Thai Journal of Mathematics
Volume 14 (2016) Number 2 : 417–429
http://thaijmath.in.cmu.ac.th
ISSN 1686-0209

P-Adic Qth Roots via Newton-Raphson Method

Paul Samuel Ignacio[†,1], **Joel Addawe**[†] **and Job Nable**[‡]

[†]Department of Mathematics and Computer Science, College of Science,
University of the Philippines Baguio, Baguio City, Philippines
e-mail : ppignacio@up.edu.ph (P.S. Ignacio)
joel.addawe@gmail.com (J. Addawe)

[‡]Department of Mathematics, School of Science and Engineering,
Ateneo de Manila University, Quezon City, Philippines
e-mail : jnable@ateneo.edu

Abstract : Hensel's lemma has been the basis for the computation of the square roots of p-adic numbers in $\mathbb{Z}_p$. We generalize this problem to the computation of qth roots of p-adic numbers in $\mathbb{Q}_p$, where q is a prime and p is greater than q. We provide necessary and sufficient conditions for the existence of qth roots of p-adic numbers in $\mathbb{Q}_p$. Then, given a root of order r, we use the Newton-Raphson method to approximate the qth root of a p-adic number a. We also determine the rate of convergence of this method and the number of iterations needed for a specified number of correct digits in the approximate.

Keywords : p-adic numbers; Newton-Raphson; p-adic roots.
2010 Mathematics Subject Classification : 11J61; 11S05.

1 Introduction

The basic idea behind the calculation of the square roots of p-adic numbers in $\mathbb{Z}_p$ using Hensel's lemma is to "*construct*" the root by choosing the coefficients in its p-adic expansion. This method has actually been extended to provide the

[1]Corresponding author.

necessary conditions for the existence of square roots in $\mathbb{Q}_p$ by establishing the conditions for a p-adic number to be a square. Zerzaihi et al. followed this approach in [1] to establish the existence of cube roots of p-adic numbers in $\mathbb{Q}_p$. Recent developments on this problem include the use of numerical methods to extend the p-adic root-finding problem to $\mathbb{Q}_p$ ([1–3]), or to calculate multiplicative inverses ([4, 5]) in $\mathbb{Q}_p$.

In this paper, we address the generalized root-finding problem to the qth roots of p-adic numbers in $\mathbb{Q}_p$, where q is prime, and $p > q$. We establish sufficient conditions for the existence of qth roots in $\mathbb{Q}_p$ and approximate the values using the Newton-Raphson method. Given a root of order r, we determine the order of the approximate root after n iterations. We also determine the rate of convergence of this method and provide the number of iterations required for any desired number of correct digits in the approximate.

2 Preliminaries

The field of p-adic numbers $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the p-adic norm $|\cdot|_p$. Because the p-adic norm $|\cdot|_p$ is non-Archimedean, we call $(\mathbb{Q}_p, |\cdot|_p)$ a *complete ultrametric space*. An important property of $\mathbb{Q}_p$ is that a unique representation exists for every element. This representation is described in the following theorem.

Theorem 2.1 ([6])**.** *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 $0 \leq a_i \leq p-1$ for $i \geq n$ and $n < 0$.

Notice that this representation of p-adic numbers coincides with the base p expansion of integers. We use a short notation for writing a p-adic number $a = a_n p^n + a_{n+1} p^{n+1} + ... + a_{-1} p^{-1} + a_0 + a_1 p + a_2 p^2 + ...$ by writing only the coefficients of the powers of p. That is, $a_n a_{n+1} ... a_{-1} a_0 a_1 a_2 ...$ represents the same p-adic number as a.

Definition 2.2 ([7])**.** *The set $\mathbb{Z}_p^{\times}$ of* p-adic units *is given by*

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

The p-adic units offer an alternative (and convenient) way of writing p-adic numbers using their p-adic valuation.

Theorem 2.3 ([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 central to our discussion.

Lemma 2.4 ([7]). *Let $a, b \in \mathbb{Q}_p$. Then $a \equiv b(\text{mod } p^k) \Leftrightarrow |a - b|_p \leq p^{-k}$.*

We can also talk about the analysis of functions defined on $\mathbb{Q}_p$.

Definition 2.5 ([7]). *Let $X \subseteq \mathbb{Q}_p$, $a \in X$ 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 $a \in X$.

Following this definition, it may be verified that polynomials in $\mathbb{Q}_p$ have continuous derivatives. One of the most important results on finding solutions of polynomials in $\mathbb{Q}_p$ is given by the following theorem.

Theorem 2.6 ([7]). *(Hensel's lemma) Let $F(x) = c_0 + c_1x + ... + c_nx^n$ be a polynomial whose coefficients are p-adic integers and $F'(x) = c_1 + 2c_2x + ... + nc_nx^{n-1}$ be its derivative. Suppose $\overline{a_0}$ is a p-adic integer which satisfies $F(\overline{a_0}) \equiv 0(\text{mod } p)$ and $F'(\overline{a_0}) \not\equiv 0(\text{mod } p)$. Then, there exists a unique p-adic integer a such that $F(a) = 0$ and $a \equiv \overline{a_0}(\text{mod } p)$.*

Hensel's lemma paves the way for the study of roots of p-adic integers since in particular, it provides the condition for the existence of solutions in $\mathbb{Z}_p$ for $f(x) = x^n - a = 0$ where $f \in \mathbb{Z}_p[x]$. Serre in [8] provides a general result on the existence of solutions of p-adic polynomials in $\mathbb{Z}_p$. The following is a special case of this result.

Theorem 2.7 ([7]). *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 this result is the following proposition.

Proposition 2.8 ([7]). *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 2.9 ([7]). *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.*

These results are consistent with the following definition.

Definition 2.10. *A p-adic number $b \in \mathbb{Q}_p$ is said to be a* square root of $a \in \mathbb{Q}_p$ of order $k \in \mathbb{N}$ *if and only if $b^2 \equiv a (\text{mod } p^k)$.*

In this paper, we shall adopt the generalization of the nth roots of p-adic numbers in the following definition.

Definition 2.11. *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 $b^n \equiv a (\text{mod } p^k)$.*

In [1], the authors used this definition with $n = 3$ to define the cube roots of p-adic numbers.

We end this section by introducing the Newton-Raphson method. For a function, say $f(x)$ and its derivative $f'(x)$, this method makes use of the iterative function

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

from which the recurrence relation will be obtained. The method is employed by first having an initial appropriate 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. Formally, we define the rate of convergence as follows.

Definition 2.12. *If the sequence $\{x_n\}$ converges to r and if there exist real numbers $\lambda > 0$ and $\alpha \geq 1$ such that*

$$\lim_{n \to +\infty} \frac{|x_{n+1} - r|_p}{|x_n - r|_p^\alpha} = \lambda$$

then we say that α is the rate of convergence of the sequence.

3 Main Results

We shall now present the results of this paper. We first establish the existence of the qth roots of p-adic numbers in $\mathbb{Q}_p$. We then proceed to compute them using the Newton-Raphson method.

3.1 Existence of Roots

We begin with proving the existence of the qth root of a p-adic number a in $\mathbb{Q}_p$, where q is prime. We do this by generalizing the necessary and sufficient conditions for the existence of these qth roots in $\mathbb{Q}_p$. We first provide the generalization of Proposition 2.8 in the following result:

Proposition 3.1. *A rational integer a not divisible by p has a qth root in $\mathbb{Z}_p$ $(p \neq q)$ if and only if a is a qth residue modulo p.*

Proof. Suppose that a is not a qth residue modulo p, that is, $a \not\equiv a_0^q (\text{mod } p)$ for any $a_0 \in \{1, 2, 3, ..., p-1\}$. Then, a has no qth integer root modulo $p^k, k = 1$. Theorem 2.7, implies the non-existence of qth roots in $\mathbb{Z}_p$. Conversely, consider the p-adic continuous function $f(x) = x^q - a$ and its derivative $f'(x) = qx^{q-1}$. If $a \equiv a_0^q (\text{mod } p)$ for some $a_0 \in \{1, 2, 3, ..., p-1\}$, then $f(a_0) = (a_0)^q - a \equiv 0 (\text{mod } p)$ and $f'(a_0) = q(a_0)^{q-1} \not\equiv 0 (\text{mod } p)$ since $p \neq q$ and $a_0 \in \{1, 2, 3, ..., p-1\}$. By Hensel's Lemma, $f(x)$ has a zero in $\mathbb{Z}_p$, that is, a has a qth root in $\mathbb{Z}_p$. □

This result ensures the existence of roots in $\mathbb{Z}_p$. The next result extends the existence of qth roots to $\mathbb{Q}_p$.

Proposition 3.2. *Let p and q be prime numbers and $a = p^{v_p(a)} u \in \mathbb{Q}_p$ for some $u = a_0 + a_1 p + a_2 p^2 + ... \in \mathbb{Z}_p^\times$. Then a has a qth root in $\mathbb{Q}_p$ if and only if $v_p(a) = mq$, $m \in \mathbb{Z}$ and $u = v^q$ for some $v \in \mathbb{Z}_p^\times$.*

Proof. Consider the polynomial $F(X) = X^q - a \in \mathbb{Q}_p[X]$.
($\Rightarrow$) Let $a = p^{v_p(a)} u \in \mathbb{Q}_p$ for some $u = \big(a_0 + a_1 p + a_2 p^2 + ...\big) \in \mathbb{Z}_p^\times$ and $b = p^{v_p(b)} v \in \mathbb{Q}_p$ for some $v = \big(b_0 + b_1 p + b_2 p^2 + ...\big) \in \mathbb{Z}_p^\times$. If $b^q = a$, we have that $p^{q v_p(b)} v^q = p^{v_p(a)} u$. Note that, since $v \in \mathbb{Z}_p^\times$, this equation is equivalent to the following system

$$q v_p(b) = v_p(a) \tag{3.1}$$

$$v^q = u. \tag{3.2}$$

($\Leftarrow$) We wish to find $b \in \mathbb{Q}_p$ such that $F(b) = b^q - a = 0$, that is a qth root b of a in $\mathbb{Q}_p$. Note that equation (3.2) reduces to

$$b_0^q \equiv a_0 (\text{ mod } p). \tag{3.3}$$

Consider now the function $f(x) = x^q - a_0 \in \mathbb{Z}_p[x]$. Note that

(i) If $p \neq q$, then by Proposition 3.1, $f(x) = x^q - a_0$ has a solution in $\mathbb{Z}_p$. With this solution, we can find $b_1, b_2, ...$ by reducing equation (3.3) respectively mod p^2, mod p^3, etc. These b_i's are exactly the coefficients in the p-adic expansion of the solution $b \in \mathbb{Q}_p$ for $F(X) = X^q - a = 0$.

(ii) If $p = q$, then equation (3.3) becomes $b_0^q \equiv a_0 (\text{mod } q)$. By Fermat's Little Theorem, $b_0 \equiv a_0 (\text{mod } q)$. Hence, for b_0 satisfying this congruence, by equations (3.1) and (3.2) we can find a solution $b \in \mathbb{Q}_p$ for $F(X) = X^q - a = 0$ by following the same method in the previous case. □

3.2 The qth Roots of p-Adic Numbers

We now compute the qth roots of p-adic numbers using the Newton-Raphson method. By Proposition 3.2, we limit our discussion to p-adic numbers $a \in \mathbb{Q}_p$ such that $|a|_p = p^{-mq}$ where $m \in \mathbb{Z}$. Applying the Newton-Raphson method, we obtain the recurrence relation

$$x_{n+1} = \frac{x_n^q (q-1) + a}{q x_n^{q-1}} \tag{3.4}$$

With this recurrence relation, we then obtain the following result.

Proposition 3.3. *Let $\{x_n\}$ be the sequence of p-adic numbers obtained from the Newton-Raphson iteration. If x_0 is a qth root of a of order r, $|x_0|_p = p^{-m}$, $r > qm$, and $p > q$, then*

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

(ii) $x_n^q \equiv a (\text{mod } p^{2^n r - qm(2^n - 1)})$;

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

Proof. We first prove (i) and (ii) by induction. Let $n = 1$, then by our assumption, we have $x_0^q = a + bp^r$ where $0 < b < p$. Using equation (3.4), we have

$$\begin{aligned}|x_1|_p &= \frac{|x_0^q(q-1)+a|_p}{|qx_0^{q-1}|_p}\\ &= \frac{|qa+(q-1)bp^r|_p}{|qx_0^{q-1}|_p}\\ &= \frac{\max\{|qa|_p, |(q-1)bp^r|_p\}}{|qx_0^{q-1}|_p}\\ &= \frac{p^{-qm}}{p^{-(q-1)m}}\\ &= p^{-m}.\end{aligned}$$

Also by equation (3.4), we have

$$\begin{aligned}x_1^q - a &= \frac{(x_0^q(q-1)+a)^q - aq^q x_0^{q(q-1)}}{q^q x_0^{q(q-1)}}\\ &= \frac{(x_0^q-a)^2\left(\sum_{i=2}^{q}\left[\left(\sum_{j=0}^{i-2}(i-(j+1))\binom{q}{j}(q-1)^{q-j}\right)-(i-2)q^q\right]x_0^{q(q-i)}a^{i-2}\right)}{q^q x_0^{q(q-1)}}.\end{aligned}$$

Now, let

$$\phi(x_0) = \frac{\left(\sum_{i=2}^{q}\left[\left(\sum_{j=0}^{i-2}(i-(j+1))\binom{q}{j}(q-1)^{q-j}\right)-(i-2)q^q\right]x_0^{q(q-i)}a^{i-2}\right)}{q^q x_0^{q(q-1)}}.$$

So, we can write $x_1^q - a = (x_0^q - a)^2\,\phi(x_0)$. Since x_0 is a root of a of order r, that is $x_0^q \equiv a (\text{mod } p^r)$, we have $|x_0^q - a|_p \leq p^{-r}$. Hence

$$\begin{aligned}|x_1^q - a|_p &= |\,(x_0^q - a)^2\,|_p|\phi(x_0)|_p\\ &\leq p^{-2r}|\phi(x_0)|_p.\end{aligned}$$

For $|\phi(x_0)|_p$, we have

$$|\phi(x_0)|_p = \frac{\left|\sum_{i=2}^{q}\left[\left(\sum_{j=0}^{i-2}(i-(j+1))\binom{q}{j}(q-1)^{q-j}\right)-(i-2)q^q\right]x_0^{q(q-i)}a^{i-2}\right|_p}{\left|q^q x_0^{q(q-1)}\right|_p}$$

$$= \frac{\max\left\{\left|\left[\left(\sum_{j=0}^{i-2}(i-(j+1))\binom{q}{j}(q-1)^{q-j}\right)-(i-2)q^q\right]x_0^{q(q-i)}a^{i-2}\right|_p\right\}_{i=2}^{q}}{|q^q|_p|x_0^{q(q-1)}|_p}.$$

Note that for $2 \leq i \leq q$

$$|x_0^{q(q-i)}a^{i-2}|_p = p^{-mq(q-2)}.$$

So we have

$$\left|\sum_{i=2}^{q}\left[\left(\sum_{j=0}^{i-2}(i-(j+1))\binom{q}{j}(q-1)^{q-j}\right)-(i-2)q^q\right]x_0^{q(q-i)}a^{i-2}\right|_p \leq p^{-mq(q-2)}.$$

Hence

$$\begin{aligned}|\phi(x_0)|_p &\leq p^{-mq(q-2)+mq(q-1)}\\ &= p^{mq}.\end{aligned}$$

Therefore $|x_1^q - a|_p \leq p^{mq-2r}$. By Lemma 2.4

$$x_1^q - a \equiv 0(\bmod p^{2r-mq}).$$

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

$$|x_{n-1}|_p = p^{-m} \tag{3.5}$$

$$x_{n-1}^q \equiv a(\bmod p^{2^{n-1}r-qm(2^{n-1}-1)}). \tag{3.6}$$

Note that equation (3.6) implies that

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

where $0 < b < p$. Using equation (3.4), we have

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

Also, we have that

$$\begin{aligned}x_n^q - a &= \frac{(x_{n-1}^q(q-1)+a)^q - aq^q x_{n-1}^{q(q-1)}}{q^q x_{n-1}^{q(q-1)}}\\ &= \frac{(x_{n-1}^q - a)^2\left(\sum_{i=2}^{q}\left[\left(\sum_{j=0}^{i-2}(i-(j+1))\binom{q}{j}(q-1)^{q-j}\right)-(i-2)q^q\right]x_{n-1}^{q(q-i)}a^{i-2}\right)}{q^q x_{n-1}^{q(q-1)}}.\end{aligned}$$

Now, let

$$\phi(x_{n-1}) = \frac{\left(\sum_{i=2}^{q}\left[\left(\sum_{j=0}^{i-2}(i-(j+1))\binom{q}{j}(q-1)^{q-j}\right)-(i-2)q^q\right]x_{n-1}^{q(q-i)}a^{i-2}\right)}{q^q x_{n-1}^{q(q-1)}}.$$

So, we can write $x_n^q - a = \left(x_{n-1}^q - a\right)^2 \phi(x_{n-1})$. Since x_{n-1} is a root of a of order $2^{n-1}r - qm(2^{n-1}-1)$, that is $x_{n-1}^q \equiv a(\mathrm{mod}\ p^{2^{n-1}r-qm(2^{n-1}-1)})$, we then have $|x_{n-1}^q - a|_p \le p^{-(2^{n-1}r-qm(2^{n-1}-1))}$. Hence

$$\begin{aligned}|x_n^q - a|_p &= |\left(x_{n-1}^q - a\right)^2|_p|\phi(x_{n-1})|_p\\ &\le p^{-2(2^{n-1}r-qm(2^{n-1}-1))}|\phi(x_{n-1})|_p.\end{aligned}$$

For $|\phi(x_{n-1})|_p$, we have

$$|\phi(x_{n-1})|_p = \frac{\left|\sum_{i=2}^{q}\left[\left(\sum_{j=0}^{i-2}(i-(j+1))\binom{q}{j}(q-1)^{q-j}\right)-(i-2)q^q\right]x_{n-1}^{q(q-i)}a^{i-2}\right|_p}{\left|q^q x_{n-1}^{q(q-1)}\right|_p}$$
$$= \frac{\max\left\{\left|\left[\left(\sum_{j=0}^{i-2}(i-(j+1))\binom{q}{j}(q-1)^{q-j}\right)-(i-2)q^q\right]x_{n-1}^{q(q-i)}a^{i-2}\right|_p\right\}_{i=2}^{q}}{|q^q|_p|x_{n-1}^{q(q-1)}|_p}.$$

Again, observe also that for $2 \leq i \leq q$

$$\begin{aligned}|x_{n-1}^{q(q-i)}a^{i-2}|_p &= |x_{n-1}^{q(q-i)}|_p|a^{i-2}|_p \\ &= |x_{n-1}|_p^{q(q-i)}|a|_p^{i-2} \\ &= p^{-mq(q-i)}p^{-mq(i-2)} \\ &= p^{-mq(q-2)}.\end{aligned}$$

So we have

$$\left|\sum_{i=2}^{q}\left[\left(\sum_{j=0}^{i-2}(i-(j+1))\binom{q}{j}(q-1)^{q-j}\right)-(i-2)q^q\right]x_{n-1}^{q(q-i)}a^{i-2}\right|_p \leq p^{-mq(q-2)}.$$

Hence

$$\begin{aligned}|\phi(x_{n-1})|_p &\leq p^{-mq(q-2)+mq(q-1)} \\ &= p^{mq}.\end{aligned}$$

Therefore

$$\begin{aligned}|x_n^q - a|_p &\leq p^{qm-2(2^{n-1}r-qm(2^{n-1}-1))} \\ &= p^{qm(2^n-1)-2^n r}.\end{aligned} \tag{3.7}$$

By Lemma 2.4

$$x_n^q - a \equiv 0(\mod p^{2^n r-qm(2^n-1)}).$$

Finally, (iii) follows clearly from equation (3.7) as we take $n \to \infty$. □

We now turn to the rate of convergence of the method.

Proposition 3.4. *Let $\{x_n\}$ be the sequence of p-adic numbers converging to a qth root of $a \in \mathbb{Q}_p$ obtained using the Newton-Raphson method. Then the sequence converges quadratically with asymptotic error p^{mq}.*

Proof. We prove this result in two parts. We first determine an approximate value of α and show using Definition (2.12) that this value of α is indeed the rate of convergence of the method. Note that equation (2.12) means that, if n is sufficiently large, then for some α we have

$$\begin{aligned}|x_{n+1}^q - a|_p &\approx \lambda |x_n^q - a|_p^\alpha \\ |x_n^q - a|_p &\approx \lambda |x_{n-1}^q - a|_p^\alpha.\end{aligned}$$

Then by Proposition 3.3,

$$\frac{|x_{n+1}^q - a|_p}{|x_n^q - a|_p} \approx \left|\frac{x_n^q - a}{x_{n-1}^q - a}\right|_p^\alpha.$$

And we have that

$$\begin{aligned}\alpha &\approx \frac{\log\left(\dfrac{|x_{n+1}^q - a|_p}{|x_n^q - a|_p}\right)}{\log\left(\dfrac{|x_n^q - a|_p}{|x_{n-1}^q - a|_p}\right)} \\ &\approx \frac{\log\left(\dfrac{p^{mq(2^{n+1}-1)-2^{n+1}r}}{p^{mq(2^n-1)-2^n r}}\right)}{\log\left(\dfrac{p^{mq(2^n-1)-2^n r}}{p^{mq(2^{n-1}-1)-2^{n-1}r}}\right)} \\ &= \frac{\log p^{2^n mq - 2^n r}}{\log p^{2^{n-1}mq - 2^{n-1}r}} \\ &= 2.\end{aligned}$$

Then

$$\begin{aligned}\lim_{n\to+\infty} \frac{|x_{n+1}^q - a|_p}{|x_n^q - a|_p^2} &= \lim_{n\to+\infty} \frac{p^{mq(2^{n+1}-1)-2^{n+1}r}}{p^{2mq(2^n-1)-2^{n+1}r}} \\ &= \lim_{n\to+\infty} p^{mq((2^{n+1}-1)-(2(2^n-1)))-r(2^{n+1}-2^{n+1})} \\ &= p^{mq} > 0.\end{aligned}$$

□

We also have the following result.

Proposition 3.5. *Let $\{x_n\}$ be the sequence of approximates converging to the qth root of a obtained from the Newton-Raphson method in Proposition 3.3. If $p > q$*

1. *Then for every iteration, the number of correct digits in the approximate increases by $\lambda_n - m(q-1)$.*
2. *The number of iterations n to obtain at least M correct digits is*

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

Proof. Note that for two consecutive approximates x_i and x_{i+1},

$$\begin{aligned} x_{n+1} - x_n &= \left(\frac{(q-1)x_n^q + a}{qx_n^{q-1}}\right) - x_n \\ &= \frac{-(x_n^q - a)}{qx_n^{q-1}}. \end{aligned}$$

Let $\psi(x_n) = \dfrac{-1}{qx_n^{q-1}}$. So that $x_{n+1} - x_n = (x_n^q - a)\psi(x_n)$. But note that $|\psi(x_n)|_p = p^{m(q-1)}$. Then

$$\begin{aligned} |x_{n+1} - x_n|_p &= |(x_n^q - a)|_p |\psi(x_n)|_p \\ &\leq p^{m(q-1)-\lambda_n}. \end{aligned}$$

By Lemma 2.4 we have

$$x_{n+1} - x_n \equiv 0(\bmod p^{\lambda_n - m(q-1)}).$$

Note that if the order of the root x_n is K (that is, $x_n^q - a \equiv 0(\bmod p^K)$), the number of correct digits in the approximate is $K - m$ since $|\sqrt[m]{a}|_p = p^{-m}$. Hence, to find the number of iterations n such that we have M correct digits in the approximate, we must set the order to $M + m$. Hence, we get $2^n(r - mq) = M - (q-1)m$. Since $\{x_n\}$ is the sequence of p-adic numbers converging to the qth root of a obtained from the Newton-Raphson iteration in Proposition 3.3, we have $r - qm > 0$. Hence we take

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

This n gives sufficient iterations to obtain at least M correct digits in the approximate. □

References

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

[2] P.S. Ignacio, J. Addawe, J. Nable, W. Alangui, Computation of the square and cube roots of p-adic numbers via Newton-Raphson method, J. Math. Res. 5 (2) (2013) 31–38.

[3] T. Zerzaihi, M. Kecies, M. Knapp, Hensel codes of square roots of p-adic numbers, Applic. Anal. and Disc. Math. 4 (2010) 32–44.

[4] J. Dumas, On Newton-Raphson iteration for multiplicative inverses modulo prime powers, IEEE Trans. on Comp. 63 (8) (2014) 2106–2109.

[5] M. Knapp, C. Xenophontos, Numerical analysis meets number theory: using rootfinding methods to calculate inverses modulo P^n, Applic. Anal. and Disc. Math. 4 (2010) 23–31.

[6] F. Gouvea, P-adic Numbers: An Introduction, Springer-Verlag, 2003.

[7] S. Katok, P-adic analysis compared with real, Amer. Math. Soc., 2007.

[8] P. Serre, A Course in Arithmetic, Grad. Texts in Math. 7, Springer-Verlag (1973).

(Received 20 August 2013)
(Accepted 8 September 2014)