MALAYA JOURNAL OF MATEMATIK
Malaya J. Mat. **09(02)**(2021), 28–38.
http://doi.org/10.26637/mjm0902/004

The performance of the secant method in the field of p-adic numbers

KECIES MOHAMED*[1]

[1] *Laboratoire LMPEA, Université de Jijel, Jijel, Algeria.*

Received 12 January 2021; Accepted 28 March 2021

Abstract. In this paper, we compute the square roots of p-adic numbers in $\mathbb{Q}_p$, using the secant method. We also study the performance of this method: the speed of its convergence and the number of iterations necessary to obtain the desired precision M which represents the number of p-adic digits in the development of $\sqrt{a}$.

AMS Subject Classifications: 26E30, 11E95, 34K28.

Keywords: p-adic numbers, square roots, secant method, hensel's lemma, speed of convergence.

Contents

1. Introduction and Background

For a few hundred years theoretical physics has been developed on the basis of real and, later, complex numbers. This mathematical model of physical reality survived even in the process of the transition from classical to quantum physics, complex numbers became more important than real, but not essentially more so than in the Fourier analysis which was already being used, e.g., in classical electrodynamics and acoustics. However, in the last 20 years the field of p-adic numbers $\mathbb{Q}_p$ (as well as its algebraic extensions, including the field of complex p-adic numbers $\mathbb{C}_p$) has been intensively used in theoretical and mathematical physics. Thus, notwithstanding the fact that p-adic numbers were only discovered by K. Hensel around the end of the nineteenth century, the theory of p-adic numbers has already penetrated intensively into several areas of mathematics and its applications.

For each prime p, we will get a new field called the field of p-adic numbers denoted by $\mathbb{Q}_p$. These fields will be constructed in a manner analogous to the way the real number system $\mathbb{R}$ is constructed from $\mathbb{Q}$ (see [1, 4, 6, 7]). The p-adic numbers can be used to consider and study congruences modulo p and modulo p^n and have many applications in classical number theory.

The root-finding problem is one of the most important computational problems. It arises in a wide variety of practical applications in physics, chemistry, biosciences, engineering, etc. As a matter of fact, determination of any unknown appearing implicitly in scientific or engineering formulas gives rise to a root-finding problem. The

*Corresponding author. Email address: **m.kecies@centre-univ-mila.dz** (Kecies Mohamed)

Root-Finding Problem is the problem of finding a root of the equation $f(x)=0$, where f is a function of a single variable x. Specifically, the problem is stated as follows: Given a function f. Find a number $x=\alpha$ such that $f(\alpha)=0$.

Except for some very special functions, it is not possible to find an analytical expression for the root, from where the solution can be exactly determined. Thus, most computational methods for the root-finding problem have to be iterative in nature. Two important aspects of an iterative method are convergence and stopping criterion.

The idea behind an iterative method is the following: Starting with an initial approximation x_0, construct a sequence of iterates $(x_n)_n$ using an iteration formula with a hope that this sequence converges to a root of $f(x)=0$.

In this present paper we will see how we can use classical root-finding method (secant method) and explore a very interesting application of tools from numerical analysis to number theory. We use this method to calculate the zero noted α of a p-adic continuous function f defined on $\mathbb{Q}_p$. The number α represents the square root of a p-adic number $a\in\mathbb{Q}_p^*$.

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

$$f(x)=x^2-a=0, a\in\mathbb{Q}_p^*. \tag{1.1}$$

Our goal is to calculate the first numbers of the p-adic development of the solution of the previous equation, and this solution is approached by a sequence of the p-adic numbers $(x_n)_n\subset\mathbb{Q}_p$ constructed by the secant method.

In fact, several studies have been made with regards to finding square roots and cubic roots of p-adic numbers. In 2010, for instance, Knapp and Xenophontos [12] showed how classical root-finding methods from numerical analysis can be used to calculate inverses of units modulo prime powers. In the same year, Zerzaihi, Kecies and Knapp [15] applied some classical root-finding methods, such as the fixed-point method, in finding square roots of p-adic numbers through Hensel's lemma. In 2011, Zerzaihi and Kecies [13] used secant method to find the cubic roots of p-adic numbers. These authors [14] then applied the Newton method to find the cubic roots of p-adic numbers in $\mathbb{Q}_p$. A similar problem also appeared in [8] wherein Ignacio et al. computed the square roots of p-adic numbers via Newton-Raphson method.

The paper is organized as follows. The next section recalls several concepts about $\mathbb{Q}_p$ which will be used through the paper. Our main contribution is formally stated and proved in section 3. The paper ends with conclusions and final remarks.

2. Preliminaries

Definition 2.1. *Let p be a prime number. We define the p-adic valuation $v_p(\cdot)$ of a rational number $x\in\mathbb{Q}$ by the following definition:*
(i) *If $x\in\mathbb{Z}^*$, then $v_p(x)$ is equal to the highest power of p which divides x.*
(ii) *If $x=\frac{a}{b}\in\mathbb{Q}^*$, then $v_p(x)=v_p(a)-v_p(b)$. The $p-$adic valuation of $x\in\mathbb{Q}$ is also called the p-adic order and denoted as $ord(x)$.*
(iii) *We set $v_p(0)=+\infty$. The reason to set $v_p(0)=+\infty$ is that we can divide 0 by p^n for each $n\in\mathbb{N}$.*

Definition 2.2. *Let the function $|\cdot|_p:\mathbb{Q}\longrightarrow\mathbb{R}$ be defined as*

$$|x|_p=\begin{cases} p^{-v_p(x)}, & \textit{if } x\neq 0,\\ \\ 0, & \textit{if } x=0.\end{cases} \tag{2.1}$$

$|\cdot|_p$ *is called the p-adic norm on $\mathbb{Q}$.*

Remark 2.3.
$1)$ *The p-adic norm satisfies the non-archimedean property*

$$|x+y|_p\leq\max\left\{|x|_p,|y|_p\right\} \textit{ for all } x,y\in\mathbb{Q}, \tag{2.2}$$

and we say that the p-adic norm is ultra-metric or non-archimedean.
2) *An important property of the p-adic norm is the discreteness of its image. It is clear that the function $|\cdot|_p$ takes its values in a discrete subset of $\mathbb{R}^+$(namely $\{0\} \cup \{p^n, n \in \mathbb{Z}\}$).*

Since for any prime p the p-adic norm is a norm hence it defines a p-adic distance function on $\mathbb{Q}$ given by

Definition 2.4. *The p-adic norm induces a metric $d_p : \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{R}^+$ given by*

$$d_p(x,y) = |x-y|_p \textit{ for all } x, y \in \mathbb{Q}, \tag{2.3}$$

this metric is called the p-adic metric.

Further since the p-adic norm is non-archimedean it follows that the p-adic distance function is an ultrametric and satisfies

$$d_p(x,y) \leq \max\{d_p(x,z), d_p(z,y)\} \text{ for all } x, y, z \in \mathbb{Q}. \tag{2.4}$$

Definition 2.5. *For each prime p, the normed field $\mathbb{Q}_p$ of p-adic numbers is the completion of the field of rational numbers $\mathbb{Q}$ with respect to the p-adic norm $|\cdot|_p$ which contains the rational numbers $\mathbb{Q}$ as a dense subset. The norm on $\mathbb{Q}_p$ induced by the p-adic norm on $\mathbb{Q}$, will be considered an extension of the p-adic norm, and will therefore also be denoted by $|\cdot|_p$. Further each of these fields is distinct from the real numbers $\mathbb{R}$ and for different primes p_1, p_2 the fields are distinct.*

Remark 2.6. *The elements of $\mathbb{Q}_p$ are equivalent classes of Cauchy sequences in $\mathbb{Q}$ with respect to the extension of the p-adic norm. For some $x \in \mathbb{Q}_p$, let $(x_n)_n$ be a Cauchy sequence of rational numbers representing a. Then by definition*

$$|x|_p = \lim_{n \longrightarrow +\infty} |x_n|_p \,. \tag{2.5}$$

Proposition 2.7. *[2] Let p be a fixed prime and $\mathbb{Q}_p$ the field of p-adic numbers. Given $x \in \mathbb{Q}_p$, there exists a unique sequence of integers $(\beta_N)_{n \geq N}$, with $N = v_p(x)$, such that $0 \leq \beta_n \leq p-1$ for all n and*

$$x = \beta_N p^N + \beta_{N+1} p^{N+1} + ... + \beta_n p^n + ... = \sum_{k=N}^{\infty} \beta_k p^k. \tag{2.6}$$

Remark 2.8.
1) *The representation* (2.6) *is called the canonical p-adic expansion of p-adic number x.*
2) *There is a one-to-one correspondence between the power series expansion*

$$\beta_N p^N + \beta_{N+1} p^{N+1} + ... + \beta_n p^n + ... \tag{2.7}$$

and the short representation $\beta_N \beta_{N+1} \beta_{N+2}...$, where only the coefficients of the powers of p are shown. We can use the p-adic point as a device for displaying the sign of N.

$$\begin{array}{ll} \beta_N \beta_{N+1} \beta_{N+2} ... \beta_{-2} \beta_{-1} \cdot \beta_0 \beta_1 \beta_2 ... & \textit{for } N < 0, \\ \cdot \beta_0 \beta_1 \beta_2 ... & \textit{for } N = 0, \\ \cdot 000...0 \beta_0 \beta_1 \beta_2 ... & \textit{for } N > 0. \end{array} \tag{2.8}$$

The most important fact has already been noted: $\mathbb{Q}_p$ is a complete metric space, hence every Cauchy sequence converges. Cauchy sequences are characterized as follows

Theorem 2.9. *[10] A sequence (a_n) in $\mathbb{Q}_p$ is a Cauchy sequence, and therefore convergent, if and only if it satisfies*

$$\lim_{n \longrightarrow +\infty} |a_{n+1} - a_n|_p = 0. \tag{2.9}$$

The following result is an important tool for determining whether a series of p-adic numbers converge in $\mathbb{Q}_p$ or not.

Proposition 2.10. *[10] A series $\sum\limits_{n=0}^{\infty} a_n$ with $a_n \in \mathbb{Q}_p$ converges in $\mathbb{Q}_p$ if and only if $\lim\limits_{n \longrightarrow +\infty} a_n = 0$, in which case*

$$\left| \sum_{n=0}^{\infty} a_n \right|_p \leq \max_n |a_n|_p . \tag{2.10}$$

Definition 2.11. *A p-adic number $x \in \mathbb{Q}_p$ is a p-adic integer if its p-adic norm is less than or equal to 1, $|x|_p \leq 1$. We denote the set of p-adic integers by $\mathbb{Z}_p$ and hence*

$$\mathbb{Z}_p = \left\{ x \in \mathbb{Q}_p : |x|_p \leq 1 \right\} . \tag{2.11}$$

Lemma 2.12. *[6] A p-adic number $x \in \mathbb{Q}_p$ is a p-adic integer if and only if its canonical expansion has only positive powers of p. That is*

$$\mathbb{Z}_p = \left\{ x \in \mathbb{Q}_p : x = \sum_{n=0}^{\infty} \beta_n p^n \right\} . \tag{2.12}$$

The p-adic integers form a subring of $\mathbb{Q}_p$ which contains $\mathbb{Z}$.

Recall that a unit in a ring R with identity is an element which has amultiplicative inverse. In the rational integers $\mathbb{Z}$ the only units are $\{-1, 1\}$. The situation is quite different in $\mathbb{Z}_p$ where there are many units and in fact every rational integer m relatively prime to p is invertible.

Definition 2.13. *A p-adic integer $x \in \mathbb{Z}_p$ is said to be a p-adic unit (or invertible) if the first digit β_0 in the p-adic p-adic expansion is different from zero. The set of p-adic units is denoted by $\mathbb{Z}_p^{\times}$ or $U(\mathbb{Z}_p)$. Hence we have*

$$\mathbb{Z}_p^{\times} = \left\{ x = \sum_{n=0}^{\infty} \beta_n p^n : \beta_0 \neq 0 \right\} . \tag{2.13}$$

It is also easy to see that

$$\mathbb{Z}_p^{\times} = \left\{ x \in \mathbb{Z}_p : |x|_p = 1 \right\} . \tag{2.14}$$

$\mathbb{Z}_p^{\times}$ is also called the group of p-adic units.

The next result shows that any element of $\mathbb{Q}_p$ is a product of an invertible p-adic integer and a power of p.

Proposition 2.14. *[10] Let x be a p-adic number of norm p^{-n}. Then x can be written as the product $x = p^n u$, where $u \in \mathbb{Z}_p^{\times}$.*

The following result is very useful for our work.

Proposition 2.15. *[10] We say that a and $b \in \mathbb{Q}_p$ are congruent mod p^n and write $a \equiv b \mod p^n$ if and only if $|a - b|_p \leq \frac{1}{p^n}$.*

Proposition 2.16. *[1] Let $(x_n)_n$ be a p-adic number sequence. If*

$$\lim_{n \longrightarrow +\infty} x_n = x, x \in \mathbb{Q}_p, |x|_p \neq 0,$$

then the sequence of norms $\left\{ |x_n|_p : n \in \mathbb{N} \right\}$ must stabilize for sufficiently large n, i.e., there exists N such that

$$|x_n|_p = |x|_p , \forall n \geq N. \tag{2.15}$$

The following proposition is modestly known as Hensel's lemma.

Theorem 2.17. *[3] (Hensel's Lemma, first form). Let $F(x) \in \mathbb{Z}_p[x]$ be a p-adic polynomial and assume there exists $\alpha_0 \in \mathbb{Z}_p$ such that $F(\alpha_0) \equiv 0 \mod p$ but $F'(\alpha_0) \not\equiv 0 \mod p$. Then there exists a unique $\alpha \in \mathbb{Z}_p$ such that $F(\alpha) = 0$ and $\alpha \equiv \alpha_0 \mod p$.*

Sometimes the stated Hensel's lemma is not enough and one should use its generalization:

Theorem 2.18. *[3] (Hensel's Lemma, strong form). Let $F(x) \in \mathbb{Z}_p[x]$ be a p-adic polynomial and assume there exists $\alpha_0 \in \mathbb{Z}_p$ such that $F(\alpha_0) \equiv 0 \mod p^{2k+1}$ but $F'(\alpha_0) \not\equiv 0 \mod p^{k+1}$. Then there exists a unique $\alpha \in \mathbb{Z}_p$ such that $F(\alpha) = 0$ and $\alpha \equiv \alpha_0 \mod p^{k+1}$.*

Actually Hensel's lemma is valid for any complete nonarchimedian field.

As an application of the Hensel's lemma, we investigate the squares in $\mathbb{Q}_p$.

Proposition 2.19. *Let p be a prime number, then*
$1)$ If $p \neq 2$, then a p-adic number $a \in \mathbb{Q}_p^*$ is a square if and only if $a = p^{2n}v^2$ for some $n \in \mathbb{Z}$ and $v \in \mathbb{Z}_p^{\times}$.
$2)$ If $p = 2$, then a 2-adic number $a \in \mathbb{Q}_2^*$ is a square if and only if $a = 2^{2n}v^2 = 2^{2n}u$ for some $n \in \mathbb{Z}$ and $u \equiv 1 \mod 8$.

Now, we are ready to give our main results.

3. Main Results

Solving non linear equations is one of the most important and challenging problems in science and engineering applications. The root finding problem is one of the most relevant computational problems. It arises in a wide variety of practical applications in Physics, Chemistry, Biosciences, Engineering, etc.

The Newton-Raphson method, or Newton Method, is a powerful technique for solving a nonlinear equations $f(x) = 0$ numerically. We start with an initial approximation x_0 and generate a sequence of approximations $(x_n)_n$ through the iterative formula

$$\forall n \in \mathbb{N} : x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}. \tag{3.1}$$

A major disadvantage of the Newton Method is the requirement of finding the value of the derivative of $f'(x)$ at each approximation, which may not be practical for some choices of f. When the derivative of $f(x)$ is either hard or impossible to write down (and hence, to program), or when the computational effort required to evaluate $f'(x)$ is very large compared to that for $f(x)$, Newton method is impossible or costly to carry out. An alternative is to approximate the derivative by a finite difference, that is, to write

$$f'(x_n) \approx \frac{f(x_n) - f(x_{n-1})}{x_n - x_{n-1}}. \tag{3.2}$$

The approximate Newton iteration can then be expressed in the following algorithm

$$\forall n \in \mathbb{N}^* : x_{n+1} = x_n - \frac{f(x_n)(x_n - x_{n-1})}{f(x_n) - f(x_{n-1})}. \tag{3.3}$$

This iteration is called the secant method because $f(x)$ is approximated by a secant line through two points on the graph of f, rather than a tangent line through one point on the graph. In the secant method, we always use x_n and x_{n-1} to generate x_{n+1}.

We also study the performance of the secant method. The performance of the method is estimated by:

$a)$ The speed of convergence which is an important factor of the quality of the algorithms, if the speed of convergence is high, the algorithm converges quickly and the computation time is less. To measure the speed of convergence, we study the evolution of the sequence $(e_n)_n$ defined by

$$e_n = x_{n+n_0+1} - x_{n+n_0}. \tag{3.4}$$

with $n_0 \in \mathbb{N}$. Roughly speaking, if the rate of convergence of a method is s, then after each iteration the number of correct significant digits in the approximation increases by a factor of approximately s.

$b)$ The number of iterations necessary to obtain the desired precision M which represents the number of p-adic digits in the development of $\sqrt{a}$. So, it's all about finding n such that

$$|x_{n+n_0+1} - x_{n+n_0}|_p \leq p^{-M}, \tag{3.5}$$

this is equivalent to

$$v_p(e_n) \geq p^M. \tag{3.6}$$

The general principle of calculation is as follows,
Let $a \in \mathbb{Q}_p^*$ a p-adic number such that

$$|a|_p = p^{-v_p(a)} = p^{-2m}, m \in \mathbb{Z}, \tag{3.7}$$

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

$$|x_n|_p = |\alpha|_p = p^{-m}. \tag{3.8}$$

We consider the following equation

$$f(x) = x^2 - a. \tag{3.9}$$

Then, the iteration of the secant method associated with the function f is written in the form

$$\forall n \in \mathbb{N}^* : x_{n+1} = \frac{x_n x_{n-1} + a}{x_n + x_{n-1}}. \tag{3.10}$$

The performance of the Secant method is given by the following theorem.

Theorem 3.1. *If x_{n_0-1} is the square root of a of order α and x_{n_0} is the square root of a of order β, then*
$1)$ *If $p \neq 2$, then x_{n+n_0-1} is the square root of a of order π_n, where the sequence $(\pi_n)_n$ is defined by, for all $n \in \mathbb{N}$*

$$\begin{aligned}\pi_n = &\left(\tfrac{1}{\sqrt{5}}\left(\beta - \alpha(1-\Phi)\right)\Phi^n + \tfrac{1}{\sqrt{5}}\left(-\beta + \alpha\Phi\right)(1-\Phi)^n\right) \\ &-2\left(\left(\tfrac{1}{\sqrt{5}}\left(\Phi^{n+1} - (1-\Phi)^{n+1}\right)\right) - 1\right)m.\end{aligned} \tag{3.11}$$

Furthermore

$$\forall n \in \mathbb{N} : x_{n+n_0} - x_{n+n_0-1} \equiv 0 \mod p^{\eta_n}, \tag{3.12}$$

such as

$$\forall n \in \mathbb{N} : \eta_n = \pi_n - m. \tag{3.13}$$

Where $\Phi = \frac{1+\sqrt{5}}{2}$ is the golden ratio.
$2)$ *If $p = 2$, then x_{n+n_0-1} is the square root of a of order π'_n, where the sequence $(\pi'_n)_n$ is defined by, for all $n \in \mathbb{N}$*

$$\pi'_n = \pi_n - 2\left(\left(\frac{1}{\sqrt{5}}\left(\Phi^{n+1} - (1-\Phi)^{n+1}\right)\right) - 1\right). \tag{3.14}$$

Furthermore

$$\forall n \in \mathbb{N} : x_{n+n_0} - x_{n+n_0-1} \equiv 0 \mod 2^{\eta'_n}, \tag{3.15}$$

such as

$$\forall n \in \mathbb{N} : \eta'_n = \pi'_n - (m+1). \tag{3.16}$$

Proof. Let $(x_n)_n$ be the sequence defined by (3.10). We have

$$\forall n \in \mathbb{N}^* : x_{n+1}^2 - a = \frac{(x_n^2 - a)(x_{n-1}^2 - a)}{(x_n + x_{n-1})^2}. \tag{3.17}$$

We assume that x_{n_0-1} (resp: x_{n_0}) is the square root of a of order α (resp: β), i.e,

$$\begin{cases} x_{n_0-1}^2 \equiv a \mod p^{\alpha}, \alpha \in \mathbb{N}, \\ x_{n_0}^2 \equiv a \mod p^{\beta}, \beta \in \mathbb{N}. \end{cases}$$

Then

$$\begin{cases} v_p\left(x_{n_0-1}^2 - a\right) \geq \alpha, \\ v_p\left(x_{n_0}^2 - a\right) \geq \beta. \end{cases}$$

Hence we obtain

$$\begin{cases} \left|x_{n_0-1}^2 - a\right|_p \leq p^{-\alpha}, \\ \left|x_{n_0}^2 - a\right|_p \leq p^{-\beta}. \end{cases}$$

Therefore, using the proposition (2.16) , we get

$$\begin{aligned} \left|x_{n_0+1}^2 - a\right|_p &= \frac{\left|(x_{n_0}^2 - a)(x_{n_0-1}^2 - a)\right|_p}{\left|x_{n_0} + x_{n_0-1}\right|_p^2} \\ &= \frac{1}{|4|_p} \frac{\left|x_{n_0}^2 - a\right|_p \left|x_{n_0-1}^2 - a\right|_p}{p^{-2m}}. \end{aligned}$$

Since

$$|4|_p = \begin{cases} 1, \text{ if } p \neq 2, \\ \frac{1}{4}, \text{ if } p = 2. \end{cases} \tag{3.18}$$

We have

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

Consequently

$$\begin{cases} \left|x_{n_0+1}^2 - a\right|_p \leq p^{-(\alpha+\beta-2m)}, \text{ if } p \neq 2, \\ \left|x_{n_0+1}^2 - a\right|_2 \leq 2^{-(\alpha+\beta-2m-2)}, \text{ if } p \neq 2. \end{cases}$$

This gives

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

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

$$\forall n \in \mathbb{N} : x_{n+n_0-1}^2 - a \equiv 0 \mod p^{\pi_n}. \tag{3.19}$$

The sequence $(\pi_n)_n$ is defined by

$$\forall n \in \mathbb{N} : \pi_n = J_n - mA_n, \tag{3.20}$$

Such that $(J_n)_n$ and $(A_n)_n$ are two linear recurrence sequences defined by

$$\begin{cases} J_0 = \alpha, J_1 = \beta, \\ \forall n \in \mathbb{N}^* : J_{n+1} = J_{n-1} + J_n, \end{cases}, \tag{3.21}$$

and

$$\begin{cases} A_0 = A_1 = 0, \\ \forall n \in \mathbb{N}^* : A_{n+1} = A_{n-1} + A_n + 2. \end{cases} \tag{3.22}$$

The general terms of the sequences $(J_n)_n$ and $(A_n)_n$ are given respectively by

$$\forall n \in \mathbb{N} : J_n = \frac{1}{\sqrt{5}} (\beta - \alpha(1-\Phi)) \Phi^n + \frac{1}{\sqrt{5}} (-\beta + \alpha\Phi) (1-\Phi)^n. \tag{3.23}$$

and

$$\forall n \in \mathbb{N} : A_n = 2 \left(\left(\frac{1}{\sqrt{5}} \left(\Phi^{n+1} - (1-\Phi)^{n+1} \right) \right) - 1 \right). \tag{3.24}$$

We obtain, for all $n \in \mathbb{N}$

$$\begin{aligned} \pi_n = &\left(\tfrac{1}{\sqrt{5}} (\beta - \alpha(1-\Phi)) \Phi^n + \tfrac{1}{\sqrt{5}} (-\beta + \alpha\Phi) (1-\Phi)^n \right) \\ &-2 \left(\left(\tfrac{1}{\sqrt{5}} \left(\Phi^{n+1} - (1-\Phi)^{n+1} \right) \right) - 1 \right) m. \end{aligned} \tag{3.25}$$

Furthermore

$$v_p(x_{n+n_0-1}^2 - a) \geq \pi_n. \tag{3.26}$$

On the other hand, if $p = 2$, then

$$\forall n \in \mathbb{N} : x_{n+n_0-1}^2 - a \equiv 0 \mod 2^{\pi'_n}. \tag{3.27}$$

The sequence $(\pi'_n)_n$ is defined by

$$\forall n \in \mathbb{N} : \pi'_n = J_n - (m+1)A_n, \tag{3.28}$$

Then, for all $n \in \mathbb{N}$

$$\begin{aligned} \pi'_n = &\left(\tfrac{1}{\sqrt{5}} (\beta - \alpha(1-\Phi)) \Phi^n + \tfrac{1}{\sqrt{5}} (-\beta + \alpha\Phi) (1-\Phi)^n \right) \\ &-2 \left(\left(\tfrac{1}{\sqrt{5}} \left(\Phi^{n+1} - (1-\Phi)^{n+1} \right) \right) - 1 \right) (m+1). \end{aligned} \tag{3.29}$$

Therefore

$$\forall n \in \mathbb{N} : \pi'_n = \pi_n - 2 \left(\left(\frac{1}{\sqrt{5}} \left(\Phi^{n+1} - (1-\Phi)^{n+1} \right) \right) - 1 \right). \tag{3.30}$$

Furthermore

$$v_2(x_{n+n_0-1}^2 - a) \geq \pi'_n. \tag{3.31}$$

On the other hand, we have

$$\forall n \in \mathbb{N}^* : x_{n+1} - x_n = \frac{a - x_n^2}{x_n + x_{n-1}}. \tag{3.32}$$

Since

$$|2|_p = \begin{cases} 1, \text{ if } p \neq 2, \\ \\ \frac{1}{2}, \text{ if } p = 2. \end{cases} \tag{3.33}$$

We have

$$|x_{n+n_0} - x_{n+n_0-1}|_p = \frac{\left|a - x^2_{n+n_0-1}\right|_p}{|x_{n+n_0-1} + x_{n+n_0-2}|_p}, \tag{3.34}$$

Hence we obtain

$$\begin{cases} |x_{n+n_0} - x_{n+n_0-1}|_p \leq p^m p^{-\pi_n}, \text{ if } \ p \neq 2, \\ \\ |x_{n+n_0} - x_{n+n_0-1}|_2 \leq 22^m 2^{-\pi'_n}, \text{ if } \ p = 2. \end{cases} \tag{3.35}$$

and so

$$\begin{cases} x_{n+n_0} - x_{n+n_0-1} \equiv 0 \mod p^{\pi_n - m}, \text{ if } \ p \neq 2, \\ \\ x_{n+n_0} - x_{n+n_0-1} \equiv 0 \mod 2^{\pi'_n - (m+1)}, \text{ if } p = 2. \end{cases} \tag{3.36}$$

Therefore, if $p \neq 2$, then

$$\forall n \in \mathbb{N} : x_{n+n_0} - x_{n+n_0-1} \equiv 0 \mod p^{\eta_n}. \tag{3.37}$$

Where

$$\forall n \in \mathbb{N} : \eta_n = \pi_n - m. \tag{3.38}$$

Which give

$$v_p(x_{n+n_0} - x_{n+n_0-1}) \geq \eta_n. \tag{3.39}$$

If $p = 2$, then

$$\forall n \in \mathbb{N} : x_{n+n_0} - x_{n+n_0-1} \equiv 0 \mod 2^{\eta'_n}, \tag{3.40}$$

Where

$$\forall n \in \mathbb{N} : \eta'_n = \pi'_n - (m+1). \tag{3.41}$$

It's clear that

$$\forall n \in \mathbb{N} : \eta'_n = \eta_n - \left(2\left(\frac{1}{\sqrt{5}}\left(\Phi^{n+1} - (1-\Phi)^{n+1}\right)\right) - 1\right), \tag{3.42}$$

Which give

$$v_2(x_{n+n_0} - x_{n+n_0-1}) \geq \eta'_n. \tag{3.43}$$

This completes the proof. ■

The results obtained are presented here.

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

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

   (b) Since $|1 - \Phi| < 1$, then

   $$\eta_n \simeq \frac{1}{\sqrt{5}}\left(\beta - \alpha(1-\Phi)\right)\Phi^n - \frac{2}{\sqrt{5}}(\Phi^{n+1} - 1)m, \tag{3.44}$$

   and if $(\beta - \alpha(1-\Phi) - 2\Phi m) > 0$, then the number of iterations n to obtain M correct digits is

   $$n = \left[\frac{\ln\left(\frac{\sqrt{5}(M-m)}{\beta - \alpha(1-\Phi) - 2\Phi m}\right)}{\ln \Phi}\right]. \tag{3.45}$$

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

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

   (b) If $\beta - \alpha(1-\Phi) - 2\Phi(m+1) > 0$, then the number of iterations n to obtain M correct digits is

$$n = \left[\frac{\ln\left(\frac{\sqrt{5}(M-(m+1))}{\beta-\alpha(1-\Phi)-2\Phi(m+1)}\right)}{\ln\Phi} \right]. \tag{3.46}$$

According to the results obtained in this section, we conclude the following corollary.

Corollary 3.2. *The order of convergence of the secant method is given by the positive number* $\Phi = \frac{1+\sqrt{5}}{2}$ *(superlinear order of convergence), this means the number of correct digits increases by a factor of approximately* Φ.

4. Conclusions

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

$$\begin{aligned} S_1 &= \left\{a \in \mathbb{Q}_p : |a|_p = 1\right\} \text{ if } m = 0,\\ S_2 &= \left\{a \in \mathbb{Q}_p : |a|_p < 1\right\} \text{ if } m > 0,\\ S_3 &= \left\{a \in \mathbb{Q}_p : |a|_p > 1\right\} \text{ if } m < 0. \end{aligned} \tag{4.1}$$

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

$$\begin{aligned} B_1 &= \{a \in \mathbb{Q}_2 : |a|_2 = 4\} \text{ if } m = -1,\\ B_2 &= \{a \in \mathbb{Q}_2 : |a|_2 < 4\} \text{ if } m > -1,\\ B_3 &= \{a \in \mathbb{Q}_2 : |a|_2 > 4\} \text{ if } m < -1. \end{aligned} \tag{4.2}$$

Then we have the following conclusion.

1. If $m < 0$, then the convergence for any p-adic number (Resp: 2-adic) belongs to the set S_3 (Resp: B_3) is faster than that of S_1 (Resp: B_1).

2. If $m > 0$, then the speed of convergence for any p-adic number (Resp: 2-adic) belongs to the set S_2 (Resp: B_2) is slower than that of S_1 (Resp: B_1).

5. Acknowledgement

We are grateful to Dr. Bertin Diarra (Laboratoire de Mathématiques, UMR 6620 - Université Blaise Pascal, Complexe Scientifique des Cézeaux- 63 177 Aubière Cedex, France) for several helpful conversations and also to Kecies Bouchra Nada. We thank both referees for their careful reading which allows us to improve the presentation of the paper.

References

[1] S. Albeverio, A.Y. Khrennikov and V.M. Shelkovich, *Theory of p-adic Distributions: Linear and Nonlinear Models*, Cambridge University Press, 2010.

[2] F.V. Bajers, *p-adic Numbers*, Aalborg University, Department of Mathematical Sciences, 2000.

[3] Y.F. Bilu, *p-adic Numbers and Diophantine Equations*, University of Bordeaux, 2013.

[4] W.A. Coppel, *Number Theory: An Introduction to Mathematics*, Springer Science & Business Media, 2009.

[5] J.F. Epperson, *An Introduction to Numerical Methods and Analysis*, John Wiley & Sons, 2013.

[6] B. Fine and G. Rosenberger, *Number Theory: An Introduction via the Density of Primes*, Birkhäuser, 2016.

[7] F.Q. Gouvea, *p-adic Numbers: An Introduction*, Springer Science & Business Media, 2012.

[8] P.S.P. Ignacio, J.M. Addawe, W.V. Alangui and J.A Nable, Computation of square and cube roots of p-adic numbers via Newton-Raphson method, *J*.M.R., **5**(2013), 31–38.

[9] A. Quarteroni, R. Sacco and F. Saleri, *Méthodes Numériques: Algorithmes, analyse et applications*, Springer Science & Business Media, 2008.

[10] S. Katok, *p-adic Analysis Compared with Real*, Vol. 37, American Mathematical Soc, 2007.

[11] C.k. Koç, *A Tutorial on p-adic Arithmetic*, Electrical and Computer Engineering, Oregon State University, Corvallis, Oregon 97331, 2002.

[12] M.P. Knapp and C. Xenophontos, Numerical Analysis meets Number Theory: Using root finding methods to calculate inverses $\mod p^n$, *Appl. Anal. Discrete Math.,* **4**(2010), 23–31.

[13] T. Zerzaihi and M. Kecies, Computation of the cubic root of a p-adic number, *J*ournal of Mathematics Research, **3**(2011), 40–47.

[14] T. Zerzaihi and M. Kecies, General approach of the root of a p-adic number, *F*ilomat, **27**(2013), 431–436.

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