Malaysian Journal of Mathematical Sciences 11(1): 41–51 (2017)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES

Journal homepage: http://einspem.upm.edu.my/journal

Solving Higher-Order p-Adic Polynomial Equations via Newton-Raphson Method

Julius Fergy T. Rabago

Department of Mathematics and Computer Science,
College of Science,
University of the Philippines Baguio, Philippines

E-mail: jtrabago@upd.edu.ph

Received: 11th November 2015
Accepted: 16th December 2016

ABSTRACT

We consider the root-finding problem $f(x) = 0$, $f \in \mathbb{Z}_p[x]$, and seek a root in $\mathbb{Z}_p$ of this equation through a p-adic analogue of Newton-Raphson method. We show in particular that, under appropriate assumptions, the sequence of approximants generated by the iterative formula of the Newton-Raphson method converges to a unique root of f in $\mathbb{Z}_p$. Also, we give the rate of convergence of this method in the p-adic setting. Our work generalizes previous results concerning q-th roots of p-adic numbers due to Kecies and Zerzaihi (2013) and Ignacio et al. (2016).

Keywords: Newton-Rapshon method, p-adic polynomials, p-adic numbers, roots of polynomials.

1. Introduction

Let $\mathbb{Z}_p$ and $\mathbb{Q}_p$ denote the ring of p-adic integers and the field of p-adic numbers, respectively. In this work, we are interested in solving a root-finding problem $f(x) = 0$ in the p-adic case. More precisely, we seek to find a solution $\xi \in \mathbb{Z}_p$ of the polynomial equation $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_qx^q = 0$, where $f(x) \in \mathbb{Z}_p[x]$, through an analogue of Newton-Raphson method in the p-adic case.

The p-adic numbers was first introduced by Kurt Hensel in 1897. Their creation led the way to the construction of the field $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ so radically different from $\mathbb{R}$. When these numbers were first introduced, they were considered solely as part of pure mathematics without any application in other field of the subject and related areas of applied mathematics. However, in the early 1960's and recently, various applications to physical sciences especially in the construction of physical models (e.g., string theory, quantum mechanics, quantum cosmology and dynamical systems) (see Brekke and Freund (1993), Vladimirov et al. (1994)) and biology, particularly in bioinformatics (see, e.g., Dragovich and Dragovich (2009)), have been proposed and discovered. For a popular introduction to the theory of p-adic numbers, we refer the readers to Koblitz (1984). On the other hand, a short survey of applications of p-adic numbers to mathematics, biology and physics can be found in Razikov (2013). Recently, in view of a classical application of Hensel's lemma, several authors considered the problem of finding a q-th root of a p-adic number $a \in \mathbb{Q}_p$. For instance, in Ignacio et al. (2016), the authors considered the problem of computing the q-th roots of p-adic numbers in $\mathbb{Q}_p$, where q is a prime such that q is less than p. This study was in fact inspired by an earlier results due to Kecies and Zerzaihi (2013), Zerzaihi and Kecies (2011), Zerzaihi et al. (2010) wherein some numerical methods were used to extend the p-adic root-finding problem to $\mathbb{Q}_p$. A similar work also appeared in Ignacio et al. (2013). Other related problems were also addressed in earlier works, such as in Dumas (2014) and Knapp and Xenophontos (2010), in which the authors calculated the multiplicative inverses of p-adic numbers modulo prime powers. In this note, as motivated by these aforementioned works, we will consider a more general setting of the problem by finding roots of higher-order polynomial equations with intermediate terms in the p-adic case. In particular, we consider the root-finding problem $f(x) = 0$ in the p-adic setting (i.e., $f \in \mathbb{Z}_p[x]$), and seek to find a root of this equation using the p-adic analogue of the well-known Newton-Raphson method. As an immediate consequence of our main result (see Theorem 3.1), we recover the result presented by Ignacio et al. (2016) for $a \in \mathbb{Z}_p$.

The rest of the paper is organized as follows. In the next section (Section 2), we give the essentials of the paper. Meanwhile, the main result of our work is formally stated and proven in Section 3. Lastly, a short conclusion about this present investigation is given in Section 4.

2. Preliminaries

In this section we discuss some basic properties of $\mathbb{Q}_p$. A more formal treatment of the topic can be found in Katok (2007).

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

We start with the definition of the p-adic norm $|\cdot|_p$ and the p-adic valuation v_p on $\mathbb{Q}$.

Definition 2.1. *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:*

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

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

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

Remark 2.1. *The p-adic norm $|\cdot|_p$ satisfies the following important properties: (i) $|xy|_p = |x|_p|y|_p$; (ii) $|x + y|_p \leqslant \max\{|x|_p, |y|_p\}$, where equality holds if $|x|_p \neq |y|_p$; and (iii) $|x/y|_p = |x|_p/|y|_p$.*

The field of p-adic numbers $\mathbb{Q}_p$ is formally defined as follows.

Definition 2.2. *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 2.1. *For every $a \in \mathbb{Q}_p$, there is a unique sequence of integers $(a_n)_{n \geq N}$, with $N = v_p(a)$, such that $0 \leqslant a_n \leqslant p - 1$ for all n and*

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

With such representation as above, a p-adic integer is naturally defined as a number $a \in \mathbb{Q}_p$ whose canonical expansion contains only nonnegative powers of p. The set of p-adic integers is denoted by $\mathbb{Z}_p$ and is given by

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

Definition 2.3. *The group of p-adic units in $\mathbb{Z}_p$ denoted by $\mathbb{Z}_p^\times$ is given by*

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

By virtue of Theorem 2.1, we may write in an alternative way a p-adic number in terms of their p-adic valuation. More precisely, for every $a \in \mathbb{Q}_p$, we have $a = p^{v_p(a)}u$ for some $u \in \mathbb{Z}_p^\times$ (cf. Katok (2007)). The following lemma will be central to our discussion.

Lemma 2.1. *Let $a, b \in \mathbb{Q}_p$. Then, $a \equiv b \pmod{p^m}$ if and only if $|a-b|_p \leqslant p^{-m}$.*

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

In this section we discuss some fundamental concepts on the analysis of functions defined over $\mathbb{Q}_p$.

Definition 2.4 (Continuity)**.** *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 $a \in E$.*

Definition 2.5 (Differentiability)**.** *Let $X \subset \mathbb{Q}_p$ and $a \in X$ be an accumulation point of X. A function $f : X \to \mathbb{Q}_p$ is differentiable at a if the derivative of f at a, defined by*

$$f'(a) = \lim_{x \to a} \frac{f(x) - f(a)}{x - a}$$

exists. A function $f : X \to \mathbb{Q}_p$ is 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. Ignacio et al. (2013)).

2.3 p-Adic roots.

The following lemma due to Hensel provides sufficient conditions for the existence of roots in $\mathbb{Z}_p$ of polynomials in $\mathbb{Z}_p[x]$.

Theorem 2.2 (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 $a \equiv \overline{a_0} \pmod{p}$.

Theorem 2.3. *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 $m \in \mathbb{N}$.*

Now, we are in the position to present and validate our main results in the next section.

3. Main Results

Newton-Raphson's method is an elementary root-finding algorithm defined iteratively by

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}, \qquad \forall n \in \mathbb{N}_0. \tag{NR}$$

This method is quadratically convergent and is much known as Newton's method or Newton's iteration. In this section, as alluded in Introduction, we are interested in finding a root of the polynomial equation $f(x) = 0$ in $\mathbb{Z}_p$ through Newton-Raphson's method. Throughout the discussion we denote, as usual, the derivative of f as f' and for simplicity, we use $a \equiv_p b$ to denote the congruence relation $a \equiv b \pmod{p}$. Similarly, we write $a \equiv_{p^m} b$ to denote $|a-b|_p \leqslant p^{-m}$. Regarding the rate of convergence of the method (in the p-adic setting), Zerzaihi et al. (2010) implicitly define the rate of convergence of the sequence $(x_n)_{n\in\mathbb{N}_0}$ to its limit, say L, as the value s, where s is obtain from the p-adic valuation of the difference of two neighboring approximants x_n and x_{n+1}, i.e., the rate of convergence s is such that $|x_{n+1} - x_n|_p \leq p^{-s}$. In the spirit of this taught, we formally define the rate of convergence as follows.

Definition 3.1. *We say that the sequence $(x_n)_{n\in\mathbb{N}_0}$ converges to its limit L with order s if $|x_{n+1} - x_n|_p \leq p^{-s}$.*

Our main result is given as follows.

Theorem 3.1. *Let $x_0 \in \mathbb{Z}$ 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 Newton-Raphson's iterative formula* (NR)*. Then, we have the following results:*

(i) $\forall n \in \mathbb{N}_0 :\ x_n \in \mathbb{Z}_p, \quad f(x_n) \equiv_{p^{2^n}} 0 \quad \text{and} \quad f'(x_n) \not\equiv_p 0.$

(ii) *The sequence $(x_n)_{n\in\mathbb{N}_0}$ generated by the recursion* (NR) *converges to a unique zero $\xi \equiv_p x_0$ of f in $\mathbb{Z}_p$ with order 2^n.*

Proof. Throughout the proof we assume f to take the form

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_q x^q \ \in\ \mathbb{Z}_p[x].$$

Assume that $x_0 \in \mathbb{Z}$ 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 (NR). The proof follows a similar

line of arguments as in the proof of Hensel's lemma (see, e.g., Koblitz (1984)).

Proof of (i). The proof of this part proceeds by induction on n. For $x_0 \in \mathbb{Z}$, it is evident, by definition of elements in $\mathbb{Z}_p$, that x_0 is also in $\mathbb{Z}_p$ (or equivalently, $|x_0|_p \leqslant 1$). Moreover, since $x_1 = x_0 - f(x_0)/f'(x_0)$, then by Remark 2.1 and Lemma 2.1 it follows that

$$|x_1|_p = \left| x_0 - \frac{f(x_0)}{f'(x_0)} \right|_p \leqslant \max\left\{ |x_0|_p, \frac{|f(x_0)|_p}{|f'(x_0)|_p} \right\} \leqslant \max\{1, p^{-1}\} = 1.$$

Hence, $|x_1|_p \leqslant 1$ or equivalently, $x_1 \in \mathbb{Z}_p$. Now, from the recurrence relation (NR), we have

$$f(x_1) = f\left(x_0 - \frac{f(x_0)}{f'(x_0)} \right) =: f(x_0 + y_0).$$

Since $\deg(f) = q$, then by Taylor expansion formula (TEF) we can express the left-hand side of the above equation as follows:

$$\begin{aligned} f(x_0 + y_0) &= f(x_0) + f'(x_0)y_0 + \frac{f''(x_0)}{2}y_0^2 + \ldots + \frac{f^{(q)}(x_0)}{q!}y_0^q \\ &= f(x_0) + f'(x_0)\left[-\frac{f(x_0)}{f'(x_0)} \right] + \frac{f''(x_0)}{2}y_0^2 + \ldots + \frac{f^{(q)}(x_0)}{q!}y_0^q \\ &= \frac{f''(x_0)}{2}y_0^2 + \ldots + \frac{f^{(q)}(x_0)}{q!}y_0^q. \end{aligned}$$

Hence,

$$\begin{aligned} f(x_1) &\equiv_{p^2} f(x_0 + y_0) \\ &\equiv_{p^2} \frac{[f(x_0)]^2}{[f'(x_0)]^2}\left\{ \frac{f''(x_0)}{2} + \ldots + (-1)^q \frac{f^{(q)}(x_0)}{q!}\frac{[f(x_0)]^{q-2}}{[f'(x_0)]^{q-2}} \right\} \\ &\equiv_{p^2} 0. \end{aligned}$$

Similarly, we have

$$\begin{aligned} f'(x_1) &\equiv_p f'(x_0 + y_0) \\ &\equiv_p f'(x_0) + f''(x_0)y_0 + \ldots + \frac{f^{(q)}(x_0)}{(q-1)!}y_0^{q-1} \\ &\equiv_p f'(x_0) - \frac{f(x_0)}{f'(x_0)}\left\{ f''(x_0) + \ldots + (-1)^{q-2}\frac{f^{(q)}(x_0)}{(q-1)!}\frac{[f(x_0)]^{q-2}}{[f'(x_0)]^{q-2}} \right\} \\ &\equiv_p f'(x_0) \not\equiv_p 0. \end{aligned}$$

We have just shown that (i) holds for $n = 1$. Now, for the induction step, we assume that for some $n_0 \in \mathbb{N}$ the following statement holds:

$$\text{for } n = n_0 : \ x_n \in \mathbb{Z}_p, \quad f(x_n) \equiv_{p^{2^n}} 0 \quad \text{and} \quad f'(x_n) \not\equiv_p 0.$$

So, since the assumption $x_n \in \mathbb{Z}_p$ means that $|x_n|_p \leqslant 1$, then by Remark 2.1 we have

$$|x_{n+1}|_p = \left| x_n - \frac{f(x_n)}{f'(x_n)} \right|_p \leqslant \max\left\{ |x_n|_p, \frac{|f(x_n)|_p}{|f'(x_n)|_p} \right\} \leqslant \max\{1, p^{-2^n}\} = 1.$$

Therefore, $x_{n+1} \in \mathbb{Z}_p$. Furthermore, since $f(x_{n+1}) = f(x_n - f(x_n)/f'(x_n)) =: f(x_n + y_n)$, then by TEF we have

$$\begin{aligned} f(x_{n+1}) &= f(x_n) + f'(x_n)y_n + \frac{f''(x_n)}{2}y_n^2 + \ldots + \frac{f^{(q)}(x_n)}{q!}y_n^q \\ &= f(x_n) + f'(x_n)\left[-\frac{f(x_n)}{f'(x_n)}\right] + \frac{f''(x_n)}{2}y_n^2 + \ldots + \frac{f^{(q)}(x_n)}{q!}y_n^q \\ &= \frac{f''(x_n)}{2}y_n^2 + \ldots + \frac{f^{(q)}(x_n)}{q!}y_n^q. \end{aligned}$$

However, since

$$\begin{aligned} y_n = -\frac{f(x_n)}{f'(x_n)} \quad &\Longrightarrow \quad y_n \equiv_{p^{2^n}} -\frac{f(x_n)}{f'(x_n)} \\ &\Longleftrightarrow \quad y_n^2 \equiv_{p^{2^{n+1}}} \left[\frac{f(x_n)}{f'(x_n)}\right]^2 \ \text{(bec. } -\frac{f(x_n)}{f'(x_n)} \equiv 0 \ (\mathrm{mod}\ p^{2^n})) \\ &\Longleftrightarrow \quad y_n^2 \equiv_{p^{2^{n+1}}} 0, \end{aligned}$$

then

$$f(x_{n+1}) \equiv_{p^{2^{n+1}}} \ y_n^2 \left\{\frac{f''(x_n)}{2} + \ldots + \frac{f^{(q)}(x_n)}{q!}y_n^{q-2}\right\} \equiv_{p^{2^{n+1}}} \ 0.$$

Similarly, it may be verified using TEF that the congruence relation $f'(x_{n+1}) \equiv_p f'(x_n) \not\equiv_p 0$ holds. Thus, the results are also true for the case $n+1$. By principle of induction, we conclude that

$$\forall n \in \mathbb{N}_0 : \ x_n \in \mathbb{Z}_p, \quad f(x_n) \equiv_{p^{2^n}} 0 \quad \text{and} \quad f'(x_n) \not\equiv_p 0,$$

proving (i).

Proof of (ii). Now we prove the convergence of the sequence generated by (NR), with initial value x_0, to a unique zero $\xi \equiv_p x_0$ in $\mathbb{Z}_p$ with order 2^n. At this juncture, we remark that the convergence result is already known to hold true as stated in Greenberg (1969). However, we give our proof as follows. To begin with, we consider the norm of the difference of two consecutive approximants x_n and x_{n+1}. So, by (NR), we have

$$|x_{n+1} - x_n|_p = \left|x_n - \frac{f(x_n)}{f'(x_n)} - x_n\right|_p = \frac{|f(x_n)|_p}{|f'(x_n)|_p} \leqslant p^{-2^n}.$$

Evidently,

$$|x_{n+1} - x_n|_p \longrightarrow 0 \quad \text{as} \quad n \to \infty.$$

Hence, the sequence of approximants $(x_n)_{n\in\mathbb{N}_0}$ is Cauchy. Thus, $(x_n)_{n\in\mathbb{N}_0}$ (being well-defined) must therefore converge to a zero $\xi \equiv_p x_0$ of f in $\mathbb{Z}_p$. Since $(x_n)_{n\in\mathbb{N}_0}$ is uniquely determined by the iterative formula (NR), then ξ is unique. Next, we show that for two different values of x_0, which are congruent modulo p, their respective approximants converges to the same root ξ in $\mathbb{Z}_p$. To prove this claim, we proceed by classical arguments in proving

uniqueness. Suppose that, for a given x satisfying the condition that $f(x) \equiv_p 0$ and $f'(x) \not\equiv_p 0$, the polynomial f admits two roots in $\mathbb{Z}_p$. Let these two roots in $\mathbb{Z}_p$ be ξ_1 and ξ_2. Clearly, $\xi_1 \equiv_p \xi_2$. From TEF, expanding f in ξ_2 at ξ_1, we know that there is a non-zero integer b such that

$$f(\xi_2) = f(\xi_1) + f'(\xi_1)(\xi_2 - \xi_1) + (\xi_2 - \xi_1)^2 b.$$

However, by assumption, we have $f(\xi_1) = f(\xi_2) = 0$. So,

$$(\xi_2 - \xi_1)[f'(\xi_1) + (\xi_2 - \xi_1)b] = 0.$$

Moreover, it is evident that $f'(\xi_1) \neq 0$ since $f'(\xi_1) \not\equiv_p 0$. Therefore, we are left with $\xi_1 - \xi_2 = 0$, or equivalently $\xi_1 = \xi_2$. Here, we conclude that the root is indeed unique.

Finally, as the p-adic valuation of the difference of two consecutive approximants x_{n+1} and x_n is bounded by p^{-2^n} for every $n \in \mathbb{N}_0$, then we find that the sequence $(x_n)_{n\in\mathbb{N}_0}$ converges to ξ with order 2^n. This proves the second part (ii). □

Remark 3.1. *Ignacio et al. (2016) considered the problem of finding a q-th root of a p-adic number through the calculation of a p-adic root of the polynomial equation $f(x) = x^q - a = 0$. Their discussion was limited to p-adic numbers $a \in \mathbb{Q}_p$ such that $|a|_p = p^{-mq}b$ where $|b|_p = 1$ and $m \in \mathbb{Z}$. We point out that in order to find a q-th root of a, it suffices to find a q-th root of b and then multiply it with p^m. Thus, the author may have instead assume that $m = 0$ so to simplify the computation.*

In relation to Remark 3.1, we have the following consequence of Theorem 3.1 which is a simplified version of the main result presented in Ignacio et al. (2016).

Corollary 3.1. *Let $f(x) = x^q - a \in \mathbb{Z}_p[x]$, where p and q are primes such that $p > q$, and $(x_n)_{n\in\mathbb{N}_0}$ be the sequence of p-adic numbers obtained from the Newton-Raphson iteration* (NR)*. If x_0 is a q-th root of a modulo p, then the following statements holds:*

(i)
$$\forall n \in \mathbb{N}_0 : \begin{cases} x_n \in \mathbb{Z}_p, \\ f(x_n) \equiv_{p^{2^n}} 0 \quad \text{or equivalently,} \quad x_n^q \equiv_{p^{2^n}} a, \\ f'(x_n) \not\equiv_p 0. \end{cases}$$

(ii) $(x_n)_{n\in\mathbb{N}_0}$ *converges to a q-th root of a.*

Proof. We only provide the first few lines of the proof. The rest follows exactly from the proof of Theorem 3.1. So, let $f(x) = x^q - a \in \mathbb{Z}_p[x]$, where p and q are primes such that $p > q$. Further, assume that x_0 is a q-th root of a modulo p. Clearly, $x_0 \in \mathbb{Z}$, and so $x_0 \in \mathbb{Z}_p$. Moreover, $x_0^q \equiv_p a$. Hence,

$f(x_0) = x_0^q - a \equiv_p 0$. Meanwhile, we easily find that $f'(x_0) = qx_0^{q-1}$. Evidently, $q \not\equiv_p 0$ since $p > q$. Similarly, $x^{q-1} \not\equiv_p 0$, otherwise we'll contradict the assumption that $x_0^q \equiv_p a$. Therefore, $f'(x_0) = qx_0^{q-1} \not\equiv_p 0$. This proves (i) for $n = 0$. From here onwards, the proof follows the same line of arguments from the proof of Theorem 3.1. □

In their work, Ignacio et al. (2016) used binomial expansion (which seems to be quite complicated) in order to obtain an estimate for $|f(x_n)|_p$. However, by Remark 3.1, the computation of the bound for $|f(x_n)|_p$ given here was simplified and obtained efficiently through a mere application of TEF.

Remark 3.2 (Rate of convergence)**.** *In view of the proof of Theorem 3.1(ii) and Remark 3.1, one could expect that the p-adic valuation of the difference of two consecutive approximants x_{n+1} and x_n obtained from a root-finding algorithm, such as the Newton-Raphson* (NR)*, will always be of the form γ^n. This, as we have seen in the proof of Theorem 3.1(i), is a consequence of the congruence $f(x_0) \equiv 0 \pmod{p}$ and the valuation of $f(x_n)$. In this regard, we may call a method with a rate of convergence γ^n (dropping the exponent n) to be of order γ in the p-adic sense. For instance, in our case, we may view the Newton-Raphson's algorithm to be a method having 'quadratic' rate of convergence in the p-adic sense since the sequence of approximants $(x_n)_{n\in\mathbb{N}_0}$ obtained from* (NR) *satisfies the condition $|x_{n+1} - x_n|_p \leq p^{-2^n}$. By this notion, we could relate the convergence of the method in the real case which is in fact quadratic. Nonetheless, we could mimic the argument of showing uniqueness in the proof of Theorem 3.1(ii) to exhibit a similar definition of rate of convergence as in the real case. Indeed, given the assumptions in Theorem 3.1 and for all $n \in \mathbb{N}_0$, we can find a non-zero integer b such that, by TEF (expanding in ξ at x_n), we have*

$$0 = f(\xi) = f(x_n) + f'(x_n)(\xi - x_n) + b(\xi - x_n)^2.$$

Rearranging this equation, and taking into account the definition of x_{n+1}, we get

$$x_{n+1} - \xi = b(x_n - \xi)^2. \tag{1}$$

Here, $f'(x_n)$ is clearly non-zero since $f'(x_n) \not\equiv_p 0$. Now, taking the p-adic valuation of both sides of (1) *and employing Remark 2.1, we get*

$$|x_{n+1} - \xi|_p = |b|_p |x_n - \xi|_p^2,$$

for n sufficiently large. $|b|_p$ is certainly non-zero since, otherwise, $b = 0$ which is not the case. Apparently, the method has 'quadratic convergence' in the p-adic setting.

4. Conclusion

The approximation of roots of polynomial equations have been a longstanding application of Newton-Raphson method. In this work, we have considered an analogue of this method in the p-adic case. It was found that the sequence of approximants $(x_n)_{n\in\mathbb{N}_0}$ obtained through the p-adic analogue of Newton-Raphson method, with initial iterate x_0, converges to a unique zero $\xi \equiv_p x_0$ of

f in $\mathbb{Z}_p$ with order 2^n. As an analogy to the case of reals, the iteration scheme is viewed as a method enjoying a 'quadratic' rate of convergence in the p-adic sense. On this account, with the idea of rate of convergence in mind, we ask if there are other root-finding algorithms which are more efficient compared to Newton-Raphson method in computing roots of general polynomial equations in the p-adic setting. Consequently, the answer to this problem will be the subject of further discussion elsewhere.

Acknowledgment

The author wishes to thank the anonymous referees for carefully handling and examining his manuscript. Their constructive comments and suggestions greatly improved the quality of the paper. The proof of the main result was substantially refined due to the valuable comment of one of the referee. Prior to the publication of this work, the investigation of the p-adic analogue of Steffensen's, Halley's and Olver's method has been carried out by the author in Rabago and Bacani (2016), Rabago (2016a) and Rabago (2016b), respectively.

References

Brekke, L. and Freund, P. (1993). p-adic numbers in physics. *Phys. Rept.*, **233**(1):1–66.

Dragovich, B. and Dragovich, A. (2009). A p-adic model of dna sequence and genetic code. *p-Adic Numbers Ultrametric Anal. Appl.*, **1**(1):34–41.

Dumas, J. (2014). On newton-raphson iteration for multiplicative inverses modulo prime powers. *IEEE Trans. Comput.*, **63**(8):2106–2109.

Greenberg, M. (1969). *Lectures on Forms of Many Variables*. W. A.Benjamin, 1st edition.

Ignacio, P., Addawe, J., Alangui, W., and Nable, J. (2013). Computation of square and cube roots of p-adic numbers via newton-raphson method. *J. Math. Res.*, **5**(2):31–38.

Ignacio, P., Addawe, J., and Nable, J. (2016). p-adic qth roots via newton-raphson method. *Thai j. Math.*, **14**(2):417–429.

Katok, S. (2007). *p-Adic Analysis Compared with Real*, volume **37** of *Student Mathematical Library*. American Mathematical Society.

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

Knapp, M. and Xenophontos, C. (2010). Numerical analysis meets number theory: Using root finding methods to calculate inverses mod p^n. *Appl. Anal. Discrete Math.*, **4**:23–31.

Koblitz, N. (1984). *p-adic Numbers, p-adic Analysis and zeta Functions*. Springer-Verlag, 2nd edition.

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

Rabago, J. F. T. (2016b). Olver's method for solving roots of p-adic polynomial equations. *Ital. J. Pure. Appl. Math.*, **36**(2):739–748.

Rabago, J. F. T. and Bacani, J. B. (2016). Steffensen's analogue for approximating roots of p-adic polynomial equations. In *Numerical Computations: Theory and Algorithms (NUMTA–2016)*, volume **1776**, page 090038. AIP Conference Proceedings.

Razikov, U. A. (2013). What are p-adic numbers? what are they used for? *Asia Pac. Math. Newsl.*, **3**(4):1–6.

Vladimirov, V., Volovich, I., and Zelenov, E. (1994). *p-Analysis and Mathematical Physics*. World Scientific, Singapore.

Zerzaihi, T. and Kecies, M. (2011). Computation of the cubic root of a p-adic number. *J. Math. Res.*, **3**(3):40–47.

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