

Computation of Square and Cube Roots of p -Adic Numbers via Newton-Raphson Method

Paul Samuel P. Ignacio¹, Joel M. Addawe¹, Wilfredo V. Alangui¹ & Job A. Nable²

¹ Department of Mathematics and Computer Science, University of the Philippines Baguio, Baguio City, Philippines

² Department of Mathematics, Ateneo de Manila University, Quezon City, Philippines

Correspondence: Paul Samuel P. Ignacio, Department of Mathematics and Computer Science, University of the Philippines Baguio, Baguio City, Philippines. Tel: 63-917-507-071. E-mail: paul_spi12@yahoo.com

Received: January 28, 2013 Accepted: February 24, 2013 Online Published: March 14, 2013

doi:10.5539/jmr.v5n2p31 URL: <http://dx.doi.org/10.5539/jmr.v5n2p31>

Abstract

The problem of finding square roots of p -adic integers in $\mathbb{Z}_p$, $p \neq 2$, has been a classic application of Hensel's lemma. A recent development on this problem is the application and analysis of convergence of numerical methods in approximating p -adic numbers. For a p -adic number a , Zerzaihi, Kecies, and Knapp (2010) introduced a fixed-point method to find the square root of a in $\mathbb{Q}_p$. Zerzaihi and Kecies (2011) later extended this problem to finding the cube root of a using the secant method. In this paper, we compute for the square roots and cube roots of p -adic numbers in $\mathbb{Q}_p$, using the Newton-Raphson method. We present findings that confirm recent results on the square roots of p -adic numbers, and highlight the advantages of this method over the fixed point and secant methods. We also establish sufficient conditions for the convergence of this method, and determine the speed of its convergence. Finally, we determine how many iterations are needed to obtain a specified number of correct digits in the approximate.

Keywords: p -adic numbers, square roots, Newton-Raphson method

1. Introduction

Let p be a prime, $\mathbb{Q}_p$ and $\mathbb{Z}_p$ be the fields of p -adic numbers and p -adic integers respectively. The introduction of the p -adic norm in the field $\mathbb{Q}$ paves the way to the construction of $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ so radically different from $\mathbb{R}$. Hensel's lemma has had a significant impact in the study of these fields by providing sufficient conditions for the existence of roots in $\mathbb{Z}_p$ of polynomials in $\mathbb{Z}_p[x]$. A survey of some characterizations of m th roots of unity in $\mathbb{Q}_p$ for any positive integer m appears in Koblitz (1984). A classic application of Hensel's lemma deals with the problem of finding the square roots of a p -adic number a in $\mathbb{Q}_p$, where $p \neq 2$. A recent development on this problem is the application and analysis of convergence of numerical methods in approximating p -adic numbers. In fact, this recent development led to several related problems. Knapp and Xenophontos (2010) applied several root-finding methods for computing the multiplicative inverses of integers modulo p^n , $n \in \mathbb{N}$. A similar problem was addressed by Dumas (2012) by using the Newton-Raphson iteration over $\mathbb{Q}_p$ to compute for multiplicative inverses of p -adic numbers modulo p^n . Zerzaihi, Kecies, and Knapp (2010) used a fixed point iteration to approximate the solutions of $x^2 = a$, $a \in \mathbb{Q}_p$ in $\mathbb{Q}_p$. Zerzaihi and Kecies (2011) 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 method.

In this paper, we compute for the square root and cube root of a p -adic number a in $\mathbb{Q}_p$, where $p > 2$ and $p > 3$ respectively, using the Newton-Raphson method. Given a root of order r , we determine the order of the approximate root after n iterations. The paper confirms earlier results on the square roots of p -adic numbers, and highlights the advantages of the Newton-Raphson method over the fixed point and the secant methods. We give conditions on r to ensure convergence and we determine the speed of convergence. Finally, we determine how many iterations are needed to obtain a specified number of correct digits in the approximate.

2. Preliminaries

We shall begin our discussion by introducing the basic properties of $\mathbb{Q}_p$. For a much detailed presentation of this field, see Katok (2001).

2.1 The Field $\mathbb{Q}_p$ of p -Adic Numbers

We begin by introducing a *valuation* on $\mathbb{Q}$.

Definition 1 Let $p \in \mathbb{N}$ be a prime number, $0 \neq x \in \mathbb{Q}$. The p -adic valuation $v_p(x)$ of x is defined as

$$v_p(x) = \begin{cases} r, & \text{if } x \in \mathbb{Z} \text{ and } r \text{ is the largest power of } p \text{ such that } p^r | x; \\ v_p(a) - v_p(b), & \text{if } x = \frac{a}{b}, a, b \in \mathbb{Z}, (a, b) = 1 \text{ and } b \neq 0. \end{cases} \quad (1)$$

With this valuation, we can define a map $|\cdot|_p : \mathbb{Q} \rightarrow \mathbb{R}^+$ as follows:

Definition 2 Let p be a prime number, and $x \in \mathbb{Q}$. We define the p -adic norm $|\cdot|_p$ of x as

$$|x|_p = \begin{cases} p^{-v_p(x)}, & \text{if } x \neq 0; \\ 0, & \text{if } x = 0. \end{cases} \quad (2)$$

With this definition of $|\cdot|_p$ on $\mathbb{Q}$, the p -adic norm takes only integral powers of p and zero, that is the range of this mapping is the set $\{p^n | n \in \mathbb{Z}\} \cup \{0\}$. It may be verified that the p -adic norm $|\cdot|_p$ satisfies the following properties

- 1) $|xy|_p = |x|_p |y|_p$;
- 2) $|x + y|_p \leq \max\{|x|_p, |y|_p\}$ where equality holds if $|x|_p \neq |y|_p$;
- 3) $\left| \frac{x}{y} \right|_p = \frac{|x|_p}{|y|_p}$.

An interesting consequence of the application of the p -adic norm to $\mathbb{Q}$ is the new formulation of distance in the metric space $(\mathbb{Q}, |\cdot|_p)$. Note that for $a, b \in \mathbb{Q}$, a and b are “close” if $|a - b|_p$ is close to zero. Hence, in the metric space $(\mathbb{Q}, |\cdot|_3)$, 12 is actually closer to three than two is!

We are now in the position to define formally the field $\mathbb{Q}_p$ of p -adic numbers.

Definition 3 The field of p -adic numbers $\mathbb{Q}_p$ 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

$$|a|_p = \lim_{n \rightarrow \infty} |a_n|_p \quad (3)$$

where $\{a_n\}$ is a Cauchy sequence of rational numbers representing $a \in \mathbb{Q}_p$.

The following theorem provides a way to write any element of $\mathbb{Q}_p$ in a unique representation.

Theorem 4 Let $a \in \mathbb{Q}_p$. Then a has unique p -adic expansion

$$a = a_n p^n + a_{n+1} p^{n+1} + \dots + a_{-1} p^{-1} + a_0 + a_1 p + a_2 p^2 + \dots = \sum_{i=n}^{\infty} a_i p^i \quad (4)$$

where $a_i \in \mathbb{Z}$ and $0 \leq a_i \leq p - 1$ for $i \geq n$.

Note that this representation of p -adic numbers is exactly the base p expansion of integers. A short notation for a p -adic number $a = a_n p^n + a_{n+1} p^{n+1} + \dots + a_{-1} p^{-1} + a_0 + a_1 p + a_2 p^2 + \dots$ is $a_n a_{n+1} \dots a_{-1} \cdot a_0 a_1 a_2 \dots$ where we only write the coefficients in the expansion.

Definition 5 The set $\mathbb{Z}_p^\times$ of p -adic units is given by

$$\mathbb{Z}_p^\times = \left\{ a \in \mathbb{Z}_p : a = \sum_{i=0}^{\infty} a_i p^i, a_0 \neq 0 \right\} = \{a \in \mathbb{Q}_p : |a|_p = 1\} \quad (5)$$

Since every p -adic number has its unique representation described by Theorem 4, the p -adic units offer an alternative way of writing them in terms of their p -adic valuation.

Theorem 6 Let $a \in \mathbb{Q}_p$, then

$$a = p^{v_p(a)} u \quad (6)$$

for some $u \in \mathbb{Z}_p^\times$.

Definition 7 Let $a, b \in \mathbb{Q}_p$. Then b is an n th root of a of order $k \in \mathbb{N}$ if and only if $b^n \equiv a \pmod{p^k}$.

The following result will be central to our discussion.

Lemma 8 Let $a, b \in \mathbb{Q}_p$. Then

$$a \equiv b \pmod{p^k} \Leftrightarrow |a - b|_p \leq p^{-k}. \quad (7)$$

2.2 Functions over $\mathbb{Q}_p$

In this section, we introduce fundamental concepts on the analysis of functions defined over $\mathbb{Q}_p$. We start by defining continuous functions.

Definition 9 Let $X \subset \mathbb{Q}_p$. A function $f : X \rightarrow \mathbb{Q}_p$ is said to be **continuous at** $a \in X$ if for each $\epsilon > 0$ there exists a $\delta > 0$ such that if $|x - a|_p < \delta$, then $|f(x) - f(a)|_p < \epsilon$. A function f is said to be **continuous on** $E \subseteq X$ if f is continuous for every $a \in E$.

We shall show in the next example that, as in the real case, polynomial functions with coefficients in $\mathbb{Q}_p$ are continuous in any subset of $\mathbb{Q}_p$.

Example 10 Let $a \in \mathbb{Q}_p$, and $P(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in \mathbb{Q}_p[x]$. Then for $\epsilon > 0$, we seek a suitable $\delta > 0$ such that if $|x - a|_p < \delta$, then $|P(x) - P(a)|_p < \epsilon$ for all $x \in \mathbb{Q}_p$. Without loss of generality, assume $|x|_p < |a|_p$. Then,

$$|P(x) - P(a)|_p \leq |x - a|_p \max \left\{ |a_i a^{i-1}|_p \right\}_{i=1}^n. \quad (8)$$

Let $\max \left\{ |a_i a^{i-1}|_p \right\}_{i=1}^n = M$, and choose $\delta = \frac{\epsilon}{M}$ so that if

$$|x - a|_p < \frac{\epsilon}{M} \quad (9)$$

$$\Rightarrow |x - a|_p M < \epsilon \quad (10)$$

$$\Rightarrow |P(x) - P(a)|_p < \epsilon \quad (11)$$

Therefore, $P(x)$ is continuous at a .

We define next the derivative of p -adic functions.

Definition 11 Let $X \subseteq \mathbb{Q}_p$, $a \in X$ be an accumulation point of X . A function $f : X \rightarrow \mathbb{Q}_p$ is **differentiable** at a if the **derivative of f at a** , defined by

$$f'(a) = \lim_{x \rightarrow a} \frac{f(x) - f(a)}{x - a} \quad (12)$$

exists. A function $f : X \rightarrow \mathbb{Q}_p$ is differentiable on X if $f'(a)$ exists at all $a \in X$.

With this definition of derivative, if $P(x) = \sum_{i=0}^n a_i x^i$ where $a_i \in \mathbb{Q}_p$, then $P'(x) = \sum_{i=1}^n i a_i x^{i-1}$. It may also be verified that polynomials in $\mathbb{Q}_p$ have continuous derivatives.

2.3 p -Adic Roots

We shall now narrow our discussion of p -adic functions on p -adic polynomials. In particular, we are concerned with finding the solutions of these polynomials in $\mathbb{Q}_p$. The next lemma has been the basis for many existing results on p -adic roots.

Theorem 12 (Hensel's Lemma) Let $F(x) = c_0 + c_1x + \dots + c_nx^n \in \mathbb{Z}_p[x]$ and $F'(x) = c_1 + 2c_2x + \dots + nc_nx^{n-1}$ be its derivative. If for some $\overline{a_0} \in \mathbb{Z}_p$ we have $F(\overline{a_0}) \equiv 0 \pmod{p}$ and $F'(\overline{a_0}) \not\equiv 0 \pmod{p}$. Then, there exists a unique $a \in \mathbb{Z}_p$ such that $F(a) = 0$ and $a \equiv \overline{a_0} \pmod{p}$.

Hensel's lemma paves the way for the study of roots of p -adic numbers. The following result provides the condition for the existence of roots in $\mathbb{Z}_p$.

Theorem 13 (Katok, 2007) A polynomial with integer coefficients has a root in $\mathbb{Z}_p$ if and only if it has an integer root modulo p^k for any $k \geq 1$.

A natural consequence of the previous result are the following propositions with their corresponding corollaries.

Proposition 14 A rational integer a not divisible by p has a square root in $\mathbb{Z}_p$, ($p \neq 2$) if and only if a is a quadratic residue modulo p .

Corollary 15 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 $x = p^{2m}y^2$ with $m \in \mathbb{Z}$ and $y \in \mathbb{Z}_p^\times$ a p -adic unit.

Proposition 16 (Zerzaihi and Kecies, 2011) A rational integer a not divisible by p has a cubical root in $\mathbb{Z}_p$ ($p \neq 3$) if and only if a is a cubic residue modulo p .

Corollary 17 (Zerzaihi and Kecies, 2011) Let p be a prime, then

- 1) If $p \neq 3$, then a has a cube root in $\mathbb{Q}_p$ if and only if $v_p(a) = 3m$, $m \in \mathbb{Z}$ and $u = v^a$ for some $v \in \mathbb{Z}_p^\times$.
- 2) If $p = 3$, then a has a cube root in $\mathbb{Q}_3$ if and only if $v_p(a) = 3m$, $m \in \mathbb{Z}$ and $u \equiv 1 \pmod{9}$ or $u \equiv 2 \pmod{3}$.

Note that Corollary 15 and Corollary 17 provide the condition for the existence of square roots and cube roots in $\mathbb{Q}_p$.

2.4 The Newton-Raphson Method

One common method of approximating roots of functions is the Newton-Raphson method. This method requires that functions, whose roots are to be approximated, be differentiable. For a function, say $f(x)$ and its derivative $f'(x)$, the method makes use of the iterative function

$$g(x) = x - \frac{f(x)}{f'(x)} \quad (13)$$

from which the recurrence relation will be obtained. The method is employed by first having an initial guess x_0 and then, using the formula $x_{n+1} = g(x_n)$, obtain a recurrence relation which will be used for approximation. If the initial guess x_0 and the iterative function are suitably chosen, the sequence $\{x_n\}$ should converge to a root of f . The rate of convergence of the method gives the rate at which the number of correct digits in the approximation increases. For instance, if the rate of convergence is of order two (quadratic convergence), then the number of correct digits in the approximate doubles after each iteration. In Knapp and Xenophontos (2010), the authors used this method to find multiplicative inverses of p -adic units modulo p^n .

Example 18 We have seen that p -adic polynomials have continuous derivatives. Hence, for $a \in \mathbb{Q}_p$, the function $f(x) = x^2 - a$ satisfies the conditions of the Newton-Raphson method with recurrence relation

$$\begin{aligned} x_{n+1} &= x_n - \frac{f(x_n)}{f'(x_n)} \\ &= x_n - \frac{x_n^2 - a}{2x_n} \\ &= \frac{x_n^2 + a}{2x_n} \end{aligned} \quad (14)$$

3. Results

The existence of the square and cube roots of p -adic numbers justifies our effort to approximate them.

3.1 The Square Roots of p -Adic Numbers

By Corollary 15, we limit our discussion to $a \in \mathbb{Q}_p$ such that

$$|a|_p = p^{-2m}, m \in \mathbb{Z} \quad (15)$$

Proposition 19 Let $\{x_n\}$ be the sequence of p -adic numbers obtained from the Newton-Raphson iteration. If x_0 is a square root of a of order r , $|x_0|_p = p^{-m}$, $r > 2m$, and $p > 2$, then

- (i) $|x_n|_p = p^{-m}$ for $n = 1, 2, 3, \dots$;
- (ii) $x_n^2 \equiv a \pmod{p^{2^n r - 2m(2^n - 1)}}$;
- (iii) $\{x_n\}$ converges to the square root of a .

Proof. We first prove (i) and (ii) by induction. Let $n = 1$, then by our assumption, we have

$$x_0^2 = a + bp^r, \quad (16)$$

where $0 < b < p$. Using Equation (14), we have

$$|x_1|_p = \frac{|x_0^2 + a|_p}{|2x_0|_p} = \frac{|2a + bp^r|_p}{|2x_0|_p} = \frac{\max\{|2a|_p, |bp^r|_p\}}{|2x_0|_p} = \frac{p^{-2m}}{p^{-m}} = p^{-m}. \quad (17)$$

Also by Equation (14), we have

$$x_1^2 - a = \left(\frac{x_0^2 + a}{2x_0} \right)^2 - a = \frac{(x_0^2 - a)^2}{4x_0^2}. \quad (18)$$

Let $\phi(x_0) = \frac{1}{4x_0^2}$. So that

$$x_1^2 - a = (x_0^2 - a)^2 \phi(x_0). \quad (19)$$

Note also that

$$|\phi(x_0)|_p \leq p^{2m}. \quad (20)$$

Since x_0 is a square root of a of order r , we have

$$|(x_0^2 - a)^2|_p \leq p^{-2r} \quad (21)$$

and therefore

$$|x_1^2 - a|_p \leq p^{2m} p^{-2r} = p^{2m-2r} \quad (22)$$

By Lemma (8),

$$x_1^2 - a \equiv 0 \pmod{p^{2r-2m}}. \quad (23)$$

Now, assume that our conclusions hold for $n - 1$. That is,

$$|x_{n-1}|_p = p^{-m} \quad (24)$$

$$x_{n-1}^2 \equiv a \pmod{p^{2^{n-1}r-2m(2^{n-1}-1)}} \quad (25)$$

Note that the equivalence in (25) implies that

$$x_{n-1}^2 = a + bp^{2^{n-1}r-2m(2^{n-1}-1)}, \quad (26)$$

where $0 < b < p$. Using Equation (14), we have

$$|x_n|_p = \frac{|x_{n-1}^2 + a|_p}{|2x_{n-1}|_p} = \frac{|2a + bp^{2^{n-1}r-2m(2^{n-1}-1)}|_p}{|2x_{n-1}|_p} = \frac{\max\{|2a|_p, |bp^{2^{n-1}r-2m(2^{n-1}-1)}|_p\}}{|2x_{n-1}|_p} = \frac{p^{-2m}}{p^{-m}} = p^{-m}. \quad (27)$$

Also, we have that

$$x_n^2 - a = \left(\frac{x_{n-1}^2 + a}{2x_{n-1}} \right)^2 - a = \frac{(x_{n-1}^2 - a)^2}{4x_{n-1}^2}. \quad (28)$$

Let $\phi(x_{n-1}) = \frac{1}{4x_{n-1}^2}$. So that

$$x_n^2 - a = (x_{n-1}^2 - a)^2 \phi(x_{n-1}). \quad (29)$$

Note now that by Equation (24)

$$|\phi(x_{n-1})|_p \leq p^{2m}. \quad (30)$$

Since x_{n-1} is a square root of a of order $2^{n-1}r - 2m(2^{n-1} - 1)$, we have

$$|(x_{n-1}^2 - a)^2|_p \leq p^{-2(2^{n-1}r-2m(2^{n-1}-1))}. \quad (31)$$

Hence we have

$$|x_n^2 - a|_p \leq p^{2m} p^{-2(2^{n-1}r-2m(2^{n-1}-1))} = p^{2m2^n-4m+2m-2^n r} = p^{2m(2^n-1)-2^n r}. \quad (32)$$

By Lemma (8), we have

$$x_n^2 - a \equiv 0 \pmod{p^{2^n r - 2m(2^n - 1)}}. \quad (33)$$

Finally, (iii) follows clearly from (32) as we take $n \rightarrow \infty$.

We now turn to the convergence of the method.

Proposition 20 *Let $\{x_n\}$ be the sequence of approximates converging to the square root of a obtained from the Newton-Raphson method. If $p > 2$*

(a) *The speed of convergence of the sequence $\{x_n\}$ is of order $\lambda_n - m = 2^n r - m(2^{n+1} - 1)$;*

(b) *The number of iterations to obtain at least M correct digits is*

$$n = \left\lceil \frac{\ln \left(\frac{M-m}{r-2m} \right)}{\ln 2} \right\rceil. \quad (34)$$

Proof. For the speed of convergence, we investigate two consecutive approximates x_{n+1} and x_n . Note that

$$x_{n+1} - x_n = \frac{x_n^2 + a}{2x_n} - x_n = \frac{-1}{2x_n} (x_n^2 - a). \quad (35)$$

Then,

$$|x_{n+1} - x_n|_p = \left| \frac{-1}{2x_n} \right|_p |(x_n^2 - a)|_p \leq p^{m-\lambda_n} \quad (36)$$

Hence,

$$x_{n+1} - x_n \equiv 0 \pmod{p^{\lambda_n - m}}. \quad (37)$$

Note that if the order of the root x_i is K (that is, $x_i^2 - a \equiv 0 \pmod{p^K}$), the number of correct digits in the approximate is $K - m$ since $|\sqrt{a}|_p = p^{-m}$. Hence, to find the number of iterations n such that we have M correct digits in the approximate, we must set the order to $M + m$. That is,

$$\begin{aligned} 2^n r - 2m(2^n - 1) &= M + m \\ 2^n(r - 2m) &= M - m \\ 2^n &= \frac{M - m}{r - 2m} \end{aligned} \quad (38)$$

Since $\{x_n\}$ converges to the square root of a , by Proposition 21, $r - 2m > 0$. Hence we take

$$n = \left\lceil \frac{\ln \left(\frac{M-m}{r-2m} \right)}{\ln 2} \right\rceil \quad (39)$$

This n is a sufficient number of iterations to provide at least M correct digits in the approximate. $\square$

These results confirm the results of Zerzaihi, Kecies, and Knapp (2010) for the case when the square root of a is of multiplicity two.

3.2 The Cube Roots of p -Adic Numbers

We follow the method we used for the approximation of the square roots of p -adic numbers. We shall limit our discussion to $a \in \mathbb{Q}_p$ such that

$$|a|_p = p^{-3m}, m \in \mathbb{Z}. \quad (40)$$

Now, let $f(x) = x^3 - a$. Employing the Newton-Raphson method, we obtain the new recurrence relation

$$x_{n+1} = \frac{2x_n^3 + a}{3x_n^2}. \quad (41)$$

Proposition 21 *Let $\{x_n\}$ be the sequence of p -adic numbers obtained from the Newton-Raphson iteration. If x_0 is a cube root of a of order r , $|x_0|_p = p^{-m}$, $r > 3m$, and $p > 3$, then*

- (i) $|x_n|_p = p^{-m}$ for $n = 1, 2, 3, \dots$;
 (ii) $x_n^3 \equiv a \pmod{p^{2^n r - 3m(2^n - 1)}}$;
 (iii) $\{x_n\}$ converges to the cube root of a .

Proposition 22 Let $\{x_n\}$ be the sequence of approximates converging to the cube root of a obtained from the Newton-Raphson method. If $p > 3$, then

- a) The speed of convergence of the sequence $\{x_n\}$ is of order $\lambda_n - 2m = 2^n r - 3m2^n + m$;
 b) The number of iterations to obtain at least M correct digits is

$$n = \left\lceil \frac{\ln \left(\frac{M-2m}{r-3m} \right)}{\ln 2} \right\rceil. \quad (42)$$

Example 23 Let $p = 3$, $m = 2$ and $y = 1 + 2 \cdot 3 \in \mathbb{Z}_3^\times$. Then the p -adic number

$$\begin{aligned} a &= 3^{2m} y^2 \\ &= 3^{2(2)} (1 + 1 \cdot 3 + 2 \cdot 3^2 + 1 \cdot 3^3) \\ &= 1 \cdot 3^4 + 1 \cdot 3^5 + 2 \cdot 3^6 + 1 \cdot 3^7 \end{aligned} \quad (43)$$

has a square root in $\mathbb{Q}_3$ by Corollary 15. Now, note that

$$\begin{aligned} a &= 1 \cdot 3^4 + 1 \cdot 3^5 + 2 \cdot 3^6 + 1 \cdot 3^7 \\ &\equiv 1 \cdot 3^4 + 1 \cdot 3^5 \pmod{3^6} \\ &= 18^2 \pmod{3^6} \end{aligned} \quad (44)$$

Hence, $x_{n_0} = 18$ is a square root of $a = 3969$ of order $r = 6$. Suppose we want at least $M = 10$ correct digit in our approximate. By Equation (39), we must have

$$n = \left\lceil \frac{\ln \left(\frac{10-2}{6-2(2)} \right)}{\ln 2} \right\rceil = 2 \quad (45)$$

number of iterations. With this n and Proposition 19, we must obtain a square root of a of order

$$2^n r - 2m(2^n - 1) = 2^2(6) - 2(2)(2^2 - 1) = 12 \quad (46)$$

From Equation (14), we get the second iterate

$$(x_{n_0+2})^2 = \left(\frac{23,573,673}{309096} \right)^2 \quad (47)$$

Using GAP version 4.5.7 (with Pure Padic Number Family, precision 20), we obtain (in our short notation)

$$\begin{aligned} x_{n_0+2}^2 &= (.0020222222001212200001)^2 \\ &= .000011210000112212112112 \end{aligned} \quad (48)$$

which verifies our result since

$$3969 = .00001121 \quad (49)$$

4. Conclusion

In this paper, we set out to approximate the square and cube roots of p -adic numbers using the Newton-Raphson method for $p > 2$ and $p > 3$ respectively. Our results for the square root show that this method converges to the root in the same rate as the fixed point method introduced in Zerzaihi, Kecies, and Knapp (2010) for the case where $\sqrt{a}$ is a root of $g(x)$ of multiplicity two. Hence, for this case, the Newton-Raphson method provides an alternative

way of computing for the square roots of p -adic numbers without having to construct the function $g(x)$ described in Zerzaihi, Kecies, and Knapp (2010). Moreover, the Newton-Raphson method, which only requires one initial guess, may have an advantage over the secant method due to simplified calculations.

References

- Dumas, J. (2012). *On Newton-Raphson Iteration for Multiplicative Inverses Modulo Prime Powers*. Retrieved from <http://arxiv.org/pdf/1209.6626.pdf>
- Gouvea, F. (2003). *P-adic numbers: an introduction*. Springer-Verlag.
- Katok, S. (2001). *Real and p-adic analysis Course Notes for Math 497C MASS Program, Fall 2000*. Retrieved from http://www.math.psu.edu/katok_s/pub/p-adic.pdf
- Knapp, M., & Xenophontos, C. (2010). Numerical Analysis Meets Number Theory: Using Rootfinding Methods to calculate inverses modulo P^n . *Applicable Analysis and Discrete Mathematics*, 4, 23-31. Retrieved from <http://www.doiserbia.nb.rs/img/doi/1452-8630/2010/1452-86301000012K.pdf>
- Koblitz, N. (1984). *p-adic Numbers, p-adic Analysis and zeta Functions* (2nd ed.). Springer-Verlag.
- Zerzaihi, T., & Kecies, M. (2011). Computation of the Cubic Root of a p -adic Number. *Journal of Mathematics Research*, 3(3), 40-47. <http://dx.doi.org/10.5539/jmr.v3n3p40>
- Zerzaihi, T., Kecies, M., & Knapp, M. (2010). Hensel Codes of Square Roots of p -adic Numbers. *Applicable Analysis and Discrete Mathematics*, 4, 32-44. Retrieved from <http://www.doiserbia.nb.rs/img/doi/1452-8630/2010/1452-86301000009M.pdf>