Applicable Analysis and Discrete Mathematics
available online at http://pefmath.etf.rs

Appl. Anal. Discrete Math. **4** (2010), 32–44. doi:10.2298/AADM1000009M

HENSEL CODES OF SQUARE ROOTS OF *P*-ADIC NUMBERS

Zerzaihi Tahar, Kecies Mohamed, Michael Knapp

In this work we are concerned with the calculation of the Hensel codes of square roots of p-adic numbers, using the fixed point method and this through the calculation of the approached solution of $f(x) = x^2 - a = 0$ in $\mathbb{Q}_p$. We also determine the speed of convergence and the number of iterations.

1. INTRODUCTION

The knowledge of the arithmetic and algebraic properties of the p-adic numbers is useful to the study of their Diophantine properties and the problems of approximations. In this present paper we will see how we can use classical root-finding methods (fixed point) and explore a very interesting application of tools from numerical analysis to number theory. We use this method to calculate the zero of a p-adic continuous function f defined on a domain $D \subset \mathbb{Q}_p$, where

$$\begin{aligned} f \ &: \ \mathbb{Q}_p \to \mathbb{Q}_p \\ x \ &\mapsto f(x). \end{aligned}$$

To calculate the square root of a p-adic number $a \in \mathbb{Q}_p^*$, one studies the following problem

$$\left\{ \begin{array}{l} f(x) = x^2 - a = 0 \\ a \in \mathbb{Q}_p^*, \ \ p - \text{prime number}. \end{array} \right. \tag{1}$$

Our goal is to calculate the Hensel code of $\sqrt{a}$, which means to determine the first numbers of the p-adic development of the solution of the previous equation,

2000 Mathematics Subject Classification. 26E30. 34K28.
Keywords and Phrases. P-adic number, square root, Hensel code, fixed point, speed of convergence.

and this solution is approached by a sequence of the p-adic numbers $(x_n)_n \subset \mathbb{Q}_p^*$ constructed by the fixed point method. We first encountered this idea in [**4**] where the authors used the numerical methods to find the reciprocal of an integer modulo p^n (see [**4**] for more details).

We are grateful to Dr. Henry Alex Esbelin (Laboratoire d'Algorithmique et Image de Clermont-Ferrand) for suggesting this topic to us, and also for several helpful conversations.

2. PRELIMINARIES

Definition 2.1. *Let p be a prime number. The field of p-adic numbers $\mathbb{Q}_p$ is defined as the completion of the field of rational numbers with respect to the p-adic metric determined by the p-adic norm. Thus, $\mathbb{Q}_p$ is obtained from the p-adic norm in the same way as the real field $\mathbb{R}$ is obtained from the usual absolute value as the completion of $\mathbb{Q}$.*
Here, the function $|\cdot|_p$ is called the p-adic norm and is defined by

$$\forall x \in \mathbb{Q}_p : |x|_p = \begin{cases} p^{-v_p(x)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0, \end{cases}$$

and v_p is the p-adic valuation defined by $v_p(x) = \max\{r \in \mathbb{Z} : p^r \mid x\}$. The p-adic distance d_p is defined by

$$\begin{array}{rcl} d_p & : & \mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{R}^+ \cup \{0\} \\ (x,y) & \mapsto & d_p(x,y) = |x-y|_p . \end{array}$$

Theorem 2.2. *Every p-adic number $a \in \mathbb{Q}_p$ has a unique p-adic expansion*

$$a = \lambda_n p^n + \lambda_{n+1} p^{n+1} + \cdots + \lambda_{-1} p^{-1} + \lambda_0 + \lambda_1 p + \lambda_2 p^2 + \cdots = \sum_{k=n}^{\infty} \lambda_k p^k$$

with $\lambda_k \in \mathbb{Z}$ and $0 \leq \lambda_k \leq p-1$ for each $k \geq n$.

The short representation of a is $\lambda_n \lambda_{n+1} \ldots \lambda_{-1} \cdot \lambda_0 \lambda_1 \ldots$, where only the coefficients of the powers of p are shown. We can use the p-adic point $\cdot$ as a device for displaying the sign of n as follows:

$$\begin{array}{rl} \lambda_n \lambda_{n+1} \ldots \lambda_{-1} \cdot \lambda_0 \lambda_1 \ldots & \text{for } n < 0 \\ \cdot \lambda_0 \lambda_1 \ldots & \text{for } n = 0 \\ \cdot 00 \ldots 0 \lambda_0 \lambda_1 \ldots & \text{for } n > 0 . \end{array}$$

Definition 2.3. *A p-adic number $a \in \mathbb{Q}_p$ is said to be a p-adic integer if this canonical development contains only non negative powers of p. The set of p-adic* *integers is denoted by* $\mathbb{Z}_p$*. So we have*

$$\mathbb{Z}_p = \left\{ \sum_{k=0}^{\infty} \lambda_k p^k, 0 \leq \lambda_k \leq p-1 \right\} = \left\{ a \in \mathbb{Q}_p : |a|_p \leq 1 \right\}.$$

Definition 2.4. *A p-adic integer* $a \in \mathbb{Z}_p$ *is said to be a p-adic unit if the first digit* λ_0 *in the p-adic development is different from zero. The set of p-adic units is denoted by* $\mathbb{Z}_p^*$*. Hence we have*

$$\mathbb{Z}_p^* = \left\{ \sum_{k=0}^{\infty} \lambda_k p^k, \lambda_0 \neq 0 \right\} = \left\{ a \in \mathbb{Q}_p : |a|_p = 1 \right\}.$$

Proposition 2.5. *Let a be a p-adic number. Then a can be written as the product* $a = p^n \cdot u, n \in \mathbb{Z}, u \in \mathbb{Z}_p^*$*.*

Definition 2.6. *Let p be a prime number. Then the Hensel code of length M of any p-adic number* $a = p^m \cdot u \in \mathbb{Q}_p$ *is the pair* $(\mathrm{mant}_a, \exp_a)$*, where the left most M digits and the value m of the related p-adic development are called the mantissa and the exponent, respectively. We use the notation* $H(p, M, a)$ *where p is a prime and M is the integer which specifies the number of digits of the p-adic development. One writes*

$$H(p, M, a) = (a_m a_{m+1} \ldots \cdot a_0 a_1 \ldots a_t, m),$$

where $M = |m| + t + 1$*.*

See also [**1**] for more general results concerning the Hensel code.

Lemma 2.7. (Hensel's Lemma) *Let*

$$F(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n$$

be a polynomial whose coefficients are p-adic integers. Let

$$F^{'}(x) = c_1 + 2c_2 x + \cdots + nc_n x^{n-1}$$

be the derivative of $F(x)$*. Suppose* $\overline{a}_0$ *is a p-adic integer which satisfies* $F(\overline{a}_0) \equiv 0 \pmod{p}$ *and* $F^{'}(\overline{a}_0) \not\equiv 0 \pmod{p}$*. Then there exists a unique p-adic integer a such that* $F(a) = 0$ *and* $a \equiv \overline{a}_0 \pmod{p}$*.*

Proof. For the proof of this result we refer the reader to [**5**]. □

The following theorem makes an important connection between p-adic numbers and congruences.

Theorem 2.8. *A polynomial with integer coefficients has a root in* $\mathbb{Z}_p$ *if and only if it has an integer root modulo* p^k *for every* $k \geq 1$*.*

Proof. For the proof see [**5**]. □

A practical consequence of Theorem 2.8 is the following.

Proposition 2.9. *A rational integer a not divisible by p has a square root in $\mathbb{Z}_p$ $(p \neq 2)$ if and only if a is a quadratic residue modulo p.*

Proof. Let $P(x) = x^2 - a$. Then $P^{'}(x) = 2x$. If a is a quadratic residue, then

$$a \equiv a_0^2 \pmod p$$

for some $a_0 \in \{0, 1, 2, \ldots, p-1\}$. Hence $P(a_0) \equiv 0 \pmod p$. But

$$P'(a_0) = 2a_0 \not\equiv 0 \pmod p$$

automatically since $(a_0, p) = 1$, so that the solution in $\mathbb{Z}_p$ exists by Hensel's lemma. Conversely, if a is a quadratic nonresidue, by Theorem 2.8 it has no square root in $\mathbb{Z}_p$. □

This can actually be extended to

Corollary 2.10. *Let $p \neq 2$ be a prime. An element $x \in \mathbb{Q}_p$ is a square if and only if it can be written $x = p^{2n}y^2$ with $n \in \mathbb{Z}$ and $y \in \mathbb{Z}_p^*$ a p-adic unit.*

Proof. For the proof of this result we refer the reader to [**3**]. □

3. MAIN RESULTS

Let $a \in \mathbb{Q}_p^*$ be a p-adic number such that

$$|a|_p = p^{-v_p(a)} = p^{-2m}\ , m \in \mathbb{Z}.$$

If $(x_n)_n$ is a sequence of p-adic numbers that converges to a p-adic number $\alpha \neq 0$, then from a certain rank one has

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

We also know that if there exists a p-adic number α such that $\alpha^2 = a$, then $v_p(a)$ is even and

$$|x_n|_p = |\alpha|_p = p^{-m}.$$

3.1 Fixed point method

To use the fixed point method we study the zeros of the equation $f(x) = 0$ by studying a related equation $x = g(x)$, with the condition that these two formulations are mathematically equivalent. To improve the speed of convergence of the sequence $(x_n)_n$, one defines a new sequence that converges more quickly toward the solution of the equation proposed. The conditions that permit the determination of the function $g(x)$ are:

1) $g(\sqrt{a}) = \sqrt{a}$, $g^{(1)}(\sqrt{a}) = \ldots = g^{(s-1)}(\sqrt{a}) = 0$, $g^{(s)}(\sqrt{a}) \neq 0$,

2) The polynomial $g(x)$ must not have the square root of a in its coefficients.

In order to choose $g(x)$, we know that if $\sqrt{a}$ is a root of order s of $(g(x) - \sqrt{a})$, then there is a polynomial $h(x)$ such that

$$g(x) = \sqrt{a} + (x - \sqrt{a})^s h(x). \tag{2}$$

The conditions that permit the determination of $h(x)$ are:
i. The polynomial $g(x)$ must not have $\sqrt{a}$ in its coefficients
ii. $h(x)$ depends upon the natural number s.

To determine the formula for $h(x)$, it is sufficient to work with the undetermined coefficients and to write the wanted conditions.
Let's consider the following cases.
Case 1: $s = 1$. We have

$$g(x) = \sqrt{a} + (x - \sqrt{a})h(x).$$

One chooses $h(x)$ in order to make the square roots of a in the coefficients of $g(x)$ disappear. For this, we put

$$h(x) = \alpha_0. \tag{3}$$

This gives $\alpha_0 = 1$ and

$$g(x) = x. \tag{4}$$

Case 2: $s = 2$. We have

$$g(x) = \sqrt{a} + (x - \sqrt{a})^2 h(x). \tag{5}$$

We put

$$h(x) = \alpha_0 + \alpha_1 x, \tag{6}$$

and get

$$\alpha_0 = -\frac{1}{a^{1/2}}\ ,\ \alpha_1 = -\frac{1}{2a}.$$

Then we have

$$h(x) = -\frac{1}{2a}\,(x + 2\sqrt{a}) \text{ and } g(x) = \frac{3}{2}\,x - \frac{1}{2a}\,x^3. \tag{7}$$

The sequence associated to $g(x)$ is defined by

$$\forall n \in \mathbb{N} : x_{n+1} = \frac{3}{2}\,x_n - \frac{1}{2a}\,x_n^3. \tag{8}$$

Theorem 3.1. *If x_{n_0} is the square root of a of order r, then*

1) *If* $p \neq 2$, *then* x_{n+n_0} *is the square root of* a *of order* $2^n r - 2(2^n - 1)m$.
2) *If* $p = 2$, *then* x_{n+n_0} *is the square root of* a *of order* $2^n r - 2(m+1)(2^n - 1)$.

Proof. Let $(x_n)_n$ the sequence defined by (8). Then

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

We put

$$\Omega(x) = -\frac{1}{4a^2}\left(4a - x^2\right).$$

Since

(10) $$|4|_p = \begin{cases} \frac{1}{4} & \text{if } p = 2 \\ 1 & \text{if } p \neq 2, \end{cases}$$

we have

$$\begin{aligned} |\Omega(x_{n_0})|_p &= \left|-\frac{1}{4a^2}\left(4a - x_{n_0}^2\right)\right|_p \\ &\leq \left|\frac{1}{4}\right|_p \cdot \left|\frac{1}{a^2}\right|_p \max\left\{|4a|_p, \left|x_{n_0}^2\right|_p\right\} \\ &\leq \begin{cases} p^{4m} \cdot \max\left\{p^{-2m}, p^{-2m}\right\} & \text{if } p \neq 2 \\ 2^2 \cdot 2^{4m} \max\left\{2^{-2} \cdot 2^{-2m}, 2^{-2m}\right\} & \text{if } p = 2 \end{cases} \\ &\leq \begin{cases} p^{2m} & \text{if } p \neq 2 \\ 2^{2m+2} & \text{if } p = 2. \end{cases} \end{aligned}$$

This gives

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

and so we have

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

Then

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

In this manner, we find that if $p \neq 2$, then

(11) $$\forall n \in \mathbb{N} : x_{n+n_0}^2 - a \equiv 0 \pmod{p^{\gamma_n}},$$

where the sequence $(\gamma_n)_n$ is defined by

$$\forall n \in \mathbb{N} : \gamma_n = 2^n r - 2(2^n - 1)m. \tag{12}$$

If $p = 2$, then

$$\forall n \in \mathbb{N} : x_{n+n_0}^2 - a \equiv 0 \pmod{2^{\gamma'_n}}, \tag{13}$$

where $(\gamma'_n)_n$ is defined by

$$\forall n \in \mathbb{N} : \gamma'_n = \gamma_n - 2(2^n - 1) = 2^n r - 2(m+1)(2^n - 1). \tag{14}$$

On the other hand, we have

$$\forall n \in \mathbb{N} : x_{n+1} - x_n = \left(-\frac{x_n}{2a}\right)\left(x_n^{\,2} - a\right). \tag{15}$$

Since

$$|2|_p = \begin{cases} \frac{1}{2} & \text{if } p = 2 \\ 1 & \text{if } p \neq 2, \end{cases} \tag{16}$$

we have

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

Hence we obtain

$$\begin{cases} |x_{n+n_0+1} - x_{n+n_0}|_p \leq p^{2m} \cdot p^{-m} \cdot p^{-\gamma_n} & \text{if } p \neq 2 \\ |x_{n+n_0+1} - x_{n+n_0}|_2 \leq 2 \cdot 2^{2m} \cdot 2^{-m} \cdot 2^{-\gamma'_n} & \text{if } p = 2, \end{cases}$$

and so

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

Therefore, if $p \neq 2$, then

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \pmod{p^{v_n}}, \tag{17}$$

where

$$\forall n \in \mathbb{N} : v_n = \gamma_n - m = 2^n r - (2^{n+1} - 1)m. \tag{18}$$

If $p = 2$, then

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \pmod{2^{v'_n}}, \tag{19}$$

where

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

Conclusion 3.2.

1. *If* $p \neq 2$, *then the following are true.*

   (a) *The speed of convergence of the sequence* $(x_n)_n$ *is the order* v_n.

   (b) *If* $r - 2m > 0$, *then the number of iterations to obtain* M *correct digits is*

$$n = \left[\frac{\ln\left(\frac{M-m}{r-2m}\right)}{\ln 2} \right] + 1. \tag{20}$$

   (c) *With Hensel codes the equation* (8) *takes the form*

$$\begin{aligned} H(p, 2^n r - (2^{n+1}-1)\cdot m, x) &= H(p, \infty, 3/2) \cdot H(p, 2^{n-1} r - (2^n - 1)\cdot m, x) \\ &\quad - H(p, \infty, 1/2) \cdot \frac{H^3(p, 2^{n-1} r - (2^n - 1)\cdot m, x)}{H^2(p, \infty, x)}. \end{aligned}$$

2. *If* $p = 2$, *then the following are true.*

   (a) *The speed of convergence of the sequence* $(x_n)_n$ *is the order* v'_n.

   (b) *If* $r - 2(m+1) > 0$, *then the necessary number* n *of iterations to obtain* M *correct digits is*

$$n = \left[\frac{\ln\left(\frac{M-(m+1)}{r-2(m+1)}\right)}{\ln 2} \right] + 1. \tag{21}$$

   (c) *With the Hensel codes the equation* (8) *takes the form*

$$\begin{aligned} &H(2, 2^n r - (2^{n+1}-1)\cdot(m+1), x) \\ &\qquad = H(2, \infty, 3/2) \cdot H(2, 2^{n-1} r - (2^n - 1)\cdot(m+1), x) \\ &\qquad - H(2, \infty, 1/2) \cdot \frac{H^3(2, 2^{n-1} r - (2^n - 1)\cdot(m+1), x)}{H^2(2, \infty, x)}. \end{aligned}$$

Let's consider for $p \neq 2$ the sets defined by

$$\begin{cases} S_1 = \left\{ a \in \mathbb{Q}_p : |a|_p = 1 \right\} & \text{if } m = 0 \\ S_2 = \left\{ a \in \mathbb{Q}_p : |a|_p < 1 \right\} & \text{if } m > 0 \\ S_3 = \left\{ a \in \mathbb{Q}_p : |a|_p > 1 \right\} & \text{if } m < 0. \end{cases} \tag{22}$$

We put

$$\forall n \in \mathbb{N} : \begin{cases} v_n^{(1)} = 2^n r & \text{if } m = 0 \\ v_n^{(2)} = 2^n r - (2^{n+1} - 1)m & \text{if } m > 0 \\ v_n^{(3)} = 2^n r - (2^{n+1} - 1)m & \text{if } m < 0. \end{cases} \tag{23}$$

For $p = 2$, we consider the sets defined by

$$\text{(24)} \qquad \begin{cases} B_1 = \{a \in \mathbb{Q}_2 : |a|_2 = 4\} & \text{if } m = -1 \\ B_2 = \{a \in \mathbb{Q}_2 : |a|_2 < 4\} & \text{if } m > -1 \\ B_3 = \{a \in \mathbb{Q}_2 : |a|_2 > 4\} & \text{if } m < -1. \end{cases}$$

We put

$$\text{(25)} \qquad \forall n \in \mathbb{N} : \begin{cases} v_n'^{(1)} = 2^n r & \text{if } m = -1 \\ v_n'^{(2)} = 2^n r - (2^{n+1} - 1)(m+1) & \text{if } m > -1 \\ v_n'^{(3)} = 2^n r - (2^{n+1} - 1)(m+1) & \text{if } m < -1. \end{cases}$$

Then we have the following corollary.

Corollary 3.3.

1. *If* $p \neq 2$, *then we have the following.*

(a) *If* $m = 0$, *then we have quadratic convergence for all the p-adic numbers which belong to the set* S_1.

(b) *If* $m < 0$, *then the speed of convergence is faster for all the p-adic numbers which belong to the set* S_3.

(c) *If* $m > 0$, *then the speed of convergence is slower for all the p-adic numbers which belong to the set* S_2.

2. *If* $p = 2$, *then we have the following.*

(a) *If* $m = -1$, *then one has quadratic convergence for all the* 2*-adic numbers which belong to* B_1.

(b) *If* $m < -1$, *then the speed of convergence is faster for all the* 2*-adic numbers which belong to the set* B_3.

(c) *If* $m > -1$, *then the speed of convergence is slower for all the* 2*-adic numbers which belong to the set* B_2.

Case 3: $s = 3$. We put

$$\text{(26)} \qquad \begin{cases} g(x) = \sqrt{a} + (x - \sqrt{a})^3 h(x) \\ \\ h(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2. \end{cases}$$

One finds that

$$\text{(27)} \qquad \begin{cases} h(x) = \dfrac{1}{a} + \dfrac{9}{8a\sqrt{a}}\, x + \dfrac{3}{8a^2}\, x^2 \\ \\ g(x) = \dfrac{15}{8}\, x - \dfrac{5}{4a}\, x^3 + \dfrac{3}{8a^2}\, x^5. \end{cases}$$

The sequence associated to $g(x)$ is defined by

$$\forall n \in \mathbb{N} : x_{n+1} = \frac{3}{8a^2}\, x_n^{\,5} - \frac{5}{4a}\, x_n^{\,3} + \frac{15}{8}\, x_n. \tag{28}$$

Let $(x_n)_n$ the sequence defined by (28). Then

$$\forall n \in \mathbb{N} : x_{n+1}^2 - a = \left(a - x_n^{\,2}\right)^3 \left(-\frac{1}{a^2} + \frac{33}{64a^3}\, x_n^{\,2} - \frac{9}{64a^4}\, x_n^{\,4} \right). \tag{29}$$

Theorem 3.4. *If x_{n_0} is the square root of a of order r, then the following are true.*
1) If $p \neq 2$, then x_{n+n_0} is the square root of a of order $3^n r - 2(3^n - 1)m$.
2) If $p = 2$, then x_{n+n_0} is the square root of a of order $3^n r - (3^n - 1)(2m + 3)$.

Proof. For the proof of this theorem, we use the method that we applied in the case where $s = 2$. □

From this theorem, we get that if $p \neq 2$, then

$$\forall n \in \mathbb{N} : x_{n+n_0}^2 - a \equiv 0 \pmod{p^{\pi_n}}, \tag{30}$$

where $(\pi_n)_n$ is defined by

$$\forall n \in \mathbb{N} : \pi_n = 3^n r - 2(3^n - 1)m. \tag{31}$$

If $p = 2$, then

$$\forall n \in \mathbb{N} : x_{n+n_0}^2 - a \equiv 0 \pmod{2^{\pi'_n}}, \tag{32}$$

where $(\pi'_n)_n$ is given by

$$\forall n \in \mathbb{N} : \pi'_n = 3^n r - (3^n - 1)(2m + 3). \tag{33}$$

On the other hand, we have

$$\forall n \in \mathbb{N} : x_{n+1} - x_n = \left(a - x_n^{\,2}\right) \left(\frac{7}{8a}\, x_n - \frac{3}{8a^2}\, x_n^3 \right). \tag{34}$$

Then if $p \neq 2$, we have

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \pmod{p^{\Sigma_n}}, \tag{35}$$

where $(\Sigma_n)_n$ is defined by

$$\forall n \in \mathbb{N} : \Sigma_n = 3^n r - (2 \cdot 3^n - 1)m. \tag{36}$$

If $p = 2$, then

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \pmod{2^{\Sigma'_n}}, \tag{37}$$

with

$$\forall n \in \mathbb{N} : \Sigma'_n = 3^n r - \left((2 \cdot 3^n - 1)m + 3^{n+1}\right). \tag{38}$$

Conclusion 3.5.

1. *If $p \neq 2$, then the following are true.*

(a) *The speed of convergence of the sequence $(x_n)_n$ is the order Σ_n.*

(b) *If $r - 2m > 0$, then the number n of necessary iterations to obtain M correct digits is*

$$n = \left[\frac{\ln\left(\frac{M-m}{r-2m}\right)}{\ln 3} \right] + 1. \tag{39}$$

(c) *With Hensel codes the equation* (28) *takes the form*

$$\begin{aligned} &H(p, 3^n r - (2 \cdot 3^n - 1) \cdot m, x) \\ &\qquad = H(p, \infty, 3/8) \cdot \frac{H^5(p, 3^{n-1}r - (2 \cdot 3^{n-1} - 1) \cdot m, x)}{H^4(p, \infty, x)} \\ &\qquad + H(p, \infty, -5/4) \cdot \frac{H^3(p, 3^{n-1}r - (2 \cdot 3^{n-1} - 1) \cdot m, x)}{H^2(p, \infty, x)} \\ &\qquad + H(p, \infty, 15/8) \cdot H(p, 3^{n-1}r - (2 \cdot 3^{n-1} - 1) \cdot m, x). \end{aligned}$$

2. *If $p = 2$, then the following are true.*

(a) *The speed of convergence of the sequence $(x_n)_n$ is the order Σ'_n.*

(b) *If $r - (2m + 3) > 0$, then the necessary number of iterations to obtain M correct digits is*

$$n = \left[\frac{\ln\left(\frac{M-m}{r-(2m+3)}\right)}{\ln 3} \right] + 1. \tag{40}$$

(c) *With Hensel codes the equation* (28) *takes the form*

$$\begin{aligned} &H(2, 3^n r - \left((2 \cdot 3^n - 1) \cdot m + 3^{n+1}\right), x) \\ &\qquad = H(2, \infty, 3/8) \cdot \frac{H^5(2, 3^{n-1}r - \left((2 \cdot 3^{n-1} - 1) \cdot m + 3^n\right), x)}{H^4(2, \infty, x)} \\ &\qquad + H(2, \infty, -5/4) \cdot \frac{H^3(2, 3^{n-1}r - \left((2 \cdot 3^{n-1} - 1) \cdot m + 3^n\right), x)}{H^2(2, \infty, x)} \\ &\qquad + H(2, \infty, 15/8) \cdot H(2, 3^{n-1}r - \left((2 \cdot 3^{n-1} - 1) \cdot m + 3^n\right), x). \end{aligned}$$

3.2 Generalization

Generally we can construct an iterative method that converges to $\sqrt{a}$ with a higher convergence rate. To accelerate the rate of convergence of the sequence $(x_n)_n$ as much as one wants, it is necessary to solve the problem of letting

$$g(x) = \sqrt{a} + (x - \sqrt{a})^s h(x, \sqrt{a}) \tag{41}$$

and choosing the function $h(x, \sqrt{a})$ in order to make the square roots of a in coefficients of a function $g(x)$ disappear. We take the degree of the function $h(x)$ equal to $s - 1$, giving

$$h(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_{s-1} x^{s-1} = \sum_{j=0}^{s-1} \alpha_j x^j. \tag{42}$$

Then

$$g(x) = \sqrt{a} + (x - \sqrt{a})^s (\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_{s-1} x^{s-1}) = \sum_{j=0}^{2s-1} c_j(\alpha_i, \sqrt{a}) x^j, \tag{43}$$

where, if $i \in \{0, \ldots, s-1\}$,

$$c_j(\alpha_i, \sqrt{a}) = \begin{cases} \sqrt{a} + (-1)^s (\sqrt{a})^s \alpha_0, & \text{if } j = 0 \\ \sum_{i=0}^{j} \alpha_i \binom{s}{j-i} (-1)^{s-j+i} (\sqrt{a})^{s-j+i}, & \text{if } j \in \{1, \ldots, 2s-2\} \\ \alpha_{s-1}, & \text{if } j = 2s-1, \end{cases} \tag{44}$$

and

$$\alpha_i = 0, \quad \forall i > s - 1. \tag{45}$$

To generalize the fixed point method it is necessary that the coefficients of the even powers of x are equal to zero and according to the different calculations that we made, we suppose that this condition is also sufficient until a certain s sufficiently large, i.e

$$\forall j \in \{0, \ldots, s-1\} : \{c_{2k}\}_{k \in \{0,\ldots,j\}} = \{0\} \Leftrightarrow \sqrt{a} \notin \{c_{2k+1}\}_{k \in \{0,\ldots,j\}}. \tag{46}$$

Therefore, to determine $(\alpha_i)_{i \in \{0,\ldots,s-1\}}$ for any s, it is sufficient to solve the following linear system

$$\begin{cases} c_0 = \sqrt{a} + (-1)^s (\sqrt{a})^s \alpha_0 = 0 \\ c_2(\alpha_i, \sqrt{a}) = 0 \\ c_4(\alpha_i, \sqrt{a}) = 0 \\ \quad\vdots \\ c_{2s-2}(\alpha_i, \sqrt{a}) = 0. \end{cases}, \ 0 \leq i \leq s-1 \tag{47}$$

We get

$$g(x) = c_1(a)x + c_3(a)x^3 + \ldots + c_{2s-1}(a)x^{2s-1}. \tag{48}$$

REFERENCES

1. C. K. Koc: *A Tutorial on P-adic Arithmetic.* Electrical and Computer Engineering. Oregon State University, Corvallis, Oregon 97331. Technical Report, April 2002.
2. F. B. Vej: *P-adic Numbers.* Aalborg University, Department Of Mathematical Sciences. 7E 9222 Aalborg Øst. Groupe E3-104, 18-12-2000.
3. F.Q. Gouvêa: *P-adic Numbers: An Introduction.* Second Edition. New York: Springer-Verlag, 1997.
4. M. Knapp, C. Xenophotos: *Numerical analysis meets number theory: using rootfinding methods to calculate inverses* mod p^n. Appl. Anal. Discrete Math., **4** (2010), 23–31.
5. S. Katok: *Real and p-adic analysis, Course notes for Math* 497C. Department of Mathematics, The Pennsylvania State University, Mass Program, Fall 2000 revised, November (2001).

Laboratoire de mathématiques pures et appliquées,
BP 98 Ouled Aissa, Université de Jijel,
Algeria
E-mails: zerzaihi@yahoo.com
kecmohamed@yahoo.fr

(Received September 10, 2009)

Department of Mathematical Sciences,
Loyola University Maryland,
4501 N. Charles Street,
Baltimore, MD 21210,
USA
E-mail: mpknapp@loyola.edu