Filomat 27:3 (2013), 429–434
DOI 10.2298/FIL1303429M

Published by Faculty of Sciences and Mathematics,
University of Niš, Serbia
Available at: http://www.pmf.ni.ac.rs/filomat

General approach of the root of a p-adic number

Kecies Mohamed[a], Zerzaihi Tahar[b]

[a]*Laboratoire de mathématiques pures et appliquées.Université de Jijel. BP 98 Ouled Aissa, 18000 Jijel, Algérie*
[b]*Laboratoire de mathématiques pures et appliquées.Université de Jijel. BP 98 Ouled Aissa, 18000 Jijel, Algérie*

Abstract. In this work, we applied the Newton method in the p-adic case to calculate the cubic root of a p-adic number $a \in \mathbb{Q}_p^*$ where p is a prime number, and through the calculation of the approximate solution of the equation $x^3 - a = 0$. We also determined the rate of convergence of this method and evaluated the number of iterations obtained in each step of the approximation.

1. Introduction

The p-adic numbers were discovered by K. Hensel around the end of the nineteenth century. In the course of one hundred years, the theory of p-adic numbers has penetrated into several areas of mathematics, including number theory, algebraic geometry, algebraic topology and analysis (and rather recently to physics). In papers [6], the authors used classical rootfinding methods to calculate the reciprocal of integer modulo p^n, where p is prime number. But in [1], the author used the Newton method to find the reciprocal of a finite segment padic number, also referred to as Hensel codes. The Hensel codes and their properties are studied in [2–4]. In [8], the authors used fixed point method to calculate the Hensel code of square root of a p-adic number $a \in \mathbb{Q}_p$, it means the first numbers of the p-adic development of the $\sqrt{a}$.

In this work, we will see how we can use classical root-finding method and explore a very interesting application of tools from numerical analysis to number theory.

One considers the following equation

$$x^3 - a = 0. \tag{1}$$

The solution of (1) is approximated by a p-adic number sequence $(x_n)_n \subset \mathbb{Q}_p^*$ constructed by the Newton method.

2. Preliminaries

Definition 2.1. *Let p be a prime number.*
1) 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 $|\cdot|_p$ defined by

$$\forall x \in \mathbb{Q}_p : |x|_p = \begin{cases} p^{-v_p(x)}, \textit{if } x \neq 0 \\ 0, \textit{if } x = 0, \end{cases}$$

2010 *Mathematics Subject Classification*. Primary 11E95 ; Secondary 34K28.
Keywords. Newton method; Hensel's lemma; rate of convergence.
Received: 05 November 2012; Revised 12 February 2013; Accepted: 16 February 2013
Communicated by Eberhard Malkowsky
Email addresses: kecmohamed@yahoo.fr (Kecies Mohamed), zerzaihi@yahoo.com (Zerzaihi Tahar)

where v_p is the p-adic valuation defined by

$$v_p(x) = \max\{r \in \mathbb{Z} : p^r \mid x\}.$$

2) The p-adic norm induces a metric d_p given by

$$\begin{array}{llll} d_p: & \mathbb{Q}_p \times \mathbb{Q}_p & \longrightarrow & \mathbb{R}^+ \\ & (x,y) & \longmapsto & d_p(x,y) = \left|x-y\right|_p, \end{array}$$

this metric is called the p-adic metric.

Theorem 2.2. *[5] Given a p-adic number $a \in \mathbb{Q}_p$, there exists a unique sequence of integers $(\beta_n)_{n\geq N}$, with $N = v_p(a)$, such that $0 \leq \beta_n \leq p-1$ for all n and*

$$a = \beta_N p^N + \beta_{N+1} p^{N+1} + ... + \beta_n p^n + ... = \sum_{k=N}^{\infty} \beta_k p^k$$

The short representation of a is $\beta_N\beta_{N+1}...\beta_{-1} \cdot \beta_0\beta_1...$, where only the coefficients of the powers of p are shown. We can use the p-adic point $\cdot$ as a device for displaying the sign of N as follows:

$$\begin{array}{l} \beta_N\beta_{N+1}...\beta_{-1} \cdot \beta_0\beta_1..., \text{ for } N < 0 \\ \cdot\beta_0\beta_1\beta_2..., \text{ for } N = 0 \\ \cdot 00...0\beta_0\beta_1..., \text{ for } N > 0. \end{array}$$

Definition 2.3. *A p-adic number $a \in \mathbb{Q}_p$ is said to be a p-adic integer if this canonical expansion contains only non negative power of p.*
The set of p-adic integers is denoted by $\mathbb{Z}_p$. We have

$$\mathbb{Z}_p = \left\{ \sum_{k=0}^{\infty} \beta_k p^k, 0 \leq \beta_k \leq p-1 \right\} = \left\{ a \in \mathbb{Q}_p : v_p(a) \geq 0 \right\} = \left\{ a \in \mathbb{Q}_p : |a|_p \leq 1 \right\}.$$

Definition 2.4. *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 of zero. The set of p-adic units is denoted by $\mathbb{Z}_p^*$. Hence we have*

$$\mathbb{Z}_p^* = \left\{ \sum_{k=0}^{\infty} \beta_k p^k, \beta_0 \neq 0 \right\} = \left\{ a \in \mathbb{Q}_p : |a|_p = 1 \right\}.$$

Lemma 2.5. *[5] Given $a \in \mathbb{Q}_p$ and $k \in \mathbb{Z}$, then*

$$\left\{ y \in \mathbb{Q}_p : \left|y-a\right|_p \leq p^k \right\} = a + p^{-k}\mathbb{Z}_p$$

Proposition 2.6. *[7] Let x be a p-adic number of norm p^{-n}. Then x can be written as the product $x = p^n u$, where $u \in \mathbb{Z}^*$.*

Proposition 2.7. *[7] Let $(a_n)_n$ be a p-adic number sequence. If $\lim\limits_{n\to\infty} a_n = a \in \mathbb{Q} \setminus \{0\}$, then $\lim\limits_{n\to\infty} |a_n|_p = |a|_p$. The sequence of norms $\left(|a_n|_p\right)_n$ must stabilize for sufficiently large n.*

Theorem 2.8. *[7](Hensel's lemma) Let $F(x) = c_0 + c_1 x + ... + c_n x^n$ be a polynomial whose coefficients are p-adic integers i.e. $\left(F \in \mathbb{Z}_p[x]\right)$. Let*

$$F'(x) = c_1 + 2c_2 x + 3c_3 x^2 + ... + nc_n x^{n-1}$$

be the derivative of $F(x)$. Suppose $\overline{a_0}$ is a p-adic integer which satisfies $F(\overline{a_0}) \equiv 0 \pmod p$ and $F'(\overline{a_0}) \not\equiv 0 \pmod p$. Then there exists a unique p-adic integer a such that $F(a) = 0$ and $a \equiv \overline{a_0} \pmod p$.

Theorem 2.9. *[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 $k \geqslant 1$.*

Definition 2.10. *A p-adic number $b \in \mathbb{Q}_p$ is said to be a cubic root of $a \in \mathbb{Q}_p$ of order k if $b^3 \equiv a \left(mod p^k\right)$, where $k \in \mathbb{N}$.*

Proposition 2.11. *[9] 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 2.12. *[9] Let p be a prime number, then*

1. *If $p \neq 3$, then $a = p^{v_p(a)}.u \in \mathbb{Q}_p \left(u \in \mathbb{Z}_p^*\right)$ has a cubic root in $\mathbb{Q}_p$ if and only if $v_p(a) = 3m$, $m \in \mathbb{Z}$ and $u = v^3$ for some unit $v \in \mathbb{Z}_p^*$.*
2. *If $p = 3$, then $a = 3^{v_3(a)}.u \in \mathbb{Q}_3 \left(u \in \mathbb{Z}_3^*\right)$ has a cubic root in $\mathbb{Q}_3$ if and only if $v_3(a) = 3m$, $m \in \mathbb{Z}$ and $u \equiv 1 (\mod 9)$ or $u \equiv 2(\mod 3)$.*

3. Main Results

Let $a \in \mathbb{Q}_p^*$ be a p-adic number such that

$$|a|_p = p^{-v_p(a)} = p^{-3m},\ m \in \mathbb{Z}. \tag{2}$$

We know that if there exists a p-adic number β such that $\beta^3 = a$ and $(x_n)_n$ is a sequence of the p-adic numbers that converges to a p-adic number $\beta \neq 0$, then from a certain rank one has

$$|x_n|_p = \left|\beta\right|_p = p^{-m}. \tag{3}$$

The Newton method: An elementary method to determine zeros of a given function is the Newton method where the iterative formula is defined by

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}, \forall n \in \mathbb{N}. \tag{4}$$

Obtaining the following recurrence relation

$$x_{n+1} = \frac{1}{3x_n^2}\left(a + 2x_n^3\right), \forall n \in \mathbb{N}. \tag{5}$$

Therefore

$$x_{n+1}^3 - a = \frac{1}{27x_n^6}\left(a + 8x_n^3\right)\left(a - x_n^3\right)^2, \forall n \in \mathbb{N}, \tag{6}$$

and

$$x_{n+1} - x_n = \frac{1}{3x_n^2}\left(a - x_n^3\right), \forall n \in \mathbb{N}. \tag{7}$$

Determining the rate of convergence of an iterative method is to study the comportment of the sequence $(e_{n+n_0})_n$ defined by $e_{n+n_0} = x_{n+n_0+1} - x_{n+n_0}$ obtained at each step of the iteration where $n_0 \in \mathbb{N}$.

Roughly speaking, if the rate of convergence of a method is s, then after each iteration the number of correct significant digits in the approximation increases by a factor of approximately s.

Theorem 3.1. *If x_{n_0} is the cubic root of a of order r. Then*
1) If $p \neq 3$, then x_{n+n_0} is the cubic root of a of order $2^n r - 3m(2^n - 1)$.
2) If $p = 3$, then x_{n+n_0} is the cubic root of a of order $2^n r - 3(m+1)(2^n - 1)$.

Proof. Let $(x_n)_n$ the sequence defined by (5) and x_{n_0} is the cubic root of a of order r. Then

$$x_{n_0}^3 - a \equiv 0 \mod p^r \Longrightarrow \left|x_{n_0}^3 - a\right|_p \leq p^{-r}.$$

We put

$$h(x) = a + 8x_n^3,$$

We have

$$|h(x)|_p = \left|a + 8x_n^3\right|_p \leq \max\left\{|a|_p, \left|8x_{n_0}^3\right|_p\right\} = p^{-3m}.$$

Since

$$|27|_p = \begin{cases} \frac{1}{27}, \text{ if } p = 3 \\ 1, \text{ if } p \neq 3. \end{cases} \tag{8}$$

This gives

$$\left|x_{n_0+1}^3 - a\right|_p = \left|\frac{1}{27x_{n_0}^6}\right|_p \cdot \left|a + 8x_{n_0}^3\right|_p \cdot \left|a - x_{n_0}^3\right|_p^2 \leq \left|\frac{1}{27x_{n_0}^6}\right|_p \cdot p^{-3m} \cdot p^{-2r}.$$

And so we have

$$\begin{cases} \left|x_{n_0+1}^3 - a\right|_p \leq p^{6m} \cdot p^{-3m} \cdot p^{-2r}, \text{ if } p \neq 3 \\ \\ \left|x_{n_0+1}^3 - a\right|_3 \leq 3^3 \cdot 3^{6m} \cdot 3^{-3m} \cdot 3^{-2r}, \text{ if } p = 3. \end{cases} \tag{9}$$

Or, in virtue of lemma 2.5

$$\begin{cases} x_{n_0+1}^3 - a \equiv 0 \mod p^{2r-3m}, \text{ if } p \neq 3 \\ \\ x_{n_0+1}^3 - a \equiv 0 \mod 3^{2r-3(m+1)}, \text{ if } p = 3. \end{cases} \tag{10}$$

In this manner, we find that if $p \neq 3$, then

$$\forall n \in \mathbb{N} : x_{n+n_0}^3 - a \equiv 0 \mod p^{v_n}, \tag{11}$$

Where the sequence $(v_n)_n$ is defined by

$$\forall n \in \mathbb{N} : \begin{cases} v_0 = r \\ v_{n+1} = 2v_n - 3m \end{cases} \Longleftrightarrow \forall n \in \mathbb{N} : v_n = 2^n r - 3m(2^n - 1).$$

If $p = 3$, then

$$\forall n \in \mathbb{N} : x_{n+n_0}^3 - a \equiv 0 \mod 3^{v'_n}, \tag{12}$$

Where the sequence $(v'_n)_n$ is defined by

$$\forall n \in \mathbb{N} : \begin{cases} v'_0 = r \\ v'_{n+1} = 2v'_n - 3(m+1) \end{cases} \Longleftrightarrow \forall n \in \mathbb{N} : v'_n = 2^n r - 3(m+1)(2^n - 1).$$

□

Corollary 3.2. *If x_{n_0} is the cubic root of a of order r. Then the sequence $(e_{n+n_0})_n$ is defined by*

$$\forall n \in \mathbb{N} : \begin{cases} x_{n+n_0+1} - x_{n+n_0} \equiv 0 \mod p^{\varphi_n}, \text{ if } p \neq 3 \\ x_{n+n_0+1} - x_{n+n_0} \equiv 0 \mod 3^{\varphi'_n}, \text{ if } p = 3, \end{cases} \tag{13}$$

Where

$$\forall n \in \mathbb{N} : \begin{cases} \varphi_n = 2^n r - m(3 \cdot 2^n - 1) \\ \varphi'_n = 2^n r - (m(3 \cdot 2^n - 1) + (3 \cdot 2^n - 2)). \end{cases} \tag{14}$$

Proof. We have

$$x_{n+1} - x_n = \frac{1}{3x_n^2}\left(a - x_n^3\right), \forall n \in \mathbb{N}, \tag{15}$$

Since

$$|3|_p = \begin{cases} \frac{1}{3}, \text{ if } p = 3 \\ 1, \text{ if } p \neq 3, \end{cases} \tag{16}$$

This gives

$$\left|x_{n+n_0+1} - x_{n+n_0}\right|_p = \left|\frac{1}{3x_{n+n_0}^2}\left(a - x_{n+n_0}^3\right)\right|_p = p^{2m} \cdot \left|\frac{1}{3}\right|_p \cdot \left|a - x_{n+n_0}^3\right|_p \tag{17}$$

$$\Longrightarrow \begin{cases} \left|x_{n+n_0+1} - x_{n+n_0}\right|_p \leq p^{2m} \cdot p^{-v_n}, \text{ if } p \neq 3 \\ \left|x_{n+n_0+1} - x_{n+n_0}\right|_3 \leq 3^{2m+1} \cdot 3^{-v'_n}, \text{ if } p = 3, \end{cases} \tag{18}$$

Or, in virtue of lemma 2.5

$$\forall n \in \mathbb{N} : \begin{cases} x_{n+n_0+1} - x_{n+n_0} \equiv 0 \mod p^{v_n - 2m}, \text{ if } p \neq 3 \\ x_{n+n_0+1} - x_{n+n_0} \equiv 0 \mod 3^{v'_n - (2m+1)}, \text{ if } p = 3. \end{cases} \tag{19}$$

We put

$$\forall n \in \mathbb{N} : \begin{cases} \varphi_n = v_n - 2m = 2^n r - m(3 \cdot 2^n - 1) \\ \varphi'_n = v'_n - (2m+1) = 2^n r - (m(3 \cdot 2^n - 1) + (3 \cdot 2^n - 2)). \end{cases} \tag{20}$$

□

3.1. Conclusion

According to the results obtained in the previous section, we obtain the following conclusions:

1. If $p \neq 3$,then
   (a) The rate of convergence of the sequence $(x_n)_n$ is of order φ_n.

(b) If $r - 3m > 0$, then the number of iterations to obtain M correct digits is

$$n = \left[\frac{\ln(\frac{M-m}{r-3m})}{\ln 2} \right]. \tag{21}$$

2. If $p \neq 3$,then
   (a) The rate of convergence of the sequence $(x_n)_n$ is of order φ'_n.
   (b) If $r - 3(m+1) > 0$, then the number of iterations to obtain M correct digits is

$$n = \left[\frac{\ln(\frac{M-(m+2)}{r-3(m+1)})}{\ln 2} \right]. \tag{22}$$

References

[1] A. Vimawala, p-adic Arithmetic Methods for Exact Computation of Rational Numbers, School of Electrical Engineering and Computer Science, Oregon State University. [Online] Available: http://cs.ucsb.edu/ koc/cs290g/project/2003/vimawala.pdf. June 2003.
[2] C.J. Zarowski, H.C. Card, On Addition and Multiplication with Hensel Codes, IEEE transactions on computers 39(12)(1990)1417–1423.
[3] C.k. Koc, A Tutorial on p-adic Arithmetic, Electrical and Computer Engineering. Oregon State University, Corvallis, Oregon 97331. Technical Report.[Online] Available: http://islab.oregonstate.edu/papers/r09padic.pdf. 2002.
[4] E.V Krishnamurthy, On the Conversion of Hensel Codes to Farey Rationals, IEEE Transactions on Computers 32(4)(1983) 331–337.
[5] F. B. Vej, P-adic Numbers, Aalborg University. Department Of Mathematical Sciences. [Online] Available: http://www.control.auc.dk/ jjl/oldpro/oldstu/mat3.ps. 2000.
[6] M. Knapp, C. Xenophotos, Numerical analysis meets number theory: using rootfinding methods to calculate inverses mod p^n, Appl. Anal. Discrete Math. 4 (2010) 23–31.
[7] S. Katok, p-adic analysis compared with real, Student Mathematical Library Vol. 37, American Mathematical Society, 2007.
[8] T. Zerzaihi, M. Kecies, M. Knapp, Hensel codes of square roots of p-adic numbers, Appl. Anal. Discrete Math. 4(2010) 32-44.
[9] T. Zerzaihi, M. Kecies, Computation of the Cubic Root of a p-adic Number, Journal of Mathematics Research 3(3)(2011)40–47.