CONTINUED FRACTIONS AND INDEFINITE BINARY QUADRATIC FORMS OVER $\mathbb{F}_q[t]$

JORGE MORALES

Abstract. The relation between cycles of indefinite binary quadratic forms over $\mathbb{Z}$ and continued fractions is classical and well-known. We describe a similar relation for binary quadratic forms over the polynomial ring $\mathbb{F}_q[t]$, where q is a power of an odd prime. In this context, the cycles of the classical theory are replaced by orbits of the metacyclic group $\mathbb{F}_q^* \rtimes \mathbb{Z}$ acting on the set of reduced forms of a given discriminant, where each orbit corresponds to a proper equivalence class.

Introduction

Gauss, in his celebrated *Disquisitiones* [6, Art. 183–184], defined the notion of a *reduced form* for indefinite binary quadratic forms over $\mathbb{Z}$ and showed that every such form is properly equivalent to a reduced one by an explicit algorithm (two forms are properly equivalent if related by an integer change of variables with determinant +1). However, the reduced representatives are not unique; instead, they are organized into cycles, with each cycle corresponding to a proper equivalence class.

The relation between Gauss's cycles and simple regular continued fractions is classical but rather convoluted. See, for instance, [5, Ch. 8] or [2, §3.3] for more details.

Zagier [16] observed that with a modified definition of a reduced form, there is a clean and straightforward correspondence between cycles of reduced forms and so-called *negative* simple continued fractions. This idea was already present in a short communication by De la Vallée Poussin [3]. Negative continued fractions allow one to remain within the special linear group $\mathbf{SL}(2,\mathbb{Z})$, thereby avoiding the complications of improper equivalence.

At the referee's suggestion, I have included in Section 1 an overview—without proofs—of the theory of negative regular continued fractions and their relation to the classification of indefinite binary quadratic forms over $\mathbb{Z}$. Readers already familiar with this material may wish to skip this section and proceed directly to Section 2.

We adopt the 'negative' continued fraction perspective to address the case of indefinite quadratic forms over the ring $A = \mathbb{F}_q[t]$, where $\mathbb{F}_q$ is the finite field with q elements, and q is a power of an odd prime. The results we obtain mirror the classical results over $\mathbb{Z}$.

2020 *Mathematics Subject Classification.* Primary: 11E16 , 11J70. Secondary: 11G20, 11R29 .

Section 2 develops the results on continued fractions necessary for the reduction theory of indefinite quadratic forms. Continued fraction expansions of Laurent series are well-studied in the literature, but predominantly over $\mathbb{C}$ or in characteristic 0. We prove (Theorem 2.10) an analogue for Laurent series of Serret's classical theorem on $\mathbf{GL}(2,\mathbb{Z})$-equivalence of real irrationals [11, Satz 2.4]. We have included details specifically addressing the finite field case, such as the periodicity of expansions of quadratic surds (Proposition 2.16). Notably, although these results are certainly not unexpected, they do not appear to be explicitly documented in the literature. The main result in this section is the classification of quadratic surds of fixed discriminant up to $\mathbf{SL}(2,A)$-equivalence (Theorem 2.20 and Proposition 2.21).

In Section 3, we define an $\mathbf{SL}(2,A)$-compatible correspondence between quadratic surds and indefinite binary quadratic forms via their principal root (Proposition 3.1). Continued fractions provide, by means of this correspondence, a reduction algorithm for quadratic forms (Theorem 3.5). Starting with any form, this algorithm eventually enters a cycle of reduced forms properly equivalent to the initial one.

However, unlike the case over $\mathbb{Z}$, different cycles may contain properly equivalent forms, but this is controlled by a natural action of the multiplicative group $\mathbb{F}_q^*$ on the set of reduced forms (Corollary 3.11). This situation is formalized by defining an action of the metacyclic group $\mathbb{F}_q^* \rtimes \mathbb{Z}$ on the set of reduced forms. The orbits for this action are in one-to-one correspondence with the proper equivalence classes (Theorem 3.12).

We conclude Section 2 by recalling the relation of binary quadratic forms with Picard groups and the class group of divisors of degree 0 of the associated hyperelliptic curve. Explicit numerical examples are provided at the end.

I am grateful to the referee for a careful review and helpful comments.

Notation

Symbol	Meaning
$\mathbb{F}_q$	A finite field of characteristic $\neq 2$ and order q
A	The polynomial ring $\mathbb{F}_q[t]$
K	The field of fractions $\mathbb{F}_q(t)$
v_∞	The normalized valuation at infinity on K.
$\lvert\ \rvert_\infty$	The absolute value at infinity on K i. e. $\lvert x\rvert_\infty = q^{-v_\infty(x)}$.
K_∞	The completion of K with respect to $\lvert\ \rvert_\infty$
	i.e. the field $\mathbb{F}_q((t^{-1}))$ of formal Laurent series in t^{-1} over $\mathbb{F}_q$
O_∞	The ring $\mathbb{F}_q[[t^{-1}]]$ of formal power series in t^{-1} over $\mathbb{F}_q$
P_∞	The valuation ideal $t^{-1}\mathbb{F}_q[[t^{-1}]]$

1. Negative regular continued fractions over $\mathbb{Z}$

This is an overview of the main results of the theory of negative regular continued fractions (NRCFs for short) over $\mathbb{Z}$ and its relation to the theory

of binary quadratic forms. The most comprehensive reference for NRCFs remains the paper by Erna Zurl [18]. For the relation with quadratic forms, we refer to Zagier [16].

Let $a_0, a_1, \ldots, a_n$ be a finite sequence of integers with $a_i \geq 2$ for $i \geq 1$. The symbol $[\![\, a_0, a_1, \ldots, a_n \,]\!]$ denotes the expression

$$a_0 + \cfrac{-1}{a_1 + \cfrac{-1}{\ddots + \cfrac{-1}{a_n}}} \tag{1}$$

which we call a *negative regular continued fraction* or *"minus" continued fraction.*

It is not difficult to see that if $\{a_n\}_{n\geq 0}$ is an infinite sequence of integers with $a_i \geq 2$ for $i \geq 1$, then the limit

$$\lim_{n\to\infty} [\![\, a_0, a_1, \ldots, a_n \,]\!]$$

exists. This limit is denoted simply by $[\![\, a_0, a_1, \ldots \,]\!]$.

Negative regular continued fractions differ from classical or regular continued fractions (RCFs for short) by the presence of the sign -1, as opposed to $+1$, in the numerators of the expression (1). One of the advantages of NRCFs over RCFs is that they allow a more direct description of the orbits of the action by Möbius transformations of $\mathrm{SL}(2,\mathbb{Z})$ on the projective line $\mathbb{P}^1(\mathbb{R})$.

It can be shown that every rational number has a unique finite NRCF expansion and every irrational real number has a unique infinite one.

We define

$$\delta x = \frac{-1}{x - \lceil x \rceil}, \quad (x \in \mathbb{R} \setminus \mathbb{Z}), \tag{2}$$

$\lceil x \rceil$ is the *ceiling* of x, that is, the unique integer n satisfying $n - 1 < x \leq n$.

It is shown that if $x \in \mathbb{R} \setminus \mathbb{Q}$, then its NRCF expansion is given by

$$x = [\![\, a_0, a_1, \ldots \,]\!], \quad \text{where } a_i = \lceil \delta^i x \rceil.$$

Note that $\delta x > 1$, so $\lceil \delta^i x \rceil \geq 2$ for $i \geq 1$.

The group $\mathbf{SL}(2,\mathbb{Z})$ acts on the projective line $\mathbb{P}^1(\mathbb{R}) = \mathbb{R} \cup \{\infty\}$ by Möbius transformations:

$$U \cdot x = \frac{ax + b}{cx + d}, \quad \text{where} \quad U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}(2,\mathbb{Z}).$$

Two elements $x, y \in \mathbb{P}^1(\mathbb{R})$ are called $\mathbf{SL}(2,\mathbb{Z})$-*equivalent* if they are in the same orbit under this action, that is, if there exists $U \in \mathbf{SL}(2,\mathbb{Z})$ such that $U \cdot x = y$.

It follows from the definition of δ that x and δx are $\mathbf{SL}(2,\mathbb{Z})$-equivalent, since δx is the the image of x under the Möbius transformation associated with the matrix

$$\begin{pmatrix} 0 & -1 \\ 1 & \lceil x \rceil \end{pmatrix}$$

of determinant +1. Thus, δ preserves $\mathbf{SL}(2,\mathbb{Z})$-equivalence classes.

It is easy to see that $\mathbb{P}^1(\mathbb{Q})$ is a single orbit. The orbits of points in $\mathbb{R}\setminus\mathbb{Q}$ are more complicated, it is here where NRCFs show their usefulness.

Theorem 1.1. *Let $x, y \in \mathbb{R}\setminus\mathbb{Q}$ with NRCF expansions $x = [\![a_0, a_1, \dots]\!]$ and $y = [\![b_0, b_1, \dots]\!]$. Then the following conditions are equivalent:*

(1) x and y are $\mathbf{SL}(2,\mathbb{Z})$-equivalent.

(2) There exist $m, l \geq 0$ such that $a_{m+j} = b_{l+j}$ for all $j \geq 0$.

(3) There exist $m, l \geq 0$ such that $\delta^m x = \delta^l y$.

Theorem 1.1 is an analogue of a classical theorem by Serret[pp. 34–37][13] for RCFs under the action of $\mathbf{GL}(2,\mathbb{Z})$.

1.1. **Quadratic numbers.** A real number x is *quadratic* if it is a root of an irreducible quadratic polynomial with coefficients in $\mathbb{Q}$. It is clear the if x is quadratic, so are all the elements of its orbit under $\mathbf{SL}(2,\mathbb{Z})$. In this subsection, we discuss the classification of $\mathbf{SL}(2,\mathbb{Z})$-orbits of real quadratic numbers.

A sequence $\{a_n\}_{n\geq 0}$ is called *ultimately periodic* if there exist $l \geq 1$ and $k \geq 0$ such that $a_{m+l} = a_m$ for all $m \geq k$. The smallest l satisfying this condition is called the *period length*. If $k = 0$, we say that $\{a_n\}_{n\geq 0}$ is *purely periodic*.

Theorem 1.2. *The following conditions are equivalent for $x \in \mathbb{R}\setminus\mathbb{Q}$.*

(1) x is quadratic

(2) The NRCF expansion of x is ultimately periodic.

(3) $\{\delta^n x\}_{n\geq 0}$ is ultimately periodic.

Theorem 1.2 is the analogue for NRCFs of Lagrange's theorem for classical continued fractions.

Ultimately periodic NRCFs will be denoted

$$[\![a_0, \dots, a_{k-1}, \overline{a_k, \dots, a_{k+l-1}}]\!],$$

where $\overline{a_k, \dots, a_{k+l-1}}$ indicates a *period* or repeating block.

Combining Theorems 1.1 and 1.2, we obtain immediately the following result:

Theorem 1.3. *Two quadratic numbers x and y are $\mathbf{SL}(2,\mathbb{Z})$-equivalent if and only if they have the same period up to circular permutation.*

Example 1.4.

$$\frac{1+\sqrt{13}}{2} = [\![3, \overline{2, 2, 5}]\!] \quad \text{and} \quad \frac{25+\sqrt{13}}{102} = [\![1, 2, 2, 3, \overline{5, 2, 2}]\!]$$

are $\mathbf{SL}(2,\mathbb{Z})$-equivalent.

Corollary 1.5. *Every quadratic number is $\mathbf{SL}(2,\mathbb{Z})$-equivalent to a purely periodic one, unique up to circular permutation of the period.*

We will see below a geometric characterization of pure periodicity.

Definition 1.6. A quadratic real number x is called Z-reduced[(a)] if $x > 1$ and $0 < x' < 1$, where x' is the conjugate of x.

Geometrically, a quadratic number x is Z-reduced if the pair (x, x') lies on the infinite rectangle $(1, \infty) \times (0, 1) \subset \mathbb{R}^2$.

Theorem 1.7. *A quadratic number is Z-reduced if and only if its NRCF expansion is purely periodic.*

It is not difficult to see that if $x = [\![a_0, a_1, \dots]\!]$, then $\delta^k x = [\![a_k, a_{k+1}, \dots]\!]$.

Theorem 1.8. *Let $x \in \mathbb{R}$ be a quadratic number. Then*

(1) If x is Z-reduced, then so is δx.

(2) $\delta^k x$ is Z-reduced for some $k \geq 0$.

If x is quadratic, all its iterations $x, \delta x, \delta^2 x, \dots$ lie in the same $\mathbf{SL}(2, \mathbb{Z})$-orbit, so δ provides an algorithm to find a reduced representative of its orbit in the infinite rectangle $(1, \infty) \times (0, 1)$. However, this representative is in general not unique; thus, $(1, \infty) \times (0, 1)$ is not a fundamental domain *stricto sensu*.

Example 1.9. Consider $x = -\sqrt{11} = [\![-3, 4, \overline{2, 2, 2, 2, 2, 5}]\!]$. The Z-reduced elements in the $\mathbf{SL}(2, \mathbb{Z})$-orbit of x are $\delta^3 x, \delta^4 x, \dots, \delta^8 x$. The corresponding points in the (x, x')-plane are plotted in Figure 1.

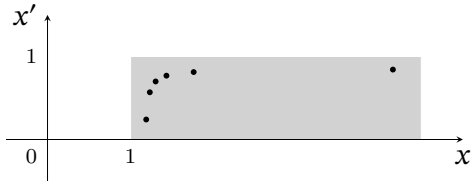

FIGURE 1. Z-reduced representatives of the orbit of $x = -\sqrt{11}$.

The *minimal integral polynomial* of a quadratic number x is the unique polynomial $P_x(t) = at^2 + bt + c \in \mathbb{Z}[t]$ such that $P_x(x) = 0$, $a > 0$ and $\gcd(a, b, c) = 1$. We say that x *belongs to the discriminant* D if $\operatorname{disc} P_x = D$, i.e., $b^2 - 4ac = D$. Note that since x is real, $D > 0$.

Define

$$\mathcal{S}_D = \{x \in \mathbb{Q}(\sqrt{D}) : \operatorname{disc}(P_x) = D\}. \tag{3}$$

It is straightforward to see that the set $\mathcal{S}_D$ is preserved by both $\mathbf{SL}(2, \mathbb{Z})$ and by the operator δ.

For nonsquare $D > 0$ with $D \equiv 0$ or $1 \pmod 4$, there are only finitely many Z-reduced quadratic numbers belonging to the discriminant D.

(a) The "Z" stands for Zurl. She actually called these numbers *quasireduced* (*quasireduzierte*).

Let $\mathcal{S}_D^{\mathrm{red}} \subset \mathcal{S}_D$ be the subset of Z-reduced elements. We can summarize the discussion above in the following statements:

Theorem 1.10. *Every* $\mathbf{SL}(2,\mathbb{Z})$*-orbit of* $\mathcal{S}_D$ *intersects* $\mathcal{S}_D^{\mathrm{red}}$.

If x is Z-reduced, the sequence $\{\delta^n x\}_{n\geq 0}$ is purely periodic, so the restriction $\delta : \mathcal{S}_D^{\mathrm{red}} \to \mathcal{S}_D^{\mathrm{red}}$ is surjective. Since the set $\mathcal{S}_D^{\mathrm{red}}$ is finite, this restriction is a bijection. It follows that δ defines an action of $\mathbb{Z}$ on $\mathcal{S}_D^{\mathrm{red}}$. The orbits of this action will be called *cycles*.

If $x, y \in \mathcal{S}_D^{\mathrm{red}}$ are in the same $\mathbf{SL}(2,\mathbb{Z})$-orbit, then by Theorem 1.1, they are in the same cycle, so we can give a more precise version of Theorem1.10:

Theorem 1.11. *The inclusion map* $\iota : \mathcal{S}_D^{\mathrm{red}} \hookrightarrow \mathcal{S}_D$ *induces a bijection*

$$\mathcal{S}_D^{\mathrm{red}}/\mathbb{Z}\delta \xrightarrow{\simeq} \mathcal{S}_D/\mathbf{SL}(2,\mathbb{Z}).$$

1.2. **Indefinite binary quadratic forms over** $\mathbb{Z}$**.** A *binary quadratic form* f over $\mathbb{Z}$ is a homogeneous polynomial of degree two in two variables x, y:

$$f(x,y) = ax^2 + bxy + cy^2 \quad \text{with} \quad a,b,c \in \mathbb{Z}. \tag{4}$$

We will use the more succinct notation $f = \langle a,b,c\rangle$ to indicate the form (4). We will say that f is *primitive* if $\gcd(a,b,c) = 1$. We will often identify f with the polynomial function it defines on $\mathbb{Z}^2$.

The group $\mathbf{SL}(2,\mathbb{Z})$ acts on the set of primitive binary quadratic forms over $\mathbb{Z}$ by linear substitution, that is,

$$Uf = f \circ U^T \quad \text{for} \quad U \in \mathbf{SL}(2,\mathbb{Z}),$$

where U^T is the transpose of U.

Two forms f and g are *properly equivalent* if there exists $U \in \mathbf{SL}(2,\mathbb{Z})$ such that $Uf = g$. We shall write $f \sim g$.

The *discriminant* of $f = \langle a,b,c\rangle$ is defined by $d(f) = b^2 - 4ac$. Note that $d(f) \equiv 0$ or $1 \pmod 4$.

It is straightforward to verify that the discriminant is an invariant of the proper equivalence class of a form f, that is, if $f \sim g$, then $d(f) = d(g)$.

Definition 1.12. We say that a binary quadratic form f is *indefinite* if it takes both positive and negative values on $\mathbb{Z}^2$. It can be shown that f is indefinite if and only if $d(f) > 0$.

For $D > 0$, we define the set

$$\mathcal{Q}_D = \{f = \langle a,b,c\rangle : \gcd(a,b,c) = 1; d(f) = D\}$$

If $f = \langle a,b,c\rangle \in \mathcal{Q}_D$, we define its *principal root* ρ_f as

$$\rho_f = \frac{b + \sqrt{D}}{2a},$$

where $\sqrt{D}$ is the positive square root of D. Note that ρ_f is a root of the polynomial $f(t,-1)$. Since f is primitive, we have $f(t,-1) = \mathrm{sgn}(a)P_{\rho_f}(t)$, where

$\operatorname{sgn}(a) = \pm 1$ is the sign of a and $P_{\rho_f}(t)$ is the minimal integral polynomial of ρ_f.

It is straightforward to see that the map $\phi : \mathcal{Q}_D \to \mathcal{S}_D$ defined by

$$f = \langle a, b, c \rangle \longmapsto \rho_f = \frac{b + \sqrt{D}}{2a} \tag{5}$$

is a bijection.

More crucially, the map ϕ is $\mathbf{SL}(2, \mathbb{Z})$-equivariant provided we "twist" the standard action of $\mathbf{SL}(2, \mathbb{Z})$ on $\mathcal{Q}_D$ by the automorphism of $\mathbf{SL}(2, \mathbb{Z})$ given by

$$U \mapsto U^* = WUW^{-1}, \quad \text{where} \quad W = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Note that $\det W = -1$, so $U \mapsto U^*$ is an outer automorphism of $\mathbf{SL}(2, \mathbb{Z})$.

Theorem 1.13. *The map $\phi : \mathcal{Q}_D \to \mathcal{S}_D$ satisfies*

$$\phi(U^* f) = U \cdot \phi(f).$$

The verification of the above identity is tedious but straightforward. An immediate consequence is:

Corollary 1.14. *Two primitive binary quadratic forms f, g of nonsquare discriminant $D > 0$ are properly equivalent if and only if their principal roots ρ_f and ρ_g are in the same $\mathbf{SL}(2, \mathbb{Z})$-orbit.*

To summarize: The classification of primitive binary quadratic forms of given nonsquare discriminant $D > 0$ up to proper equivalence is tantamount to the classification of real quadratic numbers belonging to the discriminant D modulo the action of $\mathbf{SL}(2, \mathbb{Z})$ by Möbius transformations.

We know that every element of $\mathcal{S}_D$ is $\mathbf{SL}(2, \mathbb{Z})$-equivalent to a Z-reduced one. We will mirror the reduction process we have seen for $\mathcal{S}_D$ to the quadratic form context using the bijection (5).

We define $\Delta : \mathcal{Q}_D \to \mathcal{Q}_D$ by $\Delta = \phi^{-1} \circ \delta \circ \phi$. Explicitly:

$$\Delta f = \begin{pmatrix} a_f & -1 \\ 1 & 0 \end{pmatrix} f, \quad \text{where} \quad a_f = \lceil \rho_f \rceil. \tag{6}$$

In particular, f and Δf are properly equivalent. Notice that by the definition of Δf, the following diagram commutes:

$$\begin{array}{ccc} \mathcal{Q}_D & \xrightarrow[\simeq]{\phi} & \mathcal{S}_D \\ {\scriptstyle\Delta}\downarrow & & \downarrow{\scriptstyle\delta} \\ \mathcal{Q}_D & \xrightarrow[\simeq]{\phi} & \mathcal{S}_D. \end{array} \tag{7}$$

Definition 1.15. A form $f = \langle a, b, c \rangle \in \mathcal{Q}_D$ is *Z-reduced* if its principal root $\rho_f = (b + \sqrt{D})/(2a)$ is Z-reduced. More explicitly, $f = \langle a, b, c \rangle$ is Z-reduced if

$$a > 0, \ c > 0, \ \text{and} \ b > a + c. \tag{8}$$

The notion of Z-reduced form is different from the classical notion of reduced form defined by Gauss [6, p. 152] and has the advantage of relating cleanly to negative regular continued fractions and Z-reduced quadratic irrationals. For the precise relationship between Gauss-reduced forms and Zagier-reduced forms, and a map between the two sets, see [14].

The map $\Delta : \mathcal{Q}_D \to \mathcal{Q}_D$ provides a reduction algorithm in the sense that successive application of Δ to any given form produces a reduced form; subsequent applications of Δ to that form produce all the reduced forms in its $\mathbf{SL}(2,\mathbb{Z})$-equivalence class. We illustrate this process in Example 1.16 below.

Example 1.16. Let $f = \langle 13, 75, 105\rangle$. We see in this example that $\Delta^2 f$ is already Z-reduced. Subsequent iterations $\Delta^m f$ $(m \geq 2)$ run over a cycle of length 4, as illustrated in Figure 2.

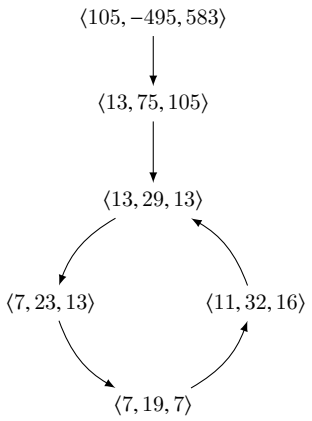

FIGURE 2. Iterations of Δ.

Let $\mathcal{Q}_D^{\mathrm{red}} \subset \mathcal{Q}_D$ be the subset of Z-reduced forms. It is clear that the restriction of ϕ to $\mathcal{Q}_D^{\mathrm{red}}$ is bijective. Since Δ is periodic on each element of $\mathcal{Q}_D^{\mathrm{red}}$ and this set is finite, Δ is bijective. Thus, Δ defines an action of $\mathbb{Z}$ on the set $\mathcal{Q}_D^{\mathrm{red}}$ and the set of orbits (cycles) is in one-to-one correspondence with the set of proper equivalence classes of forms of discriminant D. In summary, the inclusion map $\mathcal{Q}_D^{\mathrm{red}} \hookrightarrow \mathcal{Q}_D$ induces a bijection

$$\mathcal{Q}_D^{\mathrm{red}}/\mathbb{Z}\Delta \xrightarrow{\simeq} \mathcal{Q}_D/\mathbf{SL}(2,\mathbb{Z}).$$

Example 1.17. There are ten Z-reduced forms of discriminant $D = 40$ grouped into two proper equivalence classes, which coincide with the orbits of the operator Δ. In Figure 3, each arrow represents an application of Δ.

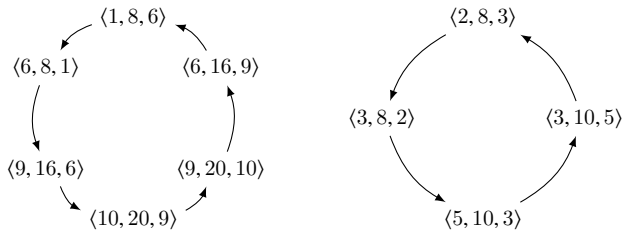

FIGURE 3. Cycles of Z-reduced forms of discriminant $D = 40$.

2. Continued Fractions over $\mathbb{F}_q[t]$

In this section, we develop the results on continued fractions necessary for the reduction theory of indefinite quadratic forms over $\mathbb{F}_q[t]$. Continued fraction expansions of Laurent series are well-studied in the literature, but predominantly over $\mathbb{C}$ or in characteristic 0. Our focus is on the finite field case and its arithmetic implications.

2.1. **Definitions.**

A *continued fraction*[(b)] $[\![a_0, a_2, \dots, a_n]\!]$ is the expression formally defined as in (1), but where the a_i are elements of the polynomial ring $A = \mathbb{F}_q[t]$.

The continued fraction $[\![a_0, \dots, a_n]\!]$ can be defined recursively by

$$\begin{aligned} [\![a_0]\!] &= a_0 \ ; \\ [\![a_0, \dots, a_n]\!] &= a_0 + \frac{-1}{[\![a_1, \dots, a_n]\!]} \quad (\text{for } n \geq 1). \end{aligned} \tag{9}$$

It is useful to express this recursion using matrices. Recall that the group $\mathbf{SL}(2, A)$ acts on $\mathbb{P}^1(K_\infty)$ by Möbius transformations. We will denote this action by a 'fat dot' $\bullet$.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \bullet x = \frac{ax + b}{cx + d}.$$

For $a \in A$, we let

$$T(a) = \begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix}. \tag{10}$$

Setting $A_n = T(a_0) \cdots T(a_n)$ and $A_{-1} = I$, we have

$$A_n \begin{pmatrix} 0 \\ 1 \end{pmatrix} = -A_{n-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{for } n \geq 0,$$

Thus, denoting by $\left(\begin{smallmatrix} p_n \\ q_n \end{smallmatrix}\right)$ the first column of A_n for $n \geq -1$, we have

$$A_n = \begin{pmatrix} p_n & -p_{n-1} \\ q_n & -q_{n-1} \end{pmatrix} \quad \text{for } n \geq 0. \tag{11}$$

Since $A_n = A_{n-1} T(a_n)$, the coefficients p_n, q_n satisfy the recursions

$$\begin{aligned} p_{-1} &= 1, \qquad p_0 = a_0, \quad p_n = a_n p_{n-1} - p_{n-2} \quad \text{for } n \geq 1. \\ q_{-1} &= 0, \qquad q_0 = 1, \quad q_n = a_n q_{n-1} - q_{n-2} \quad \text{for } n \geq 1. \end{aligned} \tag{12}$$

(b) For brevity, we will call them simply *continued fractions* since no other type will be considered.

Proposition 2.1.

(1) $[\![a_0, \ldots, a_n, x]\!] = A_n \cdot x$.

(2) $[\![a_0, \ldots, a_n]\!] = p_n/q_n$.

Proof. (1) By induction on n. The case $n = 0$ follows from the identity $[\![a_0, x]\!] = T(a_0) \cdot x$, which also provides the induction step:

$$[\![a_0, \ldots, a_n, x]\!] = [\![a_0, \ldots, a_{n-1}, [\![a_n, x]\!]]\!] = A_{n-1}T(a_n) \cdot x = A_n \cdot x.$$

(2) It suffices to take $x = \infty$ in Part 1:

$$[\![a_0, \ldots, a_n]\!] = [\![a_0, \ldots, a_n, \infty]\!] = A_n \cdot \infty = \frac{p_n}{q_n}.$$

■

The fractions p_k/q_k $(0 \le k \le n)$ are called *convergents* to $[\![a_0, \ldots, a_n]\!]$, and p_k and q_k are called *continuants*.

It should be noted that $\det(A_k) = 1$. Thus, we have the identity

$$-p_k q_{k-1} + p_{k-1} q_k = 1 \quad \text{for} \quad k \ge 0, \tag{13}$$

which shows in particular that the continuants p_k and q_k have no nontrivial common divisors.

2.2. **The Map δ.**

We have a canonical direct sum decomposition as $\mathbb{F}_q$-vector spaces

$$K_\infty = A \oplus P_\infty. \tag{14}$$

The component of $x \in K_\infty$ in A is called *the polynomial part* of x and will be denoted $\lfloor x \rfloor$.

Let $\delta : K_\infty \to K_\infty \cup \{\infty\}$ be the map defined by

$$\delta x = \frac{-1}{x - \lfloor x \rfloor}. \tag{15}$$

Note that $\delta x = \infty$ if and only if $x \in A$.

Lemma 2.2. *An element $x \in K_\infty$ is rational (i.e., $x \in K$) if and only if $\delta^{m+1} x = \infty$ for some $m \ge 0$.*

Proof. If $x \in K$, then $x = a/b$ for some $a, b \in A$ with $b \ne 0$. Using Euclidean division, we can write $a = bs + r$ where $s, r \in A$ and $\deg(r) < \deg(b)$. This implies $\delta x = -b/r$. Repeating this process, we eventually reach a point where the denominator has degree zero, i.e., $\delta^m x \in A$. Therefore $\delta^{m+1} x = \infty$.

Conversely, if $\delta^{m+1} x = \infty$, then $\delta^m x \in A$. Working backwards, we see that x is rational. ■

Lemma 2.3. *Let $x = [\![a_0, \ldots, a_n]\!]$, where each $a_i \in A$ and $|a_i| > 1$ for $i \ge 1$. Then the following hold:*

(1) $a_m = \lfloor \delta^m x \rfloor$ *for* $0 \le m \le n$. .

(2) $\delta^{m+1} x = [\![a_{m+1}, \ldots, a_n]\!]$ *for* $0 \le m < n$.

Proof. We prove both statements at the same time. We will show only the case $m = 0$, i.e., $a_0 = \lfloor x \rfloor$ and $\delta x = [\![a_1, \ldots, a_n]\!]$, by induction on n. The general case follows by iteration.

The base case $n = 0$ is trivial. Assuming $n \geq 1$ and applying the induction hypothesis to $y = [\![a_1, \ldots, a_n]\!]$ we have $\lfloor y \rfloor = a_1$, which implies $|y|_\infty = |a_1|_\infty > 1$. It follows that the polynomial part of $x = a_0 - y^{-1}$ is a_0 as claimed. Therefore, $\delta x = y = [\![a_1, \ldots, a_n]\!]$.

■

2.3. **Continued Fraction Expansion of Rational Functions.**

Theorem 2.4. *Every element x in K can be uniquely expressed as $x = [\![a_0, \ldots, a_n]\!]$, where each $a_m \in A$ and $|a_m| > 1$ for $m \geq 1$.*

Proof. We first prove the existence of such an expansion. Define $a_m = \lfloor \delta^m x \rfloor$. Since $|\delta^m x| > 1$ for $m \geq 1$, we have $|a_m| > 1$. We can show by induction that $x = [\![a_0, \ldots, a_m, \delta^{m+1} x]\!]$ for $m \geq 0$. According to Lemma 2.2, there exists an $m \geq 0$ such that $\delta^{m+1} x = \infty$. Therefore, $x = [\![a_0, \ldots, a_m, \infty]\!] = [\![a_0, \ldots, a_m]\!]$.

The uniqueness of this representation follows from Lemma 2.3, Part 1. ■

2.4. **Continued Fraction Expansion of Irrational Functions.**

Lemma 2.5. *Consider a sequence $\{a_n\}_{n \geq 0}$ of elements in A where $|a_n| > 1$ for $n \geq 1$ and let $p_m/q_m = [a_0, a_1, \ldots, a_m]$. Then, for all $m \geq 1$, we have*

(1) $|q_m| \geq q|q_{m-1}|$.

(2) $|q_m| \geq q^m$.

Proof. The second statement immediately follows from the first, so we only need to prove the first.

We proceed by induction. The case $m = 1$ is trivial since $q_0 = 1$ and $|q_1| = |a_1| \geq q$. Assume $|q_m| \geq q|q_{m-1}|$ for some $m \geq 1$. Particularly, $|q_m| > |q_{m-1}|$, hence $|q_{m+1}| = |a_{m+1} q_m - q_{m-1}| = |a_{m+1} q_m| \geq q|q_m|$. ■

Proposition 2.6. *Let $(a_n)_{n \geq 0}$ be a sequence of elements of A with $|a_n|_\infty > 1$ for $n \geq 1$. Then*

$$\frac{p_k}{q_k} = [\![a_0, \ldots, a_k]\!]$$

is a Cauchy sequence, hence convergent in K_∞.

Proof. Applying Equation (13) and Lemma 2.5, we get

$$\left| \frac{p_k}{q_k} - \frac{p_{k+1}}{q_{k+1}} \right|_\infty = \left| \frac{1}{q_k q_{k+1}} \right|_\infty \leq \frac{1}{q^{2k+1}}.$$

Therefore,

$$\left| \frac{p_k}{q_k} - \frac{p_{k+n}}{q_{k+n}} \right|_\infty \leq \frac{1}{q^{2k+1}} \sum_{j=0}^{n-1} \frac{1}{q^{2j}} < \frac{2}{q^{2k+1}},$$

showing that (p_k/q_k) is a Cauchy sequence. ■

Proposition 2.6 establishes that infinite continued fractions are meaningful in K_∞. We shall denote by $[\![a_0, a_1, \dots]\!]$ the limit of $[\![a_0, a_1, \dots, a_k]\!]$ as $k \to \infty$.

Theorem 2.7. *Every element x in $K_\infty \setminus K$ has a unique infinite continued fraction expansion.*

Proof. Define $a_m = \lfloor \delta^m x \rfloor$ and $x_m = \delta^m x$ for $m \geq 0$. Using the identity $x = [\![a_0, \dots, a_m, x_{m+1}]\!]$, we obtain

$$\begin{aligned} \frac{p_m}{q_m} - x &= \frac{p_m}{q_m} - \frac{p_m x_{m+1} - p_{m-1}}{q_m x_{m+1} - q_{m-1}} \\ &= \frac{1}{q_m(q_m x_{m+1} - q_{m-1})}. \end{aligned}$$

Since $|q_m(q_m x_{m+1} - q_{m-1})| = |q_m^2||x_{m+1}| > |q_m^2| \geq q^{2m}$, we have

$$| x - p_m/q_m |_\infty < 1/| q_m |_\infty^2 . \tag{16}$$

By Lemma 2.5, $| q_m |_\infty^2 \leq q^{2m}$; thus, $\lim_{m\to\infty} p_m/q_m = x$.

For uniqueness, assume $x = [\![a_0, a_1, \dots]\!]$. By taking limits as $n \to \infty$ in Lemma 2.3, we find that the equality $a_m = \lfloor \delta^m x \rfloor$ holds for an infinite expansion as well, proving that the a_m are uniquely determined by x. ∎

The convergents provide best approximations to Laurent series in the following sense:

Theorem 2.8. *If $a, b \in A$ are such that $| a/b - x |_\infty < 1/| b |_\infty^2$, then a/b is a convergent to x.*

Proof. Consider the continued fraction expansion $a/b = [\![a_0, \dots, a_m]\!]$ and let $y \in K$ be such that $x = [\![a_0, \dots, a_m, y]\!]$.

We will show that $|y| > 1$, which implies that the continued fraction expansion of y can be concatenated with that of a/b to obtain the expansion of x, proving that a/b is the m-th convergent to x.

Let p_k/q_k, $0 \leq k \leq m$, be the convergents to a/b. Note that $p_m/q_m = a/b$. By the same computation as in the proof of Theorem 2.7, we have:

$$\frac{a}{b} - x = \frac{1}{q_m(q_m y - q_{m-1})}.$$

Solving for y, we get:

$$y = \frac{q_m^2}{z} + \frac{q_m}{q_{m-1}},$$

where $z = a/b - x$. Since $|q_m^2/z| = |b^2/z| > 1$ by hypothesis and $|q_m/q_{m-1}| < 1$ by Lemma 2.5, we conclude $|y| > 1$. ∎

2.5. **The Action of $\mathbf{SL}(2,A)$.**

The special linear group $\mathbf{SL}(2,A)$ acts on $\mathbb{P}^1(K_\infty)$ by Möbius transformations as described in the previous section. Two elements $x, y \in \mathbb{P}^1(K_\infty)$ will be called $\mathbf{SL}(2,A)$-equivalent if they are in the same orbit under this action.

It is easy to see and well known that $\mathbb{P}^1(K)$ consists of a single orbit. The orbits of elements in $K_\infty \setminus K$ are more interesting and are described in the following statement, which is an analogue of a classical theorem by Serret (see, for instance, [11, Satz 2.24] or [7, Thm. 175]).

We begin by observing that x and δx are always $\mathbf{SL}(2,A)$-equivalent since

$$\delta x = \begin{pmatrix} 0 & 1 \\ -1 & \lfloor x \rfloor \end{pmatrix} \cdot x.$$

For $u \in \mathbb{F}_q^*$, let $S(u) = \left(\begin{smallmatrix} u & 0 \\ 0 & u^{-1} \end{smallmatrix}\right)$. Note that $S(u) \cdot x = u^2 x$, so x and $u^2 x$ are also in the same $\mathbf{SL}(2,A)$-orbit. Our aim is to show that if x and y are $\mathbf{SL}(2,A)$-equivalent, then $\delta^m y = u^2 \delta^n x$ for some $m, n \geq 0$ and $u \in \mathbb{F}_q^*$.

We will prove this theorem later in this section. We establish first a preliminary result that is interesting in its own right.

Proposition 2.9. *Let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{SL}(2,A)$ with $|c|_\infty > |d|_\infty > 0$, and let $[\![a_0, \ldots, a_n]\!]$ be the continued fraction expansion of a/c. Then there exists $u \in \mathbb{F}_q^*$ such that*

$$M = T(a_0) \cdots T(a_n) S(u).$$

Proof. Let p_k/q_k be the convergents to a/c and let $A_n = T(a_0) \cdots T(a_n)$. We have $A_n = \left(\begin{smallmatrix} p_n & -p_{n-1} \\ q_n & -q_{n-1} \end{smallmatrix}\right)$ with $p_n/q_n = a/c$. Since the fractions p_n/q_n and a/c are in lowest terms, we have $a = up_n$ and $c = uq_n$ for some $u \in \mathbb{F}_q^*$.

Comparing determinants $(\mathrm{mod}\ q_n)$, we have $up_n d \equiv -p_n q_{n-1} \equiv 1 \ (\mathrm{mod}\ q_n)$, which implies $ud \equiv -q_{n-1} \ (\mathrm{mod}\ q_n)$. Since $|q_{n-1}|_\infty < |q_n|_\infty$ and, by hypothesis, we also have $|d|_\infty < |c|_\infty = |q_n|_\infty$, we can conclude that $ud = -q_{n-1}$ and $ub = -p_{n-1}$. ∎

We can now prove the Laurent series analogue of Serret's theorem.

Theorem 2.10. *Two elements $x, y \in K_\infty \setminus K$ are $\mathbf{SL}(2,A)$-equivalent if and only if there exist $m, n \in \mathbb{Z}_{\geq 0}$ and $u \in \mathbb{F}_q^*$ such that $\delta^n y = u^2 \delta^m x$.*

Proof of Theorem 2.10. The 'if' part is clear from the remarks at the beginning of the subsection.

For the 'only if' part, suppose $y = N \cdot x$, where $N = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{SL}(2,A)$. Let $x = [\![a_0, a_1, \ldots]\!]$ and let $A_k = T(a_0) \cdots T(a_k) = \left(\begin{smallmatrix} p_k & -p_{k-1} \\ q_k & -q_{k-1} \end{smallmatrix}\right)$. Since $x = A_k \cdot \delta^{k+1} x$, we have $y = NA_k \cdot \delta^{k+1} x$.

The idea is to show that $M_k = NA_k$ satisfies the hypotheses of Proposition 2.9 for k large enough. We have

$$M_k = \begin{pmatrix} e_k & f_k \\ g_k & h_k \end{pmatrix}.$$

where $g_k = cp_k + dq_k$ and $h_k = -(cp_{k-1} + dq_{k-1})$. By Theorem 2.8, we have

$$p_k = xq_k + \epsilon_k$$
$$p_{k-1} = xq_{k-1} + \epsilon_{k-1},$$

where $\epsilon_k, \epsilon_{k-1} \to 0$ as $k \to \infty$. Substituting in the expressions for g_k and h_k, we get

$$g_k = (cx + d)q_k + c\epsilon_k$$
$$h_k = -(cx + d)q_{k-1} - c\epsilon_{k-1}.$$

Taking k large enough, we can make $|\, c\epsilon_k \,|_\infty$ and $|\, c\epsilon_{k-1} \,|_\infty$ strictly less than $|\, cx + d \,|_\infty$ (note that $cx + d \neq 0$ since $x \notin K$). For such k, we have $|\, g_k \,|_\infty = |\, cx + d) \,|_\infty \,|\, q_k \,|_\infty$ and $|\, h_k \,|_\infty = |\, cx + d) \,|_\infty \,|\, q_{k-1} \,|_\infty$. Thus,

$$|\, g_k/h_k \,|_\infty = |\, q_k/q_{k-1} \,|_\infty > 1,$$

which shows that M_k satisfies the hypotheses of Proposition 2.9. Thus,

$$M_k = T(c_0) \cdots T(c_n)S(u)$$

where $[\![\, c_0, \ldots, c_n \,]\!] = e_k/g_k$ and $u \in \mathbb{F}_q^*$. Consequently,

$$\begin{aligned} y =& M_k \cdot \delta^{k+1}x \\ =& [\![\, c_0, \ldots, c_n, u^2\delta^{k+1}x \,]\!]. \end{aligned}$$

It follows that $\delta^n y = u^2\delta^{k+1}x$ as desired. ■

2.6. **Quadratic Surds.**

An element $x \in K_\infty \setminus K$ is called a *quadratic surd* if $[K(x) : K] = 2$, that is, if x satisfies un equation

$$ax^2 + bx + c = 0,$$

where $a, b, c \in A$ and $a \neq 0$. We can assume without loss of generality that $\gcd(a, b, c) = 1$ and that a is monic. In this case, the polynomial $P_x(X) = aX^2 + bX + c$, will be called *the (integral) minimal polynomial* of x.

The conjugate root, that is, the second root of $P_x(X)$, will be denoted by x'.

A nonzero polynomial $d \in A$ has a square root in K_∞ if and only if d has even degree and its leading coefficient is a square in $\mathbb{F}_q$. We can always write such a polynomial in the form $d = u^2D$, where $u \in \mathbb{F}_q^*$,and D is monic of even degree. We will denote by $\sqrt{D}$ the square root of D in K_∞ that has monic polynomial part.

Definition 2.11. Let $D \in A$ be a monic nonsquare polynomial of even degree. We say that a quadratic surd $x \in K_\infty$ *belongs to the discriminant* D if $\operatorname{disc}(P_x) = u^2D$ for some $u \in \mathbb{F}_q^*$.

We will denote by S_D the set of quadratic surds that belong to the discriminant D.

It is easy to see that the elements of S_D can be written *uniquely* in the form $x = (b + \sqrt{D})/2a$, where $a, b \in A$.

Definition 2.12. A quadratic surd x is called *reduced* if $|\, x' \,|_\infty < 1 < |\, x \,|_\infty$.

We denote by $\mathcal{S}_D^{\mathrm{red}}$ the subset of reduced elements of $\mathcal{S}_D$.

Proposition 2.13. *The set $\mathcal{S}_D^{\mathrm{red}}$ is finite.*

Proof. Write $x = (b + \sqrt{D})/2a$ with $a, b \in A$. If x is reduced, we have in particular $\left|b + \sqrt{D}\right|_\infty > \left|b - \sqrt{D}\right|_\infty$. It follows that $|b|_\infty = \left|\sqrt{D}\right|_\infty$, which implies that there are only finitely many possibilities for b. Since x belongs to the discriminant D, the denominator a must be a divisor of $b^2 - D$. Thus, there are also only finitely many possibilities for a. ∎

Lemma 2.14. *The map δ takes $\mathcal{S}_D$ into $\mathcal{S}_D$.*

Proof. Let $x \in \mathcal{S}_D$ and $m = \lfloor x \rfloor$. Let $P_x(X) = aX^2 + bX + c$ be the minimal integral polynomial of x. Then δx is a root of the polynomial

$$X^2 P_x(m - 1/X) = (am^2 + bm + c)X^2 - (2am + b)X + a, \tag{17}$$

which is primitive and has the same discriminant as P_x. Thus, δx belongs also to the discriminant D. ∎

Proposition 2.15. *Let $x \in \mathcal{S}_D$. Then*

(1) If x is reduced, then so is δx.

(2) $\delta^n x$ is reduced for some $n \geq 0$.

Proof. (1) Assume x reduced. The condition $|\delta x|_\infty > 1$ is automatic; we need only to show $|(\delta x)'|_\infty < 1$. Since $|x|_\infty > 1$ and $|x'|_\infty < 1$, we have $|m - x'|_\infty = |m|_\infty = |x|_\infty > 1$, where $m = \lfloor x \rfloor$. Thus, $|(\delta x)'|_\infty < 1$.

(2) Let $x_k = \delta^k x$ and $m_k = \lfloor x_k \rfloor$. Let $P_k(X) = A_k X^2 + B_k X + C_k$ be the integral minimal polynomial of x_k.

By (17), we have $A_{k+1} = uP_k(m_k)$, where $u \in \mathbb{F}_q^*$. Thus,

$$A_{k+1} = uA_k(m_k - x_k)(m_k - x_k').$$

If $x_{k+1} = \delta x_k$ is not reduced, then $\left|m_k - x_k'\right|_\infty \leq 1$. Since $|m_k - x_k|_\infty < 1$, we conclude from the above equality that $|A_{k+1}|_\infty < |A_k|_\infty$.

This leads to a strictly decreasing sequence $|A_0| > |A_1| > \cdots$, which cannot continue indefinitely. Therefore, there must exist $k \geq 0$ such that $|m_k - x_k'| > 1$, implying $x_{k+1} = \delta^{k+1} x$ is reduced.

∎

A sequence $\{a_k\}_{k \geq 0}$ is *ultimately periodic* if it becomes periodic after some time, that is, if there exist $n \geq 0$ and $l > 0$ such that $a_{k+l} = a_k$ for all $k \geq n$.

Proposition 2.16. *Let $x \in K_\infty \setminus K$. The following conditions are equivalent*

(1) The element x is quadratic over K.

(2) The sequence $\{\delta^k x\}_{k \geq 0}$ is ultimately periodic.

(3) The continued fraction expansion $[\![a_0, a_1 \ldots]\!]$ of x is ultimately periodic.

Proof.

[1 ⇒ 2] We know by proposition 2.15 that there exists n such that $\delta^k x$ is reduced for all $k \geq n$. By Lemma 2.14, the $\delta^k x$ belong to the same discriminant, and by Proposition 2.13 there are only finitely many reduced elements for a given discriminant. Thus, there exists $l > 0$ such that $\delta^{l+n} x = \delta^n x$.

[2 ⇒ 1] Suppose $\delta^{l+n} x = \delta^n x$ for some $l > 0$. Let $P = T(a_0) \cdots T(a_{n-1})$ and $Q = T(a_n) \cdots T(a_{n+l-1})$. Then $Q^{-1}P^{-1} \cdot x = P^{-1} \cdot x$, which is clearly a quadratic equation for x.

[2 ⇔ 3] This is clear, since $a_k = \lfloor \delta^k x \rfloor$.

■

Remark 2.17. In the proof of Proposition 2.16, specifically in the part [1 ⇒ 2], we have used the fact that the ground field $\mathbb{F}_q$ is finite in an essential way. In fact, quadratic surds need not have periodic continued fraction expansions if the ground field is infinite. It has been known since Abel that there are even-degree square-free polynomials $D \in \mathbb{C}[t]$ with non-periodic continued fraction expansions for $\sqrt{D}$. These polynomials are called *non-Pellian*[(c)]. Masser-Zannier show in [10] that the polynomial $D = t^6 + t + a$ is non-Pellian for all but finitely many $a \in \mathbb{C}$. However, the *degrees* of the partial quotients in the expansion of $\sqrt{D}$ do form an ultimately periodic sequence, see [17].

We will use henceforth the notation

$$[\![\, a_0, \ldots, a_{n-1}, \overline{a_n, \ldots a_{n+l-1}} \,]\!]$$

to designate an ultimately periodic continued fraction with repeating bloc $(a_n, \ldots a_{n+l-1})$. If $n = 0$, we say that the continued fraction is *purely periodic*.

Note that if $x = [\![\, \overline{a_0, a_1 \ldots a_{l-1}} \,]\!]$ is purely periodic, then x is reduced since $x = \delta^{kl} x$ and $\delta^{kl} x$ is reduced for k large enough by Proposition 2.15. We will prove later that the converse is also true.

Proposition 2.18. *If* $x = [\![\, \overline{a_0, a_1 \ldots a_{l-1}} \,]\!]$, *then* $1/x' = [\![\, \overline{a_{l-1}, \ldots, a_1, a_0} \,]\!]$.

Proof. Let $W = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Observe the identity

$$WT(a)W^{-1} = T(a)^{-1}. \tag{18}$$

The continued fraction $y = [\![\, \overline{a_{l-1}, \ldots, a_1, a_0} \,]\!]$ satisfies the equation

$$y = T(a_{l-1}) \cdots T(a_0) \cdot y$$

Using (18), this equation can be written

$$W \cdot y = (T(a_0) \cdots T(a_{l-1}))^{-1} W \cdot y,$$

that is, $W \cdot y = 1/y$ is one of the two fixed points of $T(a_0) \cdots T(a_{l-1})$, which are x and x'. It follows that $1/y = x$ or $1/y = x'$. The first case can be discarded since both x and y are reduced. Thus, $y = 1/x'$, as claimed. ■

(c) Thus called due to the fact that the polynomial Pell equation $X^2 - DY^2 = 1$ has nontrivial solutions if and only if $\sqrt{D}$ has an ultimately periodic continued fraction expansion.

Corollary 2.19. *A quadratic surd $x \in K_\infty$ is reduced if and only if it is purely periodic.*

Proof. The 'if' part was already observed, we will only discuss the 'only if' part. Let $x = [\![a_0, a_1 \dots]\!]$. We know that $y = \delta^n x$ is purely periodic for some $n \geq 0$, so $x = T(a_0) \cdots T(a_{n-1}) \cdot y$. Conjugating, we have $x' = T(a_0) \cdots T(a_{n-1}) \cdot y'$ and using (18), we obtain

$$\begin{aligned} \frac{1}{y'} &= T(a_{n-1}) \cdots T(a_0) \cdot \frac{1}{x'} \\ &= [\![a_{n-1}, \dots, a_0, 1/x']\!] . \end{aligned}$$

Since $|1/x'|_\infty > 1$ (x is reduced) and $1/y'$ is purely periodic by Proposition 2.18, we conclude that $1/x'$ is purely periodic and therefore so is x. ∎

The following theorem summarizes the main results in this section.

Theorem 2.20. *Let $D \in A$ be a nonsquare monic polynomial of even degree. Then*

(1) The set $\mathcal{S}_D^{\mathrm{red}}$ is finite and the restriction $\delta : \mathcal{S}_D^{\mathrm{red}} \to \mathcal{S}_D^{\mathrm{red}}$ is bijective.

(2) Every $\mathbf{SL}(2, A)$-equivalence class in $\mathcal{S}_D$ has a representative in $\mathcal{S}_D^{\mathrm{red}}$.

(3) Two elements $x, y \in \mathcal{S}_D$ are $\mathbf{SL}(2, A)$-equivalent if and only if there exist $m, n \in \mathbb{Z}_{\geq 0}$ and $u \in \mathbb{F}_q^*$ such that $\delta^m x = u^2 \delta^n y$.

Proof. (1) By Proposition 2.13, the set $\mathcal{S}_D^{\mathrm{red}}$ is finite. Therefore, we need only to show that $\delta : \mathcal{S}_D^{\mathrm{red}} \to \mathcal{S}_D^{\mathrm{red}}$ is surjective. If $x \in \mathcal{S}_D^{\mathrm{red}}$, then x is purely periodic by Corollary 2.19. Thus, $x = \delta^l x$ for some $l > 0$.

(2) Follows from Proposition 2.15

(3) This is a particular case of Theorem 2.10.

∎

Let G be the semi-direct product $\mathbb{F}^* \rtimes \mathbb{Z}$, where $\mathbb{Z}$ acts on $\mathbb{F}_q^*$ by sending the generator 1 to the automorhism $u \mapsto u^{-1}$ of $\mathbb{F}_q^*$.

The group of matrices of the form $\left(\begin{smallmatrix} u & 0 \\ 0 & u^{-1} \end{smallmatrix}\right)$, $u \in \mathbb{F}_q^*$, preserves $\mathcal{S}_D^{\mathrm{red}}$, as does δ. Since δ is invertible on $\mathcal{S}_D^{\mathrm{red}}$ and satisfies $\delta u x = u^{-1} \delta x$, we can define an action of G on $\mathcal{S}_D^{\mathrm{red}}$ by $(u, k) \cdot x = \left(\begin{smallmatrix} u & 0 \\ 0 & u^{-1} \end{smallmatrix}\right) \cdot \delta^k x = u^2 \delta^k x$.

The following Proposition is essentially a rephrasing of Part 3 of Theorem 2.20 for $\mathcal{S}_D^{\mathrm{red}}$ in terms of this action:

Proposition 2.21. *Two elements $x, y \in \mathcal{S}_D^{\mathrm{red}}$ are $\mathbf{SL}(2, A)$-equivalent if and only if they are in the same orbit under the action of G.*

3. Indefinite Binary Quadratic Forms

By analogy with the classical case over $\mathbb{Z}$, a binary quadratic form $f = aX^2+bXY+cY^2$ with coefficients in A is called *indefinite* if $\operatorname{disc}(f) = b^2-4ac$ is a square in K_∞. We say that f is *primitive* if $\gcd(a,b,c) = 1$.

We will use the notation $\langle a,b,c\rangle$ to designate the quadratic form $aX^2 + bXY + cY^2$.

Two binary quadratic forms f and g are *properly equivalent* if there exists $M \in \mathbf{SL}(2,A)$ such that $f \circ M = g$. It is immediate that properly equivalent quadratic forms have the same discriminant.

Let $D \in A$ be a nonzero polynomial of even degree with a square leading coefficient so that D has a square root in K_∞. Let $\mathcal{Q}_D$ be the set of primitive binary quadratic forms of discriminant D. The group $\mathbf{SL}(2,A)$ acts on $\mathcal{Q}_D$ on the left by

$$Mf = f \circ M^T \tag{19}$$

where M^T is the transpose of M. We are interested in the orbits of this action, i.e., the proper equivalence classes of primitive binary forms of discriminant D.

Let $\lambda \in \mathbb{F}_q^*$. The map $\mathcal{Q}_D \to \mathcal{Q}_{\lambda^2 D}$ given by $f \mapsto \lambda f$ is clearly a bijection that commutes with the action of $\mathbf{SL}(2,A)$. Since our goal is to describe the orbits of $\mathbf{SL}(2,A)$ in $\mathcal{Q}_D$, we can assume without loss of generality that D is monic.

3.1. The Maps ρ and Δ.

Assume from now on that D is *monic* and denote by $\sqrt{D}$ the square root of D such that $\left\lfloor \sqrt{D} \right\rfloor$ is monic.

Let $f = \langle a,b,c\rangle \in \mathcal{Q}_D$. We define the *principal root* of f by

$$\rho_f = \frac{b+\sqrt{D}}{2a}. \tag{20}$$

Note that ρ_f is a root of the polynomial $f(X,-1)$.

Let $\mathcal{S}_D$ be the set of elements of $K(\sqrt{D})$ that belong to the discriminant D in the sense of Definition 2.11.

Let $W = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. For $M \in \mathbf{SL}(2,A)$, we let $M^* = WMW^{-1}$.

Proposition 3.1. *The map $\rho : \mathcal{Q}_D \to \mathcal{S}_D$ given by $f \mapsto \rho_f$ is bijective and satisfies*

$$\rho_{Mf} = M^* \cdot \rho_f \tag{21}$$

for all $M \in \mathbf{SL}(2,A)$.

Proof. The bijectivity of ρ is clear from its definition. We shall only prove (21).

Let $M = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \mathbf{SL}(2,A)$ and $f = \langle a,b,c\rangle$. By direct computation, we have:

$$Mf = \langle ap^2 + bpq + cq^2, 2apr + bqr + bps + 2cqs, ar^2 + brs + cs^2\rangle.$$

Therefore,

$$\rho_{Mf} = \frac{2apr + 2bqr + b + 2cqs + \sqrt{D}}{2(ap^2 + bpq + cq^2)}.$$

On the other hand,

$$\begin{aligned} M^* \cdot \rho_f &= \frac{2ar + bs + s\sqrt{D}}{2ap + bq + q\sqrt{D}} \\ &= \frac{2apr + 2bqr + b + 2cqs + \sqrt{D}}{2(ap^2 + bpq + cq^2)} \\ &= \rho_{Mf}. \end{aligned}$$

■

Corollary 3.2. *Two forms $f, g \in \mathcal{Q}_D$ are properly equivalent if and only if their principal roots ρ_f and ρ_g are $\mathbf{SL}(2, A)$-equivalent.*

Proof. Evident from Equation (21) and the fact that ρ is bijective. ■

We have seen in the previous section that the map δ preserves the set S_D. We define the corresponding map Δ on the quadratic form side. We define $\Delta : \mathcal{Q}_D \to \mathcal{Q}_D$ so that the following diagram commutes:

$$\begin{array}{ccc} \mathcal{Q}_D & \xrightarrow[\simeq]{\rho} & \mathcal{S}_D \\ {\scriptstyle\Delta}\downarrow & & \downarrow{\scriptstyle\delta} \\ \mathcal{Q}_D & \xrightarrow[\simeq]{\rho} & \mathcal{S}_D. \end{array} \tag{22}$$

The explicit expression for Δ is

$$\Delta f = \begin{pmatrix} r_f & -1 \\ 1 & 0 \end{pmatrix} f, \quad \text{where} \quad r_f = \lfloor \rho_f \rfloor. \tag{23}$$

Note that f and Δf are properly equivalent.

Definition 3.3. A quadratic form $f = \langle a, b, c \rangle \in \mathcal{Q}_D$ is called *reduced* if its principal root $\rho_f = (b + \sqrt{D})/2a$ is reduced (in the sense of Definition 2.12).

Remark 3.4. It is straightforward to see that $f = \langle a, b, c \rangle$ is reduced if and only if $|b| > \max\{|a|, |c|\}$ and b is monic. This equivalent condition is easier to verify 'visually' on any given form f.

Let $\mathcal{Q}_D^{\mathrm{red}}$ be the subset of reduced forms in $\mathcal{Q}_D$. By definition, $\mathcal{Q}_D^{\mathrm{red}} = \rho^{-1} S_D^{\mathrm{red}}$. In particular, the set $\mathcal{Q}_D^{\mathrm{red}}$ is finite. Restricting the maps of (22) to reduced elements, we get a commutative diagram

$$\begin{array}{ccc} \mathcal{Q}_D^{\mathrm{red}} & \xrightarrow[\simeq]{\rho} & \mathcal{S}_D^{\mathrm{red}} \\ {\scriptstyle\Delta}\downarrow & & \downarrow{\scriptstyle\delta} \\ \mathcal{Q}_D^{\mathrm{red}} & \xrightarrow[\simeq]{\rho} & \mathcal{S}_D^{\mathrm{red}}. \end{array} \tag{24}$$

We know by Theorem 2.20, Part 1, that δ restricted to $\mathcal{S}_D^{\mathrm{red}}$ is bijective; therefore, Δ restricted to $\mathcal{Q}_D^{\mathrm{red}}$ is also bijective..

We will now transfer the results on quadratic surds from the previous section to the quadratic form setting via the bijection ρ.

Theorem 3.5. *Let $f \in \mathcal{Q}_D$. Then:*

(1) If f is reduced, then so is Δf.

(2) $\Delta^n f$ is reduced for some $n \geq 0$.

Proof. This follows from Proposition 2.15 and the commutative diagram (22). ∎

Corollary 3.6. *Every proper equivalence class in $\mathcal{Q}_D$ has a representative in $\mathcal{Q}_D^{\mathrm{red}}$.*

Proof. This is clear from Part (2) of Theorem 3.5. ∎

We can think of Δ as a reduction algorithm, since its iterations on an input f produce a reduced output in the proper equivalence class of f. The following result shows that the algorithm eventually enters a cycle.

Theorem 3.7. *Let $f \in \mathcal{Q}_D$. Then:*

(1) The sequence $(\Delta^k f)_{k\geq 0}$ is ultimately periodic.

(2) f is reduced if and only if the sequence $(\Delta^k f)_{k\geq 0}$ is purely periodic.

Proof. (1) Follows from Proposition 2.16, Part 2.

(2) Follows from the analogous statement for quadratic surds in Corollary 2.19.

∎

We already observed that Δ is a bijection on on the set of reduced forms $\mathcal{Q}_D^{\mathrm{red}}$, so we can define an action of $\mathbb{Z}$ on $\mathcal{Q}_D^{\mathrm{red}}$ by sending the generator 1 to Δ. The orbits of this action are called *cycles*. A natural question arises: can different cycles represent the same proper equivalence class? In the classical theory of Gauss cycles over $\mathbb{Z}$, tthe answer is no. However, in the present setting, the situation is slightly different due to the presence of units from $\mathbb{F}_q^*$.

We need to introduce the subgroup $\mathbf{H} \subset \mathbf{SL}(2, A)$ of diagonal matrices. Note that $\mathbf{H}$ consists of matrices of the form $\left(\begin{smallmatrix} u^{-1} & 0 \\ 0 & u \end{smallmatrix}\right)$, where $u \in \mathbb{F}_q^*$, so $\mathbf{H}$ is isomorphic to $\mathbb{F}_q^*$.

Lemma 3.8.

(1) $\mathbf{H}$ preserves the set of reduced forms $\mathcal{Q}_D^{\mathrm{red}}$.

(2) $U^{-1}\Delta = \Delta U$ for all $U \in \mathbf{H}$.

Proof. Let $U = \left(\begin{smallmatrix} u^{-1} & 0 \\ 0 & u \end{smallmatrix}\right)$, $u \in \mathbb{F}_q^*$.

(1) It is evident from Definition 3.3 that if $f = \langle a, b, c\rangle$ is reduced, then so is $Uf = \langle u^{-1}a, b, uc\rangle$ for $u \in \mathbb{F}_q^*$.

(2) By Proposition 3.1, we have $\rho_{Uf} = U^* \cdot \rho_f = u^2\rho_f$, hence $r_{Uf} = u^2 r_f$. The result follows from the matrix identity

$$U^{-1}\begin{pmatrix} r_f & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} u^2 r_f & -1 \\ 0 & 1 \end{pmatrix} U.$$

■

Remark 3.9. The identity $U^{-1}\Delta = \Delta U$ also follows from the corresponding identity $u^{-2}\delta x = \delta u^2 x$ for quadratic surds.

Theorem 3.10. *Two forms $f, g \in \mathcal{Q}_D$ are properly equivalent if and only if there exist $m, n \in \mathbb{Z}_{\geq 0}$ and $U \in \mathbf{H}$ such that $U\Delta^n f = \Delta^m g$.*

Proof. By Proposition 3.1, the principal roots ρ_f and ρ_g are $\mathbf{SL}(2, A)$-equivalent. By Theorem 2.10, there exist $m, n \in \mathbb{Z}_{\geq 0}$ and $u \in \mathbb{F}_q^*$ such that $\delta^n \rho_f = u^2\delta^m \rho_g$.

Using the commutativity of the diagram (22) and Equation (21), we have $\rho_{\Delta^n f} = U \cdot \rho_{\Delta^m g} = \rho_{U^*\Delta^m g}$, where $U = \left(\begin{smallmatrix} u & 0 \\ 0 & u^{-1} \end{smallmatrix}\right)$. Since ρ is bijective, this implies $\Delta^n f = U^{-1}\Delta^m g$ (note that $U^* = U^{-1}$). ■

Corollary 3.11. *Two reduced forms $f, g \in \mathcal{Q}_D^{\mathrm{red}}$ are properly equivalent if and only if there exist $m \in \mathbb{Z}$ and $U \in \mathbf{H}$ such that $Uf = \Delta^m g$.*

Proof. This follows from Part (3.10) together with the relation $U^{-1}\Delta = \Delta U$ for $U \in \mathbf{H}$ and the fact that Δ restricted to $\mathcal{Q}_D^{\mathrm{red}}$ is invertible. ■

Since $U\Delta = \Delta U^{-1}$, the actions of $\mathbb{Z}$ and $\mathbf{H}$ on $\mathcal{Q}_D^{\mathrm{red}}$ can be combined into a single action of the semidirect product $G = \mathbb{F}_q^* \rtimes \mathbb{Z}$ (where $\mathbb{Z}$ acts on $\mathbb{F}_q^*$ by inversion) defined for $(u, k) \in G$ and $f \in \mathcal{Q}_D^{\mathrm{red}}$ by

$$(u, k) \cdot f = U\Delta^k f.$$

The following statement summarizes a good part of the discussion above:

Theorem 3.12. *The inclusion $\mathcal{Q}_D^{\mathrm{red}} \hookrightarrow \mathcal{Q}_D$ induces a bijection*

$$\mathcal{Q}_D^{\mathrm{red}}/G \xrightarrow{\simeq} \mathcal{Q}_D/\mathbf{SL}(2, A).$$

Proof. The surjectivity follows from Corollary 3.6, and the injectivity from Corollary 3.11 ■

3.2. **Relation with Class Groups.**

Gauss showed in the *Disquisitiones* [6] that the set of proper equivalence classes of binary quadratic forms over $\mathbb{Z}$ with a given discriminant is an abelian group under a law he called 'composition.' This group was later interpreted in terms of ideal class groups of quadratic fields by Dedekind [9, Suppl. X, pp. 380-497]. A good modern exposition can be found in [1].

Generalizations of composition for forms over other rings have been known; see, for example, [4], [15], and [8]. The most far-reaching generalization was given by Kneser [8], who showed in a very simple and elegant way that composition can be defined for forms over any commutative ring using Clifford algebras.

The case of function fields that we discuss here follows easily (for example) from Kneser's work mentioned above. We will only summarize the main results.

Let $\mathcal{H}_D = \mathcal{Q}_D/\mathbf{SL}(2,A)$[(d)], which is an abelian group under composition. We will denote by $h(D)$ its order. Let $B = A[\sqrt{D}]$, and let $N : B^* \to A^* = \mathbb{F}_q^*$ be the norm map. There is an exact sequence:

$$B^* \xrightarrow{N} \mathbb{F}^* \xrightarrow{\iota} \mathcal{H}_D \xrightarrow{\phi} \mathrm{Pic}(B) \longrightarrow 0, \tag{25}$$

where $\iota(u) = \langle u, 0, u^{-1}D\rangle$, $\phi(f) = (A\rho_f + A)$, and $\mathrm{Pic}(B)$ is the Picard group of B. It is easily verified that $A\rho_f + A$ is an invertible B-ideal. Note that $[\mathbb{F}^* : N(B)^*] = 1$ or 2 depending on whether the norm of the fundamental unit of B is a square in $\mathbb{F}_q^*$ or not.

Although it is not strictly necessary, we will assume henceforth, for simplicity of exposition, that D is squarefree.

Let E be the (nonsingular) hyperelliptic curve defined over $\mathbb{F}_q$ by the equation $s^2 = D(t)$. We mention the classical short exact sequence relating $\mathrm{Pic}(B)$ and the class group $\mathrm{Cl}^0(E)$ of divisors of degree 0 on E:

$$0 \longrightarrow \mathbb{Z}/\log_q |\epsilon|_\infty \mathbb{Z} \longrightarrow \mathrm{Cl}^0(E) \longrightarrow \mathrm{Pic}(B) \longrightarrow 0, \tag{26}$$

where $\epsilon \in B^*$ is a fundamental unit. In particular,

$$|\mathrm{Pic}(B)| = \left|\mathrm{Cl}^0(E)\right| / \log_q |\epsilon|_\infty .$$

It is also classical that $\left|\mathrm{Cl}^0(E)\right| = L_E(1)$, where L_E is the L-polynomial of E (the numerator of the zeta function of E). We refer to Rosen [12, Prop. 14.7 and Thm. 5.9] for these results.

The fundamental unit ϵ can be computed using the continued fractions defined in Section 2, as in the classical case over $\mathbb{Z}$. It is easy to see, using Theorem 2.8, Part (2), that if $\epsilon = a + b\sqrt{D}$ is a fundamental unit, then a/b is a convergent to $\sqrt{D}$; it is, in fact, the first convergent p_n/q_n that satisfies $\left|p_n + q_n\sqrt{D}\right|_\infty = 1$.

(d) Note that $\mathcal{H}_D$ can also be described as $\mathcal{Q}_D^{\mathrm{red}}/G$ by Theorem 3.10.

3.3. **Explicit Examples.**

The following examples have been computed using the software packages `MAGMA`, `SAGE`, and `Mathematica`. The (non-optimized, unpolished) code is available from the author.

Example 3.13. Let $q = 11$ and $D = t^4 + 7t^2 + 7t + 6$. A fundamental unit is

$$\epsilon = (10t^4 + 10t^3 + 9t^2 + 4t + 9) + (10t^2 + 10t + 7)\sqrt{D},$$

which has nonsquare norm and $|\epsilon|_\infty = q^4$. We have $L_E(u) = 11u^2 + 1$, courtesy of `MAGMA`. Thus, $h(D) = L_E(1)/4 = 3$.

This can be confirmed by considering the action of G on $\mathcal{Q}_D^{\mathrm{red}}$. There are 110 reduced quadratic forms of discriminant D distributed in three G-orbits of sizes $30, 40, 40$.

Representatives of these orbits are

$$\langle 6t + 8, t^2 + 7, 9t + 1\rangle, \langle 6t + 1, t^2 + 1, 3t + 7\rangle, \langle 6t + 3, t^2 + 1, 3t + 6\rangle.$$

Example 3.14. Let $q = 5$ and $D = (t + 2)(t + 4)(t^4 + 4t^3 + 3t^2 + 3)$. Here $L_E(u) = 25u^4 + 10u^3 + 6u^2 + 2u + 1$ and a fundamental unit is

$$\epsilon = (4t^{11} + 3t^{10} + 2t^9 + 2t^7 + t^4 + 3t^2 + 1) + (4t^8 + 3t^7 + 2t^6 + 3t^4 + t^3 + 3t^2 + 2t)\sqrt{D},$$

which has square norm and $|\epsilon|_\infty = q^{11}$. Thus, $h(D) = 2L_E(1)/11 = 2{\times}44/11 = 8$.

One can show that there are 144 reduced forms of discriminant D distributed in eight G-orbits of sizes $16, 16, 18, 18, 18, 18, 20, 20$.

Representatives of these orbits are

$$\langle 3, t^3, 4t^2 + t + 3\rangle, \langle 4, t^3, 3t^2 + 2t + 1\rangle, \langle 3t, t^3 + 2, 2t^2 + 4t + 1\rangle,$$
$$\langle 4t, t^3 + 2, 4t^2 + 3t + 2\rangle, \langle 3t^2 + t + 4, t^3 + 2, 2t\rangle, \langle 4t^2 + 3t + 2, t^3 + 2, 4t\rangle,$$
$$\langle 3t^2 + t + 3, t^3 + 4, 4t + 1\rangle, \langle 4t^2 + 3t + 4, t^3 + 4, 3t + 2\rangle.$$

References

[1] A. I. Borevich and I. R. Shafarevich. *Number theory.* Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20. New York: Academic Press, 1966, pp. x+435.

[2] Duncan A. Buell. *Binary quadratic forms. Classical theory and modern computations.* English. New York, NY etc.: Springer-Verlag, 1989.

[3] Ch. J. De la Vallée Poussin. *Sur les fractions continues et les formes quadratiques.* Brux. S. sc. XIX A. 111-113 (1895). 1895.

[4] Bill J. Dulin and H. S. Butts. "Composition of binary quadratic forms over integral domains." In: *Acta Arith.* 20 (1972), pp. 223–251.

[5] Daniel E. Flath. *Introduction to number theory.* A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989, pp. xii+212.

[6] Carl Friedrich Gauß. *Disquisitiones arithmeticae. Transl. from the Latin by Arthur A. Clarke, Rev. by William C. Waterhouse, with the help of Cornelius Greither and A. W. Grootendorst. (Reprint of the 1966 ed.)* English. New York etc.: Springer-Verlag. xx, 472 p. DM 148.00 (1986). 1986.

[7] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Sixth. Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles. Oxford University Press, Oxford, 2008, pp. xxii+621.

[8] Martin Kneser. "Composition of binary quadratic forms." In: *J. Number Theory* 15.3 (1982), pp. 406–413.

[9] P. G. Lejeune-Dirichlet. *Vorlesungen über Zahlentheorie, herausgegeben von R. Dedekind. Zweite Auflage.* German. Braunschweig. Vieweg (1871). 1871.

[10] David Masser and Umberto Zannier. "Torsion points on families of simple abelian surfaces and Pell's equation over polynomial rings." In: *J. Eur. Math. Soc. (JEMS)* 17.9 (2015). With an appendix by E. V. Flynn, pp. 2379–2416.

[11] Oskar Perron. *Die Lehre von den Kettenbrüchen. Bd I. Elementare Kettenbrüche*. 3te Aufl. B. G. Teubner Verlagsgesellschaft, Stuttgart, 1954, pp. vi+194.

[12] Michael Rosen. *Number theory in function fields*. Vol. 210. Graduate Texts in Mathematics. New York: Springer-Verlag, 2002, pp. xii+358.

[13] Joseph-Alfred Serret. *Cours d'algèbre supérieure. Tome I.* Les Grands Classiques Gauthier-Villars. [Gauthier-Villars Great Classics]. Reprint of the fourth (1877) edition. Éditions Jacques Gabay, Sceaux, 1992, pp. xiii+648.

[14] Barry R. Smith. "Constructing minimal periods of quadratic irrationalities in Zagier's reduction theory." In: *J. Number Theory* 187 (2018), pp. 1–26.

[15] Jacob Towber. "Composition of oriented binary quadratic form-classes over commutative rings." In: *Adv. in Math.* 36.1 (1980), pp. 1–107.

[16] D. B. Zagier. *Zetafunktionen und quadratische Körper*. Eine Einführung in die höhere Zahlentheorie. [An introduction to higher number theory], Hochschultext. [University Text]. Springer-Verlag, Berlin-New York, 1981, pp. viii+144.

[17] Umberto Zannier. "Hyperelliptic continued fractions and generalized Jacobians." In: *Amer. J. Math.* 141.1 (2019), pp. 1–40.

[18] Erna Zurl. "Theorie der reduziert-regelmäßigen Kettenbrüche." In: *Math. Ann.* 110.1 (1935), pp. 679–717.

Louisiana State University

Email address: morales@math.lsu.edu