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

BMST 2025
p-adic numbers and applications
Copenhagen

Xi Feihu ^{*}
Noemi Gennuso [†]
April 17, 2025

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

Contents

1	Pre	3
2	p-adic analytic funnction	5
3	Interpolation Method	7

1 Pre

Theorem 1.1 (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 group.

Proof. A standard proof can be founded in [1], 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 difficult to give a perfect algorithm to how to exactly compute the fundamental unit, here it is a criterion about the fundamental unit.

Lemma 1.2. 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 [2, 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 chosen 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 rational number, and we denote $\theta = \sqrt[3]{2}$, then each element in it 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 1.3. 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 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 embeddings, 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 $u = \eta^{-k}$. In this case we have negative discriminant $\Delta = -108$, then by lemma 1.2 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 chosen as a fundamental unit. □

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

Proposition 1.4. 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

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

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

Notice that if $k = 0$ we can get the trivial 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 coefficient 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 coefficient 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 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 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, a pure algebraic method can be founded in [3, Chapter 24] by discussing binomial units.

2 p-adic analytic function

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. Firstly we formally define the two functions.

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 $\log_p : B_p(1, 1) \rightarrow \mathbb{Q}_p$ 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 $\exp_p : B_p(0, p^{-1/(p-1)}) \rightarrow \mathbb{Q}_p$ 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

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

We will check exponentials and it will be a little complicated.

Lemma 2.1. 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 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

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

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 take $a \in 1, \dots, p-1$, then the formula can be generalized

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

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

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

which means the definition is well-defined. In fact the domain of the convergence we give in the definition is the largest, we do not discuss the detail here and complete argument can be founded in [4, Chapter 5]

Logarithm and exponential 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 2.2. 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) $\exp(\log(1+a)) = 1+a$

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)

□

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, which needs some work and here we will not use binomial, so we consider the extension of the function from \mathbb{Z} and notice \mathbb{Z} is a dense subset of p-adic integer.

Proposition 2.3. Let S be a dense subset of \mathbb{Z}_p , if $f : S \rightarrow \mathbb{Q}_p$ is a bounded and uniformly continuous function, then there exists a unique extension $\hat{f} : \mathbb{Z}_p \rightarrow \mathbb{Q}_p$.

Proof.

□

Definition. Let $a \in \mathbb{Q}_p$ with $|a|_p < p^{-1/(p-1)}$, then the binomial interpolation can be defined by a p-adic analytic function $f_a : \mathbb{Z}_p \rightarrow \mathbb{Q}_p$: This construction satisfies $f_a(n) = (1+a)^n$ for any integer n .

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

Theorem 2.4 (Strassman's Theorem).

Let $f(X)$ be a non-zero power series in Tate algebra over \mathbb{C}_p as following

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

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.

□

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 $n^3 = 2 \pmod{9}$ 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

- The absolute value of the field is

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

- $v = -1 + \theta$ is a fundamental unit and $v^3 = 1 + 3\theta - 3\theta^2$.

-

References

- [1] J. Neukirch, *Algebraic number theory*. Springer Science & Business Media, 2013, vol. 322.
- [2] 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.
- [3] L. J. Mordell, *Diophantine Equations: Diophantine Equations*. Academic press, 1969, vol. 30.
- [4] F. Q. Gouvêa and F. Q. Gouvêa, *p-adic Numbers*. Springer, 1997.