JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **28**, No. 4, November 2015
http://dx.doi.org/10.14403/jcms.2015.28.4.575

NEWTON-RAPHSON METHOD FOR COMPUTING p-ADIC ROOTS

Gwangoo Yeo*, Seong-Jin Park**, and Young-Hee Kim***

Abstract. The Newton-Raphson method is used to compute the q-th roots of a p-adic number for a prime number q. The sufficient conditions for the convergence of this method are obtained. The speed of its convergence and the number of iterations to obtain a number of corrected digits in the approximation are calculated.

1. Introduction

Let p be a prime and $\mathbb{Q}_p$ be the field of p-adic numbers. The theories of p-adic numbers have been applied in several areas not only in mathematics but also in scientific areas ([9]). Many efforts have been made to find solutions of p-adic equations, but it was difficult to find it out right away, so people started to research ways to compute the approximate solutions using numerical methods ([8]). To start with, there has been a research on how to find square roots of p-adic numbers ([10]). Also, a variety of ways to find roots has been researched, such as Newton's method or other methods in numerical analysis like secant method. The researches continued on finding the cubic root of p-adic numbers. These were done using the same technique that was used in finding square roots of p-adic numbers ([2], [3], [5]). The latest research was on computing fifth roots of p-adic numbers ([7]).

In this paper, we use the Newton-Raphson method for computing p-adic roots and generalize previous results in [5] to the case of the q-th roots of a p-adic number in $\mathbb{Q}_p$ for any prime number q. Consequently, we have the sufficient conditions for the convergence of Newton-Raphson method for computing the q-th roots of a p-adic number. We calculate

Received July 31, 2015; Accepted November 05, 2015.

2010 Mathematics Subject Classification: Primary 65H04; Secondary 11E95.

Key words and phrases: Newton-Raphson method, p-adic roots.

Correspondence should be addressed to Young-Hee Kim, yhkim@kw.ac.kr.

the speed of its convergence and the number of iterations to obtain a number of corrected digits in the approximation.

2. Preliminaries

Let p be a prime number and $x \in \mathbb{Q}$ $(x \neq 0)$. The *p-adic order of x*, $\mathrm{ord}_p x$, is defined by

$$\mathrm{ord}_p x = \begin{cases} \text{the highest power of } p \text{ which divides } x, & \text{if } x \in \mathbb{Z}, \\ \mathrm{ord}_p a - \mathrm{ord}_p b, & \text{if } x = \frac{a}{b},\ a, b \in \mathbb{Z},\ b \neq 0. \end{cases}$$

Consider a map $|\cdot|_p : \mathbb{Q} \to \mathbb{R}^+$ defined by

$$|x|_p = \begin{cases} p^{-\mathrm{ord}_p x}, & \text{if } x \neq 0, \\ 0, & \text{if } x = 0. \end{cases}$$

The field $\mathbb{Q}_p$ of p-adic numbers is the completion of the field $\mathbb{Q}$ of rational numbers with respect to the p-adic norm $|\cdot|_p$ ([4]).

A p-adic number $a \in \mathbb{Q}_p$ is said to be a p-adic integer if this canonical expansion contains only nonnegative powers of p. The set of p-adic integers is denoted by $\mathbb{Z}_p$, and we have

$$\mathbb{Z}_p = \{\sum_{k=0}^{\infty} \beta_k p^k : 0 \leq \beta_k \leq p-1\} = \{a \in \mathbb{Q}_p : \mathrm{ord}_p a \geq 0\}.$$

A p-adic integer $a \in \mathbb{Z}_p$ is said to be a p-adic unit if the first digit β_0 in the p-adic expansion is different from zero. The set of p-adic units is denoted by $\mathbb{Z}_p^*$ ([4]).

A p-adic number $b \in \mathbb{Q}_p$ is said to be a q-th root of $a \in \mathbb{Q}_p$ of order k if $b^q \equiv a \pmod{p^k}$ for $k \in \mathbb{N}$ ([9]).

To discuss the q-th roots of p-adic numbers, the following lemma and proposition are needed ([4], [9]).

LEMMA 2.1. *Let $a, b \in \mathbb{Q}_p$. Then a and b are congruent modulo p^k and write $a \equiv b$ (mod p^k) if and only if $|a-b|_p \leq 1/p^k$.*

PROPOSITION 2.2. *Let x be a p-adic number of norm p^{-n}. Then x can be written as the product $x = p^n u$, where $u \in \mathbb{Z}_p^*$.*

The next theorem is the basic for the existing results on p-adic roots in $\mathbb{Z}_p$ ([4]).

THEOREM 2.3. *(Hensel's Lemma) Let $F(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n$ be a polynomial whose coefficients are p-dic integers. Let*

$$F'(x) = c_1 + 2c_2 x + \cdots + nc_n x^{n-1}$$

be the derivative of $F(x)$. Suppose $\bar{a}_0$ is a p-adic integer which satisfies $F(\bar{a}_0) \equiv 0$ (mod p) and $F'(\bar{a}_0) \not\equiv 0$ (mod p). Then there exists a unique p-adic integer a such that $F(a) = 0$ and $a \equiv \bar{a}_0$(mod p).

The following result is obtained from Hensel's Lemma ([4]).

Theorem 2.4. *A polynomial with integer coefficients has a root in $\mathbb{Z}_p$ if and only if it has an integer root of modulo p^k for any $k > 1$.*

The following theorem provides the conditions for the existence of the q-th roots of p-adic numbers ([6]).

Theorem 2.5. *A rational integer a is not divisible by p has a q-th root in $\mathbb{Z}_p (p \neq q)$ if and only if a is a q-th root residue modulo p.*

From this, we have the following result by the similar ways in [6].

Theorem 2.6. *Let p be a prime number.*

(1) *If $p \neq q$, then $a = p^{ord_p a} u \in \mathbb{Q}_p$ for some $u \in \mathbb{Z}_p^*$ has a q-th root in $\mathbb{Q}_p$ if and only if $\mathrm{ord}_p a = qm$ for $m \in \mathbb{Z}$ and $u = v^q$ for some unit $v \in \mathbb{Z}_p^*$.*

(2) *If $p = q$, then $a = q^{ord_q a} u \in \mathbb{Q}_q$ for some $u \in \mathbb{Z}_q^*$ has a q-th root in $\mathbb{Q}_q$ if and only if $\mathrm{ord}_p a = qm$ for $m \in \mathbb{Z}$ and $u \equiv 1$ (mod q^2) or $u \equiv k$ (mod q) for some k $(2 \leq k \leq q-1)$.*

3. Main results

To compute a q-th root of a p-adic number a is to find a solution of $x^q = a$. There are many numerical methods to find roots of p-adic numbers, but we use the Newton-Raphson method because of the speed of convergence of the approximate solutions ([1], [3]).

Let $a \in \mathbb{Q}_p$ $(a \neq 0)$ be a p-adic number such that $|a|_p = p^{-qm}$ $(m \in \mathbb{Z})$ and let $\{x_n\}$ be a sequence of p-adic numbers derived by the Newton-Raphson method. We know that if there is a p-adic number β that satisfies $\beta^q = a$, then $|x_n|_p = |\beta|_p = p^{-m}$.

The iterative formula for the Newton-Raphson method to find the solution of the equation $f(x) = 0$ is that for $n \in \mathbb{N} \cup \{0\}$

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}. \tag{3.1}$$

Let $f(x) = x^q - a$. Then the iteration (3.1) becomes the recurrence relation

$$x_{n+1} = \frac{(q-1)x_n^q + a}{q x_n^{q-1}}, \quad n = 0, 1, 2, \dots . \tag{3.2}$$

We have from the binomial theorem that

$$\begin{aligned} f(x_{n+1}) &= x_{n+1}^q - a \\ &= \frac{1}{q^q x_n^{(q-1)q}} \{ {}_qC_0(q-1)^q x_n^{q^2} + [{}_qC_1(q-1)^{q-1} - q^q] x_n^{q(q-1)} a \\ &\quad + {}_qC_2(q-1)^{q-2} x_n^{q(q-2)} a^2 + {}_qC_3(q-1)^{q-3} x_n^{q(q-3)} a^3 + \cdots \\ &\quad + {}_qC_{(q-1)}(q-1) x_n^q a^{q-1} + {}_qC_q a^q \}, \end{aligned} \tag{3.3}$$

where ${}_qC_r = \frac{q!}{(q-r)!r!}$ for $0 \le r \le q$.

Let $P(x_n^q)$ be

$$\begin{aligned} P(x_n^q) = {}& {}_qC_0(q-1)^q x_n^{q^2} + [{}_qC_1(q-1)^{q-1} - q^q] x_n^{q(q-1)} a \\ & + {}_qC_2(q-1)^{q-2} x_n^{q(q-2)} a^2 + {}_qC_3(q-1)^{q-3} x_n^{q(q-3)} a^3 \\ & + \cdots + {}_qC_{(q-1)}(q-1) x_n^q a^{q-1} + {}_qC_q a^q \end{aligned} \tag{3.4}$$

in (3.3). By substituting a for x_n^q in (3.4), we have

$$\begin{aligned} P(a) &= a^q \{ {}_qC_0(q-1)^q + {}_qC_1(q-1)^{(q-1)} + \cdots + {}_qC_{q-1}(q-1) + {}_qC_q - q^q \} \\ &= a^{q^2} \{ (q-1+1)^q - q^q \} = 0. \end{aligned}$$

Therefore $P(x_n^q)$ can be factored by $(x_n^q - a)$. And so we can write

$$P(x_n^q) = (x_n^q - a) G(x_n^q), \tag{3.5}$$

where

$$\begin{aligned} G(x_n^q) &= (q-1)^q x_n^{q(q-1)} + \left\{ {}_qC_0(q-1)^q + {}_qC_1(q-1)^{q-1} - q^q \right\} x_n^{q(q-2)} a \\ &+ \left\{ {}_qC_0(q-1)^q + {}_qC_1(q-1)^{q-1} + {}_qC_2(q-1)^{q-2} - q^q \right\} x_n^{q(q-2)} a^2 + \cdots \\ &+ \left\{ {}_qC_0(q-1)^q + {}_qC_1(q-1)^{q-1} + {}_qC_2(q-1)^{q-2} + \cdots + {}_qC_{q-1}(q-1) - q^q \right\}. \end{aligned} \tag{3.6}$$

Substituting x_n^q by a in (3.6), we have

$$\begin{aligned} & G(a) \\ &= {}_qC_0 q(q-1)^q + {}_qC_1(q-1)(q-1)^{q-1} + {}_qC_2(q-2)(q-1)^{q-2} \\ &\quad + \cdots + 2{}_qC_{q-2}(q-1)^2 + {}_qC_{q-1}(q-1) - q^q(q-1) \\ &= -q^q(q-1) + \sum_{n=0}^{q} \frac{q!}{(q-n)!n!}(q-n)(q-1)^{q-n} \\ &= -q^q(q-1) + \sum_{n=0}^{q} q(q-1)\{ {}_{q-1}C_n(q-1)^{q-1-n} \cdot 1^n \} \\ &= q^q(q-1) - q^q(q-1) = 0. \end{aligned} \tag{3.7}$$

Therefore $G(x_n^q)$ can be factored by $(x_n^q - a)$. By (3.5) and (3.7), we have

$$\begin{aligned}P(x_n^q) =&(x_n^q - a)^2(z_1x_n^{q(q-2)} + z_2x_n^{q(q-3)}a + z_3x_n^{q(q-4)}a^2 + \cdots \\ &+ z_{q-3}x_n^q a^{q-3} + a^{q-2}),\end{aligned} \tag{3.8}$$

where z_k is a natural number for $1 \leq k \leq q-2$. Also we have

$$x_{n+1} - x_n = \frac{1}{qx_n^{q-1}}(a - x_n^q). \tag{3.9}$$

Therefore we have the following result.

Theorem 3.1. *Let x_0 be a q-th root of a of order r.*
(1) If $p \neq q$, then x_n is a q-th root of a of order $2^nr - qm(2^n-1)$.
(2) If $p = q$, then x_n is a q-th root of a of order $2^nr - q(m+1)(2^n-1)$.

Proof. Let $\{x_n\}$ be the sequence defined by (3.2) and x_0 be the q-th root of a of order r. Then, by the assumption and Lemma 2.1,

$$x_0^q - a \equiv 0 \pmod{p^r} \Rightarrow |x_0^q - a|_p \leq p^{-r}. \tag{3.10}$$

We have from (3.8) that

$$\begin{aligned}|P(x_n^q)|_p \leq p^{-2r}\max\{&|z_1x_n^{q(q-2)}|_p,\, |z_2x_n^{q(q-3)}a|_p,\, |z_3x_n^{q(q-4)}a^2|_p, \\ &\ldots,\, |z_{q-3}x_n^q a^{q-3}|_p,\, |a^{q-2}|_p\},\end{aligned} \tag{3.11}$$

where $z_k \in \mathbb{N}$ with $1 \leq k \leq q-2$. The sum of exponents of x_n^q and a at each element of $z_kx_n^{q(q-k-1)}a^{k-1}$ is a constant $q-2$. If there is a j number of factor of q in z_k's, the p-norm of the element is equal to $p^{-q(q-2)-j}$, which is smaller than $|a^{q-2}|_p$. Since $|x_n^q|_p = p^{-qm}$ and $|a|_p = p^{-qm}$, it follows from (3.3), (3.10) and (3.11) that

$$|x_1^q - a|_p \leq \left|\frac{1}{q^q x_0^{(q-1)q}}\right|_p \cdot p^{-2r} \cdot p^{-q(q-2)}. \tag{3.12}$$

By (3.12), we have

$$\begin{cases} |x_1^q - a|_p \leq p^{qm-2r}, & (p \neq q), \\ |x_1^q - a|_p \leq p^{q(m+1)-2r}, & (p = q). \end{cases} \tag{3.13}$$

We also have from Lemma 2.1 that

$$\begin{cases} x_1^q - a \equiv 0 \pmod{p^{2r-qm}}, & (p \neq q), \\ x_1^q - a \equiv 0 \pmod{p^{2r-q(m+1)}}, & (p = q). \end{cases}$$

In this manner, we have that if $p \neq q$, then

$$x_n^q - a \equiv 0 \pmod{p^{\phi_n}}. \tag{3.14}$$

Here ϕ_n is expressed as

$$\phi_0 = r, \ \phi_{n+1} = 2\phi_n - qm,$$

which is equivalent to

$$\phi_n = 2^n r - qm(2^n - 1). \tag{3.15}$$

When $p = q$, we have

$$x_n^q - a \equiv 0 \ (\mathrm{mod}\ p^{\phi'_n}). \tag{3.16}$$

Similarly, ϕ'_n can be expressed as

$$\phi'_n = 2^n r - q(m+1)(2^n - 1). \tag{3.17}$$

(3.14) and (3.16) are proved by the mathematical induction. Then the proof is completed. □

Let $\{e_n\}$ be the sequence defined by $e_n = x_{n+1} - x_n$ at each step of the iteration $\{x_n\}$ for $n \in \mathbb{N} \cup \{0\}$. Then we have the following result.

Theorem 3.2. *Let x_0 be a q-th root of a of order r. Then the sequence $\{e_n\}$ equals to*

$$\begin{cases} e_n \equiv 0 \quad (mod\ p^{\psi_n}), & if\ p \neq q, \\ e_n \equiv 0 \quad (mod\ q^{\psi'_n}), & if\ p = q, \end{cases} \tag{3.18}$$

where

$$\begin{cases} \psi_n = 2^n r - m(q \cdot 2^n - 1), \\ \psi'_n = 2^n r - (m+1)(q \cdot 2^n - 1) + q - 2. \end{cases} \tag{3.19}$$

Proof. We have from (3.9) that for all $n \in \mathbb{N}$

$$|x_{n+1} - x_n|_p = \left| \frac{1}{q x_n^{q-1}} \right|_p |a - x_n^q|_p. \tag{3.20}$$

By the strong triangle inequality,

$$|\, a - x_n^q|_p \leq \max\{|\, a|_p \,, |x_n^q|_p\}. \tag{3.21}$$

Then we have from (3.20) and (3.21) that

$$\begin{cases} |x_{n+1} - x_n|_p \leq p^{(q-1)m - \phi_n}, & (p \neq q), \\ |x_{n+1} - x_n|_q \leq q^{(q-1)m - \phi'_n + 1}, & (p = q). \end{cases} \tag{3.22}$$

By Lemma 2.1, (3.22) is equivalent to

$$\begin{cases} e_n \equiv 0 \quad (\mathrm{mod}\ p^{\phi_n - (q-1)m}), & (p \neq q), \\ e_n \equiv 0 \quad (\mathrm{mod}\ q^{\phi'_n - \{(q-1)m+1\}}), & (p = q). \end{cases} \tag{3.23}$$

We put

$$\begin{cases} \psi_n = \phi_n - (q-1)m, & (p \neq q), \\ \psi'_n = \phi_n{}' - \{(q-1)m+1\}, & (p = q). \end{cases} \tag{3.24}$$

By (3.15), (3.17) and (3.24), we have

$$\begin{cases} \psi_n = 2^n r - m(q \cdot 2^n - 1), & (p \neq q), \\ \psi^{'}_n = 2^n r - q(m+1)(2^n-1) - (q-1)m - 1, & (p = q). \end{cases} \tag{3.25}$$

Since (3.25) equals (3.19), (3.23) implies (3.18) and so the proof is completed. □

Remark 3.3. By Theorem 3.2, we can calculate the number of iterations to obtain a number of corrected digits in the approximation. If $p \neq q$, then the rate of convergence of the sequence $\{x_n\}$ is of order ψ_n. When $r - qm > 0$, the number of iterations to obtain M correct digits n is

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

If $p = q$, then the rate of convergence of the sequence $\{x_n\}$ is of order ψ'_n. When $r - q(m+1) > 0$, the number of iterations to obtain M correct digits n is

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

References

[1] W. Cheney and D. Kincaid, *Numerical mathematics and computing* (6th ed.), Thomson, 2007.

[2] P. S. Ignacio, *On the square and cube roots of p-adic numbers*, J. Math. Comput. Sci. **3** (2013), no. 4, 993-1003.

[3] P. S. Ignacio, J. M. Addawe, W. V. Alangui, and J. A. Nable, *Computation of square and cube roots of p-adic numbers via Newton-Raphson method*, J. Math. Research **5** (2013), no. 2, 31-38.

[4] S. Katok, *p-Adic analysis compared with real*, American Math. Soc., 2007.

[5] M. Keicies and T. Zerzaihi, *General approach of the root of a p-adic number*, Filomat **27** (2013), no. 3, 431-436.

[6] Y.-H. Kim and J. Choi, *On the existence of p-adic roots*, J. Chungcheong Math. Soc. **28** (2015), no. 2, 195-200.

[7] Y.-H. Kim, H.-M. Kim, and J. Choi, *Newton's method for computing the fifth roots of p-adic numbers*, J. Comp. Anal. Appl. (2016), accepted.

[8] M. Knapp and C. Xenophontos, *Numerical analysis meets number theory using rootfinding method to calculate inverses mod p^n*, Appl. Anal. Discrete Math. **4** (2010), 23-31.

[9] N. Koblitz, p-Adic numbers, p-adic analysis and zeta functions (2nd ed.), Springer-Verlag, 1984.

[10] T. Zerzaihi and M. Kecies, *Computation of the cubic root of a p-adic number*, J. Math. Research **3** (2011), no. 3, 40-47.

*
Hansung Science High School
Seoul 03732, Republic of Korea
E-mail: gwangoo525@naver.com

**
Hansung Science High School
Seoul 03732, Republic of Korea
E-mail: qkrtjdwls78@naver.com

***
Division of General Education-Mathematics
Kwangwoon University
Seoul 01897, Republic of Korea
E-mail: yhkim@kw.ac.kr