OLVER'S METHOD FOR SOLVING ROOTS OF p-ADIC POLYNOMIAL EQUATIONS

Julius Fergy Tiongson Rabago

Department of Mathematics and Computer Science
College of Science
University of the Philippines Baguio
Baguio City 2600, Benguet
Philippines
e-mail: jfrabago@gmail.com

Abstract. Let $\mathbb{Z}_p[x]$ be the set of all functions whose coefficients are in the field of p-adic integers $\mathbb{Z}_p$. This work considers a problem of finding a root of a polynomial equation $P(x) = 0$ where $P(x) \in \mathbb{Z}_p[x]$. The solution is approximated through an analogue of Olver's method for finding roots of polynomial equations $P(x) = 0$ in $\mathbb{Z}_p$.

Keywords: Olver's method, p-adic polynomials, p-adic numbers, roots of polynomials.
2000 Mathematics Subject Classification: Primary 11E95, Secondary 34K28.

1. Introduction

A p-adic number, which was first introduced in 1897 by Kurt Hensel, is an extension of the field of rationals $\mathbb{Q}$ such that congruences modulo powers of a fixed prime p are related to proximity in the so called *p-adic metric*. This metric provides a totally different notion of 'closeness' or absolute value. To be precise, two p-adic numbers are said to be close when their difference is divisible by a high power of p, meaning to say, the higher the power the closer they are. This notion of closeness obviously shows that the field of p-adic numbers denoted by $\mathbb{Q}_p$ extends the ordinary arithmetic in $\mathbb{Q}$ in a way different from the extension of $\mathbb{Q}$ to the real and complex number systems $\mathbb{R}$ and $\mathbb{C}$. It is worth mentioning that the creation of p-adic numbers was actually due to an attempt to bring the ideas and techniques of power series methods into number theory. In fact, when these numbers were introduced they were considered as an exotic part of pure mathematics without any application [15] (see, e.g., [10] and [18] for applications of p-adic numbers to mathematics). Nevertheless, various applications to other fields of mathematics, especially in analysis, algebraic geometry and related areas in the applied sciences (e.g., physics and bio-informatics), have been recently proposed and discovered. For instance, the field of p-adic analysis essentially provides an alternative form of calculus (cf. [2], [17]) and the p-adic numbers appear to have some applications in modeling DNA sequences and genetic codes (cf. [4]). In 1968, Monna and van der Blij proposed to apply p-adic numbers to physics and in 1972, Beltrametti and Cassinelli investigated a model of p-adic valued quantum

mechanics from the positions of quantum logic. p-adic numbers were also found to have some important applications in quantum physics since the 1980's (cf. [15]). For more applications in the physical sciences, especially in the construction of physical models (e.g., string theory, quantum mechanics, quantum cosmology and dynamical systems), we refer the readers to [3] and [17]. One may also want to consult an article of Razikov [15] (and see the references therein) for a popular introduction to the theory of p-adic numbers.

On the other hand, in a purely theoretical aspect, Hensel's lemma provides sufficient conditions for the existence of roots in $\mathbb{Z}_p$ of polynomials in $\mathbb{Z}_p[x]$. A classical application of this lemma deals with the problem of finding roots of a p-adic number a in $\mathbb{Q}_p$ and this was in fact the subject of several recent investigations about p-adic numbers. In 2010, for instance, Knapp and Xenophontos [9] 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 [19] 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 [20] used the secant method to find the cubic roots of p-adic numbers. These authors [8] then applied the Newton method to find the cubic roots of p-adic numbers in $\mathbb{Q}_p$. A similar problem also appeared in [6] wherein Ignacio et al. computed the square roots of p-adic numbers via the Newton-Raphson method. In [1] and [14], it was observed that none of these aforementioned works have considered the problem of finding roots of a general p-adic polynomial. So, motivated by this problem, Bacani and the author proposed in [1] 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 [14], 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 Newton-Raphson's method was also considered in [13]. In this work, we offer another approach in solving a root-finding problem $f(x) = 0$ in the p-adic case. In particular, we shall show that Olver's method works well in finding a root of the equation $f(x) = 0$ in $\mathbb{Z}_p$. As in our previous investigations, we shall examine the rate of convergence of the method and show that the sequence of approximants generated through the recursion for Olver's method converges to a unique root of the equation $f(x) = 0$ in $\mathbb{Z}_p$.

The rest of the paper is structured as follows. In Section 2, we provide a brief discussion about the essentials of $\mathbb{Q}_p$. Our main contribution is formally stated and proved in Section 3. This is followed by a simple example in Section 4 illustrating the method (and its convergence) in the p-adic setting and, in Section 5, a short conclusion about our present work is stated.

2. Preliminaries

In this section we discuss briefly some important properties of $\mathbb{Q}_p$. For a more detailed discussion of the topic, we refer the readers to a book of Katok on p-adic numbers [7].

2.1. The field $\mathbb{Q}_p$

The p-adic norm $|\cdot|_p$ and the p-adic valuation v_p on $\mathbb{Q}$ are formally defined as follows.

Definition 1. Let p be a fixed prime. The p-adic norm $|\cdot|_p : \mathbb{Q} \to \{p^n : n \in \mathbb{Z}\} \cup \{0\}$ is defined as follows:

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

where v_p is the p-adic valuation defined by $v_p(x) = \max\{r \in \mathbb{Z} : p^r \mid x\}$. This norm induces the so-called p-adic metric d_p given by

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

The p-adic norm $|\cdot|_p$ satisfies the following important properties (cf. [7]):

(i) $|xy|_p = |x|_p |y|_p$,

(ii) $|x + y|_p \leq \max\{|x|_p, |y|_p\}$, where equality holds if $|x|_p \neq |y|_p$ and

(iii) $|x/y|_p = |x|_p / |y|_p$.

Meanwhile, the formal definition of the field of p-adic numbers $\mathbb{Q}_p$ is given as follows.

Definition 2. The field $\mathbb{Q}_p$ of p-adic numbers is the completion of $\mathbb{Q}$ with respect to the p-adic norm $|\cdot|_p$. The elements of $\mathbb{Q}_p$ are equivalence classes of Cauchy sequences in $\mathbb{Q}$ with respect to the extension of the p-adic norm defined as $|a|_p = \lim_{n\to\infty} |a_n|_p$, where $\{a_n\}$ is a Cauchy sequence of rational numbers representing $a \in \mathbb{Q}_p$.

The following theorem provides a way to write a p-adic number in a unique representation.

Theorem 1. ([5]) *Given a p-adic number $a \in \mathbb{Q}_p$, there is a unique sequence of integers $(a_n)_{n \geq N}$, with $N = v_p(a)$, such that $0 \leq a_n \leq p - 1$ for all n and*

$$a = a_N p^N + a_{N+1} p^{N+1} + \cdots + a_n p^n + \cdots = \sum_{k=N}^{\infty} a_i p^i.$$

In view of the above statement, a p-adic number is naturally defined as a number $a \in \mathbb{Q}_p$ whose canonical expansion contains only non-negative powers of p. The set of p-adic integers is denoted by $\mathbb{Z}_p$ and is given by

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

Definition 3. The group of invertible elements in $\mathbb{Z}_p$ (or the group of p-adic units) denoted by $\mathbb{Z}_p^{\times}$ is given by

$$\mathbb{Z}_p^{\times} = \left\{ a \in \mathbb{Z}_p : a = \sum_{i=0}^{\infty} a_i p^i,\ a_0 \neq 0 \right\} = \left\{ a \in \mathbb{Q}_p : |a|_p = 1 \right\}.$$

By virtue of Theorem 1 we may write, in an alternative way, a p-adic number in terms of their p-adic valuation.

Corollary 2. *Let $a \in \mathbb{Q}_p$. Then, $a = p^{v_p(a)}u$ for some $u \in \mathbb{Z}_p^{\times}$.*

The following result will be use frequently in our discussion.

Lemma 3. ([7]) *Let $a, b \in \mathbb{Q}_p$. Then, $a \equiv b \pmod{p^m} \iff |a-b|_p \leq p^{-m}$.*

2.2. Functions over $\mathbb{Q}_p$

The continuity and differentiability in the p-adic setting are described in the usual fashion. Let $X \subset \mathbb{Q}_p$. A function $f : X \to \mathbb{Q}_p$ is said to be continuous at $a \in X$ if for each $\varepsilon > 0$ there exists a $\delta > 0$ such that if $|x-a|_p < \delta$, then $|f(x)-f(a)|_p < \varepsilon$. A function f is said to be continuous on $E \subseteq X$ if f is continuous for every $a \in E$. Also, let $a \in X$ be an accumulation point of X. Then, the function f is differentiable at a if the derivative of f at a, defined by $f'(a) = \lim\limits_{x \to a} \frac{f(x)-f(a)}{x-a}$ exists. So f will be differentiable on X if $f'(a)$ exists at all $a \in X$. Evidently, any polynomial function f in $\mathbb{Q}_p[x]$ is continuous and differentiable at every $a \in \mathbb{Q}_p$ (cf. [14]).

2.3. p-Adic roots

The following are some well-known results in the study of p-adic roots.

Theorem 4. (Hensel's lemma) *Let F be a polynomial of degree $q \in \mathbb{N}$ whose coefficients are p-adic integers, i.e., $F(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_q x^q \in \mathbb{Z}_p[x]$ and $F'(x) = c_1 + 2c_2 x + 3c_3 x^2 + \ldots + q c_q x^{q-1}$ be its derivative. Suppose for $\overline{a_0} \in \mathbb{Z}_p$ we have $F(\overline{a_0}) \equiv 0 \pmod{p}$ and $F'(\overline{a_0}) \not\equiv 0 \pmod{p}$. Then, there is a unique $a \in \mathbb{Z}_p$ such that $F(a) = 0$ and $a \equiv \overline{a_0} \pmod{p}$.*

The above theorem can be found, for instance, in [16, p. 48].

Theorem 5. *A polynomial with integer coefficients has a root in $\mathbb{Z}_p$ if and only if it has an integer root modulo p^m for any $m \in \mathbb{N}$.*

For the proof of the above theorems, one can consult a text on p-adic analysis by Katok [7].

Having these ideas understood, we are now in the position to state and prove our main result in the next section.

3. Statement and proof of the main result

Olver's method is a root-finding algorithm which is iteratively defined by

$$\text{(OM)} \qquad x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)} - \frac{1}{2}\left\{ \frac{[f(x_n)]^2 f''(x_n)}{[f'(x_n)]^3} \right\}, \qquad \forall n \in \mathbb{N}_0.$$

This method is cubically convergent; that is, for every sequence $(x_n)_{n\in\mathbb{N}_0}$ generated through the recurrence (OM), we have

$$\lim_{n\to\infty}\frac{|x_{n+1}-L|}{|x_n-L|^3}=\text{const.}>0$$

where L is the limit of the sequence $(x_n)_{n\in\mathbb{N}_0}$. So it is faster compared to the well-known Newton's (sometimes called Newton-Raphson's) method. The algorithm is named after the American mathematician Frank W.J. Olver who first introduced the method in [11].

In this section, as stated in the Introduction, we are interested in finding a root of the polynomial equation $f(x)=0$ with $f(x)\in\mathbb{Z}_p[x]$ through Olver's method. Regarding the rate of convergence of the method (in the p-adic setting), we use the following definition.

Definition 4. We say that the sequence $(x_n)_{n\in\mathbb{N}_0}$ converges to its limit L (in the p-adic sense) with order γ if $|x_{n+1}-L|_p\le p^{-\gamma^n}$.

Hereon, for simplicity, we use $a\equiv_p b$ to denote the congruence relation $a\equiv b \pmod p$. Our main result is given as follows.

Theorem 6. *Let $x_0\in\mathbb{Z}$ be such that $f(x_0)\equiv_p 0$ and $f'(x_0)\not\equiv_p 0$ where $f(x)\in\mathbb{Z}_p[x]$ is a polynomial of degree $q\in\mathbb{N}$. Define the sequence $(x_n)_{n\in\mathbb{N}_0}$ recursively by Olver's iterative formula* (OM)*. Then, we have the following results:*

(i) *For all $n\in\mathbb{N}_0$, we have $x_n\in\mathbb{Z}_p$, $f'(x_n)\not\equiv_p 0$ and*

$$f(x_n)\equiv\begin{cases}0\pmod{p^{3^n}} & \text{if } p\neq 2,\\ 0\pmod{p^{4^n}} & \text{if } p=2.\end{cases}$$

(ii) *The sequence $(x_n)_{n\in\mathbb{N}_0}$ generated by the recursion* (OM) *converges to a unique zero $\xi\equiv_p x_0$ of f in $\mathbb{Z}_p$.*

(iii) *The speed of convergence in* (ii) *is cubic for $p\neq 2$ and quartic for $p=2$.*

Before we prove the above results, we first state and prove for completeness the following lemma which is a key ingredient in our proof.

Lemma 7. ([1]) *Let $a,y\in\mathbb{Z}_p$ and suppose that $y\equiv_{p^m}0$ for some positive integer m. Then,*

$$f(a+y)\equiv_{p^{km}}\sum_{j=0}^{k-1}\frac{f^{(j)}(a)}{j!}y^j,\qquad \forall k\in\{1,2,\dots,\deg(f)\},$$

where $\deg(f)$ *denotes the degree of the polynomial $f\in\mathbb{Z}_p[x]$.*

Proof. Let $f\in\mathbb{Z}_p[x]$ with $\deg(f)=q\in\mathbb{N}$ and $k\in\{1,2,\dots,q\}$. Further, assume that $a,y\in\mathbb{Z}_p$ and suppose $y\equiv_{p^m}0$ for some positive integer m. Using the well-known Taylor expansion formula (TEF) to $f(a+y)$, we get

$$f(a+y) = f(a) + \cdots + \frac{f^{(k-1)}(a)}{(k-1)!}y^{k-1} + y^k \sum_{j=0}^{q-k} \frac{f^{(j+k)}(a)}{(j+k)!}y^j.$$

But, by assumption, $y \equiv_{p^m} 0$ for some positive integer m. Hence, $y^k \equiv_{p^{km}} 0$ for every k. Thus, we have

$$f(a+y) \equiv_{p^{km}} f(a) + \cdots + \frac{f^{(k-1)}(a)}{(k-1)!}y^{k-1},$$

as desired. ∎

In view of the above lemma, one easily finds that $f(a+y) \equiv_{p^m} f(a)$, $f(a+y) \equiv_{p^{2m}} f(a) + f'(a)y$ and $f(a+y) \equiv_{p^{3m}} f(a) + f'(a)y + f''(a)y^2/2$.

Now, we are ready to prove our main result (Theorem 6). Throughout the proof, we use $a \equiv_{p^m} b$ for $a \equiv b \pmod{p^m}$ and noting this is equivalent to $|a-b|_p \leqslant p^{-m}$.

Proof of Theorem 6. Let $x_0 \in \mathbb{Z}$ be such that $f(x_0) \equiv_p 0$ and $f'(x_0) \not\equiv_p 0$. Furthermore, define the sequence $(x_n)_{n\in\mathbb{N}_0}$ recursively by (OM). We first prove (i).

Proof of (i). In this part, we need to show that $f(x_n) \equiv_{p^{3^n}} 0$ for $p \neq 2$ and $f(x_n) \equiv_{p^{4^n}} 0$ for $p = 2$ and $f'(x_n) \not\equiv_p 0$ for all $n \in \mathbb{N}_0$. The proof of this part proceeds by induction on n. First we note that since $x_0 \in \mathbb{Z}$, then $x_0 \in \mathbb{Z}_p$. So for the basis step we have, by definition,

$$f(x_1) = f\left(x_0 - \frac{f(x_0)}{f'(x_0)} - \frac{1}{2}\left\{\frac{[f(x_0)]^2 f''(x_0)}{[f'(x_0)]^3}\right\}\right) =: f(x_0+y_0).$$

In view of Lemma 7, we have

$$f(x_0+y_0) \equiv_{p^3} f(x_0) + f'(x_0)y_0 + \frac{f''(x_0)}{2}y_0^2.$$

Note that the right hand side of the above relation can be simplified as

$$\frac{[f(x_0)]^3[f''(x_0)]^2\{4[f'(x_0)]^2 + f(x_0)f''(x_0)\}}{8[f'(x_0)]^6} =: \frac{U}{V}.$$

Clearly, for $p \neq 2$ and by the fact that $f(x_0) \equiv_p 0$ and $f'(x_0) \not\equiv_p 0$, it follows that

$$f(x_1) \equiv_{p^3} f(x_0+y_0) \equiv_{p^3} 0.$$

Now, from the form of f, we have $f''(x) = \sum_{j=0}^{q-2} = (j+1)(j+2)a_{j+2}x^j$. But since $2 \mid (j+1)(j+2)$, then $f''(x) \equiv_2 0$. Thus, for $p = 2$, we see that $U \equiv_{2^7} 0$ and $V \equiv_{2^3} 0$. Hence, $f(x_1) \equiv_{p^4} 0$ for $p = 2$. Similarly, since $f'(x_1) = f'(x_0+y_0)$, we have (by Lemma 7) $f'(x_1) \equiv_p f'(x_0)$. We have just shown that the result holds for $n = 1$.

Meanwhile, for the induction hypothesis, we suppose that for some $n_0 \in \mathbb{N}$ the following results hold:

$$\forall n \geq n_0 : \; x_n \in \mathbb{Z}_p, \quad f'(x_n) \not\equiv_p 0, \quad f(x_n) \equiv \begin{cases} 0 \pmod{p^{3^n}} & \text{if } p \neq 2, \\ 0 \pmod{p^{4^n}} & \text{if } p = 2. \end{cases}$$

Let

$$y_n := -\frac{f(x_n)}{f'(x_n)} - \frac{1}{2}\left\{\frac{[f(x_n)]^2 f''(x_n)}{[f'(x_n)]^3}\right\}.$$

Since $x_{n+1} = x_n + y_n$, it follows that

$$|x_{n+1}|_p = |x_n + y_n|_p \leq \max\{|x_n|_p, |y_n|_p\}.$$

Note, however, that we have the estimate $|y_n|_p \leq p^{-3^n}$ for any fixed prime p. So $|x_{n+1}|_p \leq \max\{1, p^{-3^n}\} = 1$. Therefore, by definition of elements in $\mathbb{Z}_p$, we have $x_{n+1} \in \mathbb{Z}_p$. On the other hand, since $f'(x_{n+1}) = f'(x_n + y_n)$, then by Lemma 7 it follows that

$$f'(x_{n+1}) = f'(x_n) + y_n \sum_{j=0}^{q-1} \frac{f^{(j+2)}(x_n)}{(j+1)!} y_n^j.$$

Taking modulo p on both sides of the above equation and using Lemma 3, we get $f'(x_{n+1}) \equiv_p f'(x_n) \not\equiv_p 0$. Moreover, since $f(x_{n+1}) = f(x_n + y_n)$ and by Lemma 7, we have the equation

$$f(x_{n+1}) \equiv_{p^{3^{n+1}}} f(x_n) + f'(x_n) y_n + \frac{f''(x_n)}{2} y_n^2.$$

Expanding the right hand side of the above relation, we get

$$\frac{[f(x_n)]^3 [f''(x_n)]^2 \left\{4[f'(x_n)]^2 + f(x_n) f''(x_n)\right\}}{8[f'(x_n)]^6} =: \frac{U_n}{V_n}.$$

Similar to what we have observed earlier, we'll obtain the congruence relation $f(x_{n+1}) \equiv_{p^{3^{n+1}}} 0$ for $p \neq 2$. Similarly, for $p = 2$ we get (as $U_n \equiv_{2^7}$ and $V \equiv_{2^3} 0$) $f(x_{n+1}) \equiv_{p^{4^{n+1}}} 0$. By principle of induction, it now follows that

$$\forall n \in \mathbb{N}_0 : \; x_n \in \mathbb{Z}_p, \quad f'(x_n) \not\equiv_p 0, \quad f(x_n) \equiv \begin{cases} 0 \pmod{p^{3^n}} & \text{if } p \neq 2, \\ 0 \pmod{p^{4^n}} & \text{if } p = 2. \end{cases}$$

This validates our first result (i).

Proof of (ii). For the second part we need to show that, with the same assumption as in the first part, the sequence $(x_n)_{n\in\mathbb{N}_0}$ defined recursively by (OM) converges to a unique zero $\xi \equiv_p x_0$ of f in $\mathbb{Z}_p$. To establish this result, we first prove that $(x_n)_{n\in\mathbb{N}_0}$ is Cauchy. So we proceed as follows. Note that

$$\begin{aligned} |x_{n+1} - x_n|_p &= \left| x_n - \frac{f(x_n)}{f'(x_n)} - \frac{1}{2}\left\{\frac{[f(x_n)]^2 f''(x_n)}{[f'(x_n)]^3}\right\} - x_n \right|_p \\ &= \frac{|2f(x_n)[f'(x_n)]^2 - [f(x_n)]^2 f''(x_n)|_p}{|2[f'(x_n)]^3|_p} =: \frac{|A|_p}{|B|_p}. \end{aligned}$$

Here we distinguish two cases: (C.1) $p \neq 2$ and (C.2) $p = 2$.

Case 1. If $p \neq 2$, then $A \equiv_{p^{3^n}} 0$ since $f(x_n) \equiv_{p^{3^n}} 0$ by (i). Furthermore, $B \not\equiv_p 0$ since $f'(x_n) \not\equiv_p 0$ by (i) and $p \neq 2$. Hence, from Lemma 3, we obtain the estimate $|x_{n+1} - x_n|_p \leq p^{-3^n}$. Letting $n \to \infty$, we see that $\lim_{n\to\infty} |x_{n+1} - x_n|_p = 0$, i.e., $(x_n)_{n\in\mathbb{N}_0}$ is Cauchy. So, for the case $p \neq 2$, we have $(x_n)_{n\in\mathbb{N}_0}$ is Cauchy.

Case 2. If, on the other hand, $p = 2$, then $A \equiv_{p^{4^{n+1}}} 0$ and $B \equiv_p 0$. Thus, by Lemma 3, we have $|A|_p \leq p^{-4^n-1}$ and $|B|_p \leq p^{-1}$. Then, $|A|_p/|B|_p \leq p^{-4^n}$ and so $|x_{n+1} - x_n|_p \to 0$ as $n \to \infty$. Therefore, for $p = 2$, $(x_n)_{n\in\mathbb{N}_0}$ is again a Cauchy sequence.

We see that, in any case, the sequence $(x_n)_{n\in\mathbb{N}_0}$ is Cauchy. Thus, it must converge to some number ξ in $\mathbb{Z}_p$. Finally, the uniqueness of the zero $\xi \equiv_p x_0$ of f in $\mathbb{Z}_p$ follows directly from the uniqueness of the sequence $(x_n)_{n\in\mathbb{N}_0}$.

Proof of (iii). As we have seen from the previous item, we have the estimate

$$\forall n \in \mathbb{N}_0 : \quad |x_{n+1} - x_n| \leq \begin{cases} p^{-3^n}, & \text{if } p \neq 2, \\ p^{-4^n}, & \text{if } p = 2. \end{cases}$$

Hence, it follows immediately that the sequence of approximants $(x_n)_{n\in\mathbb{N}_0}$ converges to a unique zero $\xi \equiv_p x_0$ of f in $\mathbb{Z}_p$ cubically for $p \neq 2$ and in quartic sense for $p = 2$. This completes the proof of the theorem. ∎

4. Example

To simply illustrate the method (and its convergence), we consider the root-finding problem $f(x) = 0$ in $\mathbb{Z}_{17}$ where $f(x) = x^3 - x - 1$. We consider several values for the initial iterate x_0 and see how many iterations does it needs before the sequence of approximants $(x_n)_{n\in\mathbb{N}_0}$ converges to a unique solution $\xi \equiv_p x_0$ of the equation $f(x) = 0$ in $\mathbb{Z}_{17}$.

First, we note that the sequence of approximants $(x_n)_{n\in\mathbb{N}_0}$ with initial condition x_0 is given by the recursion

$$x_{n+1} = x_n - \frac{x_n^3 - x_n - 1}{3x_n^2 - 1} - \frac{1}{2}\left\{\frac{(x_n^3 - x_n - 1)^2(6x_n)}{(3x_n^2 - 1)^3}\right\}.$$

One can easily verify that the assumptions in Theorem 6 are satisfied. In fact, we have $f(5) = 119 \equiv 0 \pmod{17}$ and $f'(5) = 74 \not\equiv 0 \pmod{17}$. Using the initial values $x_0 = 22, 39, 56, 73, 90$ ($\equiv_{17} 5$), we get the following table.

x_0	x_1	x_2	x_3	x_4	x_4	x_6	x_7	x_8	x_9
22	1	4	8	13	6	16	**5**		
39	8	13	6	16	**5**				
56	10	7	1	4	8	13	6	16	**5**
73	8	13	6	16	**5**				
90	11	3	**5**						

Observe from the above table that the n-th approximant x_n eventually takes the value of 5 after some iteration. Note that this value is, in fact, the unique root of the polynomial equation $f(x) = 0$ in $\mathbb{Z}_{17}$. Furthermore, notice from above table that it requires (at least) 7 (resp. $4, 9, 4, 3$) iterations before the sequence of approximants $(x_n)_{n\in\mathbb{N}_0}$ converges to the unique solution $\xi = 5$ of $f(x)=x^3-x-1=0$ in $\mathbb{Z}_{17}$ given that the initial iterate is $x_0 = 22$ (resp. $39, 56, 73, 90$). These results, in addition, corroborate our findings stated in Theorem 6.

5. Summary

We have considered in this work the problem of finding a p-adic root of a general polynomial equation $P(x) = 0$ with $P(x) \in \mathbb{Z}_p[x]$. It was shown that the sequence $(x_n)_{n\in\mathbb{N}_0}$ defined recursively by the iterative formula of Olver's method converges to a unique zero $\xi \equiv_p x_0$ of P in $\mathbb{Z}_p$. Moreover, we found that the p-adic analogue of Olver's method has rates of convergence of order 3 and 4 for values of $p \neq 2$ and $p = 2$, respectively. For future studies, it might be interesting to investigate whether Olver's method is indeed more efficient in computing p-adic roots compared to other well-known root-finding algorithms such as the Newton-Raphson's method [13] and Halley's method [14]. This, in turn, provides considerable interests to further examine these methods in the p-adic setting.

Acknowledgement. The author would like to thank Prof. Peter J. Olver of the University of Minnesota for bringing to his attention the original paper from which Olver's method first appeared. The author also wishes to thank the anonymous referee for his/her valuable comments which helped improve the manuscript.

References

[1] Bacani, J.B., Rabago, J.F.T., *Steffensen's analogue for approximating roots of p-adic polynomial equations,* submitted.

[2] Baker, A., Plymen, R.J., *p-Adic Methods and Their Applications,* Clarendon Press, 1992.

[3] Brekke, L., Freund, P.G.O., *p-Adic Numbers in Physics,* Phys. Rept., 233 (1) (1993), 1–66.

[4] Dragovich, B., Dragovich, A., *A p-adic model of DNA sequence and genetic code,* P-Adic Numbers Ultrametric Anal. Appl., 1 (1) (2009), 34–41.

[5] Gouvea, F., *p-Adic Numbers: An Introduction,* Springer-Verlag, 2003.

[6] Ignacio, P., Addawe, J., Alangui, W., Nable, J., *Computation of square and cube roots of p-adic numbers via Newton-Raphson method,* Journal of Mathematics Research, 5 (2) (2013), 31–38.

[7] S. Katok, S., *p-Adic Analysis Compared with Real,* Student Mathematical Library, vol. 37, American Mathematical Society, 2007.

[8] Kecies, M., Zerzaihi, T., *General approach of the root of a p-adic number,* Filomat, 27 (3) (2013), 431–436.

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

[10] Koblitz, N., *p-Adic Numbers, p-Adic Analysis, and Zeta-Functions,* Springer, Berlin, 1977.

[11] Olver, F.W.J., *The evaluation of zeros of high-degree polynomials*, Phil. Trans. Roy. Soc. London A, 244 (1952), 385–415.

[12] Olver, P.J., personal communication, February 24, 2016.

[13] Rabago, J.F.T., *Solving higher-order p-adic polynomial equations via Newton-Raphson's method,* preprint, 2015.

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

[15] Razikov, U.A., *What are p-Adic Numbers? What are they used for?*, Asia Pacific Mathematics Newsletter, 3 (4) (October 2013), 1–6.

[16] Robert, A., *A Course in p-Adic Analysis*, Graduate Texts in Math., vol. 198, Springer-Verlag, New York, 2000.

[17] Vladimirov, V.S., Volovich, I.V., ZelenovE.I., *p-Adic Analysis and Mathematical Physics,* World Scientific, Singapore, 1994.

[18] Manin, Yu.I., Panchishkin, A.A., *Introduction to Modern Number Theory,* Springer, Berlin, 2007.

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

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

Accepted: 07.04.2016