

JOURNAL

de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux


Hyuga YOSHIZAKI

Generalized Pell's equations and Weber's class number problem

Tome 35, n° 2 (2023), p. 373-391.

<https://doi.org/10.5802/jtnb.1249>

© Les auteurs, 2023.

 Cet article est mis à disposition selon les termes de la licence
CREATIVE COMMONS ATTRIBUTION – PAS DE MODIFICATION 4.0 FRANCE.
<http://creativecommons.org/licenses/by-nd/4.0/fr/>



*Le Journal de Théorie des Nombres de Bordeaux est membre du
Centre Mersenne pour l'édition scientifique ouverte*

<http://www.centre-mersenne.org/>

e-ISSN : 2118-8572

Generalized Pell's equations and Weber's class number problem

par HYUGA YOSHIKAZI

RÉSUMÉ. Nous étudions une généralisation de l'équation de Pell dont les coefficients sont certains entiers algébriques. Soient $X_0 = 0$ et $X_n = \sqrt{2 + X_{n-1}}$ pour chaque $n \in \mathbb{Z}_{\geq 1}$. Nous étudions les solutions de l'équation $x^2 - X_n^2 y^2 = 1$ dans $\mathbb{Z}[X_{n-1}]$. En imitant la solution de l'équation de Pell classique, nous introduisons de nouveaux développements en fraction continue de X_n sur $\mathbb{Z}[X_{n-1}]$ et obtenons une solution explicite de l'équation de Pell généralisée. De plus, nous montrons que notre solution explicite génère toutes les solutions si et seulement si la réponse au problème du nombre de classes de Weber est affirmative. Nous obtenons également une congruence pour le rapport entre les nombres de classes dans la \mathbb{Z}_2 -extension sur les rationnels et montrons la convergence de la suite des nombres de classes dans \mathbb{Z}_2 .

ABSTRACT. We study a generalization of Pell's equation, whose coefficients are certain algebraic integers. Let $X_0 = 0$ and $X_n = \sqrt{2 + X_{n-1}}$ for each $n \in \mathbb{Z}_{\geq 1}$. We study the $\mathbb{Z}[X_{n-1}]$ -solutions of the equation $x^2 - X_n^2 y^2 = 1$. By imitating the solution to the classical Pell's equation, we introduce new continued fraction expansions for X_n over $\mathbb{Z}[X_{n-1}]$ and obtain an explicit solution of the generalized Pell's equation. In addition, we show that our explicit solution generates all the solutions if and only if the answer to Weber's class number problem is affirmative. We also obtain a congruence relation for the ratios of the class numbers of the \mathbb{Z}_2 -extension over the rationals and show the convergence of the class numbers in \mathbb{Z}_2 .

1. Introduction

For a non-square positive integer m , it is well-known that the solutions in integers of Pell's equation

$$x^2 - my^2 = 1$$

are given by the regular continued fraction expansion of \sqrt{m} (cf. Section 2). The aim of this paper is to study the $\mathbb{Z}[X_{n-1}]$ -solutions of a generalization of Pell's equation:

$$(1.1) \quad x^2 - X_n^2 y^2 = 1,$$

Manuscrit reçu le 10 juillet 2021, révisé le 11 janvier 2023, accepté le 31 janvier 2023.

2020 *Mathematics Subject Classification*. 11J70, 11D57, 11R29, 11R18, 11R27.

Mots-clés. Pell's equation, Continued fraction, Weber's class number problem.

The author has been partially supported by JSPS KAKENHI Grant Number JP22J10004.

where $X_n = 2 \cos(\pi/2^{n+1})$ satisfies $X_0 = 0$ and $X_{n+1} = \sqrt{2 + X_n}$. For $n = 1$, this equation is a classical Pell's equation $x^2 - 2y^2 = 1$.

Now we explain our main results. First, we give a new continued fraction expansion of X_n (Theorem 3.4) as follows:

$$X_n = [1, \overline{2(1 + X_{n-1})^{-1}, 2}].$$

We obtain an explicit solution of (1.1) as

$$(x, y) = (1 + 2(1 + X_{n-1})^{-1}, 2(1 + X_{n-1})^{-1})$$

by imitating the classical method (cf. Section 2). We conjecture that our explicit solution “generates” all the solutions of (1.1) (Conjecture 3.6).

Secondly, we investigate the relation between our conjecture and Weber's class number problem, which asks the class number of $\mathbb{B}_n := \mathbb{Q}(X_n)$. The class numbers have been determined to be 1 for the cases $0 \leq n \leq 6$ (see [7, Theorem 2.1] for the case $n = 6$) and there are infinitely many prime numbers that do not divide the class numbers for all n (cf. [3, 4, 8]). Therefore, it is conjectured that the class number of \mathbb{B}_n is 1 for all n (Weber's conjecture). We show that our conjecture is equivalent to Weber's conjecture (Theorem 4.1). In addition, we show a certain minimality property of the explicit solutions (Theorem 5.1).

Thirdly, we obtain a congruence relation for the class numbers

$$\frac{h_n}{h_{n-1}} \equiv 1 \pmod{2^n}$$

for all $n \geq 1$ by considering the Galois action on the group generated by our explicit solution (Theorem 5.3). By this result, we have that the sequence of the class numbers $\{h_n\}_{n \geq 0}$ converges in \mathbb{Z}_2 . This is a rediscovery of Kisilevsky's result [5, Corollary 2] in a specific case from a different approach (see Remark 5.4 for details).

Finally, we state a conjecture (Conjecture 6.2) that concerns the “sizes” of our explicit solution, and give observations on the conjecture. By assuming the conjecture, we present a contribution to Weber's conjecture and Conjecture 3.6.

2. Classical method

In this section, we briefly recall the classical method for Pell's equation (see [10, Chapter 7, §7.8] for detail). For a non-square positive integer m , we consider Pell's equation

$$(2.1) \quad x^2 - my^2 = 1.$$

By mapping (x, y) to $x + \sqrt{m}y$, the solutions of Pell's equation are embedded in $\mathbb{Z}[\sqrt{m}]$, and we set P_m its image. Since P_m forms a subgroup of the multiplicative group $\mathbb{Z}[\sqrt{m}]^*$ and has a torsion element -1 , P_m is

isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$ by Dirichlet's unit theorem. A *fundamental solution* of Pell's equation is defined as a corresponding solution to a generator of $P_m/(\mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}$. It is classically known that a fundamental solution is given by the regular continued fraction of \sqrt{m} .

Let

$$[a_0, a_1, a_2, \dots] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ddots}}$$

be a continued fraction ($a_i \in \mathbb{Z}$). Let $p_{-1} = 1, p_0 = a_0$ and $q_{-1} = 0, q_0 = 1$. For a positive integer k , we define p_k and q_k as follows:

$$p_k = a_k p_{k-1} + p_{k-2},$$

$$q_k = a_k q_{k-1} + q_{k-2}.$$

Then, it holds $p_k/q_k = [a_0, \dots, a_k]$, and the rational number p_k/q_k is called the k -th convergent of the continued fraction. It is well-known that the regular continued fraction expansion of \sqrt{m} is of the form

$$\sqrt{m} = [a_0, \overline{a_1, \dots, a_l}] := [a_0, a_1, \dots, a_l, a_1, \dots, a_l, \dots]$$

and l is called the period of \sqrt{m} if we take the minimal l . Then we obtain a fundamental solution of Pell's equation

$$(p, q) = \begin{cases} (p_{l-1}, q_{l-1}) & (l: \text{even}) \\ (p_{2l-1}, q_{2l-1}) & (l: \text{odd}). \end{cases}$$

In Section 6, we observe a characterization of a fundamental solution of (1.1). For comparison, we explain why the regular continued fraction expansion of \sqrt{m} gives a fundamental solution. A solution (a, b) is a fundamental solution if and only if

$$(2.2) \quad |\log|a + \sqrt{mb}|| = \min\{|\log|x + \sqrt{my}|| \mid x, y \in \mathbb{Z}, x^2 - my^2 = 1\},$$

or equivalently,

$$|a| = \min\{|x| \in \mathbb{Z} \mid x \neq 1, x^2 - my^2 = 1\}.$$

On the other hand, the regular continued fraction of \sqrt{m} gives a best approximation to \sqrt{m} in the following sense.

Definition 2.1 (Best approximation, cf. [6, p. 9]). Let α be an irrational number. A best approximation to α is a rational number p/q ($q > 0$) such that for any rational number $p'/q' \neq p/q$ with $1 \leq q' \leq q$, we have

$$|q\alpha - p| < |q'\alpha - p'|.$$

Theorem 2.2 (cf. [6, Theorem 6]). *All of best approximations to α are convergents of the regular continued fraction expansion of α .*

Let $(x, y) \neq (\pm 1, 0)$ be a solution of the (2.1) with $x/y > 0$. Then x/y satisfies

$$(2.3) \quad \left| \sqrt{m} - \frac{x}{y} \right| < \frac{1}{2y^2}.$$

If a rational number satisfies the inequality (2.3), then the rational number is a best approximation to \sqrt{m} (cf. [6, Corollary 2]). Thus we see that x/y is a convergent of \sqrt{m} , and there exists an integer n such that $x/y = p_n/q_n$. By the theory of continued fraction, if the period l of the regular continued fraction expansion of \sqrt{m} is even (resp. odd), then $l - 1$ (resp. $2l - 1$) is the index of the convergent which has the smallest numerator in the set of convergents that can be solutions to (2.1), that is, (p_{l-1}, q_{l-1}) (resp. (p_{2l-1}, q_{2l-1})) is a fundamental solution.

3. Generalized Pell's equation

We study the generalized Pell's equation

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

with the $\mathbb{Z}[X_{n-1}]$ -solutions by imitating the classical method. We obtained a continued fraction expansion of X_n over $\mathbb{Z}[X_{n-1}]$ by a new algorithm. First, we prepare the algebraic property of X_n .

3.1. Algebraic aspects of X_n . For non-negative integer n , set $\mathbb{B}_n = \mathbb{Q}(X_n)$. Since $X_n = \zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1}$ we see that \mathbb{B}_n is the maximal real subfield of $\mathbb{Q}(\zeta_{2^{n+2}})$ where $\zeta_{2^{n+2}} := \exp(2\pi\sqrt{-1}/2^{n+2})$. By the theory of cyclotomic field (see [12, Chapter 2] in detail), we have that \mathbb{B}_n is an algebraic number field of degree 2^n , and Galois extension over \mathbb{Q} with Galois group $\mathbb{Z}/2^n\mathbb{Z}$, and the ring of integers of \mathbb{B}_n is $\mathbb{Z}[X_n]$. We see that \mathbb{B}_n is a relative quadratic extension over \mathbb{B}_{n-1} .

3.2. New continued fraction. We define a new continued fraction expansion algorithm over $\mathbb{Z}[X_{n-1}]$. For $n \geq 1$, we set $\beta_0 = 1$ and $\beta_k = 2 \cos(k\pi/2^n)$ for each $1 \leq k \leq 2^{n-1} - 1$. Then,

$$(3.1) \quad \mathcal{B}_{n-1} = \{\beta_k \mid k = 0, 1, \dots, 2^{n-1} - 1\}$$

is an integral basis of $\mathbb{Z}[X_{n-1}]$. By embedding

$$\phi_n : \mathbb{B}_{n-1} \longrightarrow \mathbb{R}^{2^{n-1}}; a \mapsto (\tau(a))_{\tau \in \text{Gal}(\mathbb{B}_{n-1}/\mathbb{Q})},$$

the basis \mathcal{B}_{n-1} is orthogonal in $\mathbb{R}^{2^{n-1}}$ (cf. [9, Lemma 6.3]), and $\mathbb{Z}[X_{n-1}]$ forms a complete lattice in $\mathbb{R}^{2^{n-1}}$. Recall $X_n = \sqrt{2 + X_{n-1}}$. We define

$$\phi_n(X_n) = (\sqrt{2 + \tau(X_{n-1})})_{\tau \in \text{Gal}(\mathbb{B}_{n-1}/\mathbb{Q})}$$

and extend ϕ_n to

$$\phi_n : \mathbb{B}_n \longrightarrow \mathbb{R}^{2^{n-1}}; a + X_n b \mapsto \phi_n(a) + \phi_n(X_n)\phi_n(b)$$

for each $a, b \in \mathbb{B}_{n-1}$ where the sum and the multiplication are component-wise. For each $x \in \mathbb{R}$, let $\text{round}(x)$ denote the integer in $(x - 1/2, x + 1/2]$. We note that for each $\alpha \in \mathbb{B}_n$, there are unique $r_k \in \mathbb{R}$ such that $\phi_n(\alpha) = \sum_{k=0}^{2^{n-1}-1} r_k \phi_n(\beta_k)$.

Definition 3.1. For $\alpha \in \mathbb{B}_n$ such that $\phi_n(\alpha) = \sum_{k=0}^{2^{n-1}-1} r_k \phi_n(\beta_k)$, we define $\lfloor \alpha \rfloor = \sum_{k=0}^{2^{n-1}-1} \text{round}(r_k) \beta_k \in \mathbb{Z}[X_{n-1}]$ and the sequence $(a_k)_{k \geq 0}$ as

$$\begin{aligned} \alpha_0 &= \alpha, & a_0 &= \lfloor \alpha_0 \rfloor, \\ \alpha_m &= (\alpha_{m-1} - a_{m-1})^{-1}, & a_m &= \lfloor \alpha_m \rfloor \quad (m \geq 1). \end{aligned}$$

If $\alpha_{m-1} \in \mathbb{Z}[X_{n-1}]$ then $a_{m-1} = \alpha_{m-1}$ and α_m is not defined.

Remark 3.2. By the orthogonality of $\phi_n(\mathcal{B}_{n-1})$, $\phi_n(\lfloor \alpha \rfloor)$ is one of the closest points to $\phi_n(\alpha)$ in $\phi_n(\mathbb{Z}[X_{n-1}])$ for Euclidean distance of $\mathbb{R}^{2^{n-1}}$.

Before stating the next proposition, we note that $1 + X_{n-1} \in \mathbb{Z}[X_{n-1}]$ is a unit. It will be explained in Section 4.

Proposition 3.3. *Let $\alpha = X_n \in \mathbb{B}_n$. Then we have*

$$\begin{aligned} a_0 &= 1, \\ a_{2k-1} &= 2(1 + X_{n-1})^{-1}, \\ a_{2k} &= 2 \end{aligned}$$

for positive integers k .

Proof. By Remark 3.2, it suffices to show that $\phi_n(0)$ is

- (a) a unique closest point to $\phi_n(\sqrt{2 + X_{n-1}} - 1)$ and
- (b) a unique closest point to $\phi_n((\sqrt{2 + X_{n-1}} - 1)^{-1} - 2(1 + X_{n-1})^{-1}) = \phi_n((1 + \sqrt{2 + X_{n-1}})^{-1})$

in $\phi_n(\mathbb{Z}[X_{n-1}])$. For (a), since $\phi_n(\mathcal{B}_{n-1})$ is orthogonal in $\mathbb{R}^{2^{n-1}}$ and the lengths of $\phi_n(\beta_k)$ ($k = 1, \dots, 2^{n-1} - 1$) are $\sqrt{2^n}$ (see [9, Lemma 6.3]), it is enough to show that

- (a-1) $\|\sqrt{2 + X_{n-1}} - 1 - 0\| < \sqrt{2^n}/2$ and
- (a-2) $\|\sqrt{2 + X_{n-1}} - 1 - 0\| < \|\sqrt{2 + X_{n-1}} - 1 - (\pm 1)\|$.

(a-1). The left-hand side of the inequality is $\|\sqrt{2 + X_{n-1}} - 1\| = \sqrt{2^n \mathfrak{A}_n / \pi}$, where

$$\mathfrak{A}_n := \frac{\pi}{2^n} \sum_{k=1}^{2^{n-1}} \left(2 \cos \left(\frac{2k-1}{2^{n+1}} \pi \right) - 1 \right)^2 < \int_{-\frac{\pi}{2^{n+1}}}^{\frac{\pi}{2} + \frac{\pi}{2^{n+1}}} (2 \cos x - 1)^2 dx =: I_n.$$

Now $(I_n)_{n \geq 6}$ is decreasing with $I_6 = 0.762 \dots < \pi/4$ and we can check numerically that $\mathfrak{A}_n < \pi/4$ for the cases $1 \leq n \leq 5$.

(a-2). We show that

(a-2-i) $\|\sqrt{2 + X_{n-1}} - 1\| < \|\sqrt{2 + X_{n-1}} - 1 - (+1)\|$ and
 (a-2-ii) $\|\sqrt{2 + X_{n-1}} - 1\| < \|\sqrt{2 + X_{n-1}} - 1 - (-1)\|$.

(a-2-i). Transform the inequality as following;

$$\sum_{k=1}^{2^{n-1}} \left(2 \cos \left(\frac{2k-1}{2^{n+1}} \pi \right) - 1 \right)^2 < \sum_{k=1}^{2^{n-1}} \left(2 \cos \left(\frac{2k-1}{2^{n+1}} \pi \right) - 2 \right)^2$$

$$\iff \frac{\pi}{2^{n-1}} \sum_{k=1}^{2^{n-1}} \cos \left(\frac{2k-1}{2^{n+1}} \pi \right) < \frac{3}{4} \pi.$$

Since the proof of the inequality is almost the same as in case (a-1), using a comparison series-integral with $\cos x$, we omit it.

(a-2-ii). Similarly, we see that it suffices to show that

$$1 < \frac{8}{2^n} \sum_{k=1}^{2^{n-1}} \cos \left(\frac{2k-1}{2^{n+1}} \pi \right)$$

for $n \geq 1$. In fact, we prove a more general case

$$1 < S_N := \frac{4}{N} \sum_{k=1}^N \cos \left(\frac{2k-1}{4N} \pi \right) \quad (N \geq 1).$$

For $N = 1$, we have $S_1 = 4 \cos(\pi/4) = 2\sqrt{2} > 1$. For $N \geq 2$, a comparison series-integral gives that

$$S_N \geq I_N := \frac{8}{\pi} \int_{\frac{\pi}{4N}}^{\frac{2N-1}{4N} \pi} \cos x \, dx.$$

Since $I_N = 8/\pi(\cos(\pi/(4N)) - \sin(\pi/(4N)))$ and the function $x \mapsto \cos x - \sin x$ decreases in $[0, \pi/4]$, we have that $S_N \geq I_N > I_2 > 1$.

Similarly to the proof of (a), we separate the proof of (b) into (b-1) and (b-2).

(b-1). We show that $\|(1 + \sqrt{2 + X_{n-1}})^{-1}\| < \sqrt{2^n}/2$, which means that

$$\frac{\pi}{2^n} \sum_{k=1}^{2^{n-1}} \left(\frac{1}{2 \cos \left(\frac{2k-1}{2^{n+1}} \pi \right) + 1} \right)^2 < \frac{\pi}{4}.$$

However, in the proof of (b-2-ii), we show that

$$\frac{\pi}{2^n} \sum_{k=1}^{2^{n-1}} \frac{1}{2 \cos \left(\frac{2k-1}{2^{n+1}} \pi \right) + 1} < \frac{\pi}{4}$$

and this implies the statement because $2 \cos(\frac{2k-1}{2^{n+1}} \pi) + 1 > 1$ for all $1 \leq k \leq 2^{n-1}$.

(b-2). Similarly to the proof of (a-2), we separate the proof into two cases.

(b-2-i). We show that

$$\left\| \left(1 + \sqrt{2 + X_{n-1}}\right)^{-1} \right\| < \left\| \left(1 + \sqrt{2 + X_{n-1}}\right)^{-1} - (-1) \right\|.$$

This is easy because

$$\begin{aligned} & \sum_{k=1}^{2^{n-1}} \left(\left(\frac{1}{2 \cos \left(\frac{2k-1}{2^{n+1}} \pi \right) + 1} + 1 \right)^2 - \left(\frac{1}{2 \cos \left(\frac{2k-1}{2^{n+1}} \pi \right) + 1} \right)^2 \right) \\ &= \sum_{k=1}^{2^{n-1}} \left(1 + \frac{2}{2 \cos \left(\frac{2k-1}{2^{n+1}} \pi \right) + 1} \right) > 0. \end{aligned}$$

(b-2-ii). $\left\| \left(1 + \sqrt{2 + X_{n-1}}\right)^{-1} \right\| < \left\| \left(1 + \sqrt{2 + X_{n-1}}\right)^{-1} - (+1) \right\|$. Similarly to the proof of (a-2-i), it suffices to show that

$$\frac{\pi}{2^n} \sum_{k=1}^{2^{n-1}} \frac{1}{2 \cos \left(\frac{2k-1}{2^{n+1}} \pi \right) + 1} < \frac{\pi}{4}.$$

Since the proof of the inequality is almost the same as in case (a-1), using a comparison series-integral with $1/(2 \cos x + 1)$, we omit it. \square

Proposition 3.3 only provides a formal expansion. We see that it does converge.

Theorem 3.4. For $n \geq 1$ and each $\tau \in \text{Gal}(\mathbb{B}_{n-1}/\mathbb{Q})$, we have

$$\sqrt{2 + \tau(X_{n-1})} = [1, \overline{2(1 + \tau(X_{n-1}))^{-1}}, 2].$$

Here, $[a_0, a_1, \dots]$ denotes $a_0 + \frac{1}{a_1 + \dots}$ and $[a_0, \dots, a_r, \overline{a_{r+1}, \dots, a_s}]$ denotes the periodicity of the part a_{r+1}, \dots, a_s , namely

$$[a_0, \dots, a_r, \overline{a_{r+1}, \dots, a_s}] = [a_0, \dots, a_r, a_{r+1}, \dots, a_s, a_{r+1}, \dots, a_s, \dots].$$

Remark 3.5. Theorem 3.4 states that the above continued fraction converges in Euclidean space $\mathbb{R}^{2^{n-1}} \xrightarrow{\phi_n} \mathbb{B}_n$. Namely we get a continued fraction expansion of $\sqrt{2 + X_{n-1}}$ over $\mathbb{Z}[X_{n-1}]$ for each metric induced by $\tau \in \text{Gal}(\mathbb{B}_{n-1}/\mathbb{Q})$. We could not make sure whether this algorithm gives a continued fraction expansion of any element of \mathbb{B}_n , and whether this algorithm terminates for any element of \mathbb{B}_{n-1} .

Proof. If the continued fraction $[1, \overline{2(1 + \tau(X_{n-1}))^{-1}}, 2]$ converges, then we see that the numerical value of it is $\sqrt{2 + \tau(X_{n-1})}$ by an easy calculation. We show the convergence of $[1, \overline{2(1 + \tau(X_{n-1}))^{-1}}, 2]$ for each $\tau \in$

$\text{Gal}(\mathbb{B}_{n-1}/\mathbb{Q})$. We check the conditions in [2, Theorem 4.3]. For $a \in \mathbb{C}$, we define

$$D(a) = \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}.$$

For a continued fraction $[a_1, a_2, \dots, a_k]$, we define

$$M([a_1, a_2, \dots, a_k]) = D(a_1)D(a_2) \dots D(a_k).$$

We should check the followings for all $n \geq 1$ and $\tau \in \text{Gal}(\mathbb{B}_{n-1}/\mathbb{Q})$;

- (a) $M([1, 2(1 + \tau(X_{n-1}))^{-1}, 2, 0, -1, 0]) \neq \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
- (b) $|M([2(1 + \tau(X_{n-1}))^{-1}, 2])_{2,2}| \leq 1$
- (b') $|M([2, 2(1 + \tau(X_{n-1}))^{-1})_{2,2}| \leq 1$
- (c) $\text{Tr}(M([1, 2(1 + \tau(X_{n-1}))^{-1}, 2, 0, -1, 0]))^2 \geq 4$

where $M_{2,2}$ denotes the $(2, 2)$ -element of a matrix M . The first three (a), (b), and (b') are trivial. We note that

$$\text{Tr}(M([1, 2(1 + \tau(X_{n-1}))^{-1}, 2, 0, -1, 0]))^2 = 4(2(1 + \tau(X_{n-1}))^{-1} + 1)^2.$$

If $\tau(X_{n-1}) > -1$, then we have $(2(1 + \tau(X_{n-1}))^{-1} + 1)^2 \geq 1$ and (c) holds. Otherwise, we have that $-2 < \tau(X_{n-1}) < -1$. So we have $(1 + \tau(X_{n-1}))^{-1} < -1$ and an easy calculation shows that (c) holds. \square

In the case $n = 1$, the above theorem states that $\sqrt{2} = [1, \overline{2, 2}]$ and this is a classical continued fraction expansion of $\sqrt{2}$.

3.3. $\mathbb{Z}[X_{n-1}]$ -solutions. By imitating the classical method, we formulate a conjecture for the $\overline{\mathbb{Z}[X_{n-1}]}$ -solutions of the generalized Pell's equation. Since the period of $[1, 2(1 + X_{n-1})^{-1}, 2]$ is 2, we look at the first convergent

$$\frac{p_1}{q_1} = \frac{1 + 2(1 + X_{n-1})^{-1}}{2(1 + X_{n-1})^{-1}}.$$

It is easy to check that

$$p_1^2 - X_n^2 q_1^2 = 1$$

for all $n \geq 1$. We set

$$\epsilon_n = p_1 + X_n q_1.$$

We conjecture that the element ϵ_n generates the $\overline{\mathbb{Z}[X_{n-1}]}$ -solutions as a Galois module.

Conjecture 3.6. *The $\overline{\mathbb{Z}[X_{n-1}]}$ -solutions of the generalized Pell's equation $x^2 - X_n^2 y^2 = 1$ is a $\text{Gal}(\mathbb{B}_n/\mathbb{Q})$ -module generated by -1 and ϵ_n , namely,*

$$\{a + X_n b \mid a, b \in \overline{\mathbb{Z}[X_{n-1}]}, a^2 - X_n^2 b^2 = 1\} = \langle -1, \epsilon_n \rangle_{\mathbb{Z}[\text{Gal}(\mathbb{B}_n/\mathbb{Q})]}.$$

4. Weber's class number problem

The aim of this section is to prove the following equivalence:

Theorem 4.1. *Conjecture 3.6 is true for all $n \geq 0$ if and only if Weber's conjecture is true for all $n \geq 0$.*

4.1. Some known results. We prepare some known results. Let E_n be the group of units of \mathbb{B}_n and

$$C_n := \left\langle -1, \zeta_{2^{n+2}}^{\frac{1-a}{2}} \frac{1 - \zeta_{2^{n+2}}^a}{1 - \zeta_{2^{n+2}}} \mid a : \text{odd integers such that } 1 < a < 2^{n+1} \right\rangle_{\mathbb{Z}}$$

be its subgroup of cyclotomic units. Then $(E_n : C_n) = h_n$, by [12, Lemma 8.1 and Theorem 8.2]. Noticing that 3 is a generator of $(\mathbb{Z}/2^{n+2}\mathbb{Z})^*/\{\pm 1\}$ and that

$$1 + X_n = \zeta_{2^{n+2}}^{\frac{1-3}{2}} \frac{1 - \zeta_{2^{n+2}}^3}{1 - \zeta_{2^{n+2}}},$$

by [12, Proposition 8.11], we have

$$C_n = \langle 1 + X_n \rangle_{\mathbb{Z}[\text{Gal}(\mathbb{B}_n/\mathbb{Q})]}.$$

We set $G_{n/n-1} = \text{Gal}(\mathbb{B}_n/\mathbb{B}_{n-1})$ and define $\sigma_{n/n-1}$ to be the non-trivial element of $G_{n/n-1}$. We note that $\sigma_{n/n-1}(X_n) = -X_n$. We define a relative norm map by

$$N_{n/n-1} : \mathbb{B}_n \longrightarrow \mathbb{B}_{n-1}; x \mapsto x\sigma_{n/n-1}(x).$$

Lemma 4.2. *The restrictions $N_{n/n-1}|_{E_n} : E_n \rightarrow E_{n-1}$ and $N_{n/n-1}|_{C_n} : C_n \rightarrow C_{n-1}$ are well-defined and surjective.*

Proof. Let $\widehat{H}^r(G_{n/n-1}, E_n)$ be the r -th Tate cohomology group. It suffices to show that $\widehat{H}^0(G_{n/n-1}, E_n) = \{1\}$ for the surjectivity of $N_{n/n-1}|_{E_n} : E_n \rightarrow E_{n-1}$. Yokoi [14, Lemma 3] showed that

$$Q(E_n) = \frac{|\widehat{H}^0(G_{n/n-1}, E_n)|}{|\widehat{H}^1(G_{n/n-1}, E_n)|} = \frac{1}{2}.$$

Therefore, it suffices to show that $|\widehat{H}^1(G_{n/n-1}, E_n)| = 2$. Let H_{n-1} be the maximal unramified abelian extension of \mathbb{B}_{n-1} . Then we have $\mathbb{B}_n \cap H_{n-1} = \mathbb{B}_{n-1}$ because $\mathbb{B}_n/\mathbb{B}_{n-1}$ ramifies at the prime ideal lying above 2. Furthermore, $\mathbb{B}_n/\mathbb{B}_{n-1}$ ramifies at only one prime, then $\mathbb{B}_n/\mathbb{B}_{n-1}$ satisfies the assumption of [14, Theorem 1]. Thus we have $h_{n-1} = |\text{Cl}_n^{G_{n/n-1}}|$. Since we have $2 \nmid h_{n-1}$ by [13, Theorem C], we get $|\widehat{H}^1(G_{n/n-1}, E_n)| = 2$ by the Corollary of [14, Theorem 2]. Thus we see that $N_{n/n-1} : E_n \rightarrow E_{n-1}$ is surjective.

Next we consider $N_{n/n-1}|_{C_n}$. The presentation $C_n = \langle 1 + X_n \rangle_{\mathbb{Z}[\text{Gal}(\mathbb{B}_n/\mathbb{Q})]}$ and the easy calculations $N_{n/n-1}(1 + X_n) = -1 - X_{n-1}$ and $N_{n/n-1}((1 + X_n)\sigma(1 + X_n) \dots \sigma^{2^{n-1}-1}(1 + X_n)) = -1$ show that $N_{n/n-1} : C_n \rightarrow C_{n-1}$ is well-defined and surjective, where σ is a generator of $\text{Gal}(\mathbb{B}_n/\mathbb{Q})$. \square

Set $RE_n^+ = \ker(N_{n/n-1}|_{E_n})$ throughout this paper. Lemma 4.2 implies the following exact sequence:

$$(4.1) \quad 0 \longrightarrow RE_n^+/A_n \longrightarrow E_n/C_n \longrightarrow E_{n-1}/C_{n-1} \longrightarrow 0,$$

where $A_n := RE_n^+ \cap C_n$. By the exact sequence (4.1), Weber’s conjecture is equivalent to

$$(4.2) \quad (RE_n^+ : A_n) = 1 \text{ for all } n \geq 1.$$

4.2. Proof of Theorem 4.1. For $\epsilon \in RE_n^+$, there exist unique $a, b \in \mathbb{Z}[X_{n-1}]$ such that $\epsilon = a + bX_n$ and we have $N_{n/n-1}(\epsilon) = a^2 - b^2X_n^2$. Thus we have a bijection;

$$\begin{array}{ccc} RE_n^+ & \longleftrightarrow & \{\text{the solutions of } x^2 - X_n^2y^2 = 1\} \\ \Downarrow & & \Downarrow \\ \epsilon = a + X_nb & \longleftrightarrow & (a, b) \end{array}$$

We recall that Conjecture 3.6 states

$$\{a + X_nb \mid a, b \in \mathbb{Z}[X_{n-1}], a^2 - X_n^2b^2 = 1\} = \langle -1, \epsilon_n \rangle_{\mathbb{Z}[\text{Gal}(\mathbb{B}_n/\mathbb{Q})]}.$$

Therefore, Conjecture 3.6 is equivalent to that $RE_n^+ = \langle -1, \epsilon_n \rangle_{\mathbb{Z}[\text{Gal}(\mathbb{B}_n/\mathbb{Q})]}$ for all n . Combining this formulation and (4.2), to prove Theorem 4.1, it suffices to prove that

$$A_n = \langle -1, \epsilon_n \rangle_{\mathbb{Z}[\text{Gal}(\mathbb{B}_n/\mathbb{Q})]}.$$

By easy calculation, we have that

$$\epsilon_n = \frac{X_n + 1}{X_n - 1}$$

for each $n \geq 1$. Since $C_n = \langle -1, 1 + X_n \rangle_{\mathbb{Z}[\text{Gal}(\mathbb{B}_n/\mathbb{Q})]}$, we have $\epsilon_n \in C_n$ and $\epsilon_n \in C_n \cap RE_n^+ = A_n$. Thus we have $\langle -1, \epsilon_n \rangle_{\mathbb{Z}[\text{Gal}(\mathbb{B}_n/\mathbb{Q})]} \subset A_n$.

We put $\tilde{N}_{n/n-1}|_{C_n} : C_n/\{\pm 1\} \rightarrow C_{n-1}/\{\pm 1\}$. Let σ be a generator of $\text{Gal}(\mathbb{B}_n/\mathbb{Q})$. We note that the basis of $C_n/\{\pm 1\}$ and $C_{n-1}/\{\pm 1\}$ are $\{\sigma(1 + X_n), \sigma^2(1 + X_n), \dots, \sigma^{2^n-1}(1 + X_n)\}$ and $\{\sigma(1 + X_{n-1}), \sigma^2(1 + X_{n-1}), \dots, \sigma^{2^{n-1}-1}(1 + X_{n-1})\}$ respectively. By considering the representation matrix of $\tilde{N}_{n/n-1}|_{C_n}$, we see that the basis of the kernel of $\tilde{N}_{n/n-1}|_{C_n}$ is

$$\left\{ \sigma^i \left(\frac{1 + X_n}{1 - X_n} \right), \prod_{j=0}^{2^{n-1}-1} \sigma^j (1 + X_n) \mid i = 1, 2, \dots, 2^{n-1} - 1 \right\}.$$

Since $\sigma^i \left(\frac{1+X_n}{1-X_n} \right) \in \left\langle -1, \frac{X_n+1}{X_n-1} \right\rangle_{\mathbb{Z}[G_n]}$, the rest of the proof is showing, for any $e \in \mathbb{Z}$, that

$$\prod_{j=0}^{2^{n-1}-1} \sigma^j(1 + X_n)^e \in \left\langle -1, \frac{X_n + 1}{X_n - 1} \right\rangle_{\mathbb{Z}[G_n]}$$

if $N_{n/n-1} \left(\prod_{j=0}^{2^{n-1}-1} \sigma^j(1 + X_n)^e \right) = 1$. Such e is even because

$$\begin{aligned} N_{n/n-1} \left(\prod_{j=0}^{2^{n-1}-1} \sigma^j(1 + X_n)^e \right) &= \left(\prod_{j=0}^{2^{n-1}-1} \sigma^j(1 + X_n) \sigma^{j+2^{n-1}}(1 + X_n) \right)^e \\ &= (-1)^e. \end{aligned}$$

Therefore it suffices to show that $\prod_{j=0}^{2^{n-1}-1} \sigma^j(1 + X_n)^2 \in \left\langle -1, \frac{X_n+1}{X_n-1} \right\rangle_{\mathbb{Z}[G_n]}$.

Since $\prod_{j=0}^{2^n-1} \sigma^j(1 + X_n) = -1$, we have

$$\prod_{j=0}^{2^{n-1}-1} \sigma^j(1 + X_n)^2 = - \prod_{j=0}^{2^{n-1}-1} \sigma^j \left(\frac{1 + X_n}{1 - X_n} \right) \in \left\langle -1, \frac{X_n + 1}{X_n - 1} \right\rangle_{\mathbb{Z}[G_n]}.$$

Then the assertion follows.

5. Results on the explicit unit ϵ_n

In this section, first we show the “minimality” of our explicit unit ϵ_n . Secondly, from the Galois action on relative units and the explicitness of ϵ_n , we obtain a congruence relation formula for the ratios of the class numbers.

5.1. The minimality of ϵ_n in RE_n^+ . For $n = 1$, $\epsilon_1 = 3 + 2\sqrt{2}$ comes from the continued fraction of $\sqrt{2}$. By the classical method, we have that ϵ_1 generates all the \mathbb{Z} -solutions of Pell's equation $x^2 - 2y^2 = 1$. This means that ϵ_1 is “minimal”, that is,

$$\epsilon_1^{\frac{l}{m}} \notin RE_1^+ \text{ for any reduced fraction } \frac{l}{m} \text{ with } 0 < \left| \frac{l}{m} \right| < 1.$$

It follows that Weber's conjecture for $n = 1$ holds true. We show that ϵ_n is also “minimal” for $n \geq 2$.

Theorem 5.1. $\epsilon_n^{\frac{l}{m}} \notin RE_n^+$ for any reduced fraction $\frac{l}{m}$ with $0 < \left| \frac{l}{m} \right| < 1$.

Proof. Let $n \geq 2$. It suffices to show the statement in case $\frac{l}{m} = \frac{1}{p}$ for each prime p . We separate the proof into two cases $p = 2$ or an odd prime.

Suppose $p = 2$. If $\epsilon_n^{1/2} \in RE_n^+ \subset \mathbb{B}_n$, then its conjugates are also included in \mathbb{B}_n . For $\tau \in \text{Gal}(\mathbb{B}_n/\mathbb{Q})$, $\tau \left(\sqrt{\frac{X_n+1}{X_n-1}} \right)^2 = \frac{\tau(X_n)+1}{\tau(X_n)-1}$. On the other hand, there exists $\tau \in \text{Gal}(\mathbb{B}_n/\mathbb{Q})$ such that $0 < \tau(X_n) < 1$. For such τ , we have

$\tau \left(\sqrt{\frac{X_n+1}{X_n-1}} \right)^2 < 0$ and this contradicts the fact that \mathbb{B}_n is a totally real field.

Thus we have $\epsilon_n^{1/2} \notin RE_n^+$.

Now assume that $p \geq 3$. By [9, Proposition 6.6] for $n \geq 2$ and $\pm 1 \neq \delta \in RE_n^+$ we have

$$(5.1) \quad \text{Tr}_n(\delta^2) \geq 2^n \cdot 17$$

where $\text{Tr}_n : \mathbb{B}_n \rightarrow \mathbb{Q}$ be the trace map of \mathbb{B}_n .

Suppose that $\epsilon_n^{1/p} \in RE_n^+$. For each $\tau \in \text{Gal}(\mathbb{B}_n/\mathbb{Q})$, the conjugate of $\epsilon_n^{1/p}$ is $\left(\frac{\tau(X_n+1)}{\tau(X_n-1)} \right)^{1/p}$. Then we have

$$\text{Tr}_n \left(\epsilon_n^{\frac{2}{p}} \right) = \sum_{k=1}^{2^n} f_p \left(\frac{2k-1}{2^{n+1}} \pi \right), \text{ where } f_p(x) := \left| \frac{2 \cos x + 1}{2 \cos x - 1} \right|^{\frac{2}{p}}.$$

Since $|2 \cos((2k-1)\pi/2^{n+1}) + 1| < |2 \cos((2k-1)\pi/2^{n+1}) - 1|$ for $k = 2^{n-1} + 1, \dots, 2^n$, we have $f_p((2k-1)\pi/2^{n+1}) < 1$ for such k . Therefore, by using (5.1) it suffices to show that $\sum_{k=1}^{2^{n-1}} f_p((2k-1)\pi/2^{n+1}) < 2^{n-1} \cdot 17$.

For $k = 1, \dots, 2^{n-1}$, we have

$$\left| \frac{2 \cos((2k-1)\pi/2^{n+1}) + 1}{2 \cos((2k-1)\pi/2^{n+1}) - 1} \right| > 1.$$

Then we have

$$f_p \left(\frac{2k-1}{2^{n+1}} \pi \right) < f_3 \left(\frac{2k-1}{2^{n+1}} \pi \right)$$

for $p > 3$. Therefore it suffices to show this in case $p = 3$. Thus our goal is to show that

$$\frac{1}{2^n} \sum_{k=1}^{2^{n-1}} f_3 \left(\frac{2k-1}{2^{n+1}} \pi \right) < \frac{17}{2}$$

for $n \geq 2$. Let K be the integer satisfying $(2K-1)\pi/2^{n+1} < \pi/3 < (2K+1)\pi/2^{n+1}$. We write

$$(5.2) \quad \frac{1}{2^n} \sum_{k=1}^{2^{n-1}} f_3 \left(\frac{2k-1}{2^{n+1}} \pi \right) = \frac{1}{2^n} \sum_{k=1}^{K-1} f_3 \left(\frac{2k-1}{2^{n+1}} \pi \right) + \frac{1}{2^n} f_3 \left(\frac{2K-1}{2^{n+1}} \pi \right) \\ + \frac{1}{2^n} f_3 \left(\frac{2K+1}{2^{n+1}} \pi \right) + \frac{1}{2^n} \sum_{k=K+2}^{2^{n-1}} f_3 \left(\frac{2k-1}{2^{n+1}} \pi \right).$$

A comparison series-integral gives that

$$(5.3) \quad \frac{\pi}{2^n} \sum_{k=1}^{K-1} f_3\left(\frac{2k-1}{2^{n+1}}\pi\right) + \frac{\pi}{2^n} \sum_{k=K+2}^{2^{n-1}} f_3\left(\frac{2k-1}{2^{n+1}}\pi\right) < \int_0^{\pi/3} f_3(x) dx + \int_{\pi/3}^{\pi/2} f_3(x) dx = 6.4669\dots$$

We used a computer for the last integral calculations.

Finally, we claim that

$$\frac{1}{2^n} f_3\left(\frac{2K-1}{2^{n+1}}\pi\right) + \frac{1}{2^n} f_3\left(\frac{2K+1}{2^{n+1}}\pi\right) < 3.$$

for $n \geq 2$. Indeed, the continuous function defined for nonzero x by $x \mapsto x \frac{2 \cos(\pi/3+x)+1}{2 \cos(\pi/3+x)-1}$ is increasing from $-\pi$ to 0 on $[-\pi/3, \pi/3] \setminus \{0\}$. So we have $f_3(\pi/3+x) \leq (\pi/|x|)^{2/3}$ on $[-\pi/3, \pi/3] \setminus \{0\}$. Set $r = 2^{n+1} + 3 - 6K$. So we see that $r \in \{1, 5\}$, $\frac{2K-1}{2^{n+1}}\pi = \frac{\pi}{3} - \frac{r}{3 \cdot 2^{n+1}}\pi$ and $\frac{2K+1}{2^{n+1}}\pi = \frac{\pi}{3} + \frac{6-r}{3 \cdot 2^{n+1}}\pi$. Since $\frac{5}{3 \cdot 2^{n+1}}\pi < \frac{\pi}{3}$ for $n \geq 2$, we obtain that

$$(5.4) \quad \frac{1}{2^n} f_3\left(\frac{2K-1}{2^{n+1}}\pi\right) + \frac{1}{2^n} f_3\left(\frac{2K+1}{2^{n+1}}\pi\right) < \frac{1}{2^n} \left(\frac{\pi}{\frac{1}{3 \cdot 2^{n+1}}\pi}\right)^{\frac{2}{3}} + \frac{1}{2^n} \left(\frac{\pi}{\frac{5}{3 \cdot 2^{n+1}}\pi}\right)^{\frac{2}{3}} = 2^{\frac{2-n}{3}} \left(3^{\frac{2}{3}} + \left(\frac{3}{5}\right)^{\frac{2}{3}}\right) < 3$$

for $n \geq 2$. Thus we have the claim and the assertion holds. □

Remark 5.2. For $n = 2$, we also show that $h_2 = 1$ by a similar method used above. Let σ be a generator of $\text{Gal}(\mathbb{B}_2/\mathbb{Q})$. Since $h_1 = 1$, we have $h_2 = (RE_2^+ : A_2)$. We recall that $A_2 = \langle -1, \epsilon_2 \rangle_{\mathbb{Z}[\text{Gal}(\mathbb{B}_2/\mathbb{Q})]}$ and note that $(RE_2^+ : A_2) < \infty$. We should show that $\epsilon_2^x \cdot \sigma(\epsilon_2)^y \notin RE_2^+$ for any $x, y \in [-1/2, 1/2] \cap \mathbb{Q}$ except for $x = y = 0$. If $\epsilon_2^x \cdot \sigma(\epsilon_2)^y \in \mathbb{B}_2$, then we have

$$\text{Tr}_2\left(\epsilon_2^{2x} \cdot \sigma(\epsilon_2)^{2y}\right) = \sum_{i=1}^4 \sigma^i(\epsilon_2)^{2x} \cdot \sigma^{i+1}(\epsilon_2)^{2y}.$$

Now we define a function $f_2(x, y) = \text{Tr}_2(\epsilon_2^{2x} \cdot \sigma(\epsilon_2)^{2y})$ on $[-1/2, 1/2]^2$. Since $\frac{\partial^2 f_2}{\partial x^2}(x, y)$ (resp. $\frac{\partial^2 f_2}{\partial y^2}(x, y)$) > 0 for each y (resp. x) $\in [-1/2, 1/2]^2$ and $f_2(\pm 1/2, 0) = f_2(0, \pm 1/2) < f_2(\pm 1/2, \pm 1/2)$, the maximum of $f_2(x, y)$ is taken at the points $(\pm 1/2, \pm 1/2)$. We have $f_2(\pm 1/2, \pm 1/2) = 28 < 2^2 \cdot 17$. This contradicts (5.1), so we have $RE_2^+ = A_2$ and $h_2 = 1$.

5.2. The ratios of the class numbers. We define the *relative class ratio* of $\mathbb{B}_n/\mathbb{B}_{n-1}$ by

$$k_n = \frac{h_n}{h_{n-1}}$$

for each $n > 0$. In this subsection, we obtain a congruence relation formula for k_n .

By (4.1) in Section 4, we have

$$k_n = \left(RE_n^+ : A_n \right).$$

For each prime l , let $(RE_n^+/A_n)_l$ denotes the Sylow l -subgroup of RE_n^+/A_n , that is the subgroup consisting of elements of l -power order. Let $(k_n)_l = |(RE_n^+/A_n)_l|$. The next theorem is our second main theorem.

Theorem 5.3. *For all prime l and all positive integer n , we have*

$$(k_n)_l \equiv 1 \pmod{2^n}.$$

This theorem shows that the sequence $\{h_n\}$ is a Cauchy sequence in 2-adic topology. Thus the sequence $\{h_n\}$ converges in \mathbb{Z}_2 .

Remark 5.4. Kisilevsky also obtained the convergence of the class numbers for more general setting in [5, Corollary 2]. He showed that for any \mathbb{Z}_p -extension over any global field, the sequence of the class numbers of the intermediate fields converges in \mathbb{Z}_p . He used the direct limit of the class groups instead of the unit groups, and the proof is different from ours. We give an extensive numerical study of the p -adic limits for elliptic curves and knots in [11].

We prepare two lemmas. We note that $\text{Gal}(\mathbb{B}_n/\mathbb{Q})$ acts on RE_n^+/A_n and also on $(RE_n^+/A_n)_l$.

Lemma 5.5. *For $\delta \in RE_n^+/A_n$, let $O(\delta)$ be the $\text{Gal}(\mathbb{B}_n/\mathbb{Q})$ -orbit of δ in RE_n^+/A_n . If $|O(\delta)| < 2^n$, then $\delta^2 = 1$ in RE_n^+/A_n .*

Proof. We recall that σ is a generator of $\text{Gal}(\mathbb{B}_n/\mathbb{Q})$. $|O(\delta)| < 2^n$ means $\sigma^{2^{n-1}}(\delta) = \delta$ in RE_n^+/A_n . Therefore, we have $N_{n/n-1}(\delta) = \delta\sigma^{2^{n-1}}(\delta) = \delta^2$ in RE_n^+/A_n . On the other hand, since $\delta \in RE_n^+$, we have $N_{n/n-1}(\delta) = 1$ in RE_n^+/A_n . Then we have $\delta^2 = 1$ in RE_n^+/A_n . □

Lemma 5.6. *Let $\delta \in RE_n^+/A_n$. If $|O(\delta)| = 1$, then $\delta = 1$ in RE_n^+/A_n .*

Proof. Set $\epsilon = (X_n + 1)/(X_n - 1)$ (abbreviate “ n ”). Suppose that there exists $\delta \in RE_n^+/A_n$ with $\delta \neq 1$ in RE_n^+/A_n and $|O(\delta)| = 1$. By Lemma 5.5, we have $\delta^2 \in A_n$. Since $A_n = \langle -1, \epsilon \rangle_{\mathbb{Z}[\text{Gal}(\mathbb{B}_n/\mathbb{Q})]}$, δ^2 can be represented as

$$\pm \epsilon^{e_0} \sigma(\epsilon)^{e_1} \dots \sigma^{2^{n-1}-1}(\epsilon)^{e_{2^{n-1}-1}}$$

by certain integers e_i . Therefore, we have

$$\delta = \pm \sqrt{\left| \epsilon^{e_0} \sigma(\epsilon)^{e_1} \dots \sigma^{2^{n-1}-1}(\epsilon)^{e_{2^{n-1}-1}} \right|}.$$

On the other hand, $|O(\delta)| = 1$ implies $\sigma(\delta) = \delta$ in $(RE_n^+/A_n)_2$. Therefore, we have

$$\begin{aligned} & \sqrt{|\epsilon^{\epsilon_0} \sigma(\epsilon)^{\epsilon_1} \dots \sigma^{2^{n-1}-1}(\epsilon)^{\epsilon_{2^{n-1}-1}}|} \\ &= \sqrt{|\sigma(\epsilon)^{\epsilon_0} \sigma^2(\epsilon)^{\epsilon_1} \dots \sigma^{2^{n-1}}(\epsilon)^{\epsilon_{2^{n-1}-1}}|} \\ &= \sqrt{|\epsilon^{-\epsilon_{2^{n-1}-1}} \sigma(\epsilon)^{\epsilon_0} \dots \sigma^{2^{n-1}-1}(\epsilon)^{\epsilon_{2^{n-1}-2}}|} \quad \text{in } (RE_n^+/A_n)_2. \end{aligned}$$

Note that $\sigma^{2^{n-1}}(\epsilon) = \epsilon^{-1}$. Since $\{\epsilon, \sigma(\epsilon), \dots, \sigma^{2^{n-1}-1}(\epsilon)\}$ are linearly independent over \mathbb{Z} in RE_n^+ , we have

$$-\epsilon_{2^{n-1}-1} \equiv \epsilon_0 \equiv \epsilon_1 \equiv \dots \equiv \epsilon_{2^{n-1}-2} \equiv \epsilon_{2^{n-1}-1} \pmod{2}.$$

This implies that $\epsilon_i \equiv 0 \pmod{2}$ for all i or $\epsilon_i \equiv 1 \pmod{2}$ for all i . Since $\delta \neq 1$, we have $\epsilon_i = 1$ for all i . Then we have $\sqrt{|\epsilon \sigma(\epsilon) \dots \sigma^{2^{n-1}-1}(\epsilon)|} \in RE_n^+$.

By easy calculation, we have

$$\left| \prod_{k=0}^{2^{n-1}-1} \sigma^k((X_n + 1)(X_n - 1)) \right| = 1.$$

It follows that

$$|\epsilon \sigma(\epsilon) \dots \sigma^{2^{n-1}-1}(\epsilon)| = \left(\frac{1}{(X_n - 1) \dots \sigma^{2^{n-1}-1}(X_n - 1)} \right)^2.$$

Thus we have

$$\sqrt{|\epsilon \sigma(\epsilon) \dots \sigma^{2^{n-1}-1}(\epsilon)|} = \left| \frac{1}{(X_n - 1) \dots \sigma^{2^{n-1}-1}(X_n - 1)} \right|.$$

Since $N_{n/n-1}((X_n - 1) \dots \sigma^{2^{n-1}-1}(X_n - 1)) = -1$ and $N_{n/n-1}(-1) = 1$, we have $N_{n/n-1}\left(\left|\frac{1}{(X_n - 1) \dots \sigma^{2^{n-1}-1}(X_n - 1)}\right|\right) = -1$. This contradicts

$$\sqrt{|\epsilon \sigma(\epsilon) \dots \sigma^{2^{n-1}-1}(\epsilon)|} \in \ker N_{n/n-1}. \quad \square$$

Proof of Theorem 5.3. First, we prove this for an odd prime l . Suppose that there exists an element $\delta \neq 1$ in $(RE_n^+/A_n)_l$ such that $|O(\delta)| < 2^n$. By Lemma 5.5, the order of δ is 2. This contradicts $2 \nmid |(RE_n^+/A_n)_l|$. Therefore, all elements except 1 in $(RE_n^+/A_n)_l$ have 2^n distinct conjugates. This implies the statement.

Next, we consider the case $l = 2$, independently of Weber's proof. Suppose that there exists an element $\delta \neq 1$ in $(RE_n^+/A_n)_2$ such that $|O(\delta)| < 2^n$ and we see that $|O(\delta)| > 1$ by Lemma 5.6. Let δ be an element with the smallest size of $|O(\delta)| = 2^m$. We note that δ satisfies $\sigma^{2^m}(\delta) = \delta$ and $\sigma^{2^{m-1}}(\delta) \neq \delta$ in $(RE_n^+/A_n)_2$. Since $\sigma^{2^{m-1}}(\delta \sigma^{2^{m-1}}(\delta)) = \sigma^{2^{m-1}}(\delta) \sigma^{2^m}(\delta) =$

$\sigma^{2^{m-1}}(\delta)\delta$ in $(RE_n^+/A_n)_2$, we have $|O(\delta\sigma^{2^{m-1}}(\delta))| \leq 2^{m-1}$. By the assumption, we have that $\delta\sigma^{2^{m-1}}(\delta) = 1$ and $\delta = \sigma^{2^{m-1}}(\delta)^{-1}$ in $(RE_n^+/A_n)_2$. By Lemma 5.5, we have $\sigma^{2^{m-1}}(\delta)^{-1} = \sigma^{2^{m-1}}(\delta)$ in $(RE_n^+/A_n)_2$. Thus we have $\delta = \sigma^{2^{m-1}}(\delta)$ in $(RE_n^+/A_n)_2$ and this is a contradiction. \square

Remark 5.7. By Theorem 5.3, we have $2 \nmid h_n$ for all $n \geq 1$. This result was first proved by Weber [13, Theorem C], but the proof we have now given is independent of the one by Weber. In the proof of Theorem 5.3, we use the fact that $N_{n/n-1} : E_n/C_n \rightarrow E_{n-1}/C_{n-1}$ is surjective and it comes from $2 \nmid h_{n-1}$ (see the proof of Lemma 4.2). Therefore it may seem like a tautology, but if we admit $h_0 = h(\mathbb{Q}) = 1$, the proof goes well by induction without using Weber’s result. Moreover, our result is a much more refined version of Weber’s result.

Remark 5.8. Recall that $h_6 = 1$, then we have $(k_7)_l = (h_7)_l$. By Theorem 5.3, we have

$$(h_n)_l \equiv 1 \pmod{2^7}$$

for all odd primes l and positive integers n .

6. Observations on the sizes of ϵ_n

In this section, by imitating the classical Pell’s equation, we observe some “sizes” of the explicit unit ϵ_n and state the conjecture on the minimality of ϵ_n . By assuming the conjecture, we give an upper bound for k_n for small n . Let σ be a generator of $\text{Gal}(\mathbb{B}_n/\mathbb{Q})$. By embedding $l_n : RE_n^+ \rightarrow \mathbb{R}^{2^{n-1}}$; $\epsilon \mapsto (\log |\sigma^i(\epsilon)|)_i$, $l_n(RE_n^+)$ forms a complete lattice in $\mathbb{R}^{2^{n-1}}$. For a positive integer p , let $\|x\|_p = (\sum_{i=1}^{2^{n-1}} |x_i|^p)^{1/p}$ denote the L^p norm of x in $\mathbb{R}^{2^{n-1}}$.

Definition 6.1 (L^p -minimal). Let S be a subset of RE_n^+ . For $\epsilon \in S \setminus \{\pm 1\}$, if $l_n(\epsilon)$ has a minimal L^p norm in $l_n(S \setminus \{\pm 1\})$, then ϵ is said to be L^p -minimal in S .

We note that this definition is independent of the choice of a generator σ of $\text{Gal}(\mathbb{B}_n/\mathbb{Q})$. In the case of $n = 1$, if $\epsilon \in RE_1^+$ corresponds to a fundamental solution, then ϵ is L^p -minimal in RE_1^+ (cf. (2.2)) for any p . For $p = 1, 2$, we conjecture the L^p -minimality of ϵ_n in RE_n^+ as an analogue of the case $n = 1$.

Conjecture 6.2. For all n , ϵ_n is L^1 and L^2 -minimal in RE_n^+ .

We observe that our explicit unit ϵ_n is L^2 -minimal in A_n for $1 \leq n \leq 10$ by using Fincke–Pohst algorithm (qfminim command in PARI/GP). Since $A_n = RE_n^+$ for $1 \leq n \leq 6$, we obtain that ϵ_n is L^2 -minimal in RE_n^+ for $1 \leq n \leq 6$. For each $\epsilon \in RE_n^+$, we see that $\|l_n(\epsilon)\|_1 = \log(\prod_{i=1}^{2^n} \max\{1, |\sigma^i(\epsilon)|\})$, and the value in log is called the Mahler measure of algebraic numbers.

Morisawa and Okazaki [9] investigate RE_n^+ by using the Mahler measure, and obtained a lower bound for $l_n(RE_n^+ \setminus \{\pm 1\})$ in L^1 norm as $2^{n-1} \log(2 + \sqrt{5})$ (cf. [9, Lemma 3.2 and Theorem 5.3]). They also obtained a lower bound in L^2 norm as $\sqrt{2^{n-1}} \log(2 + \sqrt{5})$ (cf. [8, Lemma 2.5(1)]). Note that these two lower bounds are processed into forms that fit our definitions. We compare $\|l_n(\epsilon_n)\|_p$ and lower bounds for small n in Table 6.1.

TABLE 6.1. Comparison of $\|l_n(\epsilon_n)\|_p$ and lower bounds

n	$\ l_n(\epsilon_n)\ _1$	$2^{n-1} \log(2 + \sqrt{5})$	$\ l_n(\epsilon_n)\ _2$	$\sqrt{2^{n-1}} \log(2 + \sqrt{5})$
1	1.76...	1.44...	1.76...	1.44...
2	3.22...	2.88...	2.35...	2.04...
3	6.28...	5.77...	3.54...	2.88...
4	12.47...	11.54...	5.04...	4.08...
5	24.89...	23.09...	7.20...	5.77...
6	49.76...	46.19...	10.22...	8.16...
7	99.52...	92.39...	14.48...	11.54...

In the following, by assuming that Conjecture 6.2 holds, we give upper bounds of $k_n = h_n/h_{n-1}$ for small n . Let m be a positive integer. For a Lebesgue measurable set S in \mathbb{R}^m , $\text{vol}(S)$ denote the volume of S in Lebesgue measure on \mathbb{R}^m . For a complete lattice $L \subset \mathbb{R}^m$ with a basis $\mathbf{b} = \{b_1, \dots, b_m\}$, we define the volume of L by the volume of the fundamental parallel body of \mathbf{b} , namely, $\text{vol}(L) = |\det([b_1 \cdots b_m])|$. Then we have

$$(6.1) \quad (RE_n^+ : A_n) = \text{vol}(l_n(A_n)) / \text{vol}(l_n(RE_n^+)).$$

We use the following Blichfeldt's theorem. Note that the following statement is processed into our settings.

Theorem 6.3 (cf. [1, Theorem II, III]). *There exist $\epsilon, \delta \in RE_n^+ \setminus \{\pm 1\}$ such that*

$$\|l_n(\epsilon)\|_2 \leq \sqrt{\frac{2}{\pi}} \Gamma(2 + 2^{n-2})^{1/2^{n-1}} \text{vol}(l_n(RE_n^+))^{1/2^{n-1}}$$

and

$$\|l_n(\delta)\|_1 \leq \sqrt{\frac{2^n}{\pi}} \Gamma(2 + 2^{n-2})^{1/2^{n-1}} \text{vol}(l_n(RE_n^+))^{1/2^{n-1}},$$

where Γ is the gamma function.

Conjecture 6.2 implies that ϵ_n satisfies these inequalities. Thus we have

$$(6.2) \quad \frac{\text{vol}(l_n(A_n))}{\text{vol}(l_n(RE_n^+))} \leq \frac{\text{vol}(l_n(A_n)) \sqrt{2^n/\pi}^{2^{n-1}} \Gamma(2 + 2^{n-2})}{\|l_n(\epsilon_n)\|_1^{2^{n-1}}}$$

and

$$(6.3) \quad \frac{\text{vol}(l_n(A_n))}{\text{vol}(l_n(RE_n^+))} \leq \frac{\text{vol}(l_n(A_n))\sqrt{2/\pi}^{2^{n-1}}\Gamma(2+2^{n-2})}{\|l_n(\epsilon_n)\|_2^{2^{n-1}}}.$$

We compute the numerical values of the right-hand sides of (6.2) and (6.3) for each $n \leq 7$ in Table 6.2. Combining the table at $p = 2$ and the fact that each prime factor of h_n is greater than 10^9 for all n (cf. [3, Corollary 1.2]), we obtain $k_n = 1$ for $1 \leq n \leq 6$.

TABLE 6.2. Upper bounds for k_n assuming Conjecture 6.2

$n \setminus p$	1	2
1	1.06...	1.06...
2	1.35...	1.27...
3	2.51...	1.55...
4	14.44...	4.89...
5	4345.05...	417.77...
6	17992212754.52...	147730099.26...
7	14822653597271460343569281399.70...	876387598588509574855259.98...

Remark 6.4. By using Minkowski’s convex body theorem for the L^p norm open ball of the radius $\|l_n(\epsilon_n)\|_p$, we also obtain upper bounds of k_n . In contrast to the discussion above, in this setting, the L^1 -minimality of ϵ_n gives more precise bound than the L^2 -minimality.

By these arguments, the resolution of Conjecture 6.2 contributes to Weber’s conjecture and Conjecture 3.6. However, determining the shortest vector in a lattice is generally a very difficult problem. If we propose to approach Conjecture 6.2 by imitating the classical method in Section 2, then we should establish “the best approximation to X_n at $\mathbb{Q}(X_{n-1})$ ”.

Acknowledgement. The author would like to thank Tomokazu Kashio who gave the author much useful advice in this research, Jun Ueki who gave the author much advice in writing this paper, and the anonymous referees of the journal for essential comments. Finally, the author would like to thank his mother Yukari Yoshizaki for much support.

References

- [1] H. F. BLICHFELDT, “A New Principle in the Geometry of Numbers, with Some Applications”, *Trans. Am. Math. Soc.* **15** (1914), no. 3, p. 227-235.
- [2] B. W. BROCK, N. D. ELKIES & B. W. JORDAN, “Periodic continued fractions over S -integers in number fields and Skolem’s p -adic method”, *Acta Arith.* **197** (2021), no. 4, p. 379-420.
- [3] T. FUKUDA & K. KOMATSU, “Weber’s class number problem in the cyclotomic \mathbb{Z}_2 -extension of \mathbb{Q} , III”, *Int. J. Number Theory* **07** (2011), no. 06, p. 1627-1635.
- [4] K. HORIE, “Certain primary components of the ideal class group of the \mathbb{Z}_p -extension over the rationals”, *Tôhoku Math. J.* **59** (2007), no. 2, p. 259-291.

- [5] H. KISILEVSKY, "A Generalization of a result of Sinnott", *Pac. J. Math.* **181** (1997), no. 3, p. 225-229.
- [6] S. LANG, *Introduction to Diophantine Approximations, New Expanded Edition*, Springer, 1995.
- [7] J. C. MILLER, "Class numbers of totally real fields and applications to the Weber class number problem", *Acta Arith.* **164** (2014), no. 4, p. 381-397.
- [8] T. MORISAWA & R. OKAZAKI, "Height and Weber's Class Number Problem", *J. Théor. Nombres Bordeaux* **28** (2016), no. 3, p. 811-828.
- [9] ———, "Filtrations of units of Viète field", *Int. J. Number Theory* **16** (2020), no. 05, p. 1067-1079.
- [10] I. NIVEN, H. S. ZUCKERMAN & H. L. MONTGOMERY, *An Introduction to the Theory of Numbers*, 5 ed., John Wiley & Sons, 1991.
- [11] J. UEKI & H. YOSHIKAZI, "The p -adic limits of class numbers in \mathbb{Z}_p -towers".
- [12] L. C. WASHINGTON, *Introduction to Cyclotomic Fields*, 2 ed., Springer, 1997.
- [13] H. WEBER, "Theorie der Abel'schen Zahlkörper", *Acta Math.* **8** (1886), p. 193-263.
- [14] H. YOKOI, "On the class number of a relatively cyclic number field", *Nagoya Math. J.* **29** (1967), p. 31-44.

Hyuga YOSHIKAZI
Department of Mathematics
Graduate school of science and Technology
Tokyo University of Science
2641, Yamazaki, Noda-shi, 278-8510, Chiba, Japan
E-mail: yoshikazi.hyuga@gmail.com