
Integral solutions of $x^3 - 2y^3 = 1$

BMST 2025
p-adic numbers and applications
Copenhagen

Xi Feihu ^{*}
Noemi Gennuso [†]
May 30, 2025

^{*}Sorbonne University
[†]University of Milan

Contents

1 p-adic analytic functions

The main goal of this part is to completely solve the equation by p-adic methods, the concept of p-adic analytic functions, in particular the p-adic logarithm and exponential, together with Strassman's theorem, will be the key points.

By comparison to \mathbb{C} , it is easier to apply the properties of sequence in \mathbb{C}_p by proposition 2.8 (note), similarly we can study the convergence of power series in a non-archimedean field by considering the radius convergence

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

since an ultrametric is still a metric, it shows a good properties as following:

Proposition 1.1. Let $f(X) = \sum_{n \geq 0} a_n X^n$ be a power series with coefficients in \mathbb{C}_p , let the radius of convergence be $R > 0$, then

- (1) $f(x)$ converges if $|x| < R$, and diverges if $|x| > R$
- (2) When $|x| = R$, $f(x)$ converges if and only if $\lim_{n \rightarrow \infty} |a_n| R^n = 0$.
- (3) f is continuous on the convergence domain D .

Proof. Proof of (1) is same with the proof in \mathbb{C} . For any $|x| = R$, the series $\sum_{n \geq 0} a_n x^n$ converges if and only if sequence $(|a_n x^n|)_n = (|a_n R^n|)_n$ converges by proposition 2.8. To prove (3) we take two points $x, y \in D$ and let $M = \max(|x|, |y|)$, then

$$\begin{aligned} |f(x) - f(y)| &= \left| \sum_{n \geq 0} a_n (x^{n-1} + x^{n-2}y + \dots + y^{n-1})(x - y) \right| \\ &\leq |x - y| \max_{n \geq 0} |a_n M^{n-1}| \end{aligned}$$

Notice that $f(x)$ and $f(y)$ converge, then the sequence $(|a_n M^n|)_n$ converges to zero, so it will be bounded by a constant C , which implies $|f(x) - f(y)| \leq \frac{C}{M} |x - y|$, immediately f is continuous. \square

Definition 1.2. Let $B_p(a, r) = \{x \in \mathbb{C}_p \mid |x - a|_p < r\}$ be the open ball of radius r around a in \mathbb{C}_p .

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

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

-The p-adic exponential is the p-adic analytic function $\exp_p : B_p(0, p^{-1/(p-1)}) \rightarrow \mathbb{C}_p$ 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 functions, this section can be skipped. From now on, unless stated otherwise, $\log(\cdot)$ and $\exp(\cdot)$ will denote the p-adic analytic function as above.

It is easier to check the statement for the p-adic logarithm by observing $v_p(n) \leq \frac{\ln(n)}{\ln(p)}$ for any integer $n \geq 1$, because any integer $n \in [p^k, p^{k+1})$ has valuation at most k , then for any $|x - 1|_p = p^{-r} < 1$ we have

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

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 compute the radius of convergence of the p-adic exponential function.

Lemma 1.3. 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 an integer $n \geq 2$ 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

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

Hence we finish our recurrence. And if we take $a \in 1, \dots, p - 1$, then the formula can be generalized, as the following shows:

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

Finally we prove the lemma by recurrence. Assuming that for any integer $n - 1$ the identity

holds, and $n = ap^r + m$ with $a \in \{1, \dots, p-1\}$ 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 $|x|_p < p^{-1/p-1}$, there exists $\epsilon > 0$ such that $\epsilon = (p-1)v_p(x) - 1$, so we can estimate

$$v_p(x^n/n!) = \frac{n\epsilon - S_n}{p-1} \geq \frac{n\epsilon - p(\ln(n)/\ln p + 1)}{p-1} \xrightarrow{n \rightarrow \infty} +\infty$$

which means the definition is well-defined. The upper bound of S_n holds here because integer n has at most $\lfloor \frac{\ln(n)}{\ln p} \rfloor + 1$ p-digits. When $|x| = p^{-1/p-1}$, we notice that for $n = p^k$, we have

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

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 1.4 (analytic continuation). Let $f(X)$ and $g(X)$ be two formally power series over a complete non-archimedean field K , and they all converge on the define domain D containing zero. 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. We define

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

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 coefficient, and it also converges on D . Then by continuity, we have

$$\lim_{n \rightarrow \infty} h_1(a_n) = h_1(\lim_{n \rightarrow \infty} a_n) = h_1(0) = c_r \neq 0$$

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 1.5 (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-archimedean 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 Cohen's book [?, Chapter 4, proposition 4.2.7]. \square

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 1.6. Let $a, b \in \mathbb{C}_p$ with $|a|_p, |b|_p < p^{-1/(p-1)}$, then

$$(1) \exp(a+b) = \exp(a)\exp(b)$$

$$(2) |\log(1+a)|_p = |a|_p$$

$$(3) \exp(\log(1+a)) = 1+a$$

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

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

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

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

Hence we can conclude that

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

for any $n \geq 2$. Therefore by the inequality of ultrametric, we can conlude the result, and notice here will still hold if $|a|_p < 1$.

(3) Firstly we will check the condition of the lemma ???. 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 $R = p^{-1/p-1}$, so 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 ??, we can conclude that $\exp(\log(1+a)) = 1+a$ since formally power series $\exp(\log(1+X))$ has the same coefficient with $1+X$. \square

Remark. The method of proof (3) is to avoid 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 formal power series ring $R[[X]]$ with R as a commutative \mathbb{Q} -algebra. The proof without analytic methods is not easy, it needs some combinatorial trick, a method via formal derivative can be found in [?, Chapter 3].

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 binomial theorem (see [?, section 5.9]), which needs some work and here we will not use binomial, so we consider the extension by p-adic exponentials and logarithm, and notice that \mathbb{N} is dense in \mathbb{Z}_p , which makes the following extending be natural.

Definition 1.7. Let $a \in \mathbb{C}_p$ with $|a|_p < p^{-1/(p-1)}$, then the binomial interpolation can be defined by a p-adic analytic function

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

This construction satisfies $f_a(n) = (1 + a)^n$ for any integer 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 the crucial part in the proof, we give a version which is easy to use here:

Theorem 1.8 (Strassman's Theorem).

Let $f(X)$ be a non-zero element of the Tate algebra over \mathbb{C}_p , i.e. a formal power series with coefficient $(a_n)_{n \geq 0}$ converging to zero.

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

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

Proof. It is rewritten from corollary 16.14. □

2 Dirichlet's Unit theorem

In this section, we are going to give an equivalent statement for the original equation.

Definition 2.1. Let K be the algebraic number field (an finite extension of \mathbb{Q}), an integer ring of the K is the set of all algebraic integral numbers and we denote it by \mathcal{O}_K , i.e. for

any element a in it, there exists a polynomial in $\mathbb{Z}[X]$ having a as a root.

It is important to study the unit of the intger ring, usually the units of an integer ring will reflect the solutions of a integral equation, here is a condition to determine the unit.

Lemma 2.2. a is a unit of \mathcal{O}_K if and only if its algebraic norm is ± 1 .

Proof. Suppose that $a \in \mathcal{O}_K$ is an unit, then there exists $b \in \mathcal{O}_K$ such that

$$1 = N(ab) = N(a)N(b)$$

notice that the minimal polynoimal $\pi_{a,K} \in \mathbb{Z}[X]$, which implies $N(a) \in \mathbb{Z}$, the only two choices are $N(a) = \pm 1$. Conversely, if $N(a) = \pm 1$, then by its minimal polynoimal we have

$$c_n a^n + c_{n-1} a^{n-1} + \cdots + c_1 a - 1 = 0$$

for some $c_i \in \mathbb{Z}$, here n is the degree of $\pi_{a,K}$ and $c_n \neq 0$. Hence a is a unit with its inverse of the form $\sum_{k=0}^{n-1} c_{k+1} a^k$. \square

A better result about the unit is unit theorem which is firstly proved by Dirichlet, it shows that the units of the intger ring has an abelian free group structure under multiplication.

Theorem 2.3 (Dirichlet's unit theorem).

Let K be a algebraic number field with r real embeddings and $2s$ complex embeddings, and let \mathcal{O}_K be its integer ring, then its unit group has the following structure:

$$\mathcal{O}_K^\times \cong \mu_K \times \mathbb{Z}^{r+s-1}$$

where μ_K is the group of roots of unity in K , and it is a finite cyclic group.

Proof. A standard proof can be founded in Neukirch's book [?, section 1.7], here we will just consider the case of $r = 1$ and $s = 1$, i.e. an extension $[K : \mathbb{Q}] = 3$. Suppose that σ_r and σ_s are the real embedding and one of the complex embedding, then an unit $u \in \mathcal{O}_K^\times$ satisfying $|\sigma_r(u)| |\sigma_s(u)|^2 = N(u) = 1$ by lemma ???. Hence we consider a hyperplan of \mathbb{R}^2

$$H := \{(a, b) \in \mathbb{R}^2 | a + b = 0\}$$

then we will naturally get a exact sequence

$$1 \longrightarrow \mu_K \xrightarrow{e} \mathcal{O}_K^\times \xrightarrow{l} l(H) \longrightarrow 0$$

here e is a trival embedding by $e(a) = a$, l is the logarithm map (in the real sense) deifend by

$$u \mapsto (\ln |\sigma_r(u)|, 2 \ln |\sigma_s(u)|)$$

which is a homomorphism from the multiplicative group to the additive group, with $\ker l = \{u \in \mathcal{O}_K^\times | |\sigma_r(u)| = |\sigma_s(u)| = 1\} = \mu_K$, it holds generally by Kronecker's theorme. Immediately we have the isomorphic

$$\mathcal{O}_K^\times / \mu_K \cong l(H)$$

Then we need to prove that $l(H)$ is a nontrivial discrete subgroup of H , i.e. a complete lattice of H , which ensures $l(H) \cong \mathbb{Z}$. We consider the embedding $j : \mathcal{O}_K^\times \rightarrow \mathbb{R} \times \mathbb{C}$ by

$$u \mapsto (\sigma_r(u), \sigma_s(u))$$

Notice that integr ring \mathcal{O}_K^\times is a free \mathbb{Z} -module, then there exists integral base $\{w_1, w_2, w_3\}$ such that for any $u \in \mathcal{O}_K^\times$, there exists $x, y, z \in \mathbb{Z}$ such that

$$u = xw_1 + yw_2 + zw_3$$

hence it invites a integral base for $j(\mathcal{O}_K^\times)$ by

$$\begin{aligned} j(u) &= x \begin{pmatrix} w_1 \\ \sigma_s(w_1) \end{pmatrix} + y \begin{pmatrix} w_2 \\ \sigma_s(w_2) \end{pmatrix} + z \begin{pmatrix} w_3 \\ \sigma_s(w_3) \end{pmatrix} \\ &= xe_1 + ye_2 + ze_3 \end{aligned}$$

hence under the base $B = \{e_1, e_2, e_3\}$ we can see $j(\mathcal{O}_K^\times)$ as the integer lattice of $\mathbb{R} \times \mathbb{C}$. Now for any $(\ln |\sigma_r(u)|, \ln |\sigma_s(u)|) \in l(H)$, we take a bounded open voisinage V of the point, then $\overline{j \circ l^{-1}(V)}$ implies a compact set of $\mathbb{R} \times \mathbb{C}$, so it must contain finite integer lattices under the base B , therefore V covers finite points, so $l(H)$ is discrete.

Finally $l(H)$ must be nontrivial, it is not clear and even difficult, it is essential to prove the existence of the nontrivial unit of \mathcal{O}_K^\times ... \square

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

Lemma 2.4 (Artin). Let K be a cubic extension of \mathbb{Q} with negative discriminant Δ_K , and let u be the fundamental unit with $u > 1$, then

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

Proof. Let u be the fundamental unit ($u > 1$), then $x = u^2$ is the unit, so the norm $\sigma_r(x)\sigma_s(x)\overline{\sigma_s(x)}=1$, which implies the complex conjugates $\sigma_s(x) = u^{-1}e^{i\theta}$ with $0 \leq \theta \leq \pi$, then the discriminant under the base $\{1, x, x^2\}$

$$\begin{aligned} \Delta(1, x, x^2) &= \begin{vmatrix} 1 & x & x^2 \\ 1 & u^{-1}e^{i\theta} & u^{-2}e^{2i\theta} \\ 1 & u^{-1}e^{-i\theta} & u^{-2}e^{-2i\theta} \end{vmatrix} \\ &= -4(u^3 + u^{-3} - 2\cos\theta)^2 \sin^2\theta \end{aligned}$$

Let $y = \frac{u^3 + u^{-3}}{2}$ and $\phi(\theta) = (y - \cos(\theta)) \sin\theta > 0$, and then $\Delta(1, x, x^2) = -16\phi^2(\theta)$, so we study the maximum of ϕ on $[0, \pi]$. $\phi'(\theta) = -2\cos^2\theta + y\cos\theta + 1$, $\phi'(0) = y - 1 > 0$ and $\phi(\pi) = -y - 1 < 0$, then by continuity there exists a zero $a \in (0, \pi)$ such that $\phi'(0)$. By

Vieta's formula, a is the unique zero so ϕ attains maximum at $\theta = a$. Hence

$$\begin{aligned}
|\Delta(1, x, x^2)| &\leq 16\phi^2(a) \\
&= 16(y^2 + 1 - \cos^2(a) - \cos^4(a)) \\
&= 4u^6 + 24 + 4(u^{-6} - 4\cos^2(a) - 4\cos^4(a)) \\
&< 4u^3 + 24
\end{aligned}$$

Let $A \in \text{GL}_3(\mathbb{Q})$ be the matrix from the integral basis of K to the basis $\{1, x, x^2\}$, then $\det A$ must be an integer, so

$$|\Delta_K| = |\det A|^2 |\Delta(1, x, x^2)| \leq |\Delta(1, x, x^2)| < 4u^3 + 24$$

□

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

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

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

Now for solve the equation, we take $K = \mathbb{Q}(\sqrt[3]{2})$ be the extension field of the rational numbers and we denote $\theta = \sqrt[3]{2}$, then each element in K 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 3.1. 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.
- $\mathcal{O}_K = \mathbb{Z}[\theta]$

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 polynomial, 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 $s = 1$. 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 consider 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 $u = \eta^{-k}$. By the general formual for cubic equation $ax^3 + bx^2 + cx + d$ is

$$\Delta = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd$$

In this case we have negative discriminant $\Delta = -108$, then by lemma ?? 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 3.2. The integral solutions of the equation $x^3 - 2y^3 = 1$ are

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

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

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

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

Notice that if $k = 0$ we get the trival solution $(1, 0)$; if $k = 1$, we find another solution $(-1, -1)$; By known result, they are exact the only two solutions, so we need to prove that for any other k , $x - y\theta = u^k$ has no solution, we will prove that for any other k , the coefficient of u^k with respect to base vector θ^2 is non-zero. For the case $k < 0$, we notice that $u^{-1} = 1 + \theta + \theta^2$ and use multinomial formula

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

with $\theta^3 = 2$ we can rewrite it to get a linear combination of $\{1, \theta, \theta^2\}$, clearly here the coefficient of θ^2 will not be zero so the choice of k will be limited to be more than zero.

However, when $k \geq 2$ we will find that it is difficult to analyse, for example

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

The problem here is that it is difficult to formulate u^k since there exists negative coefficient in $-1 + \theta$, it is not easy to deduce that whether the coefficient of θ^k will vanish in a certain k or not, the argument here will be not clear, so we will turn towards to the p-adic method.

Firstly, we notice that $\sqrt[3]{2} \notin \mathbb{Q}_3$ since by inspection $x^3 = 2 \pmod{9}$ has no solution, so we still consider the finite extension by adjoining $\theta = \sqrt[3]{2}$ to construct, then we get a new field $\mathbb{Q}_3(\theta) \cong \mathbb{Q}_3[X]/(X^3 - 2)$ containing \mathbb{Q}_3 as a subfield, with any element of the form

$$a + b\theta + c\theta^2 \quad \text{with } a, b, c \in \mathbb{Q}_3$$

The norm can be similarly calculated like in $\mathbb{Q}(\sqrt[3]{2})$ (proposition ??), so we can uniquely extend the absolute value of \mathbb{Q}_3 as following:

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

Notice that $\mathbb{Q}_3(\theta)$ is a subfield of \mathbb{C}_3 , so we will consider the binomial interpolation in this field, observing that $|u - 1| = 1 > 3^{-1/2}$ prevents us from directly using interpolation, and notice that $|u^3 - 1| = 3^{-1} < 3^{-1/2}$, so we will interpolate on u^3 .

Lemma 3.3. There exists a convergent power series $h(X)$ with coefficient in $\mathbb{Z}_3[\theta]$ such that

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

for any $x \in \mathbb{Z}_3$.

Proof. By definition ??, interpolation $(u^3)^x = \exp(x \log(u^3))$ is well-defined here, so we have

$$(u^3)^x = 1 + \log(u^3)x + 9x^2 \sum_{k \geq 0} \frac{(\log u^3)^{k+2}}{9(k+2)!} x^k$$

we can estimate the valuation by proposition ?? property (2)

$$\begin{aligned} v\left(\frac{(\log u^3)^{k+2}}{9(k+2)!}\right) &= (k+2) - 2 - \frac{(k+2) - S_{k+2}}{2} \\ &= \frac{k + S_{k+2} - 2}{2} \geq 0 \end{aligned}$$

so there exists a convergent power series $h'(X)$ with coefficient in $\mathbb{Z}_3[\theta]$ such that

$$(u^3)^x = 1 + \log(u^3)x + 9x^2 h'(x) \tag{2}$$

And we rewrite $\log(u^3)$ by the definition of p-adic logarithm

$$\log(u^3) = u^3 - 1 + 9 \sum_{k \geq 2} (-1)^{k+1} \frac{(u^3 - 1)^k}{9k}$$

similarly we estimate the valuation for any $k \geq 2$

$$\begin{aligned} v((-1)^{k+1} \frac{(u^3 - 1)^k}{9k}) &= k - 2 - v_3(k) \\ &\geq k - 2 - \frac{\ln(k)}{\ln(3)} \geq 0 \end{aligned}$$

so there exists a element $\alpha \in \mathbb{Z}_3[\theta]$ such that

$$\log(u^3) = u^3 - 1 + 9\alpha \quad (3)$$

Plugging (??) to (??), then we get

$$(u^3)^x = 1 + (u^3 - 1)x + 9x[\alpha + xh'(x)]$$

here $h(X) = \alpha + Xh'(X)$ is the power series we expect. \square

Theorem 3.4. The only solutions to the integral equation on

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

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

Proof. By the proposition ??, it is sufficient to study the coefficient with respect to θ^2 to show that the integer power of the fundamental unit u^n can not be of the form $x - y\theta$ unless $n = 0, 1$. We interpolate u^n here by defining the functions $f_r(x) = u^r \cdot (u^3)^x$ with $r = 0, 1, 2$, it is reasonable here since

$$f_0(\mathbb{Z}) \cup f_1(\mathbb{Z}) \cup f_2(\mathbb{Z}) = u^{\mathbb{Z}}$$

and for any $r = 0, 1, 2$ we can write the f_r as the form of linear combination as following

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

-When $r = 0$, by equation (??) we have

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

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 convergent 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 $-3x + 9xh_3(x) = 0$, and notice that the coefficient of x has valuation 1 while the other have that at least 2, hence we can conclude that $N = 1$ and $x = 0$ is the unique solution, which corresponds to $n = 0$.

-When $r = 1$, similiarly 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, whci corresponds to $n = 1$

- When $r = 2$, similiarly the coefficient with respect to θ^2 is

$$1 - 9x + 9x \cdot (h_1(x) - 2h_2(x) + h_3(x))$$

notice that the constant coefficient $|1| = 1$, which strictly greater than any other coefficient, hence this expression does not vanish on \mathbb{Z}_3 by Strassman's theorem.

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

4 Skolem's equation $x^3 + dy^3 = 1$

Similar technic we can apply to completely solve the diophantine equation of the form

$$x^3 + dy^3 = 1 \tag{4}$$

which we call it Skolem's equation. Skolem is influenced by the work of Thue in the beginning of the 19th. Thue improved the Liouville's approximation theorem to give a lower approxiamtion exponent $\tau(d) = \frac{d}{2} + 1 + \epsilon$, which shows that the number of the integral solution of equation (??) will be finite (see [?, Chapter 11]). However, this method of diophantine approxiamtion is not effective, in 1937 Skolem made use of p-adic interpolate method to give a same answer that the solution of the equation (More generally, he states for a irreducible homogeneous polynoimal) will be finite, even more precisely, at most two solution.

Theorem 4.1 (Skolem). There exists at most one non-trival solution for the Integral equation

$$x^3 + dy^3 = 1$$

where $d \in \mathbb{Z}$.

Proof. If d is a perfect cubic, then the solution will be related to the equation $x^3 + y^3 = 1$, which only has two solution $(1, 0)$ and $(0, 1)$, so there exists at most one non-trival solution. If d is not perfect cubic, we consider the field extension $K = \mathbb{Q}(\theta)$ with $\theta = \sqrt[3]{d}$. By unit theorem, we denote u is the positive unit, and then if (x, y) is a Integral solution, $x + y\theta$ will be of the form u^k form some integer k .

Suppose that we have two non-trival solution (x_1, y_1) and (x_2, y_2) , here $x_i y_i \neq 0$ and then there exists non-zero integer p_1 and p_2 such that $x_1 + y_1\theta = u^{p_1}$ and $x_2 + y_2\theta = u^{p_2}$. Let

$p_1/p_2 = n_1/n_2$ with $\gcd(n_1, n_2) = 1$, then n_1/n_2 or n_2/n_1 can be seen as a p-adic integer. It is sufficient to assume that $N = n_2/n_1 \in \mathbb{Z}_3$, then

$$x_2 + y_2\theta = u^{p_2} = u^{Np_1} = (x_1 + y_1\theta)^N$$

Notice that

$$(x_1 + y_1\theta)^3 = 1 + 3xy(x\theta + y\theta^2)$$

we put $N = 3M + r$ with $M \in \mathbb{Z}_3$ and $r = 0, 1, 2$, then we have

$$x_2 + y_2\theta = [1 + 3xy(x\theta + y\theta^2)]^M (x + y\theta)^r$$

with $x = x_1$ and $y = y_1$. We consider it in the completion of the finite extension $\mathbb{Q}(\theta)$ by

$$L \cong \mathbb{Q}_3 \otimes_{\mathbb{Q}} \mathbb{Q}(\theta)$$

then there exists a convergent series $B \in \mathbb{Z}_3[\theta]$ such that

$$x_2 + y_2\theta = (1 + 3Mxy(x\theta + y\theta^2) + 9Mx^2y^2B)(x + y\theta)^r \quad (5)$$

write $B = B_0 + B_1\theta + B_2\theta^2$ with $B_1, B_2, B_3 \in \mathbb{Z}_3$, and then rewrite equation (??) as the linear combination of $\{1, \theta, \theta^2\}$, the coefficient with respect to θ^2 must be zero, so we have

$$\begin{cases} 3Mxy^2(1 + 3xB_2) = 0 & \text{for } r = 0, \\ 3Mx^2y^2(2 + 3(yB_1 + xB_2)) = 0 & \text{for } r = 1, \\ y^2(1 + 9Mx^2(x + B_2x^2 + 2B_1xy + B_0y^2)) = 0 & \text{for } r = 2. \end{cases}$$

Notice that notice that $N \neq 0, 1$, which means for $r = 0$ or $r = 1$ we must have $M \neq 0$, then we can divide $3Mxy^2, 3Mx^2y^2, y^2$ respectively, and then we can get contradiction by modulo 3 ($1 \equiv 0, 2 \equiv 0, 1 \equiv 0$ respectively).

□

This result can be further refined, and we can provide a necessary and sufficient condition for the existence of nontrivial solutions to the Skolem equation. Review the proof of theorem ??, the non-trivial solution is just the fundamental unit. Notice that in our case ($r = s = 1$), we have 4 choices for fundamental unit: $u, -u, 1/u, -1/u$, here we call the the fundamental unit $0 < u < 1$ as **direct unit**, and its inverse u^{-1} as **inverse unit**, from Delone's proof [?, Chapter 11] it shows that the existence of the solution depends on the direct unit.

Theorem 4.2 (Delone). If d is not a perfect cubic, then the integral equation $x^3 + dy^3 = 1$ has unique the non-trivial solution if and only if the direct unit is of the form $a + b\sqrt[3]{d}$, which corresponds to the solution (a, b) .

The proof of Delone is out of the p-adic method and pure algebraic. We define that a binomial unit is a unit with the form $a + b\sqrt[3]{d}$, here is the outline of the proof: (1) the inverse unit must be of the form $A + B\sqrt[3]{d} + C\sqrt[3]{d^2}$ with $A, B, C > 0$, which implies any power of inverse unit is not a binomial unit. (2) Show that any power (>1) of the direct unit can not be binomial unit, the technic to explicitly denote the coefficient with respect to $\sqrt[3]{d^2}$ by roots of unity filter $\sum_{k=0}^2 \zeta^k f(\zeta^k x)$. Hence the unique possible is that direct unit

is a binomial unit.

The p-adic method here is analytic, it strongly depends on the information about d , i.e. the unit group of $\mathbb{Q}(\sqrt[3]{d})$. Therefore, the limitation is obvious because the calculation of the fundamental unit is generally difficult.

5 Other method(not formally)

Now we consider the other possible method corresponding to the integral solution. We founded that if 2 is a perfect cubic number, then the solution will be very easy, but unfortunately we can not do like that. However, p-adic number system gives us a method to extend the field, surely we consider a prime p (for example, $p=5$?) such that $\sqrt[3]{2} \in \mathbb{Z}_p$, then we just need to study the the p-adic integral equation

$$x^3 + y^3 = 1$$

with $x, y \in \mathbb{Z}_p$.

For example we take the set S as the solution of the equation, then for any $x, y \in S$, there exists sequences $(x_n)_{n \in \mathbb{N}}$ and $(y_n)_{n \in \mathbb{N}}$ with $x_n, y_n \in \mathbb{Z}_p/p^n\mathbb{Z}_p$ such that

$$\begin{cases} x_n \equiv x_{n+1} \pmod{p^n} \\ y_n \equiv y_{n+1} \pmod{p^n} \\ x_n^3 + y_n^3 \equiv 1 \pmod{p^n} \end{cases}$$

Fix n , and we take (x_n, y_n) to form a sequence S_n , the the space of the solution can be derived by the inverse limit as following

$$S = \varprojlim_n S_n$$

By computing the case $p = 3$, we take $A_n = \{(x_n, y_n) | x_n^3 + y_n^3 \equiv 1 \pmod{3^n}\}$, some example as following

$$\begin{aligned} A_1 &= \{ (1, 0), (0, 1), (2, 2) \} \\ A_2 &= \{ (0, 1), (3, 4), (6, 7), (1, 0), (4, 3), (7, 6) \} \\ A_3 &= \{ (0, 1), (9, 10), (18, 19), \\ &\quad (3, 4), (12, 13), (21, 22), \\ &\quad (6, 7), (15, 16), (24, 25), \\ &\quad (1, 0), (10, 9), (19, 18), \\ &\quad (4, 3), (13, 12), (22, 21), \\ &\quad (7, 6), (16, 15), (25, 24) \} \end{aligned}$$

With that we can do selecting: notice that the possible original solution for lifting are just three possible, so there will exist three path to consider, so we can do lifting as following -starting from $(1, 0)$:

$$\begin{array}{cccc} (1, 0) & (1, 0) & (10, 9) & (19, 18) \\ (1, 0) \rightarrow (4, 3) \rightarrow (4, 3) & (13, 12) & (22, 21) & \\ (7, 6) & (7, 6) & (16, 15) & (25, 24) \end{array}$$

starting from $(0, 1)$ is symmetrical as above, but pay attention that there exists no lifting when starting from $(2, 2)$. Then we should consider all possible lifting, that is motivated

from Hensel's lemma, for example $(1, 0)$ is exactly a solution for the equation $x^3 + y^3 = 1$, and we can find the a lifting

$$(1, 0) \rightarrow (1, 0) \rightarrow (1, 0) \rightarrow \dots$$

The choice of the prime $p = 3$ is really terrible here, since for $f(x, y) = x^3 + y^3 - 1$, the partial derivative $f_x \equiv f_y \equiv 0 \pmod{3}$, that means the algebraic curve we consider is not smooth? so we may consider the other prime.

Question: As what u show, and i have verified that there are usually infinite solutions for a p-adic integral equation, it can be done by Hensel's lemma (fix some certain y and then use Hensel's lemma for one-variable polynomial to do lifting). However, in this case each solution $(x, y) \in \mathbb{Z}_3^2$ will satisfying a properties, it must be lifted from $(1, 0)$ or $(0, 1)$, that means there will be two paths (each paths maybe contain infinite 3-adic solution), so the solution can be described as following

$$\text{solution lifted from } (1, 0) + \text{solution lifted from } (0, 1) = \text{all 3-adic solutions}$$

I think it is not easy to precise each component of solutions to get the exact integer solution instead p-adic integer solutions.

We consider above process from the view of scheme (i am not very familiar to that). we consider a algebraic variety by letting $f = (X^3 + Y^3 - 1)$

$$X = \text{Spec}(\mathbb{Z}_p[X, Y]/f)$$

so all solution in \mathbb{Z}_p can be denoted by $X(\mathbb{Z}_p)$, consider the inverse limit

$$X(\mathbb{Z}_p) = \varprojlim_n X_n(\mathbb{Z}/p^n\mathbb{Z})$$

where $X_n = \text{Spec}((\mathbb{Z}/p^n\mathbb{Z})(X, Y)/f)$ the affine scheme defined in a finite ring. In particular, when $n = 1$, X_n defines a algebraic curve in \mathbb{F}_p . So our original question is to find $X(\mathbb{Z}_p) \cap \mathbb{Z}^2$.

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.
- [7] J. H. Silverman, *The arithmetic of elliptic curves*. Springer, 2009, vol. 106.