Computation of the Cubic Root of a p-adic Number

T. Zerzaihi

Laboratory of Pure and Applied Mathematics, University of Jijel. Algeria

E-mail: zerzaihi@yahoo.com

M. Kecies

Laboratory of Pure and Applied Mathematics, University of Jijel. Algeria

E-mail: kecmohamed@yahoo.fr

Received: December 24, 2010 Accepted: January 7, 2011 doi:10.5539/jmr.v3n3p40

Abstract

In this work, we applied the classical numerical method of the secant 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 this 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.

Computing both the cubic root and other roots of a p-adic number is useful both for their theoretical values as for their theoretical applications in the field of theoretical computer science and cryptography.

Keywords: Secant methods, Hensel's lemma, Rate of convergence

2000 Mathematics Subject Classification: 11E95, 26E30, 65H04

1. Introduction

Let $\mathbb{Q}_p$ be the field of p-adic numbers where p is a prime number. Our main goal is to compute the approximate finite p-adic expansion of the cubic root for the p-adic number $a \in \mathbb{Q}_p^*$. This is done by determining the approximate solution of the 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 secant method.

Knapp and Xenophotos (2010) used numerical methods to find the reciprocal of an integer modulo p^n.

2. Preliminaries

Definition 3. *Let p be a prime number. 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*

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

where v_p is the p-adic valuation defined by $v_p(x) = \max\{r \in \mathbb{Z} : p^r \mid x\}$.

The p-adic norm induces a metric d_p given by

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

this metric is called the p-adic metric.

Theorem 4. *(F. B. Vej, 2000) Given a p-adic number $a \in \mathbb{Q}_p$, there exists a unique sequence of integers $(\beta_n)_{n \geq k}$, with $k = v_p(x)$, such that $\beta_n \in \{0, \ldots, p-1\}$ for all n and*

$$a = \beta_n p^n + \beta_{n+1} p^{n+1} + ... + \beta_{-1} p^{-1} + \beta_0 + \beta_1 p^2 ... = \sum_{k=n}^{\infty} \beta_k p^k$$

with $\beta_k \in \mathbb{Z}$ and $\beta_k \in \{0, 1, 2, ..., p-1\}$ for each $k \geq n$.

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:

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

Definition 5. *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

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

Definition 6. *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 7. *(F. B. Vej, 2000) Given $a\in\mathbb{Q}_p$ and $k\in\mathbb{Z}$, then*

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

Proposition 8. *(F. B. Vej, 2000) Given a p-adic number $a\in\mathbb{Q}_p\setminus\{0\}$, there exist $n\in\mathbb{Z}$ and $u\in\mathbb{Z}^*$ such that $a=p^n\cdot u$.*

Proposition 9. *(S. Katok, 2007) Let $(a_n)_n$ be a p-adic number sequence. If $\lim_{n\to\infty}a_n=a\in\mathbb{Q}\setminus\{0\}$, then $\lim_{n\to\infty}|a_n|_p=|a|_p$. The sequence of norms $\left(|a_n|_p\right)_n$ must stabilize for sufficiently large n.*

Definition 10. *Let p be a prime number. Then the Hensel code of length M of any p-adic number $a=p^m\cdot u\in\mathbb{Q}_p$ is the pair $(mant_a, exp_a)=(a_m a_{m+1}\ldots.a_0\cdot a_t, m)$, where the $M=|m|+t+1$ leftmost digits and the value m of the related p-adic expansion are called the mantissa and the exponent, respectively.*

We use the notation $H(p,M,a)$ where p is a prime and M is the integer which specifies the number of precision digits of the p-adic expansion.

For a general overview about p-adic numbers and their properties, the reader can consult [1, 3-5].

Theorem 11. *(Hensel's lemma) (S. Katok, 2007) Let $F(x)=c_0+c_1x+...+c_nx^n$ be a polynomial whose coefficients are p-adic integers i.e. $\left(F\in\mathbb{Z}_p[x]\right)$. Let*

$$F'(x)=c_1+2c_2x+3c_3x^2+...+nc_nx^{n-1}$$

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

Theorem 12. *(S. Katok, 2007) 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 13. *A p-adic number $b\in\mathbb{Q}_p$ is said to be a cubic root of $a\in\mathbb{Q}_p$ of order $k\in\mathbb{N}$ if $b^3\equiv a\left(\mod p^k\right)$.*

3. Main Results

Proposition 14. *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.*

Proof. Consider the p-adic continuous function $f(x)=x^3-a$ and its derivative $f'(x)=3x^2$. If a is a cubic residue modulo p, then

$$a\equiv a_0^3(\mod p)$$

for $a_0\in\{1,2,...,p-1\}$. Hence $f(a_0)\equiv 0(\mod p)$ and $f'(a_0)=3a_0^2\not\equiv 0(\mod p)$ because $p\neq 3$ and $a_0\neq 0$. Consequently, the solution is in $\mathbb{Z}_p$. Conversely, if a is a non-cubic residue, Theorem (10) implies the non-existence of cubic roots in $\mathbb{Z}_p$. □

Corollary 15. *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 $u \equiv 2(\mod 3)$.*

Proof. Let $a, x \in \mathbb{Q}_p$ be

$$a = p^{v_p(a)} \cdot (a_0 + a_1 p + a_2 p^2 + ...) = p^{v_p(a)} \cdot u, \quad a_0 \neq 0 \tag{2}$$

$$x = p^{v_p(x)} \cdot (x_0 + x_1 p + x_2 p^2 + ...) = p^{v_p(x)} \cdot v, \quad x_0 \neq 0. \tag{4}$$

Let us note that u and v are p-adic unit intergers according to definition 4

$$\begin{aligned} u &= a_0 + a_1 p + a_2 p^2 + ... = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p^* \\ v &= x_0 + x_1 p + x_2 p^2 + ... = \sum_{i=0}^{\infty} x_i p^i \in \mathbb{Z}_p^*, \end{aligned} \tag{5}$$

Then, imposing the cubic condition, we obtain

$$\begin{aligned} x^3 &= a \Longleftrightarrow p^{3v_p(x)}(x_0 + x_1 p + x_2 p^2 + ...)^3 = p^{v_p(a)}(a_0 + a_1 p + a_2 p^2 + ...) \\ &\Longleftrightarrow p^{3v_p(x)} \cdot v^3 = p^{v_p(a)} \cdot u, \end{aligned}$$

The latter is equivalent to the following system

$$\begin{cases} v_p(a) = 3v_p(x) \\ v^3 = u \\ x_0^3 - a \equiv 0 (\mod p). \end{cases} \tag{6}$$

Additionally, we consider $f(x) = x_0^3 - a$ and its derivative $f'(x_0) = 3x_0^2$ satisfies

$$\left|f'(x_0)\right|_p = |3|_p = \begin{cases} 1, & \text{if } p \neq 3 \\ \frac{1}{3}, & \text{if } p = 3 \end{cases} \tag{7}$$

Then we have

1. if $p \neq 3$, by Hensel's lemma the solution of $f(x_0) = x_0^3 - a = 0$ exists.
2. if $p = 3$, equation (6) is reduced to

$$\begin{cases} (x_0 + x_1 3 + x_2 3^2 + ...)^3 = a_0 + a_1 3 + a_2 3^2 + ... \\ x_0^3 - a_0 \equiv 0 (\mod 3), \end{cases}$$

where $x_0, a_0 \in \{1, 2\}$. This gives

$$\begin{cases} \left(1 + x_1 3 + x_2 3^2 + ...\right)^3 = 1 + a_1 3 + a_2 3^2 + ..., \text{ if } x_0 = 1 \\ \left(2 + x_1 3 + x_2 3^2 + ...\right)^3 = 2 + a_1 3 + a_2 3^2 + ..., \text{ if } x_0 = 2. \end{cases}$$

(a) If $x_0 = 1$, then

$$\left(1 + x_1 3 + x_2 3^2 + x_3 3^3 + ...\right)^3 = 1 + 3^2(x_1 + 3(x_2 + x_1^2 + x_1^3) + ...) = u,$$

we get

$$u = 1 + a_1 3 + a_2 3^2 + ... = \left(1 + x_1 3 + x_2 3^2 + x_3 3^3\right)^3 \equiv 1 (\mod 9), \tag{8}$$

and $a_1 = 0$.

(b) If $x_0 = 2$, then

$$\left(2 + x_1 3 + x_2 3^2 + x_3 3^3 + ...\right)^3 = 2 + 2 \cdot 3 + 3^2(2^2 \cdot x_1) + 3^3(2^2 x_2 + 2x_1^2 + x_1^3) + ... = u,$$

so

$$u = 2 + a_1 3 + a_2 3^2 + ... = \left(2 + x_1 3 + x_2 3^2 + ...\right)^3 \equiv 2(\mod 3), \tag{9}$$

and $a_1 = 2$.

□

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

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

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

$$|x_n|_p = |d|_p = p^{-m}. \tag{10}$$

3.1 The secant method

An elementary method to determine zeros of a given function is the secant method. This method can be derived from the Newton method, where we replace the derivative $f'(x_n)$ by the approximation

$$f'(x_n) \approx \frac{f(x_n) - f(x_{n-1})}{x_n - x_{n-1}}, \forall n \in \mathbb{N}^*. \tag{11}$$

The iterative formula of the secant method is

$$x_{n+1} = x_n - \frac{f(x_n)(x_n - x_{n-1})}{f(x_n) - f(x_{n-1})}, \forall n \in \mathbb{N}^*, \tag{12}$$

Obtaining the following recurrence relation

$$x_{n+1} = \frac{a + x_n x_{n-1}^2 + x_n^2 x_{n-1}}{x_n^2 + x_n x_{n-1} + x_{n-1}^2}, \forall n \in \mathbb{N}^*. \tag{13}$$

Determining the rate of convergence of an iterative method is to study the comportment of the sequence $(e_{n+n_0})_n$ defined by $e_{n+n_0} = x_{n+n_0} - x_{n+n_0-1}$ 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 16. *If x_{n_0-1} is the cubic root of a of order α and x_{n_0} is the cubic root of a of order β then*

1. *If $p \neq 3$, then x_{n+n_0-1} is the cubic root of a of order J_n, where the sequence $(J_n)_n$ is defined by*

$$\begin{aligned} J_n = &\left[\tfrac{1}{\sqrt{5}}\left(\beta - \alpha(1-\Phi)\right)\Phi^n + \tfrac{1}{\sqrt{5}}\left(-\beta + \alpha\Phi\right)(1-\Phi)^n\right] + \\ &-3\left(\left[\tfrac{1}{\sqrt{5}}\left(\Phi^{n+1} - (1-\Phi)^{n+1}\right)\right] - 1\right)m, \forall n \in \mathbb{N}. \end{aligned} \tag{14}$$

2. *If $p = 3$, then x_{n+n_0-1} is the cubic root of a of order J'_n, where the sequence $(J'_n)_n$ is defined by*

$$\begin{aligned} J'_n = &\left[\tfrac{1}{\sqrt{5}}\left(\beta - \alpha(1-\Phi)\right)\Phi^n + \tfrac{1}{\sqrt{5}}\left(-\beta + \alpha\Phi\right)(1-\Phi)^n\right] + \\ &-3\left(\left[\tfrac{1}{\sqrt{5}}\left(\Phi^{n+1} - (1-\Phi)^{n+1}\right)\right] - 1\right)(m+1), \forall n \in \mathbb{N}, \end{aligned} \tag{15}$$

were $\Phi = \frac{1+\sqrt{5}}{2}$ is the golden ratio and m is the exponent in the p-adic expansion of a.

Proof. Let $(x_n)_n$ be the sequence defined by (13). Then

$$x_{n+1}^3 - a = \frac{\left(a + x_n^3 + x_{n-1}^3 + 3x_n x_{n-1}^2 + 3x_n^2 x_{n-1}\right)\left(x_n^3 - a\right)\left(x_{n-1}^3 - a\right)}{\left(x_n^2 + x_n x_{n-1} + x_{n-1}^2\right)^3}, \forall n \in \mathbb{N}^*. \tag{16}$$

Since

$$\begin{cases} x_{n_0-1}^3 - a \equiv 0(\mod p^{\alpha}) \\ x_{n_0}^3 - a \equiv 0(\mod p^{\beta}) \end{cases} \Longrightarrow \begin{cases} \left|x_{n_0-1}^3 - a\right|_p \leq p^{-\alpha} \\ \left|x_{n_0}^3 - a\right|_p \leq p^{-\beta}. \end{cases}$$

This gives

$$\left|x_{n_0+1}^3 - a\right|_p = \frac{\left|a + x_{n_0}^3 + x_{n_0-1}^3 + 3x_{n_0}x_{n_0-1}^2 + 3x_{n_0}^2 x_{n_0-1}\right|_p}{\left|x_{n_0}^2 + x_{n_0}x_{n_0-1} + x_{n_0-1}^2\right|_p^3} \cdot \left|x_{n_0-1}^3 - a\right|_p \cdot \left|x_{n_0}^3 - a\right|_p$$

$$\leq p^{-\alpha}p^{-\beta} \cdot \frac{1}{\left|x_{n_0}^2 + x_{n_0}x_{n_0-1} + x_{n_0-1}^2\right|_p^3} \cdot \max\left\{|a|_p, \left|x_{n_0}^3\right|_p, \left|x_{n_0-1}^3\right|_p, \left|3x_{n_0}x_{n_0-1}^2\right|_p, \left|3x_{n_0}^2 x_{n_0-1}\right|_p\right\},$$

and, hence, we have

$$\begin{cases} \left|x_{n_0+1}^3 - a\right|_p \leq p^{-\alpha}p^{-\beta} \cdot \frac{1}{p^{-6m}} \cdot \max\left\{p^{-3m}, p^{-3m}, p^{-3m}, p^{-3m}, p^{-3m}\right\}, & \text{if } p \neq 3, \\ \left|x_{n_0+1}^3 - a\right|_3 \leq 3^{-\alpha}3^{-\beta} \cdot \frac{1}{3^{-3}\cdot 3^{-6m}} \cdot \max\left\{3^{-3m}, 3^{-3m}, 3^{-3m}, 3^{-(3m+1)}, 3^{-(3m+1)}\right\}, & \text{if } p = 3. \end{cases}$$

This is equivalent to verify either

$$\begin{cases} \left|x_{n_0+1}^3 - a\right|_p \leq p^{-(\alpha+\beta-3m)}, & \text{if } p \neq 3, \\ \left|x_{n_0+1}^3 - a\right|_3 \leq 3^{-(\alpha+\beta-3(m+1))}, & \text{if } p = 3. \end{cases}$$

Or, in virtue of lemma 5

$$\begin{cases} x_{n_0+1}^3 - a \equiv 0(\mod p^{\alpha+\beta-3m}), & \text{if } p \neq 3, \\ x_{n_0+1}^3 - a \equiv 0(\mod 3^{\alpha+\beta-3(m+1)}), & \text{if } p = 3 \end{cases}$$

On the other hand, we have

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

Consequently

$$\begin{cases} x_{n_0+2}^3 - a \equiv 0(\mod p^{\alpha+2\beta-6m}), & \text{if } p \neq 3, \\ x_{n_0+2}^3 - a \equiv 0(\mod 3^{\alpha+2\beta-6(m+1)}), & \text{if } p = 3. \end{cases}$$

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

$$\begin{cases} x_{n_0-1}^3 - a \equiv 0(\mod p^{\alpha}) \\ x_{n_0}^3 - a \equiv 0(\mod p^{\beta}) \end{cases} \Longrightarrow \begin{cases} x_{n_0+1}^3 - a \equiv 0(\mod p^{\alpha+\beta-3m}) \\ x_{n_0+2}^3 - a \equiv 0(\mod p^{\alpha+2\beta-6m}) \\ x_{n_0+3}^3 - a \equiv 0(\mod p^{2\alpha+3\beta-12m}) \\ x_{n_0+4}^3 - a \equiv 0(\mod p^{3\alpha+5\beta-21m}) \\ \quad . \\ \quad . \\ \quad . \end{cases}$$

and if $p = 3$, then

$$\begin{cases} x_{n_0-1}^3 - a \equiv 0(\mod 3^{\alpha}) \\ x_{n_0}^3 - a \equiv 0(\mod 3^{\beta}) \end{cases} \Longrightarrow \begin{cases} x_{n_0+1}^3 - a \equiv 0(\mod 3^{\alpha+\beta-3(m+1)}) \\ x_{n_0+2}^3 - a \equiv 0(\mod 3^{\alpha+2\beta-6(m+1)}) \\ x_{n_0+3}^3 - a \equiv 0(\mod 3^{2\alpha+3\beta-12(m+1)}) \\ x_{n_0+4}^3 - a \equiv 0(\mod 3^{3\alpha+5\beta-21(m+1)}) \\ \cdot \\ \cdot \\ \cdot \end{cases}$$

1. If $p \neq 3$, then

$$x_{n+n_0-1}^3 - a \equiv 0(\mod p^{J_n}), \forall n \in \mathbb{N}, \tag{17}$$

where the sequence $(J_n)_n$ is defined by

$$J_n = F_n - mA_n, \forall n \in \mathbb{N}. \tag{18}$$

Where

$$\begin{cases} F_0 = \alpha\ , F_1 = \beta \\ \forall n \in \mathbb{N}^* : F_{n+1} = F_{n-1} + F_n, \end{cases} \tag{19}$$

and

$$\begin{cases} A_0 = A_1 = 0 \\ \forall n \in \mathbb{N}^* : A_{n+1} = A_{n-1} + A_n + 3. \end{cases} \tag{20}$$

The sequences $(F_n)_n$ and $(A_n)_n$ are linear recurrent sequences whose general terms are given respectively by

$$\begin{aligned} F_n &= \left[\tfrac{1}{\sqrt{5}} \left(\beta - \tfrac{1-\sqrt{5}}{2}\alpha \right) \left(\tfrac{1+\sqrt{5}}{2} \right)^n + \tfrac{1}{\sqrt{5}} \left(-\beta + \tfrac{1+\sqrt{5}}{2}\alpha \right) \left(\tfrac{1-\sqrt{5}}{2} \right)^n \right] \\ &= \left[\tfrac{1}{\sqrt{5}} \left(\beta - \alpha(1-\Phi) \right) \Phi^n + \tfrac{1}{\sqrt{5}} \left(-\beta + \alpha\Phi \right) (1-\Phi)^n \right], \forall n \in \mathbb{N}, \end{aligned} \tag{21}$$

and

$$\begin{aligned} A_n &= 3\left(\left[\tfrac{1}{\sqrt{5}} \left(\left(\tfrac{1+\sqrt{5}}{2} \right)^{n+1} - \left(\tfrac{1-\sqrt{5}}{2} \right)^{n+1} \right) \right] - 1 \right) \\ &= 3\left(\left[\tfrac{1}{\sqrt{5}} \left(\Phi^{n+1} - (1-\Phi)^{n+1} \right) \right] - 1 \right), \forall n \in \mathbb{N}. \end{aligned} \tag{22}$$

We obtain

$$\begin{aligned} J_n = &\left[\tfrac{1}{\sqrt{5}} \left(\beta - \alpha(1-\Phi) \right) \Phi^n + \tfrac{1}{\sqrt{5}} \left(-\beta + \alpha\Phi \right) (1-\Phi)^n \right] + \\ &-3\left(\left[\tfrac{1}{\sqrt{5}} \left(\Phi^{n+1} - (1-\Phi)^{n+1} \right) \right] - 1 \right) m, \forall n \in \mathbb{N}. \end{aligned} \tag{23}$$

2. If $p = 3$, then

$$x_{n+n_0-1}^3 - a \equiv 0(\mod 3^{J'_n}), \forall n \in \mathbb{N}, \tag{24}$$

where the sequence $(J'_n)_n$ is defined by

$$\begin{aligned} J'_n &= F_n - (m+1) \cdot A_n = \\ &= \left[\tfrac{1}{\sqrt{5}} \left(\beta - \alpha(1-\Phi) \right) \Phi^n + \tfrac{1}{\sqrt{5}} \left(-\beta + \alpha\Phi \right) (1-\Phi)^n \right] + \\ &-3\left(\left[\tfrac{1}{\sqrt{5}} \left(\Phi^{n+1} - (1-\Phi)^{n+1} \right) \right] - 1 \right) (m+1), \forall n \in \mathbb{N}. \end{aligned}$$

□

Corollary 17. *Suppose that x_{n_0-1} is the cubic root of a of order α and that x_{n_0} is the cubic root of a of order β then*

1. *If $p \neq 3$, then $x_{n+n_0} - x_{n+n_0-1} \equiv 0(\mod p^{\lambda_n})$ where the sequence $(\lambda_n)_n$ is defined by*

$$\begin{aligned} \lambda_n = &\left[\tfrac{1}{\sqrt{5}} \left(\beta - \alpha(1-\Phi) \right) \Phi^n + \tfrac{1}{\sqrt{5}} \left(-\beta + \alpha\Phi \right) (1-\Phi)^n \right] + \\ &-m\left(3\left[\tfrac{1}{\sqrt{5}} \left(\Phi^{n+1} - (1-\Phi)^{n+1} \right) \right] - 1 \right). \end{aligned} \tag{25}$$

2. *If $p = 3$, then $x_{n+n_0} - x_{n+n_0-1} \equiv 0(\mod 3^{\lambda'_n})$ where the sequence $(\lambda'_n)_n$ is defined by*

$$\begin{aligned}\lambda'_n = &\left[\tfrac{1}{\sqrt{5}}(\beta-\alpha(1-\Phi))\Phi^n + \tfrac{1}{\sqrt{5}}(-\beta+\alpha\Phi)(1-\Phi)^n\right] + \\ &-\left(m\left(3\left[\tfrac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1\right)+3\left[\tfrac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-2\right), \forall n \in \mathbb{N}.\end{aligned} \tag{26}$$

Proof. Starting from equation (13), we have

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

We obtain

$$\left|x_{n+n_0} - x_{n+n_0-1}\right|_p = \left|\frac{1}{x_{n+n_0-1}^2 + x_{n+n_0-1}x_{n+n_0-2} + x_{n+n_0-2}^2}\right|_p \left|x_{n+n_0-1}^3 - a\right|_p.$$

So

$$\begin{cases} \left|x_{n+n_0} - x_{n+n_0-1}\right|_p \le p^{-J_n}\cdot p^{2m} = p^{-(J_n-2m)}, & \text{if } p \neq 3, \\ \left|x_{n+n_0} - x_{n+n_0-1}\right|_3 \le 3^{-J'_n}\cdot 3^{(2m+1)} = 3^{-(J'_n-(2m+1))}, & \text{if } p \neq 3. \end{cases}$$

Therefore

$$\begin{cases} x_{n+n_0} - x_{n+n_0-1} \equiv 0(\mod p^{\lambda_n}), & \text{if } p \neq 3, \\ x_{n+n_0} - x_{n+n_0-1} \equiv 0(\mod 3^{\lambda'_n}), & \text{si } p = 3. \end{cases}$$

Such as

$$\begin{aligned}&\lambda_n = J_n - 2m = \\ &= \left[\tfrac{1}{\sqrt{5}}(\beta-\alpha(1-\Phi))\Phi^n + \tfrac{1}{\sqrt{5}}(-\beta+\alpha\Phi)(1-\Phi)^n\right] - m\left(3\left[\tfrac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1\right), \forall n \in \mathbb{N},\end{aligned}$$

and

$$\forall n \in \mathbb{N} : \lambda'_n = J'_n - (2m+1).$$

Hence we obtain

$$\begin{aligned}\lambda'_n = J'_n - (2m+1) = \\ = \left[\tfrac{1}{\sqrt{5}}(\beta-\alpha(1-\Phi))\Phi^n + \tfrac{1}{\sqrt{5}}(-\beta+\alpha\Phi)(1-\Phi)^n\right] + \\ -\left(m\left(3\left[\tfrac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-1\right)+3\left[\tfrac{1}{\sqrt{5}}\left(\Phi^{n+1}-(1-\Phi)^{n+1}\right)\right]-2\right), \forall n \in \mathbb{N}.\end{aligned}$$

□

3.2 Conclusions

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 λ_n.
   (b) Since $|1-\Phi| < 1$, then

$$\lambda_n \simeq \frac{1}{\sqrt{5}}(\beta-\alpha(1-\Phi))\Phi^n - m\left(\frac{3}{\sqrt{5}}\Phi^{n+1} - 1\right), \tag{28}$$

   and if $\beta - \alpha(1-\Phi) - 3\Phi m > 0$, then the number of iterations n to obtain M correct digits is

$$n = \left\lfloor \frac{\ln\left(\frac{\sqrt{5}(M-m)}{\beta-\alpha(1-\Phi)-3\Phi m}\right)}{\ln\Phi} \right\rfloor. \tag{29}$$

   (c) Using Hensel codes, equation (13) can be rewritten as

$$H(p,\lambda_{n+1},x) = \frac{H^3(p,\infty,x) + H(p,\lambda_n,x)\cdot H^2(p,\lambda_{n-1},x) + H^2(p,\lambda_n,x)\cdot H(p,\lambda_{n-1},x)}{H^2(p,\lambda_n,x) + H(p,\lambda_n,x)\cdot H(p,\lambda_{n-1},x) + H^2(p,\lambda_{n-1},x)}. \tag{30}$$

2. If $p = 3$, then

   (a) The rate of convergence of the sequence $(x_n)_n$ is of order λ'_n.

   (b) If $\beta - \alpha(1-\Phi) - 3\Phi(m+1) > 0$, then the necessary number n of iterations to obtain M correct digits is

$$n = \left\lceil \frac{\ln\left(\frac{\sqrt{5}(M-(m+2))}{\beta-\alpha(1-\Phi)-3\Phi(m+1)}\right)}{\ln \Phi} \right\rceil. \tag{31}$$

   (c) Using Hensel codes, equation (13) takes the form

$$H(3, \lambda'_{n+1}, x) = \frac{H^3(3, \infty, x) + H(3, \lambda'_n, x) \cdot H^2(3, \lambda'_{n-1}, x) + H^2(3, \lambda'_n, x) \cdot H(3, \lambda'_{n-1}, x)}{H^2(3, \lambda'_n, x) + H(3, \lambda'_n, x) \cdot H(3, \lambda'_{n-1}, x) + H^2(3, \lambda'_{n-1}, x)}. \tag{32}$$

Finally, the problem to ask is to increase the rate of convergence of the sequence $(x_n)_n$ as much as we wants. For this, we search an iteration function g that allows us to accelerate the rate of convergence and which satisfies the following relation

$$g(\sqrt[3]{a}) = \sqrt[3]{a}, g^{(1)}(\sqrt[3]{a}) = g^{(2)}(\sqrt[3]{a}) = ... = g^{(s-1)}(\sqrt[3]{a}) = 0, g^{(s)}(\sqrt[3]{a}) \neq 0. \tag{33}$$

To increase the rate of convergence of the sequence $(x_n)_n$ as much as we wants, it is necessary to solve the problem of letting

$$g(x) = \sqrt[3]{a} + (x - \sqrt[3]{a})^s h(x), s \in \mathbb{N}, \tag{34}$$

and choosing the function $h(x)$ in order to make the cubic roots of a in coefficients of a function $g(x)$ disappear.

References

A. Vimawala. (2003). *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.

C.J. Zarowski, H.C. Card. (1990). On Addition and Multiplication with Hensel Codes. *IEEE transactions on computers*, 39(12):1417-1423, December 1990.

C.k. Koc. (2002). *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. April 2002.

E.V Krishnamurthy. (1983). On the Conversion of Hensel Codes to Farey Rationals. *IEEE Transactions on Computers*, 32(4): 331-337, April 1983.

F. B. Vej. (2000). *P-adic Numbers.* Aalborg University. Departement Of Mathematical Sciences. [Online] Available: http://www.control.auc.dk/ jjl/oldpro/oldstu/mat3.ps. 18-12-2000.

M. Knapp, C. Xenophotos. (2010). Numerical analysis meets number theory: using rootfinding methods to calculate inverses (mod p^n). *Appl. Anal. Discrete Math*, 23-31, 4.

S. Katok. (2007). *p-adic analysis compared with real.* Student Mathematical Library Vol. 37, American Mathematical Society.

T. Zerzaihi, M. Kecies, M. Knapp. (2010). *Hensel codes of square roots of p-adic numbers.* Appl. Anal. Discrete Math. 32-44, 4.