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

BMST 2025
p-adic numbers and applications
Copenhagen

Xi Feihu [*]
Noemi Gennuso [†]

April 14, 2025

[*]Sorbonne University
[†]University of Milan

Contents

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 gourp.

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 1.2. in $\mathbb{Q}(\sqrt[3]{2})$ we have
- $r = 1$ and $s = 1$.
- $N_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(a + b\theta + c\theta^2) = a^3 + 2b^3 + 4c^3 - 6abc$
- $u = 1 + \theta + \theta^2$ is a unit and its inverse is $v = -1 + \theta$.
- The group of the unity is $\mu = \{\pm 1\}$

Proof. Firstly we suppose that $\sigma : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$ 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.

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 $u = 1 + \theta + \theta^2$, then $N(u) = 1 + 2 + 4 - 6 = 1$, so it is a unit.

For the group of the 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 we can conclude our result. ☐

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

Proposition 1.3. 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 $\{\pm 1\} \times < u >$. 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 $\mathbb{Q}(\sqrt[3]{2})$. ☐

Notice that if $k = 0$ we can get the trival solution $(1, 0)$; if $k = -1$, we can find that $u^{-1} = -1 + \theta$ and then get another solution $(-1, -1)$; So 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 $k > 0$, by multinomial formula we can formulate

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

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 $k \leq -2$ we will find that it is difficlut to analyse, for example

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

The problem here is diffcult to formulate u^{-k} since there exists negative cofficient in $v = -1 + \theta$, 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.