ON THE EXISTENCE OF $p$-ADIC ROOTS

YOUNG-HEE KIM* AND JONGSUNG CHOI**

Abstract. In this paper, we give the condition for the existence of the $q$-th roots of $p$-adic numbers in $\mathbb{Q}_p$ with an integer $q \geq 2$ and $(p, q) = 1$. We have the conditions for the existence of the fifth root and the seventh root of $p$-adic numbers in $\mathbb{Q}_p$, respectively.

1. Introduction

Let $p$ be a prime and $\mathbb{Q}_p$ be the field of $p$-adic numbers. The $p$-adic numbers were introduced by Hensel([2]). The theory of the field of $p$-adic numbers has been related to several areas of mathematics and physics, and so the research of this field has been very important([3]).

Computing the $q$-th roots of a $p$-adic number is useful in the field of computer science and cryptography, specially when $q$ is a prime. It is necessary to confirm the existence of the $q$-th root of a $p$-adic number in $\mathbb{Q}_p$ before computing them([4], [5]). There are some results of the existence of square roots of $p$-adic numbers and the $q$-th roots of unity([1-2]). In [4], the authors gave the conditions for the existence of the cubic root of a $p$-adic number, and then applied the secant method to compute the cubic root.

In this paper, we give the condition for the existence of the $q$-th roots of $p$-adic numbers in $\mathbb{Q}_p$ with an integer $q \geq 2$ and $(p, q) = 1$. We have the conditions for the fifth root and the seventh root of $p$-adic numbers, respectively, including the case $p = q$. 

Received September 03, 2014; Accepted January 19, 2015.
2010 Mathematics Subject Classification: Primary 11E95, Secondary 26E30.
Key words and phrases: $p$-adic roots.
Correspondence should be addressed to Jongsung Choi, jeschoi@kw.ac.kr.
The present research has been conducted by the Research Grant of Kwangwoon University in 2014.
2. Preliminaries

The following definitions and theorems are necessary for our discussion. See [1] and [2] for details.

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

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

The \( p \)-adic norm \( | \cdot |_p : \mathbb{Q} \to \mathbb{R}^+ \) of \( x \) is defined by

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

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 by

\[
|a|_p = \lim_{n \to \infty} |a_n|_p,
\]

where \( \{a_n\} \) is a Cauchy sequence in \( \mathbb{Q} \) representing \( a \in \mathbb{Q}_p \).

**Theorem 2.1.** Every equivalence class \( a \) in \( \mathbb{Q}_p \) satisfying \( |a|_p \leq 1 \) has exactly one representative Cauchy sequence \( \{a_i\} \) such that

1. \( a_i \in \mathbb{Z} \), \( 0 \leq a_i < p^i \) for \( i = 1, 2, \ldots \),
2. \( a_i \equiv a_{i+1} \pmod{p^i} \) for \( i = 1, 2, \ldots \).

Hence every \( p \)-adic number \( a \in \mathbb{Q}_p \) has a unique representation

\[
a = \sum_{n=-m}^{\infty} a_np^n,
\]

where \( a_{-m} \neq 0 \) and \( a_n \in \{0, 1, 2, \ldots, p-1\} \) for \( n \geq -m \), and represent the given \( p \)-adic number \( a \) as a fraction in the base \( p \) as follows:

\[
a = \ldots a_{-1} a_{0} a_1 a_2 \ldots a_m,
\]

which is called the canonical \( p \)-adic expansion of \( a \).

Let \( \mathbb{Z}_p \) be the set of \( p \)-adic integers and \( \mathbb{Z}_p^\times \) be the set of \( p \)-adic units. It follows that \( \mathbb{Z}_p = \{a \in \mathbb{Q}_p | |a|_p \leq 1\} \) and \( \mathbb{Z}_p^\times = \{a \in \mathbb{Q}_p | |a|_p = 1\} \).

From this, the next theorem follows.

**Theorem 2.2.** Let \( a \) be a \( p \)-adic number of norm \( p^{-n} \). Then \( a = p^n u \) for some \( u \in \mathbb{Z}_p^\times \).
3. $p$-Adic roots

Let $q$ be an integer such that $q \geq 2$. A $p$-adic number $x \in \mathbb{Q}_p$ is said to be a $q$-th root of $a \in \mathbb{Q}_p$ of order $k \in \mathbb{N}$ if and only if $x^q \equiv a \pmod{p^k}$. Specially, the $q$-th root of $a \in \mathbb{Q}_p$ is called the fifth root of $a$ when $q = 5$, and the seventh root of $a$ when $q = 7$.

In this section, we provide the condition for the existence of the $q$-th root of $p$-adic numbers $a$ in $\mathbb{Q}_p$ when $(p, q) = 1$. We also have the conditions for the existence of the fifth root and the seventh root of $p$-adic numbers, respectively.

The following lemma is essential for our discussion([1]).

**Lemma 3.1.** Let $a, b \in \mathbb{Q}_p$. Then $a$ and $b$ are congruent modulo $p^k$ and write $a \equiv b \pmod{p^k}$ if and only if $|a - b|_p \leq 1/p^k$.

The next theorem is the basis for existing $p$-adic roots([2]).

**Theorem 3.2.** (Hensel’s lemma) Let $F(x) = c_0 + c_1 x + \cdots + c_n x^n$ be a polynomial whose coefficients are $p$-adic integers. Let $F'(x) = c_1 + 2c_2 x + 3c_3 x^2 + \cdots + nc_n x^n$ be the derivative of $F(x)$. Let $a_0$ be a $p$-adic integer such that $F(a_0) \equiv 0 \pmod{p}$ and $F'(a_0) \not\equiv 0 \pmod{p}$. Then there exists a unique $p$-adic integer $a$ such that

$$F(a) = 0 \quad \text{and} \quad a \equiv a_0 \pmod{p}.$$

The following theorem follows from Theorem 3.2, and provides the condition between $p$-adic numbers and congruence([1]).

**Theorem 3.3.** 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 $k \geq 1$.

Some results of the existence of square roots of $p$-adic numbers are obtained from Theorem 3.3([1]). In [4], the authors gave the condition for the existence of cubic roots in $\mathbb{Q}_p$. We generalize the result to the $q$-th root, and we have the condition for the existence of a $q$-th root of $p$-adic numbers in $\mathbb{Q}_p$ when $q \geq 2$ and $(p, q) = 1$.

**Theorem 3.4.** Let $(p, q) = 1$. Then a rational integer $a$ 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 residue modulo $p$.

**Proof.** Consider the $p$-adic continuous function $f(x) = x^q - a$ and its derivative $f'(x) = qx^{q-1}$. If $a$ is not a $q$-th residue modulo $p$, then it has no $q$-th roots in $\mathbb{Z}_p$ by Theorem 3.3.
Conversely, if \( a \) is a \( q \)-th residue modulo \( p \), then \( a \equiv a_0^q \pmod p \) for \( a_0 \in \{1, 2, \ldots, p-1\} \). Hence \( f(a_0) \equiv 0 \pmod p \) and \( f'(a_0) = qa_0^{q-1} \not\equiv 0 \pmod p \), because \( p \neq q \) and \( a_0 \neq 0 \). From Hensel’s lemma, the solution is in \( \mathbb{Z}_p \), and so \( a \) has a \( q \)-th root in \( \mathbb{Z}_p \).

From Theorem 3.4, we have the conditions for the existence of the fifth root of a \( p \)-adic number in \( \mathbb{Q}_p \) including \( p = q \).

**Theorem 3.5.** Let \( p \) be a prime number. Then we have:

1. If \( p \neq 5 \), then \( a = p^{\text{ord}_p a}u \in \mathbb{Q}_p \) for some \( u \in \mathbb{Z}_p^* \) has a fifth root in \( \mathbb{Q}_p \) if and only if \( \text{ord}_p a = 5m \) for \( m \in \mathbb{Z} \) and \( u = v^5 \) for some unit \( v \in \mathbb{Z}_p^* \).

2. If \( p = 5 \), then \( a = 5^{\text{ord}_p a}u \in \mathbb{Q}_5 \) for some \( u \in \mathbb{Z}_5^* \) has a fifth root in \( \mathbb{Q}_5 \) if and only if \( \text{ord}_p a = 5m \) for \( m \in \mathbb{Z} \) and \( u \equiv 1 \pmod{25} \) or \( u \equiv k \pmod{5} \) for some \( k \) (\( 2 \leq k \leq 4 \)).

**Proof.** Let \( a \) and \( x \in \mathbb{Q}_p \). Then \( a = p^{\text{ord}_p a}u \) and \( x = p^{\text{ord}_p x}v \) for some \( u, v \in \mathbb{Z}_p^* \) such that

\[
u = a_0 + a_1 p + a_2 p^2 + \cdots, \quad v = x_0 + x_1 p + x_2 p^2 + \cdots \tag{3.1}\]

with \( a_0 \neq 0 \) and \( x_0 \neq 0 \). Then we have

\[
x^5 = a \iff p^{\text{ord}_p x}v^5 = p^{\text{ord}_p a}u \tag{3.2}
\]

The equation (3.2) is equivalent to the following system:

\[
\begin{cases}
5\text{ord}_p x = \text{ord}_p a \\
v^5 = u \\
x_0^5 - a_0 \equiv 0 \pmod p.
\end{cases} \tag{3.3}
\]

Let \( f(x) = x^5 - a_0 \). Then its derivative \( f'(x) = 5x^4 \) satisfies

\[
|f'(x_0)|_p = |5|_p = \begin{cases}
1, & \text{if } p \neq 5, \\
\frac{1}{5}, & \text{if } p = 5.
\end{cases}
\]

1. If \( p \neq 5 \), then the solution of \( f(x_0) = x_0^5 - a_0 \) exists by Hensel’s lemma. Thus the result follows.

2. If \( p = 5 \), then the equation (3.3) is reduced to the following system:

\[
\begin{cases}
(x_0 + 5x_1 + 5^2x_2 + \cdots)^5 = a_0 + 5a_1 + 5^2a_2 + \cdots \\
x_0^5 - a_0 \equiv 0 \pmod 5,
\end{cases} \tag{3.4}
\]

where \( x_0, a_0 \in \{1, 2, 3, 4\} \). Thus (3.4) gives

\[
(x_0 + 5x_1 + 5^2x_2 + \cdots)^5 = x_0 + 5a_1 + 5^2a_2 + \cdots \tag{3.5}
\]
On the existence of \( p \)-adic roots 199

From (3.5), we have the followings.

(i) If \( x_0 = 1 \), then

\[
u = 1 + 5a_1 + 5^2a_2 + \cdots = (1 + 5x_1 + 5^2x_2 + \cdots)^5
\]

\[= 1 + 5^2x_1 + 5^3(x_1^2 + x_2^2) + \cdots \equiv 1 \pmod{25}.
\]

In the similar manner, we have the results in the other cases.

(ii) If \( x_0 = 2 \), then

\[
u = 2 + 5 \cdot 1 + 5^2(1 + x_1) + \cdots \equiv 2 \pmod{5}.
\]

(iii) If \( x_0 = 3 \), then

\[
u = 3 + 5 \cdot 3 + 5^2(4 + x_1) + \cdots \equiv 3 \pmod{5}.
\]

(iv) If \( x_0 = 4 \), then

\[
u = 4 + 5 \cdot 4 + 5^2(x_1 + 3x_2^2) + \cdots \equiv 4 \pmod{5}.
\]

Hence the proof is completed.

We also have the condition for the existence of the seventh root of a \( p \)-adic number in \( \mathbb{Z}_p \).

Theorem 3.6. Let \( p \) be a prime number. Then we have:

(1) If \( p \neq 7 \), then \( a = p^{\text{ord}_p a} u \in \mathbb{Q}_p \) for some \( u \in \mathbb{Z}_p^\times \) has a seventh root in \( \mathbb{Q}_p \) if and only if \( \text{ord}_p a = 7m \) for some \( m \in \mathbb{Z} \) and \( u = v^7 \) for some unit \( v \in \mathbb{Z}_p^\times \).

(2) If \( p = 7 \), then \( a = 7^{\text{ord}_7 a} u \in \mathbb{Q}_7 \) for some \( u \in \mathbb{Z}_7^\times \) has a seventh root in \( \mathbb{Q}_7 \) if and only if \( \text{ord}_7 a = 7m \) for some \( m \in \mathbb{Z} \) and \( u \equiv 1 (\pmod{7}) \) or \( u \equiv k (\pmod{49}) \) for some \( k (2 \leq k \leq 6) \).

Proof. Let \( a, x \in \mathbb{Q}_p \) be \( a = p^{\text{ord}_p a} u \) and \( x = p^{\text{ord}_p x} v \), where \( u, v \in \mathbb{Z}_p^\times \) as same as in (3.1). Then we have

\[
x^7 = a \Leftrightarrow p^{\text{ord}_p x} v^7 = p^{\text{ord}_p a} u
\]

\[
\Leftrightarrow p^{\text{ord}_p x}(x_0 + x_1 p + \cdots)^7 = p^{\text{ord}_p a}(a_0 + a_1 p + \cdots).
\]

The equation (3.6) is equivalent to the following system:

\[
\begin{cases}
7\text{ord}_p x = \text{ord}_p a \\
v^7 = u \\
x_0^7 - a_0 \equiv 0 \pmod{p}.
\end{cases}
\]

(3.7)

Let \( f(x) = x^7 - a_0 \). Then its derivative \( f'(x) = 7x^6 \) satisfies

\[
|f'(x_0)|_p = |7|_p = \begin{cases} 1, & \text{if } p \neq 7, \\ \frac{1}{7}, & \text{if } p = 7. \end{cases}
\]

(1) If \( p \neq 7 \), then the solution of \( f(x_0) = x_0^7 - a_0 \) exists by Hensel’s lemma. Thus the result follows.

(2) If \( p = 7 \), then the equation (3.7) is reduced to the following system:

\[
\begin{cases}
(x_0 + 7x_1 + 7^2x_2 + \cdots)^7 = a_0 + 7a_1 + 7^2a_2 + \cdots \\
x_0^7 - a_0 \equiv 0 \pmod{7},
\end{cases}
\]

(3.8)
where \( x_0, a_0 \in \{1, 2, 3, 4, 5, 6\} \). Thus (3.8) gives
\[
(x_0 + 7x_1 + 7^2x_2 + \cdots)^7 = x_0 + 7a_1 + 7^2a_2 + \cdots
\] (3.9)
with \( x_0 = 1, 2, 3, 4, 5, 6 \). From (3.9), we have the followings.

(i) If \( x_0 = 1 \), then \( u = 1 + 7^2x_1 + 7^3(3x_1^2 + x_2^2) + \cdots \equiv 1 \pmod{49} \).

(ii) If \( x_0 = 2 \), then \( u = 2 + 7 \cdot 4 + 7^2(2 + x_1) + \cdots \equiv 2 \pmod{7} \).

(iii) If \( x_0 = 3 \), then \( u = 3 + 7 \cdot 4 + 7^2(2 + x_1) + \cdots \equiv 3 \pmod{7} \).

(iv) If \( x_0 = 4 \), then \( u = 4 + 7 \cdot 2 + 7^2(5 + x_1) + \cdots \equiv 4 \pmod{7} \).

(v) If \( x_0 = 5 \), then \( u = 5 + 7 \cdot 2 + 7^2(5 + 3x_1) + \cdots \equiv 5 \pmod{7} \).

(vi) If \( x_0 = 6 \), then \( u = 6 + 7 \cdot 6 + 7^2x_1 + \cdots \equiv 6 \pmod{7} \).

Hence the proof is completed.

\[ \square \]

References

[1] S. Katok, \textit{p-Adic analysis compared with real}, American Math. Soc., 2007

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

[3] V. S. Vladimirov, I. V. Volvich, and E. I. Zelenov, \textit{p-Adic analysis and mathematical physics}, Nord Scientific, 1994.

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

[5] T. Zerzaihi, M. Kecies, and M. Knapp, \textit{Hensel codes of square roots of p-adic numbers}, Appl. Anal. Discrete Math. 4 (2010), 32-44.