MALAYA JOURNAL OF MATEMATIK
Malaya J. Mat. **10(01)**(2022), 36–46.
http://doi.org/10.26637/mjm1001/003

Householder's method for solving the p-adic polynomial equations

KECIES MOHAMED*[1]

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

Received 10 July 2021; Accepted 02 December 2021

Abstract. This work offers an analogue of Householder's Method for solving a root-finding problem $f(x) = 0$ in the p-adic setting. We apply this method to calculate the square roots of a p-adic number $a \in \mathbb{Q}_p$ where p is a prime number, and through the calculation of the approached solution of the p-adic polynomial equation $f(x) = x^2 - a = 0$. We establish the rate of convergence of this method. Finally, we also determine how many iterations are needed to obtain a specified number of correct digits in the approximate.

AMS Subject Classifications: 26E30, 11E95, 65H04.

Keywords: p-adic number, square roots, Householder iterative method, Hensel's lemma, rate of convergence.

Contents

1. Introduction and Background

Given a prime number p, the field of p-adic numbers $\mathbb{Q}_p$ were first introduced by Kurt Hensel at the end of the 19th century in a short paper written in German [8], which can be thought of as the completion of the field of rationals $\mathbb{Q}$ with respect to the p-adic norm, similar to how one constructs the field of real numbers $\mathbb{R}$ from $\mathbb{Q}$ (see [1], [3], [5], [6]). The p-adic numbers are useful because they provide another toolset for solving problems, one which is sometimes easier to work with than the real numbers. They have applications in number theory, analysis, algebra, and more. For about a century after the discovery of p-adic numbers, they were mainly considered as objects of pure mathematics. However, numerous applications of these numbers to theoretical physics have been proposed, to quantum mechanics, to p-adic - valued physical observables and many others. The field of p-adic numbers $\mathbb{Q}_p$ endowed with a metric d_p generated by p-adic valuation is also a fundamental example in the theory of ultrametric spaces. Nevertheless, many metric properties of the space $(\mathbb{Q}_p, d_p)$ remain unexplored now.

Finding the approximate solution of the nonlinear equation $f(x) = 0$ is one of the basic problems and frequently occurs in scientific work of various fields. Due to the higher order of the equation and the involvement of the transcendental functions, analytical methods for obtaining the exact root cannot be employed and therefore, it is only possible to obtain approximate solutions by relying on numerical methods based on iteration procedure [4], [15]. If we come across a problem that the function f is not known explicitly or the derivatives of the function are difficult to compute, then a method that uses only computed values of the function is more appropriate.

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

In fact, there are some results of the existence of square and cubic roots of p-adic numbers. For instance, in [13], the authors demonstrated how classical root-finding methods from numerical analysis can be employed to compute the multiplicative inverses of integers modulo $p^n, n \in \mathbb{N}$. A similar problem was addressed by Zerzaihi, Kecies, and Knapp [21] by using the fixed point iteration to compute the Hensel codes of square roots p-adic numbers. In [19] and [20] Zerzaihi and Kecies then extended the root-finding problem to the cube roots in $\mathbb{Q}_p$ of p-adic numbers by approximating the zeroes of $g(x) = x^3 - a, a \in \mathbb{Q}_p$, using the secant and Newton method. A related study was also carried out in [14] where Kecies considered the problem of finding the square roots of p-adic numbers in $\mathbb{Q}_p$ through the secant method. A similar problem also appeared in [11] wherein Ignacio et al. computed the square and cube roots of p-adic numbers via Newton-Raphson method.

Lately, a series of investigations explored the problem of finding square roots and the q-th roots of p-adic numbers. For instance, in [2], the authors proposed an analogue of Steffensen's method in finding roots of a general p-adic polynomial equation $f(x) = 0$ in $\mathbb{Z}_p$. Meanwhile, in [17], the author described an analogue of Halley's method for approximating roots of p-adic polynomial equations $f(x) = 0$ in $\mathbb{Z}_p$. A related study which examines a p-adic analogue of Olver's method was also considered in [16]. On the other hand, In [10], the authors gave the conditions for the existence of the q-th roots of p-adic numbers, and then applied the Newton-Raphson method to compute the q-th roots.

Our contribution in the present paper is to show how we can use classical root-finding method (Householder's method [9], [18]) to calculate the zero of a p-adic polynomial equation given by

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

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 Householder method.

The rest of 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, and a short concluding remark is given in the last section.

2. Preliminaries

Definition 2.1. *Fix a prime number $p \in \mathbb{Z}$. The p-adic valuation on $\mathbb{Z}$ is the function $v_p : \mathbb{Z} - \{0\} \longrightarrow \mathbb{R}$ defined as follows: for each integer $n \in \mathbb{Z}, n \neq 0$, let $v_p(n)$ be the unique positive integer satisfying*

$$n = p^{v_p(n)} n' \text{ with } p \nmid n'.$$

In other words, the p-adic valuation of n is the highest power of p that divides n.
We extend v_p to the field of rational numbers as follows: if $x = \frac{a}{b} \in \mathbb{Q}^*$, then

$$v_p(x) = v_p(a) - v_p(b).$$

Definition 2.2. *For any $x \in \mathbb{Q}$, we define the p-adic absolute value (or the p-adic norm) of x by*

$$|x|_p = p^{-v_p(x)},$$

if $x \neq 0$, and we set $|0|_p = 0$.
This norm satisfies the so called strong triangle inequality

$$|x+y|_p \leq \max\left\{|x|_p, |y|_p\right\} \text{ for all } x, y \in \mathbb{Q}, \tag{2.1}$$

and this is a non-Archimedean norm. The p-adic norm leads us to the p-adic metric on $\mathbb{Q}$ defined by

$$d_p(x,y) = |x-y|_p \text{ for all } x, y \in \mathbb{Q}. \tag{2.2}$$

We actually have something stronger than a metric. Thanks to the non-Archimedean property d_p is an ultrametric. Rather than the ordinary Triangle Inequality, d_p satisfies the Strong Triangle Inequality

$$d_p(x,y) \leq \max\{d_p(x,z), d_p(z,y)\} \text{ for all } x,y,z \in \mathbb{Q}. \tag{2.3}$$

We note that the range of the map $|\cdot|_p$ is the set $\{0\} \cup \{p^n : n \in \mathbb{Z}\}$ unlike the usual $|\cdot|_p$ on $\mathbb{R}$ whose values include all non-negative real numbers.

Definition 2.3. *For each prime p, the field of p-adic numbers denoted $\mathbb{Q}_p$ 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 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 x. Then by definition

$$|x|_p = \lim_{n \longrightarrow +\infty} |x_n|_p \,. \tag{2.4}$$

Each equivalence class of Cauchy sequences defining some element of $\mathbb{Q}_p$ contains a unique canonical representative Cauchy sequence. In order to describe its construction, we need the following theorem.

Theorem 2.4. *[7] Any p-adic number $\alpha \in \mathbb{Q}_p$ can be written in the form*

$$\alpha = \sum_{j=n}^{\infty} a_j p^j,$$

where each $a_j \in \mathbb{Z}$, and n is such that $|\alpha|_p = p^{-n}$. Moreover, if we choose each $a_j \in \{0,1,2,...,p-1\}$, then the expansion is unique. (In this case, the expansion is the canonical representation of α.)

Remark 2.5. *Notice that there is a one-to-one correspondence between the power series expansion*

$$\alpha = a_n p^n + a_{n+1} p^{n+1} + a_{n+2} p^{n+2} ... \tag{2.5}$$

and the abbreviated representation

$$\alpha = a_n a_{n+1} a_{n+2} ...$$

where only the coefficients of the powers of p are exhibited. Because of this correspondence we can use the power series expansion and the abbreviated representation interchangeably. In fact, we shall refer to each of them as the p-adic expansion for α. The abbreviated representation is completely analogous to the representation of the decimal expansion of a real number. In fact, we complete the analogy by introducing a p-adic point as a device for displaying the sign of n. Thus, we write

$$\alpha = \begin{cases} a_n a_{n+1} a_{n+2} ... a_{-2} a_{-1} \cdot a_0 a_1 a_2 ..., \text{ for } n < 0, \\ \cdot a_0 a_1 a_2 ..., \text{ for } n = 0, \\ \cdot 0 ... 0 a_n a_{n+1} ..., \text{ for } n > 0. \end{cases} \tag{2.6}$$

Definition 2.6.
(1) *A p-adic number is said to be a p-adic integer if its canonical expansion contains only nonnegative powers of p. The set of p-adic integers is denoted by $\mathbb{Z}_p$, so*

$$\mathbb{Z}_p = \left\{ x \in \mathbb{Q}_p : x = \sum_{j=0}^{\infty} a_j p^j \right\}. \tag{2.7}$$

It is easy to see that

$$\mathbb{Z}_p = \left\{ x \in \mathbb{Q}_p : |x|_p \leq 1 \right\}. \tag{2.8}$$

In other words, $\mathbb{Z}_p$ appears as the closed unit ball in $\mathbb{Q}_p$.
(2) *Any p-adic integer whose first digit is non-zero is called a p-adic unit. The set of p-adic units is denoted by $\mathbb{Z}_p^{\times}$. Hence we have*

$$\mathbb{Z}_p^{\times} = \left\{ x = \sum_{j=0}^{\infty} a_j p^j : a_0 \neq 0 \right\} = \left\{ x \in \mathbb{Z}_p : |x|_p = 1 \right\}, \tag{2.9}$$

meaning that the group of units of $\mathbb{Z}_p$ is then the unit sphere in $\mathbb{Q}_p$.

The following proposition follows at once from the definition of the p-adic norm and the p-adic unit.

Proposition 2.7. *[12] Let x be a p-adic number of norm p^{-n}. Then x can be written as the product $x = p^n u$, where $u \in \mathbb{Z}_p^{\times}$.*

According to the above definition 2.3, $\mathbb{Q}_p$ is a complete metric space, and, consequently, every Cauchy sequence converges. Cauchy sequences are characterized as follows.

Theorem 2.8. *[1] A sequence (a_n) in $\mathbb{Q}_p$ is a Cauchy sequence, and therefore convergent, if and only if it satisfies*

$$\lim_{n \longrightarrow +\infty} |a_{n+1} - a_n|_p = 0. \tag{2.10}$$

Now let us consider a numerical series $\sum\limits_{j=0}^{\infty} a_j, a_j \in \mathbb{Q}_p$. We say that this series converges if the sequence of its partial sums $s_n = \sum\limits_{j=0}^{n} a_j$ converges in $\mathbb{Q}_p$, and it converges absolutely if the series $\sum\limits_{j=0}^{\infty} |a_j|_p$ converges in $\mathbb{R}$. The following result is an important tool for determining whether a series of p-adic numbers converge in $\mathbb{Q}_p$ or not.

Proposition 2.9. *[1] 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*

$$\left| \sum_{n=0}^{\infty} a_n \right|_p \leq \max_n |a_n|_p. \tag{2.11}$$

Proposition 2.10. *[1] If*

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

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

$$|x_n|_p = |x|_p, \forall n \geq N. \tag{2.12}$$

For fixed primes p the p-adic numbers have many applications to ordinary number theory especially to solving congruences modulo p. Important in this regard is Hensel's Lemma. The lemma says that if a polynomial equation has a simple root modulo a prime number p, then this root corresponds to a unique root of the same equation modulo any higher power of p. This root can be found by iteratively lifting the solution modulo successive powers of p and is an analog of Newton's method. First, we define congruence in $\mathbb{Q}_p$.

Definition 2.11. *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 $|a-b|_p \leq p^{-n}$.*

Theorem 2.12. *[5] (Hensel's Lemma)*
Let $f(x) = c_0 + c_1 x + ... + c_n x^n$ be a polynomial in $\mathbb{Z}_p[x]$ (coefficients are p-adic integers). Let $f'(x)$ be the formal derivative of $f(x)$. Suppose $\bar{a}_0 \in \mathbb{Z}_p$ with $f(\bar{a}_0) \equiv 0 \mod p$ and $f'(\bar{a}_0) \not\equiv 0 \mod p$. Then, there exists a unique p-adic integer a such that $f(a) = 0$ and $a \equiv \bar{a}_0 \mod p$.

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

Corollary 2.13. *[6] 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 $y \in \mathbb{Z}_p^{\times}$ a p-adic unit.*

3. Main Results

Finding iterative methods for solving nonlinear equations is an important area of research in numerical analysis at it has interesting applications in several branches of pure and applied science can be studied in the general framework of the nonlinear equations $f(x) = 0$. Due to their importance, several numerical methods have been suggested and analyzed under certain condition. These numerical methods have been constructed using different techniques. It arises in a wide variety of practical applications in Physics, Chemistry, Biosciences, Engineering, etc.

Let us consider the nonlinear equation of the type

$$f(x) = 0. \tag{3.1}$$

For simplicity, we assume that r is a simple root of the equation (3.1) and x_0 is an initial guess sufficiently close to r. Using the Taylor's series expansion of the function f, we have

$$f(x_0) + (x - x_0)f'(x_0) + \frac{(x - x_0)^2}{2} f''(x_0) = 0. \tag{3.2}$$

First two terms of the equation (3.2) gives the first approximation, as

$$x = x_0 - \frac{f(x_0)}{f'(x_0)}. \tag{3.3}$$

This allows us to suggest the following one-step iterative method for solving the nonlinear equation (3.1).

For a given x_0, find the approximate solution x_{n+1} by the iterative scheme

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}, n = 0, 1, 2, ... \tag{3.4}$$

Algorithm (3.4) is known as Newton method and has second-order convergence [4].

Again from (3.2) we have

$$x = x_0 - \frac{f(x_0)}{f'(x_0)} - \frac{f''(x_0)(x - x_0)^2}{2f'(x_0)}. \tag{3.5}$$

Substitution again from (3.3) into the right hand side of (3.5) gives the second approximation

$$x = x_0 - \frac{f(x_0)}{f'(x_0)} - \frac{f''(x_0)\left(f(x_0)\right)^2}{2\left(f'(x_0)\right)^3}. \tag{3.6}$$

This formula allows us to suggest the following iterative methods for solving the nonlinear equation (3.1).

For a given x_0, compute approximates solution x_{n+1} by the iterative scheme

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)} - \frac{\left(f(x_n)\right)^2 f''(x_n)}{2\left(f'(x_n)\right)^3}, n = 0, 1, 2, ... \tag{3.7}$$

Algorithm (3.7) is known as Householder method for solving the nonlinear equations [9]. This method is one of the famous methods in producing a sequence of approximation roots of (3.1) with initial point x_0.

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

$$f(x) = x^2 - a = 0, a \in \mathbb{Q}_p^*. \tag{3.8}$$

The solution of the previous equation is approached by a sequence of the p-adic numbers $(x_n)_n \subset \mathbb{Q}_p$ constructed by the Householder method.

In this section we analyze the convergence of the method described previously. The important part of the convergence is about the convergence rate. In practice, a numerical method may take a large number of iterations to reach the optimum point. Therefore, it is important to employ methods having a faster rate of convergence.

The rate of convergence plays an important role in the theory of any iterative procedure that is producing a convergent sequence to the exact solution. The method converges faster to the solution for high order of convergence. Therefore, it requires a lesser number of iterations for a given accuracy. Rate of convergence of a numerical method is usually measured by the numbers of iterations and function evaluations needed to obtain an acceptable solution.

A practical method to calculate the rate of convergence is to calculate the sequence $(e_n)_n$ defined by

$$e_n = x_{n+n_0+1} - x_{n+n_0}. \tag{3.9}$$

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. Moreover, the number of iterations necessary to obtain the desired precision M which represents the number of p-adic digits in the development of $\sqrt{a}$ is very important for our objectives. it's all about finding n such that

$$|x_{n+n_0+1} - x_{n+n_0}|_p \leq p^{-M}, \tag{3.10}$$

this is equivalent to

$$v_p(e_n) \geq M. \tag{3.11}$$

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

$$|a|_p = p^{-v_p(a)} = p^{-2m}, m \in \mathbb{Z}. \tag{3.12}$$

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

$$|x_n|_p = |\alpha|_p\,. \tag{3.13}$$

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

$$|x_n|_p = |\alpha|_p = p^{-m}. \tag{3.14}$$

We consider the following equation

$$f(x) = x^2 - a. \tag{3.15}$$

We know that the iterative formula of the Householder method is given by

$$\forall n \in \mathbb{N} : x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)} - \frac{(f(x_n))^2 f''(x_n)}{2\,(f'(x_n))^3}.$$

Therefore the iteration of the Householder method associated with the function f given in (3.15) is written in the form

$$\forall n \in \mathbb{N} : x_{n+1} = x_n - \frac{1}{2x_n}\left(x_n^2 - a\right) - \frac{1}{8x_n^3}\left(x_n^2 - a\right)^2. \tag{3.16}$$

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 w_n, where the sequence $(w_n)_n$ is defined by*

$$\forall n \in \mathbb{N} : w_n = 3^n r + 2m(1 - 3^n). \tag{3.17}$$

2) *If $p = 2$, then x_{n+n_0} is the square root of a of order w'_n, where the sequence $(w'_n)_n$ is defined by*

$$\forall n \in \mathbb{N} : w'_n = 3^n r + (2m+3)(1 - 3^n). \tag{3.18}$$

Proof. Let $(x_n)_n$ be the sequence defined by (3.16). We have

$$\forall n \in \mathbb{N} : x_{n+1}^2 - a = \frac{1}{64}\frac{1}{x_n^6}\left(a - x_n^2\right)^3\left(a - 9x_n^2\right). \tag{3.19}$$

We assume that x_{n_0} is the square root of a of order r, i.e,

$$x_{n_0}^2 \equiv a \mod p^r, r \in \mathbb{N}. \tag{3.20}$$

Then

$$v_p\left(x_{n_0}^2 - a\right) \geq r,$$

hence we obtain

$$\left|x_{n_0}^2 - a\right|_p \leq p^{-r}.$$

On the other hand, we put

$$g(x) = \frac{1}{64}\frac{1}{x_n^6}\left(a - 9x_n^2\right). \tag{3.21}$$

Since

$$|64|_p = \begin{cases} 1, \text{ if } p \neq 2, \\ \frac{1}{64} = \frac{1}{2^6}, \text{ if } p = 2, \end{cases} \tag{3.22}$$

we have

$$|g(x_{n_0})|_p = \left|\frac{1}{64}\frac{1}{x_{n_0}^6}\left(a - 9x_{n_0}^2\right)\right|_p = \left|\frac{1}{64}\right|_p \left|\frac{1}{x_{n_0}^6}\right|_p \left|a - 9x_{n_0}^2\right|_p$$

This gives

$$|g(x_{n_0})|_p \leq \left|\frac{1}{64}\right|_p \left|\frac{1}{x_{n_0}^6}\right|_p \max\left\{|a|_p, \left|9x_{n_0}^2\right|_p\right\}$$

On the other hand, using the proposition 2.10, we get

$$|g(x_{n_0})|_p \leq \begin{cases} p^{6m}p^{-2m}, \text{ if } p \neq 2, \\ 2^6 2^{6m} 2^{-2m}, \text{ if } p = 2, \end{cases}$$

$$\leq \begin{cases} p^{4m}, \text{ if } p \neq 2, \\ 2^{4m+6}, \text{ if } p = 2. \end{cases}$$

We obtain

$$\left|x_{n_0+1}^2 - a\right|_p = |g(x_{n_0})|_p \left|a - x_n^2\right|_p^3,$$

and so we have

$$\begin{cases} \left|x_{n_0+1}^2 - a\right|_p \leq p^{4m}p^{-3r}, \text{ if } p \neq 2, \\ \left|x_{n_0+1}^2 - a\right|_2 \leq 2^{4m+6}2^{-3r}, \text{ if } p \neq 2. \end{cases}$$

Using the definition 2.11, we get

$$\begin{cases} x_{n_0+1}^2 - a \equiv 0 \mod p^{3r-4m} \text{ if } p \neq 2, \\ x_{n_0+1}^2 - a \equiv 0 \mod 2^{3r-4m-6} \text{ if } p = 2. \end{cases}$$

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

$$\forall n \in \mathbb{N} : x_{n+n_0}^2 - a \equiv 0 \mod p^{w_n}, \tag{3.23}$$

where the sequence $(w_n)_n$ is defined by

$$\forall n \in \mathbb{N} : \begin{cases} w_{n+1} = 3w_n - 4m, \\ w_0 = r. \end{cases} \tag{3.24}$$

It is clear that $(w_n)_n$ is a linear recurrence sequence of order 1, whose general term is given by

$$\forall n \in \mathbb{N} : w_n = 3^n r + 2m(1 - 3^n). \tag{3.25}$$

Furthermore

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

If $p = 2$, then

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

where the sequence $(w'_n)_n$ is defined by

$$\forall n \in \mathbb{N} : \begin{cases} w'_{n+1} = 3w'_n - (4m + 6), \\ w'_0 = r. \end{cases} \tag{3.28}$$

Which give

$$\forall n \in \mathbb{N} : w'_n = 3^n r + (2m + 3)(1 - 3^n). \tag{3.29}$$

Furthermore

$$v_2(x_{n+n_0}^2 - a) \geq w'_n. \tag{3.30}$$

and so

$$\forall n \in \mathbb{N} : w'_n = w_n + 3(1 - 3^n). \tag{3.31}$$

This complete the proof. ■

Corollary 3.2. *If x_{n_0} is the square root of a of order r, then*
1) *If $p \neq 2$, then*

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \mod p^{s_n}, \tag{3.32}$$

where the sequence $(s_n)_n$ is defined by

$$\forall n \in \mathbb{N} : s_n = 3^n r + m(1 - 2 \cdot 3^n). \tag{3.33}$$

2) *If $p = 2$, then*

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \mod 2^{s'_n}, \tag{3.34}$$

such as

$$\forall n \in \mathbb{N} : s'_n = 3^n r + m(1 - 2 \cdot 3^n) - 3^{n+1}. \tag{3.35}$$

Proof. Let $(x_n)_n$ be the sequence defined by (3.16). We have

$$\forall n \in \mathbb{N} : x_{n+1} - x_n = -\frac{1}{8}\frac{1}{x_n^3}\left(a - x_n^2\right)\left(a - 5x_n^2\right). \tag{3.36}$$

This gives

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} = -\frac{1}{8}\frac{1}{x_{n+n_0}^3}\left(a - x_{n+n_0}^2\right)\left(a - 5x_{n+n_0}^2\right). \tag{3.37}$$

We put

$$h(x) = -\frac{1}{8}\frac{1}{x^3}\left(a - 5x^2\right).$$

Since

$$|8|_p = \begin{cases} 1, \text{ if } p \neq 2, \\ \frac{1}{8} = \frac{1}{2^3}, \text{ if } p = 2, \end{cases} \tag{3.38}$$

we have

$$\begin{aligned} |h(x_{n+n_0})|_p &= \left|-\frac{1}{8}\frac{1}{x_{n+n_0}^3}\left(a - 5x_{n+n_0}^2\right)\right|_p = \left|\frac{1}{8}\right|_p \left|\frac{1}{x_{n+n_0}^3}\right|_p \left|a - 5x_{n+n_0}^2\right|_p \\ &\leq \left|\frac{1}{8}\right|_p \left|\frac{1}{x_{n+n_0}^3}\right|_p \max\left\{|a|_p, \left|5x_{n+n_0}^2\right|_p\right\} \\ &\leq \begin{cases} p^{3m}p^{-2m}, \text{ if } p \neq 2 \\ 2^3 2^{3m} 2^{-2m}, \text{ if } p = 2 \end{cases} \\ &\leq \begin{cases} p^{m}, \text{ if } p \neq 2 \\ 2^{m+3}, \text{ if } p = 2. \end{cases} \end{aligned}$$

Hence we obtain

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

On the other hand, using (3.23) and (3.27), we get

$$|x_{n+n_0+1} - x_{n+n_0}|_p \leq \begin{cases} p^m p^{-w_n}, \text{ if } p \neq 2 \\ 2^{m+3} 2^{-w'_n}, \text{ if } p = 2, \end{cases}$$

and so

$$\begin{cases} x_{n+n_0+1} - x_{n+n_0} \equiv 0 \mod p^{w_n - m}, \text{ if } p \neq 2 \\ x_{n+n_0+1} - x_{n+n_0} \equiv 0 \mod 2^{w'_n - (m+3)}, \text{ if } p = 2. \end{cases}$$

Therefore, if $p \neq 2$, then

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \mod p^{s_n}, \tag{3.39}$$

where

$$\forall n \in \mathbb{N} : s_n = w_n - m = 3^n r + m(1 - 2 \cdot 3^n). \tag{3.40}$$

Furthermore

$$v_p(x_{n+n_0+1} - x_{n+n_0}) \geq s_n. \tag{3.41}$$

If $p = 2$, then

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \mod 2^{s'_n}, \tag{3.42}$$

where

$$\forall n \in \mathbb{N} : s'_n = w'_n - (m+3) = 3^n r + m\left(1 - 2 \cdot 3^n\right) - 3^{n+1} = s_n - 3^{n+1}. \tag{3.43}$$

Furthermore

$$v_2(x_{n+n_0+1} - x_{n+n_0}) \geq s'_n. \tag{3.44}$$

This complete the proof. ■

4. Conclusion

Our main results can be summarized as follows.

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

   (a) The rate of convergence of the sequence $(x_n)_n$ is the order s_n.

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

$$n = \left\lceil \frac{\ln\left(\frac{M-m}{r-2m}\right)}{\ln 3} \right\rceil . \tag{4.1}$$

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

   (a) The rate of convergence of the sequence $(x_n)_n$ is the order s'_n.

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

$$n = \left\lceil \frac{\ln\left(\frac{M-m}{r-2m-3}\right)}{\ln 3} \right\rceil . \tag{4.2}$$

3. In the p-adic setting, the Householder's method converges cubically insofar as the number of significant digits eventually triples with each iteration.

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] J. B. Bacani, J. F. T. Rabago, Steffensen's analogue for approximating roots of p-adic polynomial equations. *Numerical Computations: Theory and Algorithms (NUMTA-2016).,* **1776(1)**(2016), 090038-1–090038-4.

[3] W.A. Coppel, *Number Theory: An introduction to mathematics*, Springer Science & Business Media, 2009.

[4] J.F. Epperson, *An introduction to numerical methods and analysis*, John Wiley & Sons, 2013.

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

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

[7] R.T. Gregory and E.V. Krishnamurthy, *Methods and applications of error-free computation*, Springer Science & Business Media, 2012.

[8] K. Hensel, Über eine neue Begründung der Theorie der algebraischen Zahlen. *JJahresber. Dtsch. Math.-Ver.,* **6**(1897), 83–88.

[9] A.S. Householder, *The Numerical Treatment of a Single Nonlinear Equation*, McGraw-Hill, New York, 1970.

[10] P.S.P. IGNACIO, J.M. ADDAWE AND J.A. NABLE, P-adic Qth Roots Via Newton-Raphson Method, *Thai J. Math.,* **14(2)**(2016), 417–429.

[11] 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(2)**(2013), 31–38.

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

[13] M.P. KNAPP AND C. XENOPHONTOS, Numerical Analysis meets Number Theory: Using rootfinding methods to calculate inverses $\mod p^n$, Appl. Anal. Discrete Math., **4**(2010), 23–31.

[14] M. KECIES, The Performance of the Secant Method in the Field of p-dic Numbers, *Malaya J. Mat.,* **9(2)**(2021), 28–38.

[15] A. QUARTERONI, R. SACCO AND F. SALERI, *Méthodes Numériques: Algorithmes, analyse et applications*, Springer Science & Business Media, 2008.

[16] J.F.T. RABAGO, Olver's Method for Solving Roots of p-adic Polynomial Equations, *Italian J. Pure and Applied Math.,* **36**(2016), 739–748.

[17] J.F.T. RABAGO, Halley's method for finding roots of p-adic polynomial equations, *Int. J. Math. Anal.,* **10(10)**(2016), 493–502.

[18] F. A. SHAH AND M. A. NOOR, Variational iteration technique and some methods for the approximate solution of nonlinear equations,*Appl. Math. Inf. Sci. Lett.,* **2(3)**(2014), 85–93.

[19] T. ZERZAIHI AND M. KECIES, Computation of the cubic root of a p-adic number, *J.M.R.,* **3**(2011), 40–47.

[20] T. ZERZAIHI AND M. KECIES, General approach of the root of a p-adic number, *Filomat.,* **27**(2013), 431–436.

[21] 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.