Integral solutions of $\mathbf{x^3 - 2y^3 = 1}$

BMST 2025
p-adic numbers and applications
Copenhagen

Xi Feihu [*]
Noemi Gennuso [†]
April 19, 2025

[*]Sorbonne University
[†]University of Milan

Contents

1 p-adic analytic funnction

The main goal of this part is to completely solve the equation by p-adic method, p-adic analytic function and Strassman's theorem will be the key, in particular logarithm and exponential function.

Proposition 1.1. Let K be a complete non-archimdean field, a series $\sum_{n\geq 0} a_n$ of K converges if and only if $(a_n)_{n\geq 0}$ converges to zero.

Proof. □

Similarly, we can study the convergence of power series in a non-archimdean field by considering the radius convergence

$$R = 1/\limsup_{n\to\infty} \sqrt[n]{|a_n|}$$

Since ultrametric is still a metric. We can formally define

Definition. Let $B_p(a,r) = \{x \in \mathbb{Q}_p \mid |x-a|_p < r\}$ be a subset of $\mathbb{Q}_p$.

- p-adic logarithm is the p-adic analytic function $\log_p : B_p(1,1) \to \mathbb{Q}_p$ defined by

$$\log_p(x) := \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(x-1)^n}{n}$$

- p-adic exponential is the p-adic analytic function $\exp_p : B_p(0, p^{-1/(p-1)}) \to \mathbb{Q}_p$ defined by

$$\exp_p(x) := \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

We will verify the statement is well-defined. For the reader who is familiar with p-adic analytic function, this section can be skipped.

It is easier to check logarithm by observing $v_p(n) \leq \log_p(n)$ for any integer $n \geq p$ and here logarithm is defined in real line, because any integer between p^k and p^{k+1} has valuation 1 and logarithm in real line is increasing. then for any $|x-1|_p = p^{-r} < 1$ we have

$$\lim_{n\to\infty} |1/n|_p |x-1|_p^n = \lim_{n\to\infty} p^{v_p(n)-nr} = p^{\lim_{n\to\infty} n(\frac{v_p(n)}{n} - r)} = 0$$

When $|x-1|_p = 1$, notice that sequence $|1/n|_p$ diverges, so the $B_p(1,1)$ is the domain of convergence. Similarly,we will check exponentials and it will be a little complicated.

Lemma 1.2. Let $n \in \mathbb{N}$ and S_n denotes the sum of the digits of n in base p, then

$$v_p(n!) = \frac{n - S_n}{p-1}$$

Proof. Firstly we prove $v_p(p^n!) = \frac{p^n-1}{p-1}$ for any positive integer n by recurrence. when $n=1$, $v_p(p) = 1$; for intger $n \geq 2$ we assume that $v_p(p^{n-1}!) = \frac{p^{n-1}-1}{p-1}$, then $p^n! = p^{n-1}! \cdot \prod_{k=1}^{p-1} A_k$ with

$$A_k = (kp^{n-1}+1) \times (kp^{n-1}+2) \times \cdots \times (k+1)p^{n-1}$$

then clearly by valuation

$$\begin{aligned}
v_p(p^n!) &= v_p(p^{n-1}!) + \sum_{k=1}^{p-1} v_p(A_k) \\
&= v_p(p^{n-1}!) + pv_p(p^{n-1}!) + 1 \\
&= \frac{p^{n-1}-1}{p-1} + p \cdot \frac{p^{n-1}-1}{p-1} + 1 \\
&= \frac{p^n-1}{p-1}
\end{aligned}$$

Hence we finish our recurrence. And if we tkae $a \in 1, ..., p-1$, then the formula can be generalized

$$\begin{aligned}
v_p(ap^n!) &= \sum_{k=0}^{a-1} v_p[(k \cdot p^n + 1) \times (k \cdot p^n + 2) \times \cdots \times (k \cdot p^n + p^n)] \\
&= \sum_{k=0}^{a-1} v_p(p^n!) = a\frac{p^n-1}{p-1}
\end{aligned}$$

Finally we prove it by recurrence. Assuming that for any integer $n-1$ the identity holds, and $n = ap^r + m$ with $a \in \{1, ..., p-1\}$ and $m < p^r < n-1$, then

$$\begin{aligned}
v_p(n!) &= v_p(ap^r!) + \sum_{k=1}^{m} v_p(ap^r! + k) \\
&= v_p(ap^r!) + v_p(m) \\
&= a \cdot \frac{p^r-1}{p-1} + \frac{m-S_m}{p-1} \\
&= \frac{(ap^r+m)-(a+S_m)}{p-1} = \frac{n-S_n}{p-1}
\end{aligned}$$

□

By above lemma, the exponentials converges in given domain. For any $|x|_p < p^{-1/p-1}$, we estimate

$$v_p(x^n/n!) = nv_p(x) - v_p(n!) > \frac{S_n}{p-1} \xrightarrow{n\to\infty} +\infty$$

which means the definition is well-defined. When $|x| = p^{-1/p-1}$, we notice that for $n = p^k$, we have

$$|\frac{x^n}{n!}|_p = p^{-p^k/p-1} \cdot p^{p^k-1/p-1} = p^{1/p-1}$$

Hence, the series diverges and the domain of the convergence is $B_p(0, p^{-1/(p-1)})$.

Some properties about the power series will be needed here for the following proof.

Lemma 1.3 (analytic continuation)**.** Let $f(X)$ and $g(X)$ be two formally power series over a complete non-archimdean field K, and they all converge on the domain D If there exists a non-stationary convergent sequence $(a_n)_{n\in\mathbb{N}}$ of D such that $f(a_n) = g(a_n)$, then $f(X) = g(X)$.

Proof. The proof is similar to the classical proof. It is sufficient to consider the case that D is a disc containing zero and $(a_n)_{n\in\mathbb{N}}$ converges to zero. Then we have

$$h(X) = f(X) - g(X) = \sum_{k\geq 1} c_k X^k$$

with $h(a_n) = 0$ for any n. Assuming that $h(X)$ is not zero, then we take $r = \{\min n \in \mathbb{N} | c_n \neq 0\}$ the smallest non-zero index, then $h(X) = X^r h_1(X)$, here h_1 is defined by a power series with the non-zero constant cofficient, and it also converges on D. Then by continuity, we have

$$\lim_{n\to\infty} h_1(a_n) = h_1(\lim_{n\to\infty} a_n) = h_1(0) = c^r \neq 0$$

Hence for a large N, $h_1(a_N) \neq 0$. Moreover, non-stationary sequence $(a_n)_{n\in\mathbb{N}}$ implies $a_N \neq 0$, so $h(a_N) = a_N^r h_1(a_N) \neq 0$, absurd. □

Lemma 1.4 (composition)**.** Let $f(X) = \sum_{n\geq 0} a_n X^n$ and $g(X) = \sum_{m\geq 1} b_m X^m$ be two formal power series, let R be the radius convergence of f. If x is an element of a complete non-archimdean field K which satisfies
(1) $g(x)$ converges.
(2) $|b_m x^m| < R$ for any $m \geq 1$.
then then the formal power series $h(X) = f \circ g(X)$ converges at x with $h(x) = f(g(x))$.

Proof. The proof can be founded in [1, Chapter 4]. □

Logarithm and exponetial function keeps the same algebraic properties in p-adic context, here we just need several properties for applications to the solution of the equation.

Proposition 1.5. Let $a, b \in \mathbb{Q}_p$ with $|a|_p, |b|_p < p^{-1/(p-1)}$, then
(1) $\exp(a+b) = \exp(a)\exp(b)$
(2) $|\log(1+a)|_p = |a|_p$
(3) $\exp(\log(1+a)) = 1 + a$
(4) $|\exp(a)|_p = 1$

Proof. (1) $|a+b| \leq max\{|a|, |b|\} < p^{-1/p-1}$, so $\exp(a+b)$ exists. By a manipulation of power series

$$\begin{aligned}
\exp(a)\exp(b) &= (\sum_{m=0}^{\infty} \frac{a^m}{m!})(\sum_{n=0}^{\infty} \frac{b^n}{n!}) \\
&= \sum_{k\geq 0} \frac{1}{k!} \sum_{m+n=k} \frac{k!}{m!\cdot n!} a^m b^n \\
&= \sum_{k\geq 0} \frac{1}{k!}(a+b)^k = \exp(a+b)
\end{aligned}$$

we finish the proof.

(2) Notice that $v_p(n!) = v_p(n) + v_p((n-1)!)$ and $v_p(n!) \geq 0$, which implies $|n!|_p \leq |n|_p$. and we can estimate that

$$v_p(\frac{a^{n-1}}{n!}) = (n-1)v_p(a) - v_p(n!) > \frac{n-1}{p-1} - \frac{n-S_n}{p-1} = \frac{S_n - 1}{p-1} \geq 0$$

Hence we can conclude that

$$|\frac{a^n}{n}|_p \leq |\frac{a^n}{n!}|_p = |\frac{a^{n-1}}{n!}|_p \cdot |a|_p < |a|_p$$

for any $n \geq 2$. Therefore by the inequality of ultrametric, we can conlude the result.

(3) Firstly we will check the condition of the lemma 1.4. Let $f(X) = \exp(X)$ and $g(X) = \log(1+X)$, then $|a| < p^{-1/p-1} < 1$ impiles that $g(a)$ converges. Notice that each term $(-1)^{m+1}\frac{x^m}{m}$ in $g(a)$, we have estimated in the proof of (2), the absolute value is strictly less than the radius $R = p^{-1/p-1}$, hence we by composition we proved that $\exp(\log(1+a))$ converges. Let $x_k = \frac{p^k}{p^k+1} < 1$ be the sequence of $\mathbb{Q}$, caculate its p-adic absolute value $|x_k|_p = p^{-k} < R$ (to avoid the equality here, we convente $k \geq 2$), hence x_k is a non-stationary sequence converging to zero by p-adic absolute value. Finally by lemma 1.3, we can conclude that $\exp(\log(1+a)) = 1+a$ since formally power series $\exp(log(1+X))$ has the same cofficient with $1+X$.

(4) notice that

$$|\exp(a) - 1| = |\sum_{n\geq 1}\frac{a^n}{n!}| < |a| < 1$$

Hence immediately by ultrametric

$$|\exp(a)| = |\exp(a) - 1 + 1| = 1$$

□

Remark. The method of proof (3) is to aviod discussing too much formal power series. Generally, we can prove the permanence of algebraic form

$$\exp(\log(1+X)) = 1+X$$

without considering the convergence over a fromal power series ring $R[[X]]$ with R as a commutative $\mathbb{Q}$-algebra. The proof without analytic method is not easy, it needs some combinatorial trick, a method via formal derivative can be founed in [2].

Applying (1) to (2), then we can get the identity

$$(1+a)^n = \exp(n\log(1+a)), \quad \forall n \in \mathbb{N}$$

For extending the definition for interpolation, i.e. let $(1+a)^x$ makes sense for any $x \in \mathbb{Z}_p$, a traditional definition is based on the Newton's binoimal theorem (see [3, Chapter 5]), which needs some work and here we will not use binoimal, so we consider the extension of the function from $\mathbb{Z}$ and notice $\mathbb{Z}$ is a dense subset of p-adic integer.

Definition. Let $a \in \mathbb{Q}_p$ with $|a|_p < p^{-1/(p-1)}$, then the binoimal interpolation can be defined by a p-adic analytic function

$$f_a : \mathbb{Z}_p \to \mathbb{Q}_p, \quad x \mapsto \exp(x\log(1+a))$$

This construnction satisfies $f_a(n) = (1+a)^n$ for any integr n.

When fixing a, we can estimate for any $x \in \mathbb{Z}_p$

$$|x \log(1+a)|_p = |x|_p |a|_p < p^{1-/p-1}$$

that means f_a is well-defined, and by convention we denote $f_a(x) = (1+a)^x$.

Strassman's Theorem will be crucial part in the proof, we give a version which is easy to use here:

Theorem 1.6 (Strassman's Theorem)**.**
Let $f(X)$ be a non-zero power series in Tate algebra over $\mathbb{C}_p$ as following

$$f(X) = \sum_{n=0}^{\infty} a_n X^n = a_0 + a_1 X + a_2 X^2 + ...$$

Let $N = \max\{m \in \mathbb{N} : |a_m|_p \geq |a_n|_p \text{ for all } n \in \mathbb{N}\}$, then $f : \mathbb{Z}_p \to \mathbb{C}_p$ has at most N zeros.

Proof. It is rewritten from corollary 16.14. □

2 Pre

Theorem 2.1 (Dirichlet's unit theorem)**.**
Let K be a number field with r real embeddings and s pairs complex embeddings, and let $\mathcal{O}_K$ be its integer ring, then its unit group has isomorphic structure:

$$\mathcal{O}_K^{\times} \cong \mu(K) \times \mathbb{Z}^{r+s-1}$$

where $\mu(K)$ is the group of roots of unity in K, and it is a finite cyclic gourp.

Proof. A standard proof can be founded in [4], here we just consider the case of $r = 1$ and $s = 1$. □

Although unit theorem can show us the structure of the unit, but it is diffcult to give a perfect algorithm to how to exactly compute the fundamental unit, here it is a criterion about the fundamental unit.

Lemma 2.2. Let K be a cubic extension of $\mathbb{Q}$ with negative discriminant, and let u be the fundamental unit with $u > 1$, then

$$|\Delta_K| < 4u^3 + 24$$

Proof. □

A more strong estimation about the upper bound of the fundamental unit in a cubic field can be founded in Box's thesis [5, Theorem 1.82], that shows for a cubic field $K = \mathbb{Q}(\sqrt[3]{a})$ with $d = |\Delta_K|$, a element $u > 1$ can be choosen as a fundamental unit if and only if

$$u < \left(\frac{d - 32 + \sqrt{d^2 - 64d + 960}}{8}\right)^{2/3}$$

Now for solve the equation, we take $K = \mathbb{Q}(\sqrt[3]{2})$ be the extension field of the raitional number, and we denote $\theta = \sqrt[3]{2}$, then each element in its has the form

$$a + b\theta + c\theta^2 \quad \text{with } a, b, c \in \mathbb{Q}$$

Then we prove some properties of the field:

Proposition 2.3. in $\mathbb{Q}(\sqrt[3]{2})$ we have

- The unit group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.
- $N_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(a + b\theta + c\theta^2) = a^3 + 2b^3 + 4c^3 - 6abc$
- $u = -1 + \theta$ is a fundamental unit.

Proof. Firstly we suppose that $\sigma : \mathbb{Q}(\sqrt[3]{2}) \hookrightarrow \mathbb{C}$ is a field embedding, then surely $\sigma(1) = 1$. Let $f(X) = X^3 - 2$ be a polynoimal, and notice that $f(\theta) = 0$, then

$$0 = \sigma(f(\theta)) = f(\sigma(\theta))$$

Clearly $\sigma(\theta)$ must be the root of f in $\mathbb{C}$, so we can conclude the roots are $\theta, \theta w, \theta w^2$, where $w = e^{2i\pi/3}$. Hence the unique real embedding is $\sigma = id$ and there are two conjugate complex embedding, which means $r = 1$ and s. For the group of roots of unity, we notice that $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ as a subfield, and $x^n = 1$ only has possible solutions $\{\pm 1\}$ in $\mathbb{R}$ for any $n \in \mathbb{N}$, so $\mu_K = \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$.

For the norm we conisder the $\mathbb{Q}$-linear map l_x with $x = a + b\theta + c\theta^2$, then

$$l_x(1) = a + b\theta + c\theta^2, l_x(\theta) = 2c + a\theta + b\theta^2, l_x(\theta^2) = 2b + 2c\theta + a\theta^2$$

so we can conclude the norm by

$$det[l_x]_{\{1,\theta,\theta^2\}} = \begin{vmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{vmatrix} = a^3 + 2b^3 + 4c^3 - 6abc$$

and we take $u = -1 + \theta$, then $N(u) = -1 + 2 = 1$, so it is a unit.

Finally we prove that u is exactly a fundamental unit by contradiction. Assuming that $\eta > 1$ is a fundamental unit, and notice that $0 < u < 1$, so there exists a integer $k \geq 1$ such that $u = \eta^{-k}$. In this case we have negative discriminant $\Delta = -108$, then by lemma 2.2 we can estimate $\eta > \sqrt[3]{21}$, then

$$-1 + \sqrt[3]{2} = \eta^{-k} < (\sqrt[3]{21})^{-k}$$

It only holds for $k = 1$, which means u is the largest positive unit less than one, so u can be choosen as a fundamental unit.

□

Return to the original equation, now we can give a equivalent statement:

Proposition 2.4. The integral solution of the equation $x^3 - 2y^3 = 1$ is

$$\{(x, y) \in \mathbb{Z} | x - y\theta = u^k, \text{for some } k \in \mathbb{Z}\}$$

Proof. We notice that $x^3 - 2y^3 = 1$ can be rewritten as $N_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(x - y\theta) = 1$. And by the Dirichlet's unit theorem, its unit group is of the form $\pm u^k$. Notice that $N_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(-1) = -1$, so

$$N_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(-u^n) = N_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(-1)N^n_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(u) = -1, \quad \forall n \in \mathbb{Z}$$

Hence the integral solution is of the form u^k in $\mathbb{Q}(\sqrt[3]{2})$. $\square$

Notice that if $k = 0$ we can get the trival solution $(1, 0)$; if $k = 1$, we can find another solution $(-1, -1)$; By known result, we need to prove that for any other k, $x - y\theta = u^k$ has no solution, one possible method is to prove that for any other u^k, the cofficient with respect to base vector θ^2 is non-zero. For the case $k < 0$, we denote $v = u^{-1} = 1 + \theta + \theta^2$ and use multinomial formula then

$$(1 + \theta + \theta^2)^k = \sum_{i+j+k=n} \frac{n!}{i!j!k!}\theta^{j+2k}$$

with $\theta^3 = 2$ we can rewrite it to get a linear combination of $\{1, \theta, \theta^2\}$, clearly here the cofficient of θ^2 will not be zero so the choice of k will be limited to be less than zero. However, when $k \geq 2$ we will find that it is difficlut to analyse, for example

$$\begin{aligned}
u^2 &= 1 - 2\theta + \theta^2 \\
u^3 &= 1 + 3\theta - 3\theta^2 \\
u^4 &= -7 - 2\theta + 6\theta^2 \\
&\cdots
\end{aligned}$$

The problem here is diffcult to formulate u^k since there exists negative cofficient in $-1 + \theta$, it is not easy to deduce that whether the cofficient of θ^k will vanish in a certain k or not, the argumment here will be not clear, a pure algebraic method can be founded in [6, Chapter 24] by discussing binoimal units.

3 Interpolation Method

Now we will solve the equation by using p-adic interpolation method. Firstly, we notice that $\sqrt[3]{2} \notin \mathbb{Q}_3$ by observing that $n^3 = 2 \mod 9$ has no solution, so we still consider the finite extension by adjoining $\theta = \sqrt[3]{2}$ to construct, then we have the similar result.

Proposition 3.1. In $\mathbb{Q}_3(\theta)$ we have

- This field is a complete non-archimdean field with the absolute value:

$$|a + b\theta + c\theta^2| = \sqrt[3]{|a^3 + 2b^3 + 4c^3 - 6abc|_3}$$

In this field, observing that $|u - 1| = 1 > 3^{-1/2}$ prevents us from directly using interpolation, and notice that $|u^3 - 1| = 3^{-1} < 3^{-1/2}$, hence we will interpolate on u^3.

Theorem 3.2. The only solutions to the integral equation on

$$x^3 - 2y^3 = 1$$

are $(x, y) = (1, 0)$ and $(x, y) = (-1, -1)$.

Proof. Let $f : \mathbb{Z}_3 \to \mathbb{Q}_3(\theta)$ be the p-adic analytic function defined by $f(x) = \exp(x \log u^3)$, and $f|_{\mathbb{Z}}(n) = u^{3n}$, it is well-efined by **lemma...**. In particular

$$\log u^3 \equiv 3\theta - 3\theta^2 \mod 9\mathbb{Z}_3$$

hence

$$\exp(x \log u^3) = 1 + (3\theta - 3\theta^2)x + 9xh(x) \tag{1}$$

for some convegrent power series $h(X)$ with cofficient on $\mathbb{Z}_3(\theta)$. Since $\mathbb{Q}_3(\theta)$ is a vector space under basis $\{1, \theta, \theta^2\}$, then $f(x)$ can be denoted by three power series with respect to basis as following

$$f(x) = (\sum_{k\geq 0} a_k x^k) + (\sum_{k\geq 0} b_k x^k)\theta + (\sum_{k\geq 0} c_k x^k)\theta^2$$

and we will study the cofficient with respect to θ^2 to show that u^n can not be of the form $x - y\theta$ unless $n = 0, 1$. we take $f_r(x) = u^r f(x)$ with $r = 0, 1, 2$.

-When $r = 0$, the equation (1) can be rewritten as

$$f_0(x) = 1 + 3x \cdot \theta + (-3\theta^2 x + 9xh(x))$$

In detail, by writing $h(x)$ as the form of linear combination

$$h(x) = h_1(x) + h_2(x) \cdot \theta + h_3 \cdot \theta^2$$

with h_1, h_2, h_3 the convegrent power series defined on $\mathbb{Z}_3$, so again

$$f_0(x) = (1 + 9xh_1(x)) + (3x + 9xh_2(x)) \cdot \theta + (-3x + 9xh_3(x)) \cdot \theta^2$$

we apply Strassman's theorem to $-3x + 9xh_1(x) = 0$, and notice that the cofficient of x is $a_1 \equiv 3 \mod 9\mathbb{Z}_p$ and the other cofficients are $a_i \equiv 0 \mod 9\mathbb{Z}_p$, hence we can conclude that $N = 1$ and $x = 0$ is the unique solution.

-When $r = 1$, simliarly the equation can be rewritten as

$$f_1(x) = [-1-6x-9xh_3(x)+18xh_1(x)]+[1-3x-9xh_2(x)+9xh_3(x)]\cdot\theta+[6x+9xh_2(x)-9xh_1(x)]\cdot\theta^2$$

applying Strassman's theorem to $6x + 9x(h_1 + h_2)(x) = 0$, we can conclude that $N = 1$ and $x = 0$ is the unique solution.

- When $r = 2$, simliarly the cofficient with respect to θ^2 is

$$1 - 9x + 9(h_3(x) - 2h_2(x) + h_3(x))$$

notice that the constant cofficient $|1| = 1$, which strictly greater than any other cofficient, hence no solution for x such that the cofficient turns zero by Strassman's theorem.

In conclusion, we can conclude the solution of the integral equation $x^3 - 2y^3 = 1$ by proposition 2.4, when $n \equiv 0 \mod 3$, the only solution is $(1, 0)$ which corresponds to $r = 0, x = 1$; when $n \equiv 1 \mod 3$, the only solution is $(-1, -1)$ which corresponds to $r = 1, x = 0$; when $n \equiv 2 \mod 3$, no solution will exists. $\square$

References

[1] H. Cohen, S. Axler, and K. Ribet, *Number theory: Volume I: Tools and diophantine equations*. Springer, 2007.

[2] B. Sambale, "An invitation to formal power series," *Jahresbericht der Deutschen Mathematiker-Vereinigung*, vol. 125, no. 1, pp. 3–69, 2023.

[3] F. Q. Gouvêa and F. Q. Gouvêa, *p-adic Numbers*. Springer, 1997.

[4] J. Neukirch, *Algebraic number theory*. Springer Science & Business Media, 2013, vol. 322.

[5] J. Box, "An introduction to skolem's p-adic method for solving diophantine equations," *Bachelor thesis, Korteweg-de Vries Instituut voor Wiskunde Faculteit der Natuurwetenschappen, Wiskunde en Informatica, Universiteit van Amsterdam*, 2014.

[6] L. J. Mordell, *Diophantine Equations: Diophantine Equations*. Academic press, 1969, vol. 30.