = -\frac{20\,252\,733\,572\,225}{2147\,483\,648a^{\frac{25}{2}}}$$

$$\alpha_7 = -\frac{133\,931\,147\,896\,975}{8589\,934\,592a^{13}}$$

$$\alpha_8 = -\frac{45\,174\,221\,524\,575}{2147\,483\,648a^{\frac{27}{2}}}$$

$$\alpha_9 = -\frac{400\,814\,212\,023\,225}{17\,179\,869\,184a^{14}}$$

$$\alpha_{10} = -\frac{91\,621\,762\,477\,245}{4294\,967\,296a^{\frac{29}{2}}}$$

$$\alpha_{11} = -\frac{275\,988\,167\,971\,425}{17\,179\,869\,184a^{15}}$$

$$\alpha_{12} = -\frac{21\,290\,994\,727\,275}{2147\,483\,648a^{\frac{31}{2}}}$$

$$\alpha_{13} = -\frac{42\,667\,801\,589\,175}{8589\,934\,592a^{16}}$$

$$\alpha_{14} = -\frac{4272\,699\,932\,325}{2147\,483\,648a^{\frac{33}{2}}}$$

$$\alpha_{15} = -\frac{5345\,824\,446\,435}{8589\,934\,592a^{17}}$$

$$\alpha_{16} = -\frac{314\,644\,493\,625}{2147\,483\,648a^{\frac{35}{2}}}$$

$$\alpha_{17} = -\frac{839\,330\,605\,575}{34\,359\,738\,368a^{18}}$$

$$\alpha_{18} = -\frac{22\,090\,789\,875}{8589\,934\,592a^{\frac{37}{2}}}$$

$$\alpha_{19} = -\frac{4418\,157\,975}{34\,359\,738\,368a^{19}}$$

$$c_1 = \frac{172\,308\,161\,025}{34\,359\,738\,368}$$

$$c_3 = -\frac{1091\,285\,019\,825}{34\,359\,738\,368a}$$

$$c_5 = \frac{5892\,939\,107\,055}{34\,359\,738\,368a^2}$$

$$c_7 = -\frac{23\,852\,372\,576\,175}{34\,359\,738\,368a^3}$$

$$c_9 = \frac{18\,551\,845\,337\,025}{8589\,934\,592a^4}$$

$$c_{11} = -\frac{45\,536\,347\,645\,425}{8589\,934\,592a^5}$$

$$c_{13} = \frac{89\,905\,096\,633\,275}{8589\,934\,592a^6}$$

$$c_{15} = -\frac{144\,704\,393\,628\,795}{8589\,934\,592a^7}$$

$$c_{17} = \frac{383\,041\,041\,958\,575}{17\,179\,869\,184a^8}$$

$$c_{19} = -\frac{418\,881\,139\,451\,775}{17\,179\,869\,184a^9}$$

$$c_{21} = \frac{378\,987\,697\,599\,225}{17\,179\,869\,184a^{10}}$$

$$c_{23} = -\frac{283\,117\,291\,882\,425}{17\,179\,869\,184a^{11}}$$

$$c_{25} = \frac{86\,822\,636\,177\,277}{8589\,934\,592a^{12}}$$

$$c_{27} = -\frac{43\,287\,639\,119\,725}{8589\,934\,592a^{13}}$$

$$c_{29} = \frac{17\,272\,407\,727\,575}{8589\,934\,592a^{14}}$$

$$c_{31} = -\frac{5386\,019\,613\,975}{8589\,934\,592a^{15}}$$

$$c_{33} = \frac{5059\,594\,182\,825}{34\,359\,738\,368a^{16}}$$

$$c_{35} = -\frac{841\,848\,443\,865}{34\,359\,738\,368a^{17}}$$

$$c_{37} = \frac{88\,482\,569\,175}{34\,359\,738\,368a^{18}}$$

$$c_{39} = -\frac{4418\,157\,975}{34\,359\,738\,368a^{19}}$$

3.3.6 Généralisation :

Généralement, on peut construire une méthode itérative $x_{n+1} = g(x_n)$ suffisamment hyper accélérée qui converge vers $\sqrt{a}$ dans $\mathbb{Q}_p^*$ avec un ordre égale à s suffisamment grand. Pour accélérer l'ordre de convergence de la suite $(x_n)_n$ autant qu'on veut, il faut résoudre le problème suivant :

$$g(x) = \sqrt{a} + (x - \sqrt{a})^s h(x)$$

Trouver la fonction h tel que $\sqrt{a}+(x-\sqrt{a})^s.h(x,\sqrt{a})$ soit de la forme $g(x,a)$. Autrement dit, trouver la fonction $h(x,\sqrt{a})$ de manière à faire disparaître les racines carrées de a dans les coefficients de la fonction g. Pour que la fonction $g(x)$ ne contient pas de $\sqrt{a}$, il faut que les coefficients de puissances paires de x soient nuls. Ce que signifie

$$g(x) = c_1 x + c_3 x^3 + \ldots\ldots\ldots\ldots + c_{2s-1} x^{2s-1} = \sum_{k=0}^{s-1} c_{2k+1}(a) x^{2k+1}$$

d'autre part, on prend le degré de la fonction $h(x)$ égal à $(s-1)$, donc $h(x)$ s'écrit sous la forme

$$h(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots\ldots\ldots + \alpha_{s-1} x^{s-1} = \sum_{j=0}^{s-1} \alpha_j x^j$$

donc

$$\begin{aligned} g(x) &= \sqrt{a} + (x - \sqrt{a})^s \sum_{j=0}^{s-1} \alpha_j x^j \\ &= \sqrt{a} + \sum_{j=0}^{s} \beta_j x^j . \sum_{j=0}^{s-1} \alpha_j x^j \qquad , \ \beta_j = C_s^j (-1)^{s-j} (\sqrt{a})^{s-j} \\ &= \sqrt{a} + \sum_{j=0}^{2s-1} \theta_j x^j \end{aligned}$$

tel que $\theta_j = \sum_{i=0}^{j} \alpha_i \beta_{j-i}$ avec les conditions suivantes

$$\begin{cases} \alpha_i = 0 \ , \ \text{si } i \succ s-1 \\ \\ \beta_i = 0 \ , \ \text{si } i \succ s \end{cases} \tag{3.61}$$

donc

$$\begin{aligned} g(x) &= \sqrt{a}+\theta_0+\sum_{j=1}^{2s-2}\theta_j x^j+\theta_{2s-1}x^{2s-1} \quad , \theta_0=\alpha_0\beta_0 \\ &= (\sqrt{a}+\alpha_0\beta_0)+\sum_{j=1}^{2s-2}\theta_j x^j+\theta_{2s-1}x^{2s-1} \quad , \beta_0=(-1)^s(\sqrt{a})^s \\ &= (\sqrt{a}+\alpha_0(-1)^s(\sqrt{a})^s)+\sum_{j=1}^{2s-2}\theta_j x^j+\theta_{2s-1}x^{2s-1} \end{aligned}$$

on obtient

$$g(x)=(\sqrt{a}+\alpha_0(-1)^s(\sqrt{a})^s)+\sum_{j=1}^{2s-2}\left(\sum_{i=0}^{j}\alpha_i C_s^{j-i}(-1)^{s-j+i}(\sqrt{a})^{s-j+i}\right)x^j+\left(\sum_{i=0}^{2s-1}\alpha_i\beta_{2s-1-i}\right)x^{2s-1}$$

on a

$$\theta_{2s-1}=\sum_{i=0}^{2s-1}\alpha_i\beta_{2s-1-i}=\sum_{i=0}^{s-1}\alpha_i\beta_{2s-1-i}+\sum_{i=s}^{2s-1}\alpha_i\beta_{2s-1-i}$$

et comme $\forall i \geq s : \alpha_i = 0$, alors

$$\begin{cases} \sum_{i=s}^{2s-1}\alpha_i\beta_{2s-1-i}=0 \\ \theta_{2s-1}=\sum_{i=0}^{s-1}\alpha_i\beta_{2s-1-i} \end{cases}$$

d'autre part, on a

$$0 \leq i \leq s-1 \Longrightarrow s \leq 2s-1-i \leq 2s-1$$

et comme $\forall i \succ s : \beta_i = 0$, alors

$$\begin{cases} \forall s \prec 2s-1-i \leq 2s-1 : \beta_{2s-1-i}=0 \\ \beta_{2s-1-i} \neq 0 \quad , \text{si } 2s-1-i=s \end{cases}$$

on obtient

$$\beta_{2s-1-i} \neq 0 \text{ si } i=s-1$$

par conséquent

$$\theta_{2s-1}=\sum_{i=0}^{s-1}\alpha_i\beta_{2s-1-i}=\sum_{i=0}^{s-2}\alpha_i\beta_{2s-1-i}+\alpha_{s-1}\beta_s=0+\alpha_{s-1}\beta_s$$

donc

$$\theta_{2s-1} = \alpha_{s-1}\beta_s = \alpha_{s-1} \quad , \ \beta_s = 1$$

on trouve

$$g(x) = (\sqrt{a} + \alpha_0(-1)^s(\sqrt{a})^s) + \sum_{j=1}^{2s-2}\left(\sum_{i=0}^{j}\alpha_i C_s^{j-i}(-1)^{s-j+i}(\sqrt{a})^{s-j+i}\right)x^j + \alpha_{s-1}x^{2s-1}$$

la fonction $g(x)$ s'écrit sous la forme

$$g(x) = \sum_{j=0}^{2s-1} c_j(\sqrt{a}, \alpha_i)x^j \quad , 0 \leq i \leq s-1$$

tels que

$$c_j(\sqrt{a}, \alpha_i) = \begin{cases} \sqrt{a} + \alpha_0(-1)^s(\sqrt{a})^s & , \text{si } j = 0 \\ \sum_{i=0}^{j}\alpha_i\left(C_s^{j-i}(-1)^{s-j+i}(\sqrt{a})^{s-j+i}\right) & , \text{si } 1 \leq j \leq 2s-2 \\ \alpha_{s-1} & , \text{si } j = 2s-1 \end{cases} \quad , 0 \leq i \leq s-1$$

avec les conditions (3.61).

Par conséquent, pour généraliser la méthode du point fixe, autrement dit pour accéléré l'ordre de convergence de la suite $(x_n)_n$ autant qu'on veut, il faut résoudre le système linéaire (3.62) qui nous donne les valeurs de α_i

$$\begin{cases} c_0(\sqrt{a}, \alpha_0) = 0 \\ c_2(\sqrt{a}, \alpha_i) = 0 \\ \qquad\qquad\qquad\qquad , \ i = \overline{0, s-1} \\ c_{2j}(\sqrt{a}, \alpha_i) = 0 \end{cases} \tag{3.62}$$

équivaut à

$$\begin{cases} \sqrt{a} + (-1)^s(\sqrt{a})^s\alpha_0 = 0 \ , \ \text{si } j = 0 \\ \left(\sum_{i=0}^{j}\alpha_i\left(C_s^{j-i}(-1)^{s-j+i}(\sqrt{a})^{s-j+i}\right)\right)_{1\leq 2j\leq 2s-1} = 0 \end{cases} , i = \overline{0, s-1}$$

autrement dit les coefficients d'ordre pairs de g doivent être nuls :

$$\forall i = \overline{0, s-1} : c_{2j}(\sqrt{a}, \alpha_i) = 0 \ , \ 0 \leq 2j \leq 2s-1 \tag{3.63}$$

on obtient

$$g(x) = c_1(a)x + c_3(a)x^3 + \ldots\ldots\ldots\ldots + c_{2s-1}(a)x^{2s-1} \qquad (3.64)$$

Conclusion Générale

1- Pour l'inverse d'un nombre p-adique :

1. Pour trouver l'inverse d'un nombre p-adique $a \in \mathbb{Q}_p^*$ il suffit de trouver l'inverse d'un entier p-adique $u \in \mathbb{Z}_p^*$ en suite, on le multiple par p^{-m}.
2. Pour déterminer le code de Hensel de l'inverse d'un nombres p-adique $a \in \mathbb{Q}_p^*$ il suffit de trouver le code de Hensel de $u \in \mathbb{Z}_p^*$ (ie : sur le bord du $D(0,1)$) en suite en change le point p-adique soit m fois à gauche si, soit $(-m)$ fois à droite.

2- Pour la racine carrée d'un nombre p-adique :

1. Pour trouver la racine carrée d'un nombre p-adique $a \in \mathbb{Q}_p^*$, il suffit de trouver la racine carrée d'un entier p-adique unitaire $u \in \mathbb{Z}_p^*$ en suite, on le multiple :
   Soit par $p^{-(2^{n+1}-1).m}$ ou bien par $p^{-(2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1).m}$.
2. La détermination du code de Hensel de la racine carrée d'un nombre p-adique $a \in \mathbb{Q}_p^*$ passe à travers la détermination de code de Hensel d'un entier p-adique unitaire $u \in \mathbb{Z}_p^*$ puis :
   (a) En change le point p-adique soit $((2^{n+1}-1)m)$ fois à gauche ou bien $(-(2^{n+1}-1)m)$ fois à droite.
   (b) En change le point p-adique soit $(2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1)m$ fois à gauche ou bien $(-(2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1)m)$ fois à droite.
3. Pour trouver la racine carrée d'un nombre 2-adique $a \in \mathbb{Q}_2^*$, il suffit de trouver la racine carrée d'un nombre 2-adique appartient à la frantière du $D(0,4) \subset \mathbb{Q}_2^*$ (ie : sur $\Gamma D(0,4)$) en suite, on le multiple
   soit par $2^{-(2^{n+1}-1)(m+1)}$ ou bien par $2^{-(2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1)(m+1)}$.
4. La détermination du code de Hensel de la racine carrée d'un nombre 2-adique $a \in \mathbb{Q}_2^*$ passe à travers la détermination de code de Hensel de la racine carrée d'un nombre 2-adique appartient à la frantière du $D(0,4) \subset \mathbb{Q}_2$ puis :

(a) En change le point 2-adique soit $(2^{n+1}-1)(m+1)$ fois à gauche ou bien $-(2^{n+1}-1)(m+1)$ fois à droite.

(b) En change le point 2-adique soit $(2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1)(m+1)$ fois à gauche ou bien $-(2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1)(m+1)$ fois à droite.

Bibliographie

[1] Ankusha Vimawala. P-adic Arithmetic Methods for Exact Computation of Rational Numbers, School of Electrical Engineering and Computer Science, Oregon State University. June 2003

[2] Amice Y, Les nombres p-adiques, Presses universitaires de france (1975).

[3] Abhijit Das, P-adic Numbers, chapter 6. Departement of mathematics. Indian Institute Of Technology, Kanpur, India.

[4] Baker A.J, An Introduction to p-adic Numbers and p-adic Analysis, Department of Mathematics, University of Glasgow, Glasgow G12 8QW, Scotland [14/06/2004]
URL :http ://www.maths.gla.ac.uk/Najb.
home.iitk.ac.in/~abhijit/course/MTH617/SS02/chap6.ps

[5] Bertin Diarra. Analyse p-adique. Cours DEA- Algèbre Commutative FAST- Université du Mali. Décembre 1999- Mars 2000

[6] Carla Limongelli, Roberto Pirastu. Exact Solution of Linear Equation Systems over Rational Numbers By Parallel P-adic Arithmetic, March 22, 1994. RISC-LINZ Report Series No. 94-25

[7] C. k. Koc. A Tutorial on P-adic Arithmetic, Electrical and Computer Engineering. Oregon State University, Corvallis, Oregon 97331. Technical Report, April 2002.

[8] C. J. Zarowski and Howard. C. Card. On addition and multiplication with Hensel codes. IEEE Transactions on Computers, Vol 39, No, (12) :1417–1423, December 1990.

[9] Emmanuel Jeandel. Suites récurrentes linéaires. Le point de vue informatique. ENS Lyon.
www.ens-lyon.fr/LIP/MC2/files/ejeandel.pdf

[10] F. Bernis, A. Liné, P. Poncet, Y.Sir. Analyse Numériques I, chapitre 3, Equation non linéaires, Villedieu -2004-2005

[11] Fredrik Bajers. Vej. P-adic Numbers. Aalborg University. Departement Of Mathematical Sciences. 7E 9222 Aalborg Øst. Groupe E3-104, 18-12-2000.

[12] Gouvea, F.Q. P-adic numbers : An introduction, Second Edition. New York : Springer-Verlag, 1997.
URL :http ://books.google.fr/

[13] H.D. Ebbinghaus, H. Hermes, F. Hirzebruch, M. Koecher, K. Lamotke, K. Mainzen, J. Neukirch, A. Prestel & R. Remment,Les nombres, leurs histoire, leur place et leur role de l'antiguité aux recherches actuelles. Springer- Verlag Berlin Heidelberg 1983,1988,1992.

[14] J.P.Bézévin. Dynamique des fractions rationnels p-adiques 23 mai 2005. www.math.unicaen.fr/~bezivin/dealatex.pdf

[15] J.Collingwood, S. Marion, M. Mazowita, P-adic Numbers padic.mathstat.uottawa.ca/~MAT3166/reports/p-adic.pdf

[16] Jan E .Holly. Pictures of Ultra metric Spaces, the p-adic Numbers, and Valued Fields

[17] Katok S, Real and p-adic analysis, Course notes for Math 497C, Mass Program, Fall 2000 (2001).

[18] Koblitz Neal, p-adic Numbers, p-adic Analysis and Zeta Functions, Springer-Verlag (1984).

[19] Michael Knapp, Christos Xenophotos. Numerical analysis meets number theory : using rootfinding methods to calculate inverses mod p^n. Mathematical Sciences Departement. Loyola College 4510 N. Charles Street, Baltimore, MD 21210- June 17, 2004.

[20] Madore D.A., A first introduction to p-adic numbers, (2000), URL :http ://www.eleves.ens.fr/home/madore/maths.

[21] Murty M.R., Introduction to p-adic analytic numbers theory, Lecture notes at Mehta research institue on p-adic, URL :http ://www.mri.ernet.in/~mathweb/lecture/murty-padic00/.

[22] Rodrigàñez C.C., P-adic Numbers and non-archimedean valuation, URL :http ://www.sunall.mat.ucm.es.

[23] Robert T.Georgy and Edayathumangalam V. Krishnamurthy. Methods and appications of Error-Free computation. Springer Verlag, 1984.

[24] Schikhof W.H., Ultrametric calculus, An introduction to p-adic analysis, Combridge university press (1984).

[25] V.S. Valdmirov, I.V. Volovich, E.I. Zelenov. P-adic Analysis and Mathematical Physics, Seteklov Mathematical Institue Russia. Vol 1

[26] Vincent Lefèvre. Les Brenoms. Janvier 1994
www.vinc17.org/math/brenoms.pdf

ملخص

خلال هذا البحث قمنا بتحديد خوارزميات لحساب الجذور التربيعية (حساب الأرقام الأولى لنشر هنسال - رموز هنسال-) لعدد $a \in Q_p^*$ بالطرق العددية الكلاسيكية نيوتن، سيكونت، النقطة الثابتة و هذا من خلال حساب الحل التقريبي لصفر تابع معرفة على Q_p . و قمنا كذلك بتحديد سرعة التقارب، رموز هنسال و عدد التكرارات.

و قد قمنا كذلك بنفس العمل من اجل حساب مقلوب عدد $a \in Q_p^*$. في الأخير تحصلنا على النتائج التالية:

لإيجاد مقلوب العدد $a \in Q_p^*$ يكفي إيجاد مقلوب عدد صحيح $u \in Z^*_p$، ثم نضربه هذا الأخير في p^{-m}.

لإيجاد رموز هنسال لمقلوب العدد $a \in Q_p^*$ يكفي إيجاد رموز هنسال لمقلوب عدد صحيح $u \in Z^*_p$، ثم نقوم بسحب النقطة الـ p-adique اما m مرة إلى اليسار إذا كان $m \succ 0$ أو $(-m)$ مرة إلى اليمين إذا كان $m \prec 0$.

إذا كان $p \neq 2$ ، اذن لإيجاد الجذر التربيعي لعدد $a \in Q_p^*$ يكفي إيجاد الجذر التربيعي لعدد صحيح $u \in Z^*_p$، ثم نضربه هذا الأخير في $p^{-(2^{n+1}-1)m}$ أو في $p^{-\left(2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1\right)m}$.

لإيجاد رموز هنسال للجذر التربيعي لعدد $a \in Q_p^*$ يكفي إيجاد رموز هنسال للجذر التربيعي لعدد صحيح $u \in Z^*_p$، ثم نقوم بسحب النقطة الـ p-adique إما:

- $(2^{n+1}-1)m$ مرة إلى اليسار إذا كان $m \succ 0$ أو $-(2^{n+1}-1)m$ مرة إلى اليمين إذا كان $m \prec 0$.
- $\left(2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1\right)m$ مرة إلى اليسار إذا كان $m \succ 0$ أو $-\left(2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1\right)m$ مرة إلى اليمين إذا كان $m \prec 0$.

إذا كان $p = 2$ ، اذن لإيجاد الجذر التربيعي لعدد $a \in Q_2^*$ يكفي إيجاد الجذر التربيعي لعدد u ينتمي إلى حافة القرص $D(0,4) \subset Q_2^*$ ، بعد ذلك نقوم بضربه إما في $2^{-(2^{n+1}-1)(m+1)}$ أو في $2^{-\left(2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1\right)(m+1)}$.

لإيجاد رموز هنسال للجذر التربيعي لعدد $a \in Q_2^*$ يكفي إيجاد رموز هنسال للجذر التربيعي لعدد u ينتمي إلى حافة القرص $D(0,4) \subset Q_2^*$، ثم نقوم بسحب النقطة الـ 2-adique إما:

- $(2^{n+1}-1)(m+1)$ مرة إلى اليسار إذا كان $m \succ -1$ أو $-(2^{n+1}-1)(m+1)$ مرة إلى اليمين إذا كان $m \prec -1$.
- $\left(2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1\right)(m+1)$ مرة إلى اليسار إذا كان $m \succ -1$ أو $-\left(2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1\right)m$ مرة إلى اليمين إذا كان $m \prec -1$.

Abstract

In this work we determined some algorithms to calculate the square roots of p-adic numbers (Hensel codes) via the classical numerical methods Newton, Secant, fixed point and this through the calculation of the approached solution of the zero of a function defined on Q_p. We also determined the speed of convergence, the number of iteration and the Hensel's codes. We made the same work for the determination of the inverse of a p-adic number.

We found the following results:

To find the inverse of a p-adic number $a \in Q_p^*$, it is sufficient to find the inverse of a p-adic integer $u \in Z_p^*$, then we it multiple by p^{-m}.

To find the Hensel code of the inverse of a p-adic number $a \in Q_p^*$, it is sufficient to find the Hensel code for a p-adic integer $u \in Z_p^*$, then to change the p-adic point to the left m time if $m>0$ or (- m) time on the right if m <0.

If $p \neq 2$, then to find the square root of a p-adic number $a \in Q_p^*$, it is sufficient to find the square root of a p-adic integer $u \in Z_p^*$, next it multiple either by $p^{-(2^{n+1}-1)m}$ or by $p^{-\left(\left[\frac{2}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1\right)m}$.

The determination of the Hensel code of square root of p-adic number $a \in Q_p^*$ pass through the determination of the Hensel code of a p-adic integer $u \in Z_p^*$ then:

i) Move the point p-adic, either $(2^{n+1}-1)m$ time on the left if $m>0$, or $-(2^{n+1}-1)m$ time on the right if $m<0$.

ii) Move the point p-adic, either $\left(2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1\right)m$ time on the left if $m>0$, or $-\left(2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1\right)m$ time on the right if $m<0$.

If $p=2$, then to find the square root of a 2-adic number $a \in Q_2^*$, it is sufficient to find the square root of a 2-adic number u belongs to the border of $D(0,4) \subset Q_2^*$, after that it multiple either by $2^{-(2^{n+1}-1)(m+1)}$ or by $2^{-\left(2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1\right)(m+1)}$.

The determination of the Hensel code of square root of 2-adic number $a \in Q_2^*$ pass through the determination of the Hensel code of a 2-adic number u belongs to the border of $D(0,4) \subset Q_2^*$ then:

i) Move the point 2-adic, either $(2^{n+1}-1)(m+1)$ time on the left if $m>-1$, or $-(2^{n+1}-1)(m+1)$ time on the right if $m<-1$.

ii) Move the point 2-adic, either $\left(2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1\right)(m+1)$ time on the left if $m>-1$, or $-\left(2\left[\frac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1\right)(m+1)$ time on the right if $m<-1$.