Available online at http://scik.org
J. Math. Comput. Sci. 3 (2013), No. 4, 993-1003
ISSN: 1927-5307

ON THE SQUARE AND CUBE ROOTS OF P-ADIC NUMBERS

PAUL SAMUEL P. IGNACIO

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

Baguio City 2600, Philippines

Abstract. The study of the field of p-adic numbers has been an important area of research in mathematics, giving rise to several important results such as the Hasse-Minkowski Theorem and the Local-Global Principle. The analysis on the complete ultrametric space $\mathbb{Q}_p$ reveals many interesting properties that are radically different from $\mathbb{R}$, the completion of $\mathbb{Q}$ with respect to the euclidean norm. The application of different numerical methods, and the analysis of their convergence in $\mathbb{Q}_p$ has been a recent development in computational number theory. The application of the Newton-Raphson, fixed-point, and secant methods to compute for the square and cube roots of p-adic numbers in $\mathbb{Q}_p$ have been respectively addressed in [2, 5, 6]. In this paper, we complete the problem in [2] by computing the qth root of p-adic numbers in $\mathbb{Q}_p$ where $p \leq q \leq 3$. Given a root of order r, we determine the order of the nth iterate of the Newton-Raphson method, provide sufficient conditions for its convergence, and give the number of iterations required for any desired number of correct digits in the approximate.

Keywords: p-adic numbers; Newton-Raphson; square roots.

2000 AMS Subject Classification: 11J61; 11S05; 11Y99

1. Introduction

The use of algorithmic techniques and concepts to compute for p-adic numbers dates back to the time when Kurt Hensel developed the foundations of p-adic analysis. The basic

Received May 12, 2013

idea behind the use of numerical root-finding methods to compute for p-adic numbers is to determine the digits in their p-adic expansion using iterative methods. A classic result in p-adic analysis that employs numerical concepts is Hensel's lemma which provides the conditions for the existence of p-adic integral solutions of polynomials in $\mathbb{Z}_p[x]$. A well-known application of Hensel's lemma is on the computation of the square roots in $\mathbb{Z}_p$ of p-adic numbers using a method now known as Hensel lifting. Serre in [4] explicitly laid the conditions for the extension of the existence of square roots of p-adic numbers in $\mathbb{Q}_p$. The computation of the square roots and cube roots of p-adic numbers respectively using the fixed-point method and the secant method have been addressed in [5, 6]. In [2], the Newton-Raphson method was used to compute the square roots and cube roots of p-adic numbers respectively for the cases where $p > 2$ and $p > 3$. In this paper, we complete the problem in [2] by addressing the case where $p = 2$ for the square root and $p \leq 3$ for the cube root of p-adic numbers. For both cases, we provide the order of the nth iterate of the Newton-Raphson method, sufficient conditions for convergence, and the number of iterations required for any desired number of correct digits in the approximate.

2. Preliminaries

We necessarily start by defining a *valuation* on $\mathbb{Q}$.

Definition 2.1 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

$$v_p(x) = \begin{cases} r & \text{if } x \in \mathbb{Z} \text{ and } r \text{ is the largest integer such that } x \equiv 0 (\text{mod } p^r) \\ v_p(a) - v_p(b) & \text{if } x = \dfrac{a}{b},\ a, b \in \mathbb{Z}, (a, b) = 1 \text{ and } b \neq 0 \end{cases}$$

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

Definition 2.2 Let $p \in \mathbb{N}$ be a prime number, $x \in \mathbb{Q}$. The *p-adic norm* $|\cdot|_p$ of x is defined as

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

Using the p-adic norm and the process of completion, we have the following definition.

Definition 2.3 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

$$|a|_p = \lim_{n\to\infty} |a_n|_p$$

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

Because the p-adic norm $|\cdot|_p$ is non-Archimedean, we call $(\mathbb{Q}_p, |\cdot|_p)$ a *complete ultrametric space*. An interesting property of this complete ultrametric space is that we get a stronger condition for convergent sequences in $\mathbb{Q}_p$.

Theorem 2.4 *A sequence $\{x_n\}$ in $\mathbb{Q}_p$ is convergent if and only if*

$$\lim_{n\to\infty} |x_{n+1} - x_n|_p = 0 \qquad (1)$$

Since each element in $\mathbb{Q}_p$ is an equivalence class, the following theorem provides a convenient way to write the elements using its (unique) canonical representative.

Definition 2.5 Every p-adic number $a \in \mathbb{Q}_p$ has a unique representation

$$a = a_n p^n + a_{n+1} p^{n+1} + ... + a_{-1} p^{-1} + a_0 + a_1 p + a_2 p^2 + ... = \sum_{i=n}^{\infty} a_i p^i$$

where $a_i \in \mathbb{Z}$ and $0 \le a_i \le p-1$ for $i \ge n$ and $n < 0$.

A quick method of writing p-adic numbers is by writing just the coefficients of the powers of p. For instance, in $\mathbb{Q}_3$, $12 = 0 \cdot 3^0 + 1 \cdot 3^1 + 1 \cdot 3^2 + 0 \cdot 3^3 + ... = .0110...$

Definition 2.6 Let $\mathbb{Z}_p$ denote the set of p-adic integers, then

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

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

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

One can verify that all integers are p-adic integers. However it can be checked that $\frac{1}{2}$, among others, is an integer in $\mathbb{Q}_7$.

An alternative way of writing p-adic numbers is in terms of their p-adic valuation.

Theorem 2.7 *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 an important tool in our discussion.

Lemma 2.8 *Let $a, b \in \mathbb{Q}_p$. Then*

$$a \equiv b(\mod p^k) \Leftrightarrow |a-b|_p \leq p^{-k}$$

We next define what we shall refer to as the nth root of a p-adic number.

Definition 2.9 A p-adic number $b \in \mathbb{Q}_p$ is said to be an nth root of $a \in \mathbb{Q}_p$ of order $k \in \mathbb{N}$ if and only if $b^n \equiv a(\mathrm{mod}\ p^k)$.

This definition is the basis for the following results, the first of which is a simpler restatement of one of Serre's result in [4].

Theorem 2.10 *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 $n \in Z$ and $y \in \mathbb{Z}_p^\times$ a p-adic unit.*

Theorem 2.11 *Let p be a prime, then*

i. *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 $u = v^q$ for some $v \in \mathbb{Z}_p^\times$.*
ii. *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 $u \equiv 1($ mod $9)$ or $u \equiv 2(\mathrm{mod}\ 3)$.*

3. Main results

Theorem 3 on page 17.

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

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

On the Square Roots of p-adic Numbers

We shall now use the Newton-Raphson method to compute the square root of p-adic numbers in $\mathbb{Q}_p$ where $p = 2$. We follow the method used in [2]. Let $a \in \mathbb{Q}_p$ such that $|a|_p = p^{-2m}, m \in \mathbb{Z}$.

Proposition 3.1. *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, $|x_0|_p = p^{-m}$, $r > 2m+1$, and $p = 2$, then*

(i) $|x_n|_p = p^{-m}$ *for* $n = 1, 2, 3, \ldots$;

(ii) $x_n^2 \equiv a(\mod p^{2^n r - 2(m+1)(2^n - 1)})$;

(iii) $\{x_n\}$ *converges to the square root of* a

Proof. We prove by induction. Note first that by our assumption, we have

$$x_0^2 = a + bp^r$$

where $0 < b < p$. Since $p = 2$ and $r > 2m+1$, Eq. (2) then gives us

$$\begin{aligned} |x_1|_p &= \frac{|2a + bp^r|_p}{|2x_0|_p} \\ &= \frac{\max\{|2a|_p, |bp^r|_p\}}{|2x_0|_p} \\ &= \frac{p^{-(2m+1)}}{p^{-(m+1)}} \\ &= p^{-m} \end{aligned} \tag{3}$$

Also, by equation (2), we have

$$x_1^2 - a = \frac{(x_0^2 - a)^2}{4x_0^2}$$

Let $\phi(x_0) = \dfrac{1}{4x_0^2}$ and notice that

$$|\phi(x_0)|_p = p^{2(m+1)}$$

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

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

and therefore

$$\begin{aligned} |x_1^2 - a|_p &\leq p^{2(m+1)}p^{-2r} \\ &= p^{2(m+1)-2r} \end{aligned}$$

By Lemma 2.8

$$x_1^2 - a \equiv 0(\mod p^{2r-2(m+1)}) \tag{4}$$

Now, assume that

$$|x_{n-1}|_p = p^{-m} \tag{5}$$

$$x_{n-1}^2 \equiv a(\mod p^{2^{n-1}r-2(m+1)(2^{n-1}-1)}) \tag{6}$$

Hence,

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

where $0 < b < p$. By Eq. (2),

$$\begin{aligned} |x_n|_p &= \frac{|2a + bp^{2^{n-1}r-2(m+1)(2^{n-1}-1)}|_p}{|2x_{n-1}|_p} \\ &= \frac{\max\{|2a|_p, |bp^{2^{n-1}r-2(m+1)(2^{n-1}-1)}|_p\}}{|2x_{n-1}|_p} \\ &= \frac{p^{-(2m+1)}}{p^{-(m+1)}} \\ &= p^{-m} \end{aligned} \tag{7}$$

We also have

$$x_n^2 - a = \frac{(x_{n-1}^2 - a)^2}{4x_{n-1}^2}$$

Let $\phi(x_{n-1}) = \dfrac{1}{4x_{n-1}^2}$ and note that by equation (7)

$$|\phi(x_{n-1})|_p = p^{2(m+1)}$$

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

$$\begin{aligned} |x_n^2 - a|_p &\le p^{2(m+1)} p^{-2(2^{n-1}r - 2(m+1)(2^{n-1}-1))} \\ &= p^{2(m+1)(2^n-1) - 2^n r} \end{aligned} \tag{8}$$

By Lemma 2.8, we have

$$x_n^2 - a \equiv 0(\mod p^{2^n r - 2(m+1)(2^n-1)}) \tag{9}$$

Finally, (iii) follows clearly from inequality (8) as $n \to +\infty$. This completes the proof.

Now, let $\gamma_n = 2^n r - 2(m+1)(2^n - 1)$. We then have the following result.

Proposition 3.2. Let $\{x_n\}$ be the sequence of approximates converging to the square root of a obtained from the Newton-Raphson method in Proposition 3.1. If $p = 2$

(a) Then for every iteration, the number of correct digits in the approximate increases by $\gamma_n - (m+1) = 2^n r - (m+1)(2^{n+1} - 1)$

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

$$n = \left\lceil \frac{\ln\left(\frac{M-(m+2)}{r-2(m+1)}\right)}{\ln 2} \right\rceil$$

Proof. Consider two consecutive approximates x_{n+1} and x_n. Note that

$$\begin{aligned} |x_{n+1} - x_n|_p &= \left|\frac{-1}{2x_n}\right|_p |(x_n^2 - a)|_p \\ &\le p^{(m+1)-\gamma_n} \end{aligned}$$

Hence,

$$x_{n+1} - x_n \equiv 0(\mod p^{\gamma_n - (m+1)})$$

Since we want M correct digits in the approximate, we must set the order to $M+m$. That is,

$$2^n r - 2(m+1)(2^n - 1) = M + m$$
$$\Rightarrow 2^n = \frac{M-(m+2)}{r-2(m+1)}$$

Since $\{x_n\}$ is the sequence of p-adic numbers in Proposition 3.1, we have $r-2(m+1)>0$. Hence we take

$$n = \left\lceil \frac{\ln\left(\frac{M-(m+2)}{r-2(m+1)}\right)}{\ln 2} \right\rceil \tag{10}$$

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

On the Cube Roots of p-adic Numbers

We now compute for the cube roots of p-adic number in $\mathbb{Q}_p$ where $p \leq 3$. Let $|a|_p = p^{-3m}, m \in \mathbb{Z}$ and $f(x) = x^3 - a$. Employing the Newton-Raphson method, we obtain the new recurrence relation

$$x_{n+1} = \frac{2x_n^3 + a}{3x_n^2} \tag{11}$$

Proposition 3.3. 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, $|x_0|_p = p^{-m}$, and $r > 3m$ for $p=2$ or $r > 3m+2$ for $p=3$, then

(i) $|x_n|_p = p^{-m}$ for $n = 1, 2, 3, ...$

(ii) $\begin{cases} x_n^3 \equiv a(\mod p^{2^n r - 3m(2^n-1)}) & \text{if } p=2 \\ x_n^3 \equiv a(\mod p^{2^n r-(3m+1)(2^n-1)}) & \text{if } p=3 \end{cases}$

(iii) $\{x_n\}$ converges to the cube root of a

Proof. We again prove by induction. By our assumption, we have

$$x_0^3 = a + bp^r$$

where $0 < b < p$. Using Eq. (11), we have

$$\begin{aligned}
|x_1|_p &= \frac{|3a + 2bp^r|_p}{|3x_0^2|_p} \\
&= \frac{\max\{|3a|_p, |2bp^r|_p\}}{|3x_0^2|_p} \\
&= \begin{cases} \dfrac{p^{-3m}}{p^{-2m}} & \text{if } p = 2 \\ \dfrac{p^{-(3m+1)}}{p^{-(2m+1)}} & \text{if } p = 3 \end{cases} \\
&= p^{-m}
\end{aligned}$$

By equation (11),

$$x_1^3 - a = \frac{(x_0^3 - a)^2(8x_0^3 + a)}{27x_0^6}$$

Let $\phi(x_0) = \dfrac{(8x_0^3 + a)}{27x_0^6}$ and note that

$$\begin{aligned}
|\phi(x_0)|_p &= \frac{|8bp^r + 9a|_p}{|27x_0^6|_p} \\
&= \frac{\max\{|8bp^r|_p, |9a|_p\}}{|27x_0^6|_p} \\
&= \begin{cases} \dfrac{p^{-3m}}{p^{-6m}} & \text{if } p = 2 \\ \dfrac{p^{-(3m+2)}}{p^{-(6m+3)}} & \text{if } p = 3 \end{cases} \\
&= \begin{cases} p^{3m} & \text{if } p = 2 \\ p^{3m+1} & \text{if } p = 3 \end{cases}
\end{aligned}$$

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

$$|(x_0^3 - a)^2|_p \leq p^{-2r}$$

and therefore

$$|x_1^3 - a|_p \leq \begin{cases} p^{3m-2r} & \text{if } p = 2 \\ p^{(3m+1)-2r} & \text{if } p = 3 \end{cases}$$

By Lemma 2.8, we have

$$\begin{cases} x_1^3 - a & \equiv 0(\mod p^{2r-3m}) \text{ if } p = 2 \\ x_1^3 - a & \equiv 0(\mod p^{2r-(3m+1)}) \text{ if } p = 3 \end{cases}$$

As in the square root, proceeding by induction completes the proof and (iii) follows as $n \to +\infty$. This completes the proof.

Now, let $\alpha = 2^n r - 3m(2^n - 1)$ and $\beta = 2^n r - (3m + 1)(2^n - 1)$. We then have the following result.

Proposition 3.4. Let $\{x_n\}$ be the sequence of approximates in Proposition 3.3.

a. Then for every iteration, the number of correct digits in the approximate increases by $\alpha_n - 2m = 2^n r - 3m2^n + m$ if $p = 2$ and $\beta_n - (2m+1) = 2^n r - (3m+1)2^n + m$ if $p = 3$.

b. The number of iterations to obtain at least M correct digits is

$$n = \begin{cases} \left\lceil \dfrac{\ln\left(\frac{M-2m}{r-3m}\right)}{\ln 2} \right\rceil & \text{if } p = 2 \\ \left\lceil \dfrac{\ln\left(\frac{M-(2m+1)}{r-(3m+1)}\right)}{\ln 2} \right\rceil & \text{if } p = 3 \end{cases}$$

Proof. Consider two consecutive approximates x_{n+1} and x_n. Note that

$$\begin{aligned} |x_{n+1} - x_n|_p &= \left|\frac{-1}{3x_n^2}\right|_p |(x_n^3 - a)|_p \\ &\leq \begin{cases} p^{2m-\alpha_n} & \text{if } p = 2 \\ p^{2m+1-\beta_n} & \text{if } p = 3 \end{cases} \end{aligned}$$

Hence,

$$x_{n+1} - x_n \equiv \begin{cases} 0(\mod p^{\alpha_n - 2m}) & \text{if } p = 2 \\ 0(\mod p^{\beta_n - (2m+1)}) & \text{if } p = 3 \end{cases}$$

Since we require M correct digits in the approximate, we must set the order to $M+m$. That is,

$$M+m=\begin{cases} 2^n r-3m(2^n-1) & \text{if } p=2 \\ 2^n r-(3m+1)(2^n-1) & \text{if } p=3 \end{cases}$$

Since $\{x_n\}$ is the sequence of p-adic numbers in Proposition 3.3, we have $r-3m>0$ if $p=2$ and $r-(3m+2)>0$ if $p=3$. Hence we take

$$n=\begin{cases} \left\lceil \dfrac{\ln\left(\frac{M-2m}{r-3m}\right)}{\ln 2} \right\rceil & \text{if } p=2 \\ \left\lceil \dfrac{\ln\left(\frac{M-(2m+1)}{r-(3m+1)}\right)}{\ln 2} \right\rceil & \text{if } p=3 \end{cases}$$

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

References

[1] F. Gouvea, P-adic numbers: an introduction, Springer-Verlag (2003)

[2] P.S. Ignacio, J. Addawe, W. Alangui, J. Nable, Computation of the Square and Cube Roots of p-adic Numbers Via Newton-Raphson Method, J. Math. Res., Vol. 5, No. 2 (2013), 31-38.

[3] S. Katok, p-adic Analysis Compared with Real, American Mathematical Society (2007)

[4] J.P. Serre, A Course in Arithmetic, Graduate Texts in Mathematics 7, Springer-Verlag (1973)

[5] T. Zerzaihi, M. Kecies, M. Knapp, Hensel Codes of Square Roots of p-adic Numbers, Appl. Anal. and Disc. Math., Vol. 4 (2010), 32-44.

[6] T. Zerzaihi, M. Kecies, Computation of the Cubic Root of a p-adic Number, J. Math. Res., Vol. 3, No. 3 (2011), 40-47.