J. Math. Tokushima Univ.
Vol. 58 (2024), 11 – 31

Rational Points on the Parabola and the Arithmetic of Related Algebraic Tori

By

Shin-ichi KATAYAMA

Professor Emeritus of Tokushima University,
e-mail address : *shinkatayama@tokushima-u.ac.jp*

Received September 30 2024

Abstract

Let D be a non-square integer and C_0 be the parabola $y = x^2 - D$. $C_0(\mathbb{Q})$ denotes the rational points of C_0. Adding the infinite point ∞ to $C_0(\mathbb{Q})$, we introduce a new multiplicative group structure on $C_0(\mathbb{Q}) \cup \{\infty\}$, which is denoted by $\overline{C_0(\mathbb{Q})}$. As an application of this group structure, we shall give several formulae of the covergents of the continued fraction expansions of $\sqrt{D}$. C_1 denotes the Pell conic $x^2 - Dy^2 = 1$ and $C_1(\mathbb{Q})$ denotes the rational points on C_1. Then $\overline{C_0(\mathbb{Q})}$ and $C_1(\mathbb{Q})$ are isomorphic as rational points of two algebraic tori. We will investigate the arithmetic of $\overline{C_0(\mathbb{Q})}$ and $C_1(\mathbb{Q})$ as the rational points of these algebraic tori.

2020 Mathematics Subject Classification. 11R29, 11A55, 11R56

1 Introduction

Let D be a non-square integer. C_0 denotes the parabola $y = x^2 - D$. C_1 denotes the corresponding Pell conic $x^2 - Dy^2 = 1$. We note that the Pell conic C_1 is a hyperbola for the case $D > 0$ and is an ellipse for the case $D < 0$. Let $C_0(\mathbb{Q})$ and $C_1(\mathbb{Q})$ be the rational points of the parabola C_0 and the Pell conics C_1, respectively. Usually, $C_0(\mathbb{Q})$ has the additive group structure and $C_1(\mathbb{Q})$ has the multiplicative group structure by so called chord and tangent processes.

In the following, we shall introduce a new group structure on $C_0(\mathbb{Q})$. Using this group structure, we shall give several formulae of the convergents and the intermediate convergents of the simple continued fraction expansions of $\sqrt{D}$.

We shall consider $C_0(\mathbb{Q})$(or more precisely $\overline{C_0(\mathbb{Q})}$) as the rational points of certain algebraic torus. $C_1(\mathbb{Q})$ is also considered as the rational points of another algebraic torus. Then these two algebraic tori are isomorphic. We shall refer the class numbers of these algebraic tori, which are considered as the geometrical versions of Gauss's genus theory. We shall investigate the heights of rational points of $C_0(\mathbb{Q})$ and $C_1(\mathbb{Q})$ and the canonical heights of these rational points.

2 Multiplicative group structure of the rational points on the parabola

2.1 The new group structure

Now we shall define a new group structure of $C_0(\mathbb{Q})$. Firstly we consider $\infty = \lim_{t\to\infty}(t, t^2 - D) = \lim_{t\to-\infty}(t, t^2 - D)$ is a rational point on C_0. Take two rational points $A = \left(\frac{a_1}{b_1}, \frac{a_1^2}{b_1^2} - D\right)$ and $B = \left(\frac{a_2}{b_2}, \frac{a_2^2}{b_2^2} - D\right)$ on C_0. The line connecting two points A and B has

the slope $\frac{a_2}{b_2} + \frac{a_1}{b_1}$ and intersects $x-$axis at the point

$$(c, 0), \text{where } c = \frac{a_1a_2 + b_1b_2D}{a_1b_2 + a_2b_1} \tag{1}$$

We call the rational point $(c, c^2 - D) \in C_0(\mathbb{Q})$ is the product of A and B and denote $A * B$, i.e.,

$$\left(\frac{a_1}{b_1}, \frac{{a_1}^2}{b_1^2} - D\right) * \left(\frac{a_2}{b_1}, \frac{{a_2}^2}{b_2^2} - D\right) = (c, c^2 - D).$$

We note, for the cases $D > 0$, this procedure is nothing but the secant method for $\sqrt{D}$.

We will add the above infinity point ∞ to $C_0(\mathbb{Q})$ and denote $C_0 \cup \{\infty\}$ by $\overline{C_0(\mathbb{Q})}$. Then $\overline{C_0(\mathbb{Q})}$ is considered as a multiplicative group by this new group law. Let K be the quadratic field $\mathbb{Q}(\sqrt{D})$. Let us consider the surjective map π from $K^\times$ to $\overline{C_0(\mathbb{Q})}$;

$$\pi : a - b\sqrt{D} \longrightarrow \left(\frac{a}{b}, \frac{a^2}{b^2} - D\right).$$

Then one can easily verify

$$(a_1 - b_1\sqrt{D})(a_2 - b_2\sqrt{D}) = (a_1a_2 + b_1b_2D) - (a_1b_2 + a_2b_1)\sqrt{D} \tag{2}$$

Combining (1) and (2), we can see the map π is a surjective homomorphism from $K^\times$ to $\overline{C_0(\mathbb{Q})}$. We note that ∞ is the unit element of $\overline{C_0(\mathbb{Q})}$ and the kernel of π is $\mathbb{Q}^\times$. Hence one knows $\overline{C_0(\mathbb{Q})} \cong K^\times/\mathbb{Q}^\times$. Let $[a + b\sqrt{D}]$ be the equivarent class $(a + b\sqrt{D})\mathbb{Q}^\times \in K^\times/\mathbb{Q}^\times$.

Theorem 2.1 *With the above notation*

$$\overline{C_0(\mathbb{Q})} \cong K^\times/\mathbb{Q}^\times,$$

where the isomorphism map is given by

$$\left(\frac{a}{b}, \frac{a^2}{b^2} - D\right) \to [a - b\sqrt{D}] = (a - b\sqrt{D})\mathbb{Q}^\times$$

One can relate $\overline{C_0(\mathbb{Q})}$ and $C_1(\mathbb{Q})$ by the following map

$$\left(\frac{a}{b}, \frac{a^2}{b^2} - D\right) \to [a - b\sqrt{D}] \to \frac{a - b\sqrt{D}}{a + b\sqrt{D}} \to \left(\frac{a^2 + Db^2}{a^2 - Db^2}, -\frac{2ab}{a^2 - Db^2}\right)$$

Here we shall recall Hilbert's theorem 90.

Proposition 2.2 *Let K/k be a finite Galois extension of fields with Galois group $G = \mathrm{Gal}(K/k)$. Then the first cohomology group of G, with coefficients in the multiplicative group of K, is trivial:*

$$H^1(G, K^\times) = 1.$$

Since the cohomological period of cyclic group is 2, we have the following corollary of Hilbert's theorem 90.

Corollary 2.3 *Let K be a finite cyclic extension of a field k with Galois group $G = \langle\sigma\rangle$. Here σ is a generator of G. Then any $a \in K^\times$ with $N_{K/k}(a) = 1$ is written in the form $a = b/b^\sigma$ for some $b \in K^\times$. Thus we have an isomorphism*

$$N_{K/k}^{-1}(1) = \{a \in K^\times \mid N_{K/k}a = 1\} \cong K^\times/k^\times$$

From this corollary, the above bijection is the isomorphism between $\overline{C_0(\mathbb{Q})}$ and $C_1(\mathbb{Q})$.

Theorem 2.4

$$\overline{C_0(\mathbb{Q})} \cong C_1(\mathbb{Q}),$$

where the isomorphism is given by

$$\left(\frac{a}{b}, \frac{a^2}{b^2} - D\right) \in \overline{C_0(\mathbb{Q})} \to \left(\frac{a^2 + Db^2}{a^2 - Db^2}, -\frac{2ab}{a^2 - Db^2}\right) \in C_1(\mathbb{Q})$$

In the following, we shall abbreviate $\left(\frac{a}{b}, \frac{a^2}{b^2} - D\right) \in \overline{C_0(\mathbb{Q})}$ to $P\left(\frac{a}{b}\right)$.

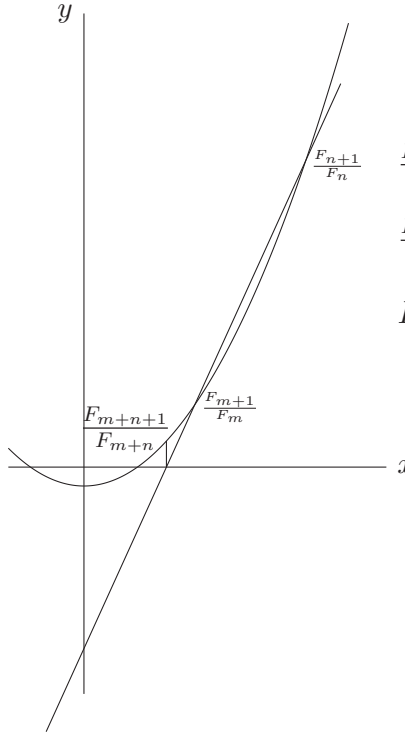
Remark 2.5 *We note that this new multiplicative structure is not compatible with the usual additive structure of* $C_0(\mathbb{Q})$. *For example,* $P(0) = (0, -D) = \left(\frac{0}{1}, -D\right)$ *is the* 0 *element in the additive structure. But the fact* $(-\sqrt{D})^2 = D \in \mathbb{Q}$ *shows* $P(0)$ *has the order* 2 *in the multiplicative group* $\overline{C_0(\mathbb{Q})}$.

Let C be the general rational parabola $y = ax^2 + bx + c = a(x - \alpha)(x - \beta)$, where $a, b, c \in \mathbb{Z}$ with the discriminant $D = b^2 - 4ac \neq \square$. Then one can verify the above multiplicative group structure on $\overline{C(\mathbb{Q})}$, where $C(\mathbb{Q}) = \{(x, f(x) \mid x \in \mathbb{Q}\}$, is generalized as follows:

$$(p/q, f(p/q) - \alpha) \in C_0(\mathbb{Q}) \to [p/q - \alpha] = [p - q\alpha] = (p - q\alpha)\mathbb{Q}^\times \in K^\times/\mathbb{Q}^\times.$$

This relation also induces the isomorphism between the groups of $\overline{C(\mathbb{Q})}$ and $K^\times/\mathbb{Q}^\times$. We shall pick up two examples as follows.

Example 2.6 *If* $f(x) = x^2 - x - 1$, *one can verify*

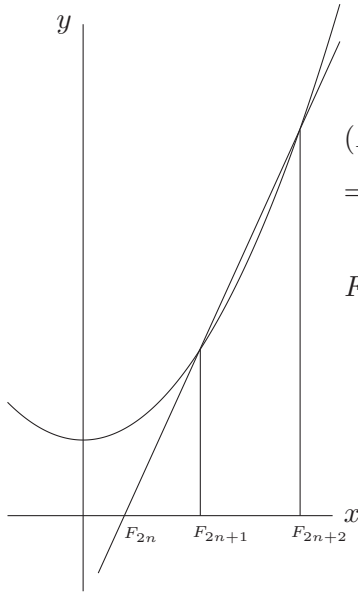


$\frac{F_{n+1}}{F_n}$ *satisies*

$$\frac{F_{n+1}}{F_n} \to [F_{n+1} - \varphi F_n] = [\bar{\varphi}^n],$$

$$P(\tfrac{F_{m+1}}{F_m}) * P(\tfrac{F_{n+1}}{F_n}) = P(\tfrac{F_{m+n+1}}{F_{m+n}})$$

Example 2.7 *The group structure is also defined for the case $D < 0$. For example, let us consider the case $f(x) = x^2 + 1$.*



$$(F_{2n+1} - \sqrt{-1})(F_{2n+2} - \sqrt{-1})$$
$$= F_{2n+3}(F_{2n} - \sqrt{-1})$$

From tangent addition formula, one knows

$$\frac{\frac{1}{F_{2n+1}} + \frac{1}{F_{2n+2}}}{1 - \frac{1}{F_{2n+1}F_{2n+2}}} = \frac{1}{F_{2n}}$$

Therefore we have verified

$$\tan^{-1}\left(\frac{1}{F_{2n+1}}\right) = \tan^{-1}\left(\frac{1}{F_{2n}}\right) - \tan^{-1}\left(\frac{1}{F_{2n+2}}\right).$$

Repeating this relations from $n = 0$ to ∞, one can verify the following well known Lenstra and Goggins's formula.

$$\frac{\pi}{2} = \sum_{n=0}^{\infty} \tan^{-1}\left(\frac{1}{F_{2n+1}}\right).$$

2.2 Newton's method and Halley's method

In this subsection, we shall restrict ourselves to the case $D > 0$. Let $y = f(x)$ be a real valued function and α be a root of the equation $f(x) = 0$. Then, in general, *Newton's method* is a root-finding algorithm which produces successively better approximations to the root α. Start with a value $x_0 = x$ with $f'(\alpha) \neq 0$ and sufficiently close to α satisfying $f'(x_0) \neq 0$. Put

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$$

Then $x_n \longrightarrow \alpha$ as $n \longrightarrow \infty$.

In the case $f(x) = x^2 - D$, it is easy to verify

$$x_{n+1} = \frac{1}{2}\left(x_n + \frac{D}{x_n}\right).$$

Assume $x_n = \dfrac{p}{q} \in \mathbb{Q}$. Then $x_{n+1} = \dfrac{p^2 + Dq^2}{2pq}$, and we have verified the following proposition.

Proposition 2.8 *Newton's method $x_n \to x_{n+1}$ for $\sqrt{D}$ satisfies*

$$P(x_{n+1}) = P(x_n) * P(x_n) = P(x_n)^2$$

Halley's method is another root-finding algorithm faster than Newton's method. Put $g(x) = \dfrac{f(x)}{\sqrt{|f'(x)|}}$. When $f'(\alpha) \neq 0$, one knows

$$f(\alpha) = 0 \Longleftrightarrow g(\alpha) = 0$$

Then $x_{n+1} = x_n - \dfrac{g(x_n)}{g'(x_n)}$ and $g'(x_n) = \dfrac{2|f'(x_n)|^2 - f(x_n)f''(x_n)}{2f'(x_n)\sqrt{|f'(x_n)}}$.

Applying Newton's methods for $g(x)$, Halley's method consists of a sequence of iterations:

$$x_{n+1} = x_n - \frac{2f(x_n)f'(x_n)}{2|f'(x_n)|^2 - f(x_n)f''(x_n)}.$$

In the case $f(x) = x^2 - D$, we have

$$x_{n+1} = \frac{x_n^3 + 3Dx_n}{3x_n^2 + D}.$$

Assume $x_n = \dfrac{p}{q} \in \mathbb{Q}$. Then $x_{n+1} = \dfrac{p^3 + Dpq^2}{3p^2q + Dq^3}$ and hence we have verified the following proposition.

Proposition 2.9 *Halley's methods $x_n \to x_{n+1}$ for $\sqrt{D}$ satisfies*

$$P(x_{n+1}) = (P(x_n) * P(x_n)) * P(x_n) = P(x_n)^3.$$

3 Secant methods and the simple continued fraction expansions of $\sqrt{D}$

In this section we restrict ourselves to the case $D > 0$. When the continued fraction expansions of $\sqrt{D}$ have the period length n, we shall write

$$\sqrt{D} = [a_0; \overline{a_1, \ldots, a_n}].$$

For $k \geq 1$, $\alpha_k > 1$ is defined by putting

$$\sqrt{D} = [a_0; a_1, \ldots, a_{k-1}, \alpha_k].$$

Then $a_k = [\alpha_k]$, where $a = [x]$ denotes the Gauss symbol., i.e. the maximal integer a satisfying $a \leq x$. There are two ways of indexing the kth convergents of the above continued fraction expansions. Here we adopt the indexing of Takagi [14], i.e., we will put as follows;

$$P_k = a_{k-1}P_{k-1} + P_{k-2}, \text{ with } P_{-1} = 0, P_0 = 1,$$

$$Q_k = a_{k-1}Q_{k-1} + Q_{k-2}, \text{ with } Q_{-1} = 1, Q_0 = 0.$$

Then kth convergent is defined by $\dfrac{P_k}{Q_k} = [a_0; a_1, \ldots, a_{k-1}]$ and satisfy;

$$\sqrt{D} = \frac{\alpha_k P_k + P_{k-1}}{\alpha_k Q_k + Q_{k-1}} \Longleftrightarrow \alpha_k = -\frac{P_{k-1} - Q_{k-1}\sqrt{D}}{P_k - Q_k\sqrt{D}}.$$

Here, for the sake of the readers who are not familiar with the sequences of convergents, we will list small values of P_k, Q_k in the following table.

k	-1	0	1	2	$\ldots$	n	$\ldots$
a_k		a_0	a_1	a_2	$\ldots$	$a_n = 2a_0$	$\ldots$
P_k	0	1	a_0	$a_1a_0 + 1$	$\ldots$	$P_n = a_{n-1}P_{n-1} + P_{n-2}$	$\ldots$
Q_k	1	0	1	a_1	$\ldots$	$Q_n = a_{n-1}Q_{n-1} + Q_{n-2}$	$\ldots$

Moreover $\alpha_{n-k+1} = -\dfrac{1}{\overline{\alpha_k}}$, which implies $a_n = 2a_0$ and the symmetrical property $a_{n-k} = a_k$ for $1 \leq k \leq n-1$. η_k denotes $P_k + Q_k\sqrt{D}$. Then $\eta_n = \varepsilon_D = P_n - Q_n\sqrt{D}$ is the fundamental unit of the order $\mathbb{Z}[\sqrt{D}]$ with the norm $(-1)^n$. For $0 \leq k \leq n$, k-th convergent satisfies the following property.

Theorem 3.1 *Take two points corresponding to the convergents*

$$P\left(\frac{P_k}{Q_k}\right) = \left(\frac{P_k}{Q_k}, \frac{P_k^2}{Q_k^2} - D\right) \text{ and } P\left(\frac{P_{n-k}}{Q_{n-k}}\right) = \left(\frac{P_{n-k}}{Q_{n-k}}, \frac{P_{n-k}^2}{Q_{n-k}^2} - D\right).$$

Then the line connecting two points intersects x-axis at the same point $\left(\dfrac{P_n}{Q_n}, 0\right)$*, that is,*

$$P\left(\frac{P_k}{Q_k}\right) * P\left(\frac{P_{n-k}}{Q_{n-k}}\right) = P\left(\frac{P_n}{Q_n}\right).$$

Proof. From Theorem 1.1, the assertion is equivalent to show $\eta_k\eta_{n-k} \in \varepsilon_D\mathbb{Q}^\times$. When $k = 0$, the assertion is true, because

$$\eta_0\eta_n = 1 \times (P_n - Q_n\sqrt{D}) = \varepsilon_D \in \varepsilon_D\mathbb{Q}^\times.$$

Assume the assertion is true for $k-1$, i.e., $\eta_{k-1}\eta_{n-k+1} \in \varepsilon_D\mathbb{Q}^\times$. Then $\alpha_{n-k+1}\overline{\alpha_k} = -1$ implies

$$\left(\frac{\eta_{k-1}}{\eta_k}\right)\left(\frac{\eta_{n-k+1}}{\eta_{n-k}}\right) = \frac{\alpha_k}{\alpha_{n-k+1}} = -\alpha_k\overline{\alpha_k} \in \mathbb{Q}^\times.$$

Hence the assertion is true for k, because

$$\eta_k\eta_{n-k} = -\frac{\eta_{k-1}\eta_{n-k+1}}{\alpha_k\overline{\alpha_k}} \in \varepsilon_D\mathbb{Q}^\times, \text{ which completes the proof.}$$

Since $\eta_{nt+k} = (\eta_n)^t\eta_k$, we can generalize the above assertion as follows.

Proposition 3.2 *For any natural numbers i, j, m which satisfy $i + j = mn$,*

$$P\left(\frac{P_i}{Q_i}\right) * P\left(\frac{P_j}{Q_j}\right) = P\left(\frac{P_n}{Q_n}\right)^m = P\left(\frac{P_{mn}}{Q_{mn}}\right)$$

Modifying the proof of the above theorem, we can also prove the following lemma.

Lemma 3.3 *For any* $1 \leq k \leq n-1$,

$$\eta_k\eta_{n-k+1} - \eta_{k-1}\eta_{n-k} \in \varepsilon_D\mathbb{Q}.$$

Proof. From the definition, we have

$$\eta_{k+1} = a_k\eta_k + \eta_{k-1}, \eta_{n-k-1} = -a_k\eta_{n-k} + \eta_{n-k+1}.$$

Multilying the both sides each other, we have

$$\eta_{k+1}\eta_{n-k-1} = -a_k^2\eta_k\eta_{n-k} + \eta_{k-1}\eta_{n-k+1} + a_k(\eta_k\eta_{n-k+1} - \eta_{k-1}\eta_{n-k}).$$

Hence

$$\eta_k\eta_{n-k+1}-\eta_{k-1}\eta_{n-k} = (\eta_{k+1}\eta_{n-k-1}+a_k^2\eta_k\eta_{n-k}-\eta_{k-1}\eta_{n-k+1})/a_k \in \varepsilon_D\mathbb{Q}.$$

From this lemma, theorem 3.1 which is established for convergents can be generalized to the following proposition which is established for intermediate convergents.

Proposition 3.4 *For any* $1 \leq k \leq n-1$ *and any integer* $0 < b_k < a_k$, *the points corresponding to the intermediate convergents satisfy*

$$P\left(\frac{b_kP_k + P_{k-1}}{b_kQ_k + Q_{k-1}}\right) * P\left(\frac{(a_k - b_k)P_{n-k} + P_{n-k-1}}{(a_k - b_k)Q_{n-k} + Q_{n-k-1}}\right) = P\left(\frac{P_n}{Q_n}\right).$$

Proof. Put

$$\xi_{k+1} = b_k\eta_k+\eta_{k-1}, \xi_{n-k+1} = (a_k-b_k)\eta_{n-k}+\eta_{n-k-1} = \eta_{n-k+1}-b_k\eta_{n-k}.$$

Then

$$\xi_{k+1}\xi_{n-k-1} = -b_k^2\eta_k\eta_{n-k} + \eta_{k-1}\eta_{n-k+1} + b_k(\eta_k\eta_{n-k+1} - \eta_{k-1}\eta_{n-k}).$$

From the above lemma $\xi_{k+1}\xi_{n-k-1} \in \varepsilon_D\mathbb{Q}$. Since $\xi_{k+1}\xi_{n-k-1} \neq 0$, $\xi_{k+1}\xi_{n-k-1} \in \varepsilon_D\mathbb{Q}^\times$, which means the corresponding rational points satisfy the claim of this proposition.

Remark 3.5 *The case cases $b_k = 0$ and $b_k = a_k$ in this proposition coincide with the above formula on convergents of Theorem 3.1.*

Now we shall refer similar results also hold for the case $f(x) = x^2 - x + \frac{1-D}{4}$, where D is a positive non square integer with $D \equiv 1 \pmod 4$. Let C_0 be the parabola $y = f(x) = x^2 - x - \frac{1-D}{4}$. Then we denote the rational point on C_0 by

$$P(p/q) = (\frac{p}{q}, f(\frac{p}{q})).$$

If the period of the continued fraction expansions of $\omega = \frac{1+\sqrt{D}}{2}$ is n. ω is written in the form

$$\omega = [a_0; \overline{a_1, \ldots, a_n}],$$

where $a_n = 2a_0 - 1$ and $a_{n-k} = a_k$ for the cases $1 \leq k \leq n-1$. Then P_k, Q_k are defined by putting $P_{-1} = 0, P_0 = 1, Q_{-1} = 1, Q_0 = 0$ and $P_{k+1} = a_k P_k + P_{k-1}$ and $Q_{k+1} = a_k Q_k + Q_{k-1}$ for $k \geq 0$. Then $P_n - Q_n\omega$ satisfies $N_{k/\mathbb{Q}}(P_n - Q_n\omega) = P_n^2 - PnQ_n + \frac{(1-D)Q_n^2}{4} = (-1)^n$ and hence the fundamental unit ε_D of the order $\mathbb{Z}[\omega]$ of $K = \mathbb{Q}(\sqrt{D})$. Putting $\eta_k = P_k - Q_k\omega$, one can verify

$$\eta_k \eta_{n-k} \in \eta_n \mathbb{Q}^\times = \varepsilon_D \mathbb{Q}^\times$$

for $0 \leq k \leq n$. Similar to the case $f(x) = x^2 - D$, we can show the following propositions.

Theorem 3.6 *For any $0 \leq k \leq n$, $P(p/q) = (\frac{p}{q}, \frac{p^2}{q^2} - \frac{p}{q} + \frac{1-D}{4})$ satisfies*

$$P\left(P_k/Q_k\right) * P\left(P_{n-k}/Q_{n-k}\right) = P\left(P_n/Q_n\right).$$

Proposition 3.7 *For any $1 \leq k \leq n-1$ and any integer $0 < b_k < a_k$, the points $P(p/q) = (\frac{p}{q}, \frac{p^2}{q^2} - \frac{p}{q} + \frac{1-D}{4})$ corresponding to the intermediate convergents satisfy*

$$\begin{aligned} &P\left((b_kP_k + P_{k-1})/(b_kQ_k + Q_{k-1})\right) \\ &*P\left(((a_k - b_k)P_{n-k} + P_{n-k-1})/((a_k - b_k)Q_{n-k} + Q_{n-k-1})\right) \\ &= P\left(P_n/Q_n\right). \end{aligned}$$

4 Algebraic tori

We shall show that $\overline{C_0(\mathbb{Q})}$ and $C_1(\mathbb{Q})$ are the rational points of certain algebraic tori. Firstly, we shall recall several definitions and notations of algebraic tori. Let k be an algebraic number field and K be its finite extension and $R_{K/k}$ be Weil restriction from K to k. There exists an exact sequence of algebraic tori defined over k.

$$1 \to R^{(1)}_{K/k}(G_m) \to R_{K/k}(G_m) \stackrel{N}{\to} G_m \to 1,$$

where N is the norm map from K to k and $R^{(1)}_{K/k}(G_m)$ is its kernel. Similarly there exists the following exact sequence of algebraic tori

$$1 \to G_m \to R_{K/k}(G_m) \to R_{K/k}(G_m)/G_m \to 1.$$

When K is a quadratic field $\mathbb{Q}(\sqrt{D})$ and $k = \mathbb{Q}$, we denote $R_{K/\mathbb{Q}}(G_m)/G_m$ and $R^{(1)}_{K/\mathbb{Q}}(G_m)$ by T_0 and T_1, respectively. Then $\overline{C_0(\mathbb{Q})} \cong T_0(\mathbb{Q})$ by the following homomorphism

$$\left(\frac{a}{b}, \frac{a^2}{b^2} - D\right) \in C_0(\mathbb{Q}) \to [a - b\sqrt{D}] \in K^\times/\mathbb{Q}^\times = T_0(\mathbb{Q}).$$

Similarly $C_1(\mathbb{Q}) \cong T_1(\mathbb{Q})$ by the following map

$$(x, y) \in C_1(\mathbb{Q}) \to x + y\sqrt{D} \in T_1(\mathbb{Q}).$$

Theorem 4.1 *With the above notation, we have*

$$\overline{C_0(\mathbb{Q})} \cong T_0(\mathbb{Q}) \cong T_1(\mathbb{Q}) \cong C_1(\mathbb{Q}).$$

Through these isomorphisms, one can define the local factor for each prime in K. Adelizations of these Euler factors imply the zeta functions and then the class numbers h_{C_0} of C_0 and h_{C_1} of C_1 as algebraic tori. In his paper [7], F. Lemmermeyer investigated another approach to the Pell conics C_1 and calculated the class number h_{C_1} directly. Finally he found the following relative class number formula for h_K and h_{C_1}.

$$\frac{h_K}{h_{C_1}} = \begin{cases} 2^{t_K-1} & D<0 \text{ or } D>0 \text{ and } N_{K/\mathbb{Q}}\, O_K^\times = \{\pm 1\}, \\ 2^{t_K-2} & D>0 \text{ and } N_{K/\mathbb{Q}}\, O_K^\times = \{1\}, \end{cases}$$

where t_K is the number of distinct primes which sprits in K and $O_K^\times$ is the unit group of K.

Now we shall recall fundamental results on the class numbers of algebraic tori. The class number relation of isogenous tori was firstly investigated by J. M. Shyr in his paper [14]. Later, using Shyr's formula on Tamagawa numbers of isogeneous tori, T. Ono and others(such as R. Sasaki, M. Morishira, V. E. Voskresenskii and the author) investigated the class number relations more precisely as follows.

We note that the class numbers of algebraic tori $R_{K/k}(G_m)$ and G_m are the usual class number of algebraic number fields K and k and denoted h_K and h_k, respectively. The isogeny between $R_{K/k}(G_m)$ and $R^{(1)}_{K/k}(G_m) \times G_m$ implies the class number relation of h_K, h_k and $h_{K/k}$, where $h_{K/k}$ denotes the class number of norm one torus $R^{(1)}_{K/k}(G_m)$. T. Ono defined the following Euler number $E(K/k)$ in his paper [11];

$$E(K/k) = \frac{h_K}{h_{K/k} h_k}.$$

Similarly, we defined $E'(K/k)$ in [3] based on the following exact sequence of algebraic tori.

$$1 \to G_m \to R_{K/k}(G_m) \to R_{K/k}/G_m \to 1.$$

Let $h'_{K/k}$ be the class number of the above algebraic tori $R_{K/k}(G_m)/G_m$. Another arithmetic invariant $E'(K/k)$ is defined by putting

$$E'(K/k) = \frac{h_K}{h'_{K/k} h_k}.$$

Since $E(K/k) = E'(K/k)$ for any cyclic extension K/k, we have rediscovered the following formulae for the cases $K = \mathbb{Q}(\sqrt{D})$ and

$k = \mathbb{Q}$;

$$\frac{h_K}{h(C_1)} = \frac{h_K}{h_{\mathbb{Q}} h(T_1)} = E(K/\mathbb{Q}) = E'(K/\mathbb{Q}) = \frac{h_K}{h_{\mathbb{Q}} h(T_0)} = \frac{h_K}{h(C_0)}.$$

Thus we have shown a geometrical interpretation of Gauss's genus theory for conics defined over $\mathbb{Q}$.

5 Height of the rational points on C_0

5.1 Height of the rational points

Here we shall define the height of the rational point $P\left(\frac{a}{b}\right) = (\frac{a}{b}, \frac{a^2}{b^2} - D)$ in $C_0(\mathbb{Q})$. Let x be a rational number written in lowest terms $x = \frac{a}{b}$. Then the naive height $H(x)$ of x is defined by $H(x) = \log \max\{|a|, |b|\}$ as usual. Denote $a_0 = a$ and $b_0 = b$. Scince 2-Desent of P is the Newton's method for P, $P\left(\frac{a_{k+1}}{b_{k+1}}\right) = P\left(\frac{a_k}{b_k}\right)^2$ means

$$[a_{k+1} - b_{k+1}\sqrt{D}] = [(a_k - b_k\sqrt{D})^2] = [(a_k^2 + Db_k^2) - 2a_k b_k \sqrt{D}].$$

In the case $D > 0$, one sees $a_k > |b_k| > 1$ for $k \geq 1$. Hence $H\left(P\left(\frac{a_k}{b_k}\right)\right) = \log |a_k|$ for $k \geq 1$. Canonical height $\hat{h}(P)$ of $P = P\left(\frac{a}{b}\right)$ is defined by putting

$$\hat{h}(P) = \lim_{n\to\infty} \frac{H\left(P\left(\frac{a_n}{b_n}\right)\right)}{2^n}$$

Therefore

$$\hat{h}(P) = \lim_{n\to\infty} \frac{\log |a_n|}{2^n}.$$

In the case $D \equiv 2, 3 \pmod 4$, put $\xi = a + b\sqrt{D}$ and $\xi_1 = |a_1| + |b_1|\sqrt{D}$. Then $|\bar{\xi}| = ||a_1| - |b_1|\sqrt{D}|| < |\xi_1|$. ξ_k denote $\xi_k = |a_k| + |b_k|\sqrt{D}$ and $\bar{\xi_k} = |a_k| - |b_k|\sqrt{D}$. Then a_1 and b_1 are coprime, and

inductively we get $\xi_k = \xi_1^{2^{k-1}}$ for $k \geq 1$. Since $|a_k| = (\xi_1{}^{2^{k-1}} + \bar{\xi_1}{}^{2^{k-1}})/2 = \xi_1{}^{2^{k-1}}(1 + (\bar{\xi_1}/\xi_1)^{2^{k-1}})/2$,

$$\hat{h}(P) = \lim_{n\to\infty} \frac{\log|a_n|}{2^n} = \lim_{n\to\infty} \frac{2^{n-1}\log|\xi_1| + \log(1 + (\bar{\xi_1}/\xi_1)^{2^{n-1}}) - \log 2}{2^n}$$

$$= \frac{\log|\xi_1|}{2} = \frac{\log(|a_1| + |b_1|\sqrt{D})}{2}.$$

In the case $D \equiv 1 \pmod 4$, we must substitute ξ_1 to $\frac{|a_1|+|b_1|\sqrt{D}}{2}$ Then $|\bar{\xi_1}| = |\frac{|a_1|-|b_1|\sqrt{D}|}{2}| < |\xi_1|$. ξ_k denote $\xi_k = \frac{|a_k|+|b_k|\sqrt{D}}{2}$. Then

$$\hat{h}(P) = \lim_{n\to\infty} \frac{\log|a_n|}{2^n} = \lim_{n\to\infty} \frac{2^{n-1}\log|\xi_1| + \log(1 + (\bar{\xi_1}/\xi_1)^{2^{n-1}}) - \log 2}{2^n}$$

$$= \frac{\log|\xi_1|}{2} = \frac{\log(\frac{a_1|+|b_1|\sqrt{D}}{2})}{2}.$$

Now we shall consider the cases $D < 0$. In the cases $D \equiv 2, 3 \pmod 4$, put $\xi_1 = |a_1| + |b_1|\sqrt{D}$. Then $|\xi_1| = \sqrt{a_1^2 - Db_1^2}$ and $\xi_k = \xi_1^{2^{k-1}} = |a_k| + |b_k|\sqrt{D}$ and $H\left(P\left(\frac{a_k}{b_k}\right)\right) = \log\max(|a_k|, |b_k|)$. If $|a_k| > |b_k|$,

$$a_k^2 < |\xi_k|^2 = a_k^2 - Db_k^2 < 2a_k^2.$$

Hence

$$\log(|\xi_k|/\sqrt{2}) < \log|a_k| = H\left(P\left(a_k/b_k\right)\right) < \log|\xi_k|.$$

If $|a_k| < |b_k|$,

$$|D|b_k^2 < |\xi_k|^2 = a_k^2 - Db_k^2 < (|D| + 1)b_k^2.$$

Hence

$$\log(|\xi_k|/\sqrt{|D| + 1}) < \log|b_k| = H(P(a_k/b_k) < \log(|\xi_k|/\sqrt{|D|}).$$

Using squeeze theorem

$$\hat{h}(P) = \lim_{n\to\infty} \frac{H\left(P\left(\frac{a_n}{b_n}\right)\right)}{2^n} = \lim_{n\to\infty} \frac{\log|\xi_1|^{2n-1}}{2^n} = \frac{\log|\xi_1|}{2}.$$

In the cases $D \equiv 1 \pmod 4$, substituting ξ_1 to $\frac{|a_1|+|b_1|\sqrt{D}}{2}$, one can similarly get the same conclusion

$$\hat{h}(P) = \frac{\log|\xi_1|}{2}.$$

Now we shall compare the corresponding heights defined by F. Lemmermeyer in his paper [7]. For the sake of simplicity, we restrict ourselves to the case $D > 0$ and $D \equiv 2, 3 \pmod 4$, because other cases can be verified in the similar manner. Recall the isomorphisms as follows;

$$\overline{C_0(\mathbb{Q})} \cong K^\times/\mathbb{Q}^\times \cong N_{K/\mathbb{Q}}^{-1}(1) \cong C_1(\mathbb{Q}),$$

where

$$\left(\frac{a_k}{b_k}, \frac{a_k^2}{b_k^2} - D\right) \mapsto [a_k - b_k\sqrt{D}] \mapsto \left(\frac{a_k - b_k\sqrt{D}}{a_k + b_k\sqrt{D}}\right)$$

$$= \left(\frac{a_k^2 + Db_k^2 - 2a_kb_k\sqrt{D}}{a_k^2 - Db_k^2}\right) = \left(\frac{a_{k+1} - b_{k+1}\sqrt{D}}{c_{k+1}}\right)$$

$$\mapsto \left(\frac{a_{k+1}}{c_{k+1}}, -\frac{b_{k+1}}{c_{k+1}}\right), \text{ where } \frac{a_{k+1}}{b_{k+1}} \text{ in lowest terms}$$

with $a_{k+1}^2 - Db_{k+1}^2 = c_{k+1}^2$.

The 2-Decents of $C_0(\mathbb{Q})$ and $C_1(\mathbb{Q})$ satisy

$$\begin{array}{ccccc}
\left(\frac{a_k}{b_k}, \frac{a_k^2}{b_k^2} - D\right) & \in C_0(\mathbb{Q}) & \longleftrightarrow & \left(\frac{a_{k+1}}{c_{k+1}}, -\frac{b_{k+1}}{c_{k+1}}\right) & \in C_1(\mathbb{Q}) \\
\downarrow & \text{2-Decent} & & \downarrow & \text{2-Decent} \\
\left(\frac{a_k}{b_{k+1}}, \frac{a_{k+1}^2}{b_{k+1}^2} - D\right) & & \longleftrightarrow & \left(\frac{a_{k+2}}{c_{k+2}}, -\frac{b_{k+2}}{c_{k+2}}\right) &
\end{array}$$

Let us denote $P_k = \left(\frac{a_k}{b_k}, \frac{a_k^2}{b_k^2} - D\right)$ and $\tilde{P}_k = \left(\frac{a_{k+1}}{c_{k+1}}, -\frac{b_{k+1}}{c_{k+1}}\right)$. Then naive heights satify $H(\tilde{P}_k) = H(P_{k+1}) = 2H(P_k)$. Denote $P = \left(\frac{a}{b}, \frac{a^2}{b^2} - D\right) \in C_0(\mathbb{Q})$, and corresponding $\tilde{P} = \left(\frac{a_1}{c_1}, -\frac{b_1}{c_1}\right) \in$

$C_1(\mathbb{Q})$. Thus the canonical heights of corresponding rational points on each conic satisfy $\hat{h}(\tilde{P}) = 2\hat{h}(P)$. One can easily verify similar results also hold for other cases $D > 0$, $D \equiv 1 \pmod 4$ and $D < 0$.

Theorem 5.1 *Let us denote* $P = \left(\frac{a}{b}, \frac{a^2}{b^2} - D\right) \in C_0(\mathbb{Q})$, *and corresponding* $\tilde{P} = \left(\frac{a_1}{c_1}, -\frac{b_1}{c_1}\right) \in C_1(\mathbb{Q})$. *Then the canonical heights satisfy* $\hat{h}(\tilde{P}) = 2\hat{h}(P)$.

Remark 5.2 *Though it holds for all cases, we restrict ourselves to the cases* $D(\equiv 1 \pmod 4) > 0$. *We shall explain the reason why we don't use* (a, b), *but use* (a_1, b_1). $\mathrm{GCD}\ (a, b) = 1$ *don't imply* $\mathrm{GCD}(a^2 + Db^2, 2ab) = 1$, *but* $\mathrm{GCD}(a_1, b_1) = 1$ *imply* $\mathrm{GCD}(a_1^2 + Db_1^2, 2a_1b_1) = 1$. *For example, consider the case* $D = 6, a = 2, b = 1$.

$$(2 - \sqrt{6})^2 = 2(5 - 2\sqrt{6}), (5 - 2\sqrt{6})^2 = 49 - 20\sqrt{6}.$$

Thus $a_1 = 5, b_1 = 2$ *and* $a_2 = 49, b_2 = 20$ *for this case.*

Remark 5.3 *Assume* D *is square free and* $D \equiv 2, 3 \pmod 4$ *and the period length of the continued fraction expansion of* $\sqrt{D}$ *is even* $n = 2m$. *Then the point* $\left(\frac{P_m}{Q_m}, \frac{P_m^2}{Q_m^2} - D\right)$ *in* $C_0(\mathbb{Q})$ *which corresponding to* m*-th convergent satisfy*

$$\left(\frac{P_m}{Q_m}, \frac{P_m^2}{Q_m^2} - D\right) \longrightarrow \frac{P_m - Q_m\sqrt{D}}{P_m + Q_m\sqrt{D}} = (-1)^m(P_n - Q_n\sqrt{D}).$$

5.2 Canberra distance

Let $x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n) \in \mathbb{R}^n$. Then the Canberra distance $d(x, y)$ is defined by

$$d(x, y) = \sum_{i=1}^{n} \frac{|x_i - y_i|}{|x_i| + |y_i|}.$$

T. Yoshida defined the distance $d(\frac{a}{b}, \sqrt{D})$ for the rational point $\left(\frac{a}{b}, \frac{a^2}{b^2} - D\right) \in C_0(\mathbb{Q})$, by putting

$$d\left(\frac{a}{b}, \sqrt{D}\right) = \left|\frac{\frac{a}{b} - \sqrt{D}}{\frac{a}{b} + \sqrt{D}}\right| = \left|\frac{a - b\sqrt{D}}{a + b\sqrt{D}}\right|.$$

He explained the relation of Newton's formula for $\sqrt{D}$ and this distance as follows

$$\begin{array}{ccccc} \left(\frac{a_k}{b_k}, \frac{a_k^2}{b_k^2} - D\right) & \in C_0(\mathbb{Q}) & \longleftrightarrow & d\left(\frac{a_k}{b_k}, \sqrt{D}\right) & \\ \downarrow & \text{Newton's method} & & \downarrow & \text{2-Decent} \\ \left(\frac{a_k}{b_{k+1}}, \frac{a_{k+1}^2}{b_{k+1}^2} - D\right) & & \longleftrightarrow & d\left(\frac{a_{k+1}}{b_{k+1}}, \sqrt{D}\right) & \end{array}$$

From the above argument, one can consider Yosida's distance is the usual abosolute value of corresponding value in $N_{K/\mathbb{Q}}^{-1}(1)$ through the isomorphism between $C_0(\mathbb{Q})$.

6 Class number one problem for algebraic tori

Let $H^+(K)$ be the class group in the narrow sense of a quadratic field $K = \mathbb{Q}(\sqrt{D})$. Then the class group of T_0 and T_1 is isomorphic to $(H^+(K))^2$ (see for example [7]). We note that the class group of C_0 and C_1 is isomorphic to $(H^+(K))^2$ as in the section 4. Let us consider the class number one problem of C_0(or C_1), i.e., to determine the algebraic torus T_0(or T_1) with class number one.

From Gauss's genus theorem, or the calculations of Ono's Euler number $E(K/\mathbb{Q})$, we have

$$\begin{array}{lll} h_{K/\mathbb{Q}} = 1 \iff & h_K = 2^{t_K - 1} & \text{, when } D < 0 \\ & & \text{or when } D > 0 \text{ and } K = \mathbb{Q}(\sqrt{D}) \\ & & \text{with the fundamental unit of norm } -1, \\ & h_K = 2^{t_K - 2} & \text{, when } D > 0 \text{ and } K = \mathbb{Q}(\sqrt{D}) \\ & & \text{with the fundamental unit of norm } 1. \end{array}$$

Since $h_{K/\mathbb{Q}} = |(H^+(K))^2|$ is the number of classes in each genus, class number one problem of $T_0 = R_{K/\mathbb{Q}}G_m/G_m$ or C_0 is the determination of such quadratic fields. In his paper [19], P. J. Weinberger investigated imaginary quadratic fields with a single class in each genus and showed that there are at most 68 such imaginary quadratic fields by using Tatuzawa's lower bound for $L(1,\chi)$. In [1], K. Dohmae determined real quadratic fields(of narrow R-D type) with a single class in each genus and shows that there are at most 70 such fields also using Tatuzawa's lower bound.

Proposition 6.1 ([1] **and** [19]) *Let K be imaginary quadratic fields. Then $h_{K/\mathbb{Q}} = 1$ for at most 68 norm 1 tori $R^{(1)}_{K/\mathbb{Q}}G_m$(or $R_{K/\mathbb{Q}}G_m/G_m$).*

Let K be real quadratic fields of narrow R-D type. Then $h_{K/\mathbb{Q}} = 1$ at most 70 norm 1 tori $R^{(1)}_{K/\mathbb{Q}}G_m$(or $R_{K/\mathbb{Q}}G_m/G_m$).

Remark 6.2 *Discriminants of the known imaginary quadratic fields with 1 class per genus are listed A003644 in Online Encyclopedia of Integer Sequences. Since the list depends on Siegel's bound (see Tatuzawa [16]), there may exist at most one more such discriminant not contained in the list. If one assumes that the generalized Rieman hypothesis is true, the list is complete.*

If $h_K = 1$, then $h_{K/\mathbb{Q}} = 1$ and $E_{K/\mathbb{Q}} = E'_{K/\mathbb{Q}} = 1$ for quadratic fields K. Thus the conjecture that there exist infinitely many real quadratic fields with class number one imply a natural weak conjecture that there exist infinitely many real quadratic fields with 1 class per genus. More precisely, $(H^+(K))^2 = 0$ means the narrow ideal class group of K is elementary abelian $2-$group. The distribution of such quadratic fields are the special cases of Cohen-Lenstra heuristic.

These results are slightly generalized to the following setting. Let K be a CM extension of the totally real number field $k = K^+$. Then the class number $h = h_K$ is divided by $h^+ = h_k$ and the quotient h/h^+. h/h^+ is called the relative class number and usually denoted by h^-. Then $h_{K/k}$ the class number of norm 1 tori $R^{(1)}_{K/k}(G_m)$ also divides h^-. Especially the class number one problem of $h_{K/k}$

for cyclotomic extension K is reduced to the determination of cyclotomic extensions with 2-power h^-, which was investigated by K. Horie around 1990. Discriminants of imaginary fields whose class group has exponent 2 are listed A316743 in Online Encyclopedia of Integer Sequences.

References

[1] K. Dohmae, On real quadratic fields with a single class in each genus, *Jap. J. Math.*, New Ser. **19** (1993), 241=250.

[2] A. Dujella, Newton's formula and the continued fraction expansion of $\sqrt{d}$, *Experiment. Math.*, **10** (1) (2001), 125-131..

[3] S. Katayama, Class number relations of algebraic tori I, *Proc. Japan Acad.*, **62 A** (1986), 216-218.

[4] S. Katayama, $E(K/k)$ and other arithmetical invariants for finite Galois extensions. *Nagoya Math. J.*, **114** (1989), 135-142.

[5] S. Katayama, Diophantine Equations and Hilbert's Theorem 90, *J. Math. Univ. Tokushima*, **48** (2014), 1-6..

[6] T. Komatsu, Continued fractions and Newton's approximations, *Math. Communications*, **4** (1999), 167–176.

[7] F. Lemmermeyer, Conics - a Poor Man's Elliptic Curves, *Preprint*, arXiv:math/0311306, (2003).

[8] J. Mikusiński, Sur la méthode d'approximation de Newton, *Annales Polonici Mathematici* **1**, 184-194, (1955)

[9] T. Ono, Arithmetic of algebraic tori, *Ann. Math.*, **74** (1961), 101-139.

[10] T. Ono, On the Tamagawa number of algebraic tori. *Ann. Math.*, **78** (1963), 47-73.

[11] T. Ono, On some class number relations for Galois extensions, *Proc. Japan Acad.* , **61 A** (1985), 311-312.

[12] T. Ono, On some class number relations for Galois extensions, *Nagoya Math. J.*, **107** (1987), 121-133.

[13] R. Sasaki, Some remarks to Ono's theorem on a generalization of Gauss' genus theory, *Nagoya Math. J.*, **111** (1988), 131-142.

[14] J. M. Shyr, On some class number relations of algebraic tori. *Michigan Math. J.*, **24** (1977), 365-377.

[15] T. Takagi, Lectures on Elementary Number Theory, Kyoritsu Tosho, Tokyo, 1971 (2nd ed. in Japanese).

[16] T. Tatuzawa, On a theorem of Siegel, Jap. J. Math. **21** (1951), 163-178.

[17] V. E. Voskresenskii, Algebraic Groups and Their Birational Invariants, Translations of Mathematical Monographs 179, American Mathematical Society 1998.

[18] A. Weil, Adeles and Algebraic Groups, Birkhauser, 1982.

[19] P. J. Weinberger, Exponents of class groups of complex quadratic fields, *Acta Arith.* **22** (1973), 117-124.

[20] T. Yoshida, Newton's methods of approximation and related area 1, 2, *Sugaku Seminar*, **704**, **705** (2020), 50-56, 44-49 (in Japanese).

[21] The On-Line Encyclopedia of Integer Sequences, http://www.oeis.org, [On line; accessed 18 September 2024].