JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

A. Muhammed ULUDAĞ, Ayberk ZEYTIN et Merve DURMUŞ

Binary quadratic forms as dessins

Tome 29, n° 2 (2017), p. 445-469.

<http://jtnb.cedram.org/item?id=JTNB_2017__29_2_445_0>

Journal de Théorie des Nombres
de Bordeaux **29** (2017), 445–469

Binary quadratic forms as dessins

par A. Muhammed ULUDAĞ, Ayberk ZEYTIN et Merve DURMUŞ

Résumé. Nous montrons que la classe de toute forme quadratique binaire indéterminée et primitive est représentée de façon naturelle par un graphe infini (appellé çark) avec un unique cycle, plongé dans une couronne conforme. Ce cycle est appelé le rachis du çark. Le choix d'un arc d'un çark donné spécifie une forme quadratique binaire indéterminée dans la classe représentée par le çark. Les formes réduites dans la classe représentée par un çark correspondent à certains arcs distingués sur son rachis. La réduction de Gauss est le processus de déplacement de l'arc vers la direction du rachis du çark. Les classes ambiguës et réciproques sont représentées par des çarks ayant une symétrie. Les çarks périodiques représentent les classes des formes non-primitives.

Abstract. We show that the class of every primitive indefinite binary quadratic form is naturally represented by an infinite graph (named çark) with a unique cycle embedded on a conformal annulus. This cycle is called the spine of the çark. Every choice of an edge of a fixed çark specifies an indefinite binary quadratic form in the class represented by the çark. Reduced forms in the class represented by a çark correspond to some distinguished edges on its spine. Gauss reduction is the process of moving the edge in the direction of the spine of the çark. Ambiguous and reciprocal classes are represented by çarks with symmetries. Periodic çarks represent classes of non-primitive forms.

1. Introduction

The Euclidean algorithm is the process of comparison of commensurable magnitudes and the modular group $\mathrm{PSL}_2(\mathbf{Z})$ is an encoding of this algorithm. Since the intellect is ultimately about comparison of magnitudes, it should come as no surprise that the modular group manifests itself in

Manuscrit reçu le 21 août 2015, révisé le 25 octobre 2015, accepté le 7 novembre 2015.
Mathematics Subject Classification. 11H55, 05C10.
Mots-clefs. binary quadratic forms, dessins d'enfants, bipartite ribbon graphs, çarks, ambiguous forms, reciprocal forms, Markoff number.
The first named author is thankful to Max Planck Institute at Bonn for their hospitality during the preparation of the current paper. This research has been funded by the TÜBİTAK grant 110T690. The first named author is funded by a Galatasaray University Research Grant 15.504.002. The second named author is funded by Galatasaray University Research Grant 13.504.001. We are thankful to the referee for useful comments and questions.

diverse contexts through its action on mathematical objects, no matter what our level of abstraction is. Among all manifestations of $\mathrm{PSL}_2(\mathbf{Z})$ the following four classical actions are of fundamental nature:

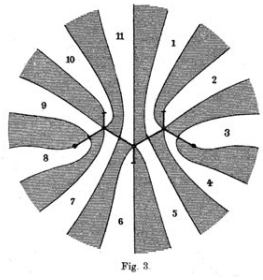
(1) its left-action on the infinite trivalent plane tree,
(2) its left action on the upper half plane $\mathcal{H}$ by Möbius transformations,
(3) its right-action on the binary quadratic forms, and
(4) its left-conjugation action on itself.

Our aim in this paper is to clarify the connections between these four actions. See [23] or [24] for an overview of the related subjects from a wider perspective. In particular, the actions in consideration will play a crucial role in observing non-trivial relations between Teichmüller theory and arithmetic. Such a point of view will be taken in a forthcoming paper where we construct a global groupoid whose objects are (roughly speaking) all ideal classes in real quadratic number fields and morphisms correspond to basic graph transformations known as flips. And this work can also be considered as an introduction to this upcoming work.

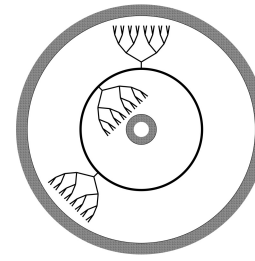
Let us turn back to our list of actions. The first one is transitive but not free on the set of neither edges nor vertices of the tree in question. In order to make it free on the set of edges, we add the midpoints as extra vertices thereby doubling the set of edges and call the resulting infinite tree the *bipartite Farey tree* $\mathcal{F}$. The modular group action is still transitive on the edge set of $\mathcal{F}$. Now since $\mathrm{PSL}_2(\mathbf{Z})$ acts on $\mathcal{F}$ by automorphisms; freely on the set of edges of $\mathcal{F}$, so does any subgroup Γ of $\mathrm{PSL}_2(\mathbf{Z})$, and by our definition a *modular graph*[1] is simply a quotient graph $\Gamma\backslash\mathcal{F}$. This is almost the same thing as a trivalent ribbon graph, except that we consider the midpoints as extra 2-valent vertices and pending edges are allowed. Modular graphs parametrize subgroups up to conjugacy and modular graphs with a base edge classify subgroups of the modular group.

The second action is compatible with the first one in the following sense: The tree $\mathcal{F}_{top} \subset \mathcal{H}$ which is built as the $\mathrm{PSL}_2(\mathbf{Z})$-orbit of the arc connecting two elliptic points on the boundary of the standard fundamental domain, is a topological realization of the Farey tree $\mathcal{F}$. Consequently, $\Gamma\backslash\mathcal{F}_{top} \subset \Gamma\backslash\mathcal{H}$ is a topological realization of the graph $\Gamma\backslash\mathcal{F}$, as a graph embedded in the orbifold $\Gamma\backslash\mathcal{H}$. This latter has no orbifold points if Γ is torsion-free but always has punctures due to the parabolic elements of Γ, or it has some boundary components. These punctures are in one-to-one correspondence with the left-turn circuits in $\Gamma\backslash\mathcal{F}$. Widening these punctures gives a deformation retract of the ambient orbifold to the graph, in particular the upper

[1]Contributing to the long list of names and equivalent/dual notions with various nuisances: trivalent diagrams, cyclic trivalent graphs, cuboid tree diagrams, Jacobi diagrams, trivalent ribbon graphs, triangulations; more generally, maps, ribbon graphs, fat graphs, dessins, polygonal decompositions, lozenge tilings, coset diagrams, etc.



(A) A dessin (linienzug of Klein) from 1879 [12]



(B) A çark in its ambient annulus

FIGURE 1.1

half plane $\mathcal{H}$ retracts to the Farey tree $\mathcal{F}_{top}$. To recover the orbifold from the modular graph one glues punctured discs along the left-turn paths of the graph.

If Γ is torsion-free of finite index, then $\Gamma\backslash\mathcal{H}$ is an algebraic curve which can be defined over a number field since it is a finite covering of the modular curve $\mathcal{M} = \mathrm{PSL}_2(\mathbf{Z})\backslash\mathcal{H}$. According to Belyĭ's theorem, [1], any arithmetic surface can be defined this way, implying in particular that the action of the absolute Galois group defined on the set of finite coverings $\{\Gamma\backslash\mathcal{H} \to \mathcal{M}\}$ is faithful. But these coverings are equivalently described by the graphs $\Gamma\backslash\mathcal{F}$. This striking correspondence between combinatorics and arithmetic led Grothendieck to study dessins from the point of view of the action of the absolute Galois group, see [14]. However, explicit computations of covering maps $\Gamma\backslash\mathcal{H} \to \mathcal{M}$ required by this approach turned out to be forbiddingly hard if one wants to go beyond some basic cases and only a few uniform theorems could be obtained. In fact, dessins are more general graphs that correspond to finite coverings of the thrice punctured sphere, which is equivalent to a subsystem of coverings of $\mathcal{M}$ since $\mathbf{P}^1\backslash\{0, 1, \infty\}$ is a degree-6 covering of $\mathcal{M}$.

The third action in our list is due to Gauss. Here $\mathrm{PSL}_2(\mathbf{Z})$ acts on the set of binary quadratic forms via change of variables in the well-known manner. Orbits of this action are called *classes* and forms in the same class are said to be *equivalent*. Here we are interested in the action on *indefinite* forms. This action always has a cyclic stabilizer group, which is called the proper automorphism group of the form f and denoted $\langle M_f \rangle$. Indefinite binary quadratic forms represent ideal classes in the quadratic number field having the same discriminant as the form and hence are tightly related to real quadratic number fields [4]. We provide a succinct introduction to binary quadratic forms later in the paper.

The correspondence between forms and dessins can be described briefly as follows: to an indefinite binary quadratic form f we associate its proper automorphism group $\langle M_f \rangle$ and to $\langle M_f \rangle$ we associate the infinite graph $\langle M_f \rangle \backslash \mathcal{F}$, which is called a *çark*[2]. Via the topological realization of $\mathcal{F}$, this is a graph embedded in the annulus $\langle M_f \rangle \backslash \mathcal{H}$. The form f_M corresponding to the matrix $M \in \mathrm{PSL}_2(\mathbf{Z})$ is found by homogenizing the fixed-point equation of M. Çarks are infinite "transcendental" graphs whereas the dessins literature consider only finite graphs. ("transcendental" since they correspond to non-algebraic extensions of the function field of the modular curve). This transcendence implies that çarks go undetected in the algebraic fundamental group approach, nevertheless we shall see that this does not keep them away from being arithmetic objects.

Equivalent forms have conjugate stabilizers (automorphism groups) and conjugate subgroups have isomorphic quotient graphs. It turns out that the set of classes is exactly the set of orbits of hyperbolic elements of $\mathrm{PSL}_2(\mathbf{Z})$ under the fourth (conjugation) action in our list. This set of orbits can be identified with the set of bracelet diagrams with beads of two colors.

In fact, çarks can be thought of as $\mathbf{Z}$-quotients of periodic rivers of Conway [5] or graphs dual to the coset diagrams of Mushtaq, [18]. As we shall see later in the paper, çarks provide a very nice reformulation of various concepts pertaining to indefinite binary quadratic forms, such as reduced forms and the reduction algorithm, ambiguous forms, reciprocal forms, the Markoff value of a form, etc. For example, çarks of reciprocal classes admit an involutive automorphism, and the quotient graph gives an infinite graph with two pending edges. These graphs parametrize conjugacy classes of dihedral subgroups of the modular group. Çarks also provide a more conceptual way to understand the relation between coset diagrams and quadratic irrationalities and their properties as studied in [18] or in [16].

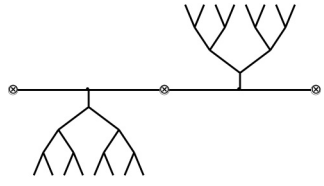


Figure 1.2. The graph of a reciprocal class. Edges of this graph parametrize the reciprocal forms in this class.

For us the importance of this correspondence between çarks and forms lies in that it suggests a concrete and clear way to consider modular graphs as arithmetic objects viz. Gauss' binary quadratic forms, as it was much

[2]Turkish *çark* (pronounced as "chark") is borrowed from the Persian, and it has a common etymology with Indian *chakra*, Greek *kyklos* and English *wheel*.

solicited by Grothendieck's dessins school. The graph language provides us with new points of view on the classical and deep questions concerning the behavior of class numbers. Yet the structure of class groups via such graphs is still a mystery. Moreover, the second named author, in [27], has presented an improvement of the age-old reduction algorithm of Gauss and gave an algorithmic solution to the representation problem of binary quadratic forms. The language of çarks might also provide a new insight to the real multiplication project of Manin and Marcoli, see [17].

Our computations concerning forms and their reduction are done in PARI/GP [22] with certain subroutines of our own (source code is available upon request, [28]).

2. Farey tree and modular graphs

It is well known that the two elliptic transformations $S(z) = -1/z$ and $L(z) = (z-1)/z$, respectively of orders 2 and 3, generate a group of Möbius transformations which is isomorphic to the projective group of two by two integral matrices having determinant 1, the modular group [3]. It is also well-known that $\mathrm{PSL}_2(\mathbf{Z}) \cong \langle S\rangle * \langle L\rangle = \mathbf{Z}/2\mathbf{Z} * \mathbf{Z}/3\mathbf{Z}$. Let us now consider the graph $\mathcal{F}$ (the bipartite Farey tree), given by the following data:

$$E(\mathcal{F}) = \{\{W\} \colon W \in \mathrm{PSL}_2(\mathbf{Z})\}$$
$$V(\mathcal{F}) = V_{\otimes}(\mathcal{F}) \sqcup V_{\bullet}(\mathcal{F});$$

where

$$V_{\otimes}(\mathcal{F}) = \{\{W, WS\} \colon W \in \mathrm{PSL}_2(\mathbf{Z})\},$$
$$V_{\bullet}(\mathcal{F}) = \{\{W, WL, WL^2\} \colon W \in \mathrm{PSL}_2(\mathbf{Z})\}.$$

is an edge between a vertex $v = \{W, WS\} \in V_{\otimes}(\mathcal{F})$ and another vertex $v' = \{W', W'L, W'L^2\}$ if and only if $\{W, WS\} \cap \{W', W'L, W'L^2\} \neq \emptyset$. There are no other edges. Thus the edge connecting v and v' *is* $v \cap v'$, if this intersection is non-empty. Observe that by construction the graph is bipartite. The edges incident to the vertex $\{W, WL, WL^2\} \in V_{\bullet}(\mathcal{F})$ are $\{W\}, \{WL\}, \{WL^2\}$, and these edges inherit a natural cyclic ordering from the vertex. Thus the Farey tree $\mathcal{F}$ is an infinite bipartite ribbon graph[3]. It is a tree since $\mathrm{PSL}_2(\mathbf{Z})$ is freely generated by S and L.

[3]A ribbon graph is a graph together with an ordering of the edges that are incident to each vertex in the graph.

The group $\mathrm{PSL}_2(\mathbf{Z})$ acts on $\mathcal{F}$ from the left, by ribbon graph automorphisms, where $M \in \mathrm{PSL}_2(\mathbf{Z})$ acts by

$$\{W\} \in E(\mathcal{F}) \mapsto \{MW\} \in E(\mathcal{F})$$
$$\{W, WS\} \in V_{\otimes}(\mathcal{F}) \mapsto \{MW, MWS\} \in V_{\otimes}(\mathcal{F})$$
$$\{W, WL, WL^2\} \in V_{\bullet}(\mathcal{F}) \mapsto \{MW, MWL, MWL^2\} \in V_{\bullet}(\mathcal{F})$$

Notice that the action on the set of edges is nothing but the left-regular action of $\mathrm{PSL}_2(\mathbf{Z})$ on itself and therefore is free. On the other hand the action is not free on the set of vertices: The vertex $\{W, WS\}$ is fixed by the order-2 subgroup generated by $M = WSW^{-1}$, and the vertex $\{W, WL, WL^2\}$ is fixed by the order-3 subgroup generated by $M = WLW^{-1}$.

Let Γ be any subgroup of $\mathrm{PSL}_2(\mathbf{Z})$. Then Γ acts on $\mathcal{F}$ from the left and to Γ we associate a quotient graph $\Gamma\backslash\mathcal{F}$ as follows:

$$E(\Gamma\backslash\mathcal{F}) = \{\Gamma \cdot \{W\} \colon W \in \mathrm{PSL}_2(\mathbf{Z})\}$$
$$V(\Gamma\backslash\mathcal{F}) = V_{\otimes}(\mathcal{F}/\Gamma) \cup V_{\bullet}(\mathcal{F}/\Gamma);$$

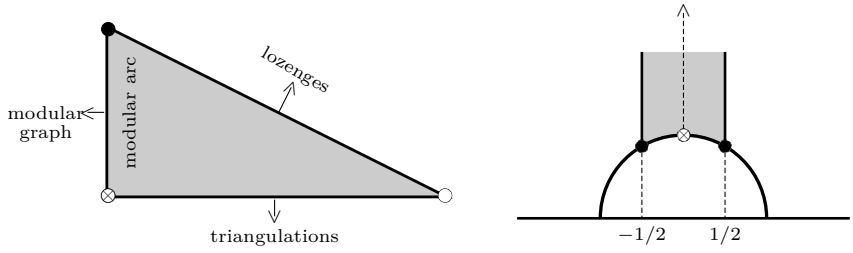
where

$$V_{\otimes}(\Gamma\backslash\mathcal{F}) = \{\Gamma \cdot \{W, WS\} \colon W \in \mathrm{PSL}_2(\mathbf{Z})\}, \text{ and}$$
$$V_{\bullet}(\Gamma\backslash\mathcal{F}) = \{\Gamma \cdot \{W, WL, WL^2\} \colon W \in \mathrm{PSL}_2(\mathbf{Z})\}.$$

It is easy to see that the incidence relation induced from the Farey tree gives a well-defined incidence relation and gives us the graph which we call a *modular graph*. Thus the edge connecting the vertices $v = \Gamma \cdot \{W, WS\}$ and $v' = \Gamma \cdot \{W', W'L, W'L^2\}$ is the intersection $v \sqcap v'$, which is of the form $\Gamma \cdot \{M\}$ if non-empty. There are no other edges. Observe that by construction the graph is bipartite. The edges incident to the vertex $\Gamma \cdot \{W, WL, WL^2\}$ are $\Gamma \cdot \{W\}, \Gamma \cdot \{WL\}, \Gamma \cdot \{WL^2\}$, and these edges inherit a natural cyclic ordering from the vertex[4]. In general $\Gamma\backslash\mathcal{F}$ is a bipartite ribbon graph possibly with pending vertices that corresponds to the conjugacy classes of elliptic elements that Γ contains. Conversely, any connected bipartite ribbon graph G, with $V(G) = V_{\otimes}(G) \sqcup V_{\bullet}(G)$, such that every $\otimes$-vertex is of degree 1 or 2 and every $\bullet$-vertex is of degree 1 or 3, is modular since the universal covering of G is isomorphic to $\mathcal{F}$. It takes a little effort to define the fundamental group of $\Gamma\backslash\mathcal{F}$ so that there is a canonical isomorphism $\pi_1(\Gamma\backslash\mathcal{F}, \Gamma \cdot \{I\}) \simeq \Gamma < \mathrm{PSL}_2(\mathbf{Z})$, with the canonical choice of $\Gamma \cdot \{I\}$ as a base edge. In general, subgroups Γ of the modular group (or equivalently the fundamental groups $\pi_1(\Gamma\backslash\mathcal{F})$) are free products of copies of $\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z}$ and $\mathbf{Z}/3Z$, see [13]. Note that two distinct isomorphic subgroups Γ_1, Γ_2 of the modular group may give rise to non-isomorphic ribbon graphs $\Gamma_1\backslash\mathcal{F}$ and $\Gamma_2\backslash\mathcal{F}$. We shall see shortly that çarks constitute good examples of this

[4]The ribbon graph structure around vertices of degree 2 is trivial.

phenomena. In other words, the fundamental group does not characterize the graph. Another basic invariant of $\Gamma\backslash\mathcal{F}$ is its genus, which is defined to be the genus of the surface constructed by gluing discs along left-turn paths. This genus is the same as the genus of the Riemann surface $\mathcal{H}/\Gamma$.



(A) The fundamental region for the modular curve in the upper half plane model.

(B) The modular curve. Note that there are two triangles, the second is on the back of the page, glued to this one.

FIGURE 2.1

The set of edges of $\Gamma\backslash\mathcal{F}$ is identified with the set of right-cosets of Γ, so that the graph $\Gamma\backslash\mathcal{F}$ has $[\mathrm{PSL}_2(\mathbf{Z}) : \Gamma]$ many edges. In case Γ is a finite index subgroup, the graph $\Gamma\backslash\mathcal{F}$ is finite. In case $\Gamma = \mathrm{PSL}_2(\mathbf{Z})$, the quotient graph $\mathrm{PSL}_2(\mathbf{Z})\backslash\mathcal{F}$ is a graph with one edge that looks like as follows:

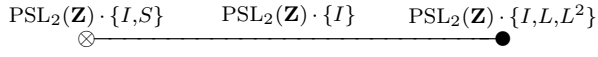
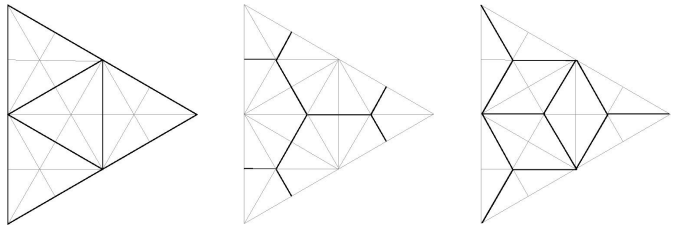


FIGURE 2.2. The modular arc.

We call this graph the *modular arc*, see Figure 2.2. It is a graph whose fundamental group is $\mathrm{PSL}_2(\mathbf{Z})$ and whose universal cover is the Farey tree $\mathcal{F}$. In other words modular graphs are coverings of the modular arc. If we consider the action of the modular group on the topological realization $\mathcal{F}_{top}$ of $\mathcal{F}$ mentioned in the introduction, the topological realization of $\mathrm{PSL}_2(\mathbf{Z})\backslash\mathcal{F}$ is the arc $\mathrm{PSL}_2(\mathbf{Z})\backslash\mathcal{F}_{top}$ in the modular curve connecting two elliptic points, see Figure 2.1b.

Every modular graph $\Gamma\backslash\mathcal{F}$ has a canonical "analytical" realization $\Gamma\backslash\mathcal{F}_{top}$ on the Riemann surface $\Gamma\backslash\mathcal{H}$ with edges being geodesic segments. Equivalently, these edges are lifts of the modular arc by $\Gamma\backslash\mathcal{H} \longrightarrow \mathrm{PSL}_2(\mathbf{Z})\backslash\mathcal{H}$. If instead we lift the geodesic arc connecting the $\otimes$- elliptic point to the cusp to the surface $\Gamma\backslash\mathcal{H}$, then we obtain another graph on the surface, which is called an *ideal triangulation*. Lifting the remaining geodesic arc gives rise to yet another type of graph, called a *lozenge tiling*, see Figure 2.1a. So

there is a triality, not just duality, of these graphs, see Figure 2.3 in which the bold figures represent the members of the triality.



(A) A triangulation (B) its dual graph (C) and its lozenge

FIGURE 2.3. Triality of graphs

In topology, there is a well-known correspondence between subgroups of the fundamental group of a space and the coverings of that space. The following two results are orbifold (or "stacky") analogues of this correspondence for coverings of the modular curve, stated in terms of graphs.

Proposition 2.1. *If* Γ_1 *and* Γ_2 *are conjugate subgroups of* $\mathrm{PSL}_2(\mathbf{Z})$*, then the graphs* $\Gamma_1\backslash\mathcal{F}$ *and* $\Gamma_2\backslash\mathcal{F}$ *are isomorphic as ribbon graphs. Hence there is a 1-1 correspondence between modular graphs and conjugacy classes of subgroups of the modular group.*

Proof. Let $\Gamma_2 = M\Gamma_1 M^{-1}$. The desired isomorphism is then the map

$$\begin{aligned} \varphi \,:\, E(\Gamma_1\backslash\mathcal{F}) &\to E(\Gamma_2\backslash\mathcal{F}) \\ \Gamma_1\cdot\{W\} &\mapsto \Gamma_2\cdot\{MW\}. \end{aligned}$$

Note that one has $\varphi(\Gamma_1\cdot\{I\}) = \Gamma_2\cdot\{M\}$. Suppose now that $\varphi : E(\Gamma_1\backslash\mathcal{F}) \to E(\Gamma_2\backslash\mathcal{F})$ is a ribbon graph isomorphism and let $\varphi(\Gamma_1\cdot\{I\}) = \Gamma_2\cdot\{M\}$. This induces an isomorphism of fundamental groups

$$\varphi_* : \pi_1(\Gamma_1\backslash\mathcal{F}, \Gamma_1\cdot\{I\}) \simeq \pi_1(\Gamma_2\backslash\mathcal{F}, \Gamma_2\cdot\{M\})$$

Since φ is a ribbon graph isomorphism, these two groups are also isomorphic as subgroups of the modular group. The former group is canonically isomorphic to Γ_1 a whereas the latter group is canonically isomorphic to

$$M^{-1}\pi_1(\Gamma_2\backslash\mathcal{F}, \Gamma_2\cdot\{I\})M \simeq M^{-1}\Gamma_2 M \qquad \square$$

Therefore modular graphs parametrize conjugacy classes of subgroups of the modular group, whereas the edges of a modular graph parametrize subgroups in the conjugacy class represented by the modular graph. In conclusion we get:

Theorem 2.2. *There is a 1-1 correspondence between modular graphs with a base edge (G, e) (modulo ribbon graph isomorphisms of pairs (G, e)) and subgroups of the modular group (modulo the isomorphisms induced by conjugation in $\mathrm{PSL}_2(\mathbf{Z})$).*

Theorem 2.3. *There is a 1-1 correspondence between modular graphs with two base edges (G, e, e') (modulo ribbon graph isomorphisms of pairs (G, e, e')) and cosets of subgroups of the modular group (modulo the isomorphisms induced by conjugation in $\mathrm{PSL}_2(\mathbf{Z})$).*

3. Çarks

A *çark* is a modular graph of the form $\c{C}_M := \langle M\rangle\backslash\mathcal{F}$ where M is a hyperbolic element of the modular group. One has

$$\pi_1(\langle M\rangle\backslash\mathcal{F}) = \langle M\rangle \simeq \mathbf{Z},$$

so the çark $\langle W\rangle\backslash\mathcal{F}$ is a graph with only one circuit, which we call the *spine* of the çark. Every çark has a canonical realization as a graph $\langle M\rangle\backslash\mathcal{F}_{top}$ embedded in the surface $\langle M\rangle\backslash\mathcal{H}$, which is an annulus since M is hyperbolic. In fact $\langle M\rangle\backslash\mathcal{H}$ is the annular uniformization of the modular curve $\mathcal{M}$ corresponding to $M \in \pi_1(\mathcal{M})$. Again by hyperbolicity of M, this graph will have infinite "Farey branches" attached to the spine in the direction of both of the boundary components of the annulus[5]. By Proposition 2.1 the graphs $\c{C}_M$ and $\c{C}_{XMX^{-1}}$ are isomorphic for every element X of the modular group and by Theorem 2.2 we deduce the following result, see [6]:

Theorem 3.1. *There are one-to-one correspondences between*

(i) *çarks and conjugacy classes of subgroups of the modular group generated by a single hyperbolic element, and*
(ii) *çarks with a base edge and subgroups of the modular group generated by a single hyperbolic element.*

A çark is said to be directed if we choose an orientation for the spine.

Corollary 3.2. *There are one-to-one correspondences between*

(i) *hyperbolic elements in the modular group and directed çarks with a base edge, and*
(ii) *conjugacy classes of hyperbolic elements in the modular group and directed çarks.*

[5]If M is parabolic, then $\langle W\rangle\backslash\mathcal{F}$ has Farey branches attached to the spine in only one direction, and its topological realization $\langle M\rangle\backslash\mathcal{F}_{top}$ sits on a punctured disc. If M is elliptic, $\langle W\rangle\backslash\mathcal{F}$ is a tree with a pending edge which abut at a vertex of type $\otimes$ when M is of order 2 and of type $\bullet$ when M is of order 3. Its topological realization $\langle M\rangle\backslash\mathcal{F}_{top}$ sits on a disc with an orbifold point.

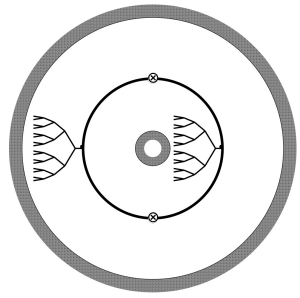
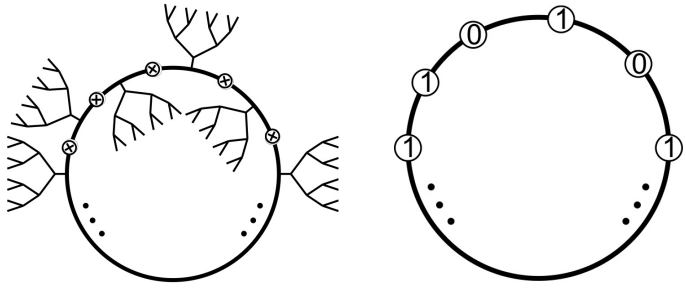


FIGURE 3.1. The çark $\mathcal{F}/\langle SL^2SL\rangle$.

3.1. Counting Çarks. Çarks are infinite graphs, and each edge of a çark carries a name which is an infinite coset. In fact, all the combinatorial information of a çark can be encoded in a finite storage as follows: First remove all $\otimes$-vertices of the çark. Next, turn once around the spine. Upon meeting a $\bullet$-vertex on which a branch attached by L, cut that branch and tag that $\bullet$-vertex with a "0". In a similar fashion, upon meeting a $\bullet$-vertex on which a branch attached by L^2, cut that branch and tag that $\bullet$-vertex with a "1". We obtain a finite graph called a *binary bracelet* which is by definition an equivalence class of binary strings under cyclic permutations (i.e. rotations) and reversals. As a çark has Farey branches expanding in the direction of both boundaries the corresponding bracelet has to have at least one 0 and one 1. Conversely, by using the convention $0 \leftrightarrow L$ and $1 \leftrightarrow L^2$ we can reconstruct the çark from its bracelet provided it contains at least one 0 and one 1, see Figure 3.2.

Rotations and reversals generate a finite dihedral group, and a binary bracelet may equivalently be described as an orbit of this action.



(A) (B)

FIGURE 3.2. From çarks to bracelets

For $n = 1, 2, ..., 15$ the number of binary bracelets with n vertices is

$$2, 3, 4, 6, 8, 13, 18, 30, 46, 78, 126, 224, 380, 687, 1224.$$

This is sequence A000029 (M0563) in OEIS [21]. The number of binary bracelets (çarks) of length n is

$$B(n) = \frac{1}{2}N(n) + \frac{3}{4}2^{n/2}$$

if n is even and

$$B(n) = \frac{1}{2}N(n) + \frac{1}{2}2^{(n+1)/2}$$

if n is odd where $N(n)$ is the number of binary necklaces of length n. An equivalence class of binary strings under rotations (excluding thus reversals) is called a *binary necklace*, or a *cyclic binary word*. They are thus orbits of words under the action of a cyclic group and they correspond to directed çarks. For $n = 1, 2, ..., 15$[6] the number of binary necklaces of length n is

$$N(n) = 2, 3, 4, 6, 8, 14, 20, 36, 60, 108, 188, 352, 632, 1182, 2192,$$

which is sequence A000031 (M0564) in OEIS. The number of necklaces (directed çarks) of length n is given by MacMahon's formula from 1892 (also called Witt's formula, see [2], [15]):

$$N(n) = \frac{1}{n}\sum_{d|n}\varphi(d)2^{n/d} = \frac{1}{n}\sum_{j=1}^{n}2^{\gcd(j,n)}$$

where φ is Euler's totient function.

A çark is called *primitive* if its spine is not periodic. Aperodic binary necklaces correspond to primitive directed çarks. For $n = 1, 2, ..., 15$ the number of aperiodic necklaces of length n is

$$L(n) = 2, 1, 2, 3, 6, 9, 18, 30, 56, 99, 186, 335, 630, 1161, 2182,$$

which is sequence A000031 (M0564) in the database. There is a formula for the number of aperiodic necklaces of length n in terms of Möbius' function μ:

$$L(n) = \frac{1}{n}\sum_{d|n}\mu(d)2^{n/d} = \frac{1}{n}\sum_{d|n}\mu(n/d)2^{d}$$

As mentioned, binary necklaces (or cyclic binary words or directed çarks) may be viewed as orbits of words under the action of the cyclic group. Choosing an ordering of our letters $\{0, 1\}$ (i.e. $0 < 1$) and imposing the lexicographic ordering of the words, one may choose a minimal representative in each orbit. The minimal representative of a primitive (aperiodic) word is called a *Lyndon word*. They were first studied in connection with the construction of bases for free Lie algebras and they appear in numerous contexts. In our case they are

$$0, 1, 01, 001, 011, 0001, 0011, 0111, 00001, 00011, 00101, 00111, 01011 \ldots$$

[6] $n = 1$ case is included for completeness. As remarked above there is no çark for $n = 1$ case.

One can similarly find representatives for aperiodic binary bracelets (=primitive indefinite binary quadratic forms; see below). There are effective algorithms to list all primitive necklaces and bracelets up to a given length (i.e. Duval's algorithm [7], the algorithm due to Fredricksen, Kessler and Maiorana [8], Sawada's algorithm [20], etc). Translated into the language of binary quadratic forms, this means that it is possible to single out a unique reduced representative in each class of a primitive indefinite binary quadratic form and that it is possible to effectively enumerate all classes of primitive indefinite binary quadratic forms by specifying those reduced representatives.

To sum up, we may represent primitive çarks by primitive bracelets. In order to shorten this representation further, we may count the number of consecutive 0's and 1's and represent çarks as sequences of natural numbers $(n_0, n_1, \dots n_{2k})^{0,1}$, if we agree that[7] this sequence encodes a bracelet that starts with a 0 if the exponent is 0 and 1 if the exponent is 1. This representation is directly connected to the "minus" continued fractions (see Zagier [25]).

A primitive word may have two types of symmetries: invariance under the swap of symbols $0 \leftrightarrow 1$ and invariance under reversal, i.e. palindromic symmetry. The first symmetry corresponds to ambiguous binary quadratic forms and the second symmetry corresponds to reciprocal binary quadratic forms, as we shall see. The swap of symbols $0 \leftrightarrow 1$ corresponds to inversion in the class group.

3.2. Çark Invariants. There are several natural invariants associated to a çark $Ç$. The combinatorial length $l_c(Ç)$ of its spine is an invariant. A hyperbolic invariant of a çark is the metric length $l_h(Ç)$ of the closed geodesic in the annular surface under its hyperbolic metric induced by the çark. A conformal invariant of a çark is the modulus $m(Ç)$ of the associated annulus. Finally, the discriminant $\Delta(Ç)$ of the associated form and the absolute value of the trace $\tau(Ç)$ of the associated matrix are two arithmetic invariants with $\Delta = \tau^2 - 4$. One has

$$l_h(Ç) = 2 \text{ arccosh } (\tau/2), \quad m(Ç) = \exp\left(\frac{\pi^2}{\log|\frac{\tau \pm \sqrt{\Delta}}{2}|}\right)$$

The modulus is found as follows: Any hyperbolic element $M \in PSL_2(\mathbf{R})$ is conjugate to an element of the form

$$N := XMX^{-1} = \begin{pmatrix} \alpha & 0 \\ 0 & \frac{1}{\alpha} \end{pmatrix}$$

where α is the multiplier of M. Since the trace is invariant under conjugation, one has $\tau := \text{tr}(M) = \alpha + 1/\alpha \Rightarrow \alpha^2 - \tau\alpha + 1 = 0 \Rightarrow \alpha = \frac{\tau \pm \sqrt{\tau^2 - 4}}{2}$.

[7] Note that a Lyndon word always start with a 0 and ends with a 1.

Now N acts by Möbius transformation $z \mapsto \alpha^2 z$, and the quotient map is $f(z) = z^{2\pi i/\log \alpha^2}$ with the annulus $f(\mathcal{H}) = \{z : e^{-2\pi^2/\log \alpha^2} < |z| < 1\}$ as its image. Hence the modulus of the ambient annulus of the çark is $e^{2\pi^2/\log \alpha^2} = e^{\pi^2/\log |\alpha|}$. It is possible to write down the uniformization $U_M : \mathcal{H} \to Ç_M$ explicitly, which is a quite involved expression. The annular uniformization $Ç_M \to \mathrm{PSL}_2(\mathbf{Z})\backslash\mathcal{H}$ can be written as $j \circ U_M^-$.

4. Binary Quadratic Forms and Çarks

A *binary quadratic form* is a homogeneous function of degree two in two variables $f(x, y) = Ax^2 + Bxy + Cy^2$ (denoted $f = (A, B, C)$ or in the matrix form:

$$W_f = \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} \tag{4.1}$$

so that $f(x, y) = (x, y)W_f(x, y)^t)$. If the coefficients A, B, C are integers the form is called *integral* with discriminant $\Delta(f) = B^2 - 4AC$. If f is integral and $\gcd(A, B, C) = 1$ then f is called *primitive*. Following Gauss we will call a form $f = (A, B, C)$ *ambiguous* if $B = kA$ for some $k \in \mathbf{Z}$. Finally a form $f = (A, B, C)$ will be referred to as *reciprocal* whenever $C = -A$, [19].

Note that $\Delta(f) = -4\det(W_f)$. Given a symmetric two by two matrix we write f_W to denote the binary quadratic form associated to W. Recall that a form f is called

- positive definite if and only if $\Delta(f) < 0$ and $A > 0$,
- negative definite if and only if $\Delta(f) < 0$ and $0 > A$,
- indefinite if and only if $\Delta(f) > 0$.

The group $\mathrm{PSL}_2(\mathbf{Z})$ acts on the set of all integral binary quadratic forms by

$$\begin{aligned} &\mathit{Forms} \times \mathrm{PSL}_2(\mathbf{Z}) \to \mathit{Forms} \\ &\qquad (f, U) \mapsto U \cdot f := f(U(x, y)^t) = (x, y)U^t W_f U(x, y)^t \end{aligned}$$

We call two binary quadratic forms *equivalent* if they belong to the same $\mathrm{PSL}_2(\mathbf{Z})$ orbit under the above action, under which discriminant is invariant. Let us denote the $\mathrm{PSL}_2(\mathbf{Z})$-orbit (or the equivalence class) of f by $[f]$. The stabilizer of f is called its *automorphism group*, denoted by $\mathrm{Aut}(f)$, and elements of $\mathrm{Aut}(f)$ are called automorphisms of f. For a positive definite binary quadratic form f, the group $\mathrm{Aut}(f)$ is trivial unless $\Delta(f) = -3$ or -4; $\mathrm{Aut}(f) \simeq \mathbf{Z}/4\mathbf{Z}$ if $\Delta(f) = -4$ and $\mathrm{Aut}(f) \simeq \mathbf{Z}/6\mathbf{Z}$ in case $\Delta(f) = -3$, [3, p. 29]. On the other hand, for an indefinite binary quadratic form one has $\mathrm{Aut}(f) \simeq \mathbf{Z}$.

Given an indefinite binary quadratic form $f = (A, B, C)$ a generator of its automorphism group will be called its *fundamental automorphism*. Note

that there are two fundamental automorphisms, one being M_f, the other being its inverse, M_f^{-1}. Every integral solution (α, β) of Pell's equation:

$$X^2 - \Delta(f)Y^2 = +4 \tag{4.2}$$

corresponds to an automorphism of f given by the matrix:

$$\begin{pmatrix} \frac{\alpha - B\beta}{2} & -C\beta \\ A\beta & \frac{\alpha + \beta B}{2} \end{pmatrix}.$$

It turns out that the fundamental automorphism is the one having minimal β, [3, Proposition 6.12.7].

Conversely, to any given (primitive) hyperbolic element[8], say

$$M = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{PSL}_2(\mathbf{Z})$$

let us associate the following binary quadratic form:

$$f_M = \frac{\mathrm{sgn}(p+s)}{\gcd(q, s-p, r)}(r, s-p, -q) \tag{4.3}$$

Observe first that $M \to f_M$ is well-defined and that its image is always primitive and indefinite. At this point let us state a direct consequence of Theorem 2.2:

Corollary 4.1. *The maps $\langle M \rangle \backslash \mathcal{F} \longleftrightarrow M \longrightarrow f_M$ defines a surjection from the set of oriented çarks with a base edge to primitive indefinite binary quadratic forms.*

Proof. We saw that an oriented çark with a base edge determines a hyperbolic element of $\mathrm{PSL}_2(\mathbf{Z})$. And this element in turn determines an indefinite binary quadratic form via $M \to f_M$. Conversely, given a primitive indefinite binary quadratic form $f = (A, B, C)$ to find $\beta \in \mathbf{Z}$ such that the matrix

$$\begin{pmatrix} \beta & A \\ -C & B + \beta \end{pmatrix} \in \mathrm{PSL}_2(\mathbf{Z})$$

we look at solutions (x, y) of Pell's equation $X^2 - \Delta(f)Y^2 = 4$. Using any such y we construct the hyperbolic element:

$$M_f = \begin{pmatrix} \beta & yC \\ yA & yB + \beta \end{pmatrix},$$

where $\beta = \frac{-yB \pm x}{2}$. Both choices of the sign produce a matrix which maps onto f. In fact, the two matrices are inverses of each other in $\mathrm{PSL}_2(\mathbf{Z})$. □

[8]There is no need to restrict to primitive elements because $f_M = f_{M^k}$ for any $k \in \mathbf{Z} \setminus \{0\}$.

Example 4.2. Consider the form $(1, 7, -1)$. It has discriminant 53. The pair $(51, 7)$ is a solution to the Pell equation $X^2 - 53Y^2 = 4$. The two β values corresponding to this solution are -50 and 1. Plugging these two values into the matrix above we get:

$$M_o = \begin{pmatrix} 1 & 7 \\ 7 & 50 \end{pmatrix} \text{ and } M_o^{-1} = \begin{pmatrix} -50 & 7 \\ 7 & -1 \end{pmatrix}.$$

The pair $(2599, 357)$ is also a solution to the above Pell equation, and the corresponding matrices are:

$$\begin{pmatrix} 50 & 357 \\ 357 & 2549 \end{pmatrix} \text{ and } \begin{pmatrix} -2549 & 357 \\ 357 & -50 \end{pmatrix}.$$

We would like to remark also that

$$M_o^2 = \begin{pmatrix} 50 & 357 \\ 357 & 2549 \end{pmatrix}.$$

In fact, M_o is one of the two fundamental automorphisms of f.

Note that the map $W \mapsto f_W$ is infinite to one because any indefinite binary quadratic form has infinite automorphism group. Any matrix in the automorphism group of f maps onto f.

Let $\mathcal{D} := \{d \in \mathbf{Z}_{>0} \colon d \equiv 0, 1 \pmod 4,\ d \text{ is not a square}\}$. Recall the following:

Proposition 4.3 ([19])**.** *There is a bijection between the set of conjugacy classes of primitive hyperbolic elements in* $\mathrm{PSL}_2(\mathbf{Z})$ *and the set of classes of primitive binary quadratic forms of discriminant* $\Delta \in \mathcal{D}$*; where a hyperbolic element is called primitive if it is not a power of another hyperbolic element.*

4.1. Reduction theory of binary quadratic forms. We say that an indefinite binary quadratic form $f = (A, B, C)$ is *reduced* if the geodesic in $\mathcal{H}$ connecting the two real fixed points of W_f, called the *axis* of W_f and denoted by $\mathfrak{a}_{W_f}$, intersects with the standard fundamental domain of the modular group. Remark that this definition is equivalent to the one given by Gauss in [9][9]. The equivalence of the two definitions is folklore.

The $\mathrm{PSL}_2(\mathbf{Z})$ class of an indefinite binary quadratic form contains more than one reduced form as opposed to definite binary quadratic forms where the reduced representative is unique, see [3, Section 6.8] or [4, Section 5.6] for further discussion. The classical reduction is the process of acting on a non-reduced form $f = (A, B, C)$ by the matrix

$$\rho(f) = \begin{pmatrix} 0 & 1 \\ 1 & t(f) \end{pmatrix} = S(LS)^{t(f)};$$

[9]Recall that Gauss defined a form to be reduced if $|\sqrt{\Delta} - 2|A|| < B < \sqrt{\Delta}$.

where

$$t(f) = \left\{ \begin{array}{ccc} \operatorname{sgn}(c) \left\lfloor \frac{b}{2|c|} \right\rfloor & \text{if} & |c| \geq \sqrt{\Delta} \\ \operatorname{sgn}(c) \left\lfloor \frac{\sqrt{\Delta}+b}{2|c|} \right\rfloor & \text{if} & |c| < \sqrt{\Delta} \end{array} \right\},$$

and checking whether the resulting form is reduced or not. It is known that after finitely many steps one arrives at a reduced form, call f_o. Applying $\rho(f_o)$ to f_o produces again a reduced form. Moreover, after finitely many iterations one gets back f_o. And this set of reduced indefinite binary quadratic forms is called the cycle of the class.

Our aim is now to reveal the reduction method due to Gauss in terms of çarks. Recall that every edge of a çark may be labeled with a unique coset of the corresponding subgroup. That is to say binary quadratic forms may be used to label the edges of the çark by Corollary 3.2. Let us denote the edge on the çark corresponding to a form g in the $\mathrm{PSL}_2(\mathbf{Z})$-class of f by e_g.

Given a hyperbolic element W as a word in L, L^2 and S we define the length of W, $\ell(W)$, to be the total number of appearances of L, L^2 and S. For instance for $W = LSL^2S(LS)^2$, $\ell(W) = 8$.

A fundamental automorphism of a given form f (or the primitive hyperbolic element corresponding to f) is obtained from the çark of f as follows let γ_f be the path starting at e_f making a one turn counterclockwise around the spine and then ending at e_f. On traversing γ_f we write S if we visit a vertex of degree 2 and L (L^2 resp.) if we visit a vertex of degree 3 and the next edge on γ_f is on the left (right resp.). For instance, the automorphism of the form $(-1, 4, -2)$ is the word $L^2S\,LS\,(L^2S)^2\,L^2$, see Figure 4.9.

Lemma 4.4. *Given an indefinite binary quadratic form (reduced or non-reduced), $f = (a, b, c)$, let W_f be a primitive hyperbolic element corresponding to f. Then*

$$\ell(W_{\rho(f)\cdot f}) \leq \ell(W_f). \tag{4.4}$$

Proof. We first observe that every reduction operator is either a left turn (i.e. a word comprised only of $(SL)^n$, for some positive integer n) or a right turn (i.e. a word comprised only of $(L^2S)^n$ for some positive integer n.) path. Say $\rho(f) \cdot f = (a', b', c')$. A simple argument allows us to conclude that $|b'| < |b|$ and we have either $|a'| < |a|$ and $c = c'$ or $|c'| < |c|$ and $a = a'$. That is, either $|a|$ or $|c|$ gets smaller. So it is enough to see that the bigger the distance (i.e. number of edges) between e_f and the spine is the higher the components a, b, c of f are. This phenomenon can be explained by a kind of arithmetic progression on the *edges* of the corresponding çark. Indeed, if $ac < 0$ it is immediate to see that $\rho(f) \cdot f$ is reduced (even if f is reduced, see Lemma 4.7) and that $\ell(W_{\rho(f)\cdot f}) = \ell(W_f)$. The action of $\rho(f)$

on f is given by:

$$(SL)^n \cdot f = (a - nb + n^2c, b - 2nc, c)$$
$$(SL^2)^n \cdot f = (a, -2an + b, n^2a - nb + c).$$

The action of S on f produces the form $(c, -b, a)$. Therefore we may assume that the sign of b is opposite to that of a and c. It is then easy to see that under these circumstances the functions $a - nb + n^2c$ and $n^2a - nb + c$ (as functions of $n \in \mathbf{N}$) are strictly increasing. □

Let us assume from now on that our çarks are embedded into an annulus, with an orientation which we will assume to be the usual one.[10] In addition, we also introduce the following shorter notation for our çarks: in traversing the spine (in either direction) if there are n consecutive Farey branches in the direction of the same boundary component, then we denote this as a single Farey component and write n on the top of the corresponding branch, see Figure 4.1. We will call such çarks *weighted*.

Definition 4.5. Let $Ç$ be a weighted çark. Edges of the spine are called *semi-reduced*. In particular, an edge on the spine of $Ç$ is called *reduced* if and only if it is on the either side of a Farey component which is in the direction of the inner boundary component.

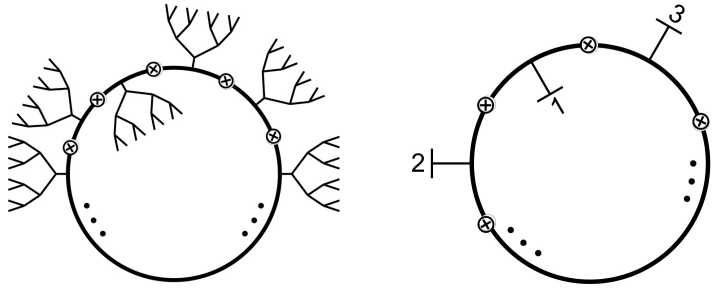


FIGURE 4.1. A çark and its short form.

Remark that as we have fixed our orientation to be the usual one, there is no ambiguity in this definition. In addition note that semi-reduced edges are in one to one correspondence between the forms $f = (A, B, C)$ in a given class for which $AC < 0$. We are now ready to describe reduction theory of binary quadratic forms in terms of çarks. We have seen that multiplication by the matrix $\rho(f)$ is, in general, the process of moving the base edge of the çark to the spine as a result of Lemma 4.4. However, this is not enough. That is, not every edge on the spine corresponds to a reduced

[10] Although theoretically unnecessary, the choice of an orientation will simplify certain issues. For instance, we shall see that inversion in the class group is reflection with respect to spine.

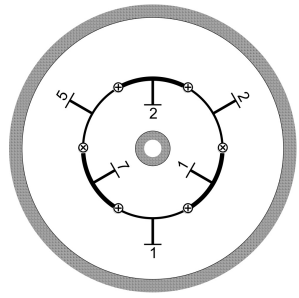


Figure 4.2. Çark corresponding to the class represented by the form $(7, 33, -15)$. Bold edges are reduced.

form. Reduced forms correspond to edges where the Farey branches switch from one boundary component to the other. More precisely, we have:

Theorem 4.6. *Reduced forms in an arbitrary indefinite binary quadratic form class $[f]$ are in one to one correspondence between the reduced edges of the çark corresponding to the given class.*

As we have remarked the action of $\mathrm{PSL}_2(\mathbf{Z})$ on binary quadratic forms is equivalent to the change of base edge on the set of çarks. Hence the above Theorem is an immediate consequence of the following:

Lemma 4.7 ([3, Corollary 6.8.11])**.** *Let $Ç_f$ denote the çark associated to an arbitrary indefinite binary quadratic form f. The reduction operator $\rho(f)$ is transitive on the set of reduced edges of $Ç_f$.*

Let us give some examples:

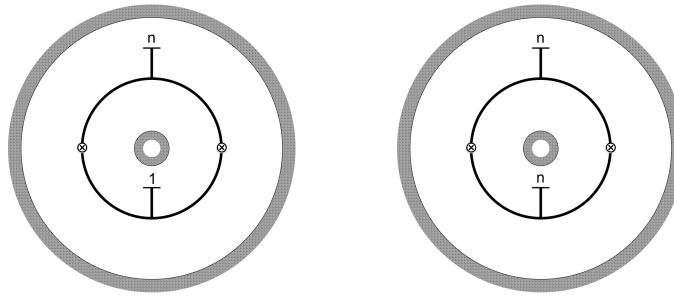
Example 4.8. Let us consider the form $f = (7, 33, -15)$. It is easy to check that f is reduced.

$$W_f = (L^2S)^2\,(LS)^2\,L^2S\,LS\,(L^2S)^7\,(LS)^5 = \begin{pmatrix} -38 & -195 \\ -91 & -467 \end{pmatrix}$$

The trace of the class is -505. By Gauss' theory the class $[f]$ is an element in the quadratic number field with discriminant 1509. We refer to Figure 4.2 for the corresponding çark.

Example 4.9. Let $\Delta = n^2 + 4n$ for some positive integer n. Then the identity in the class group is given by the çark in Figure 4.3a and the corresponding form is $(-n, n, 1)$. If $\Delta = n^2 + 4$, then the identity is represented by the form $\frac{1}{n}(-n, n^2, n) = (1, n, -1)$. The corresponding çark has two Farey branches, see Figure 4.3b.

However, one has to admit that there are very complicated çarks representing the identity of the class group. For instance, the çark corresponding to the form $(-7, 23, 16)$ has 42 Farey branches.



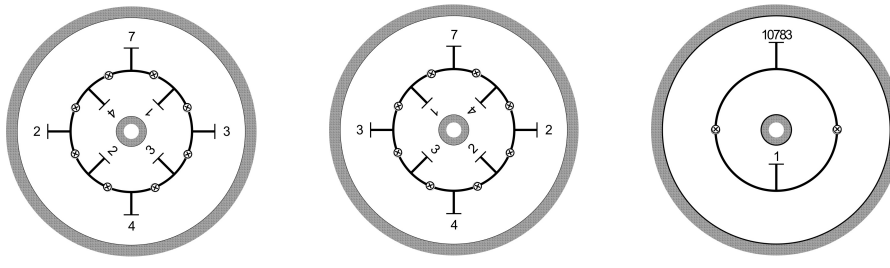
(A) Identity for $\Delta = n^2 + 4n$. (B) Identity for $\Delta = n^2 + 4$.

FIGURE 4.3.

4.2. Ambiguous and Reciprocal forms. Let us now discuss certain symmetries of a çark. For a given çark $Ç$ let $Ç^r$ be the çark which is the mirror image of $Ç$ about any line passing through the 'center" of the spine (assuming that the Farey components coming out of the spine in its shorter notation that we have introduced is evenly spaced). It is easy to see that both ideal classes represented by the two çarks $Ç$ and $Ç^r$ have the same discriminant. A straightforward computation leads to the following:

Proposition 4.10. *Given a çark $Ç$ the binary quadratic form class represented by $Ç^r$ is inverse of the class represented by $Ç$.*

Example 4.11. Let us consider the form $f = (-2377, 10173, 1349)$ having discriminant 116316221. The form $g = (-4027, 8915, 2287)$ is an element in the ideal class represented by this form. The corresponding çarks are shown in Figure 4.4. The forms are inverses of each other.



(A) Çark corresponding to $f = (-2377, 10173, 1349)$.

(B) Çark corresponding to $f^{-1} = (-4027, 8915, 2287)$.

(C) Çark of the product of $f \times f^{-1}$.

FIGURE 4.4. Two çarks inverses of one another and their product.

Recall that Gauss has defined a binary quadratic form to be ambiguous if it is equivalent to its inverse or equivalently if the corresponding equivalence

class contains (a, ka, c) for some a, c and k. Following Gauss, we define a çark $\mathcal{Ç}$ *ambiguous* if $\mathcal{Ç}$ and $\mathcal{Ç}^r$ are isomorphic as çarks, or equivalently correspond to the same subgroup of $\mathrm{PSL}_2(\mathbf{Z})$. So from Proposition 4.10 we deduce:

Corollary 4.12. *Ambiguous çarks correspond to ambiguous forms.*

In addition to all the examples considered in Example 4.9, which represent ambiguous classes as they are of the form (a, ka, c), let us give one more example:

Example 4.13. Consider the form $f = (3, 18, -11)$. The form is reduced and ambiguous as one immediately checks. The corresponding çark is given in Figure 4.5.

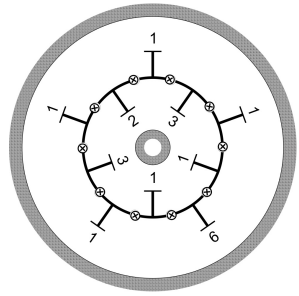


Figure 4.5. Çark corresponding to the ambiguous form $f = (3, 18, -11)$.

Let us now discuss "rotational" symmetries. In Section 3.1 we defined a directed çark with a base edge *primitive* if and only if its spine is not periodic. Let $\mathfrak{c}_{prim}$ denote the set of primitive çarks. It is easy to see that primitive hyperbolic elements[11] in $\mathrm{PSL}_2(\mathbf{Z})$ correspond to primitive çarks or equivalently to prime geodesics in $\mathbb{H}$.

Corollary 4.14. *There is a one to one correspondence between the following two sets:*

$$\mathfrak{c}_{prim} \quad \longleftrightarrow \quad \left\{ \begin{array}{c} \mathrm{PSL}_2(\mathbf{Z}) \textit{ classes of primitive} \\ \textit{indefinite binary quadratic forms} \end{array} \right\}$$

Finally, let $\mathcal{Ç}^m$ denote the mirror of a given çark, that is the çark obtained by reflecting $\mathcal{Ç}$ with respect to the spine. Once again observe that both $\mathcal{Ç}$ and $\mathcal{Ç}^m$ have the same discriminant. In fact, an indefinite binary quadratic form say $f = (A, B, C)$ is given which is represented by the çark $\mathcal{Ç}$ then the çark $\mathcal{Ç}^m$ represents the form $f' = (-A, B, -C)$ and the same

[11] Recall that an element $M \in \mathrm{PSL}_2(\mathbf{Z})$ is said to be *primitive* if it is not a positive power of another element of the modular group.

holds for every element in $[f]$. We conclude that both çarks represent ideal classes that have the same order in the class group.

Let W be a hyperbolic element in $\mathrm{PSL}_2(\mathbf{Z})$. In [19], Sarnak has defined W to be reciprocal if W is conjugate to its inverse. The conjugation turns out to be done by a unique element (up to multiplication by an element in $\langle W\rangle$) of order 2, and thus reciprocal elements correspond to dihedral subgroups of the modular group[12]. A form $f = (A, B, C)$ is called reciprocal if $C = -A$. It is known that reciprocal hyperbolic elements correspond to reciprocal indefinite binary quadratic forms, [19]. In a similar fashion we call a çark *reciprocal* if $Ç$ and $(Ç^m)^r$ are isomorphic as çarks, see Figures 4.6 and 4.7 for two examples. In fact since two operators $\cdot^m$ and $\cdot^r$ commute, if $Ç$ is a reciprocal çark then so is $Ç^m$.

Proposition 4.15. *Reciprocal forms correspond to reciprocal çarks.*

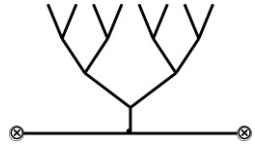


FIGURE 4.6. The graph $\mathcal{F}/\langle S, L^2SL\rangle$

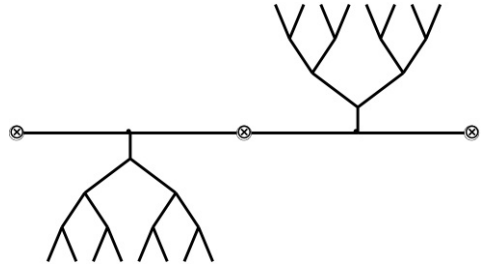


FIGURE 4.7. The graph $\mathcal{F}/\langle LSL^2, S(LSL^2)S\rangle$

Example 4.16. Consider the form $f = (-8, 11, 8)$. The corresponding hyperbolic element in $\mathrm{PSL}_2(\mathbf{Z})$ is $\begin{pmatrix} 101 & -192 \\ -192 & 365 \end{pmatrix}$. The corresponding çark is shown in Figure 4.8, where it is easy to see that $Ç$ and $(Ç^m)^r$ are same.

Example 4.17 (Reciprocal Identities)**.** The forms $f = (1, n^2, -1)$ already appeared in Example 4.9 are reciprocal and represent identity in the class group. Note also that such forms come from the word $(L^2S)^n(LS)^n$. The çarks of these reciprocal identities are in Figure 4.3b.

[12]Remember that primitive çarks correspond to maximal $\mathbf{Z}$-subgroups of $\mathrm{PSL}_2(\mathbf{Z})$.

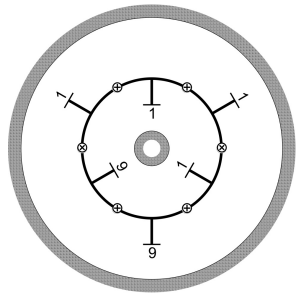


FIGURE 4.8. Çark corresponding to the reciprocal form $f = (-8, 11, 8)$.

4.3. Miscellany. Binary quadratic forms is a central and classical topic and have connections to diverse fields. Here we touch upon some of these.

4.3.1. ***Computational Problems.*** There are several important computational problems related to çarks, in connection with the class number problems in the indefinite case. The most basic invariant of a çark is the length of its spine. The (absolute) trace of the associated matrix is another, much subtler invariant. The problem of listing çarks of the same trace is equivalent to the problem of computing class numbers. Also, the Gauss product on classes of forms defines an abelian group structure on the set çarks of the same trace, namely the *class group*. It is a work in progress to reach to a new understanding of class groups in terms of the graphical representation of their elements by çarks.

4.3.2. ***Closed geodesics on the modular surface.*** Let us note in passing that primitive çarks parametrize closed geodesics on the modular curve, and so çarks are closely connected to symbolic dynamics on the modular curve, see [11], encoding of geodesics, and Selberg's trace formula, see [26].

4.3.3. ***The Markoff number of an indefinite binary quadratic form.*** There is an arithmetic invariant of indefinite binary quadratic forms called the Markoff value $\mu(F)$ which is defined as

$$\mu(F) := \frac{\sqrt{\Delta(F)}}{m(f)}, \text{ where } m(f) := \min_{(x,y)\in\mathbf{Z}^2\setminus\{(0,0)\}} |F(x,y)|$$

Alternatively one can run over the class of F and compute the minima of equivalent forms at a fixed point p_0, for example $(x, y) = (0, 1)$. Hence the choice of this fixed point p_0 defines a function on the set of edges of the associated çark, and the Markoff value of the form is the maximal value attained by this function defined on the çark. There are also çarks associated to Markoff irrationalities which we call *Markoff çarks*. A solution to the representation problem of indefinite binary quadratic forms is given

in [27] and as a by-product Markoff value of a given form can be computed. The algorithms will be available within the software developed by the first two authors and their collaborators, [10].

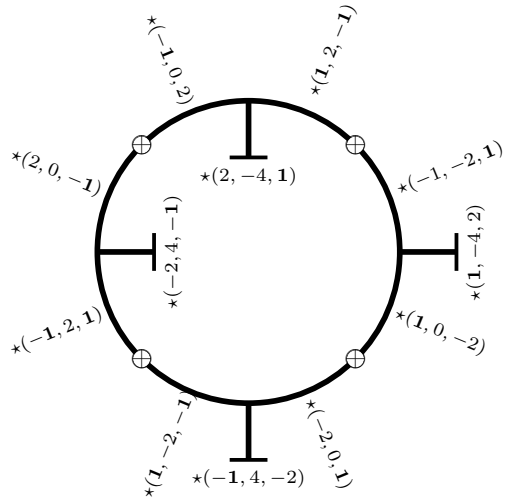


FIGURE 4.9. Minimum edges of $\mathcal{F}/Aut(\{(1,0,-2)\})$. Every form on the spine attains the minimum. This is, however, not the general case.

To conclude the paper, let us rephrase our main result: we show that the class of every primitive indefinite binary quadratic form is not simply a set but it has the extra structure of an infinite graph, namely a çark, such that the forms in the class are identified with the edges of the graph. This graph admits a topological realization as a subset of an annulus and explains very well some known phenomena around Gauss' reduction theory of forms and Zagier's reduction of elements of $\mathrm{PSL}_2(\mathbf{Z})$ as explained in [11]. In our point of view both Gauss reduced forms and Zagier reduced forms correspond to edges on the what we call spine of the çark. Various properties of forms and their classes are manifested in a natural way on the çark. The first instance of such a question concerning binary quadratic forms has been addressed by the second named author in [27], where he has given an improvement of Gauss' reduction of binary quadratic forms, and has given solutions to the minimum problem and representation problem of binary quadratic forms.

References

[1] G. V. Belyĭ, "On Galois extensions of a maximal cyclotomic field", *Math. USSR, Izv.* **14** (1980), p. 247-256.

[2] S. Bouallegue & M. Naimi, "On primitive words", *Int. J. Algebra* **4** (2010), no. 13-16, p. 693-707.

[3] J. Buchmann & U. Vollmer, *Binary quadratic forms. An algorithmic approach.*, Algorithms and Computation in Mathematics, vol. 20, Springer, 2007, xiv+318 pages.

[4] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer, 1993, xxi+534 pages.

[5] J. H. Conway, *The sensual (quadratic) form*, The Carus Mathematical Monographs, vol. 26, The Mathematical Association of America, 1997, xiii+152 pages.

[6] M. Durmuş, "Farey graph and binary quadratic forms", PhD Thesis, Istanbul Technical University, Turkey, 2012.

[7] J.-P. Duval, "Génération d'une section des classes de conjugaison et arbre des mots de Lyndon de longueur bornée", *Theor. Comput. Sci.* **60** (1988), no. 3, p. 255-283.

[8] H. Fredricksen & I. Kessler, "Lexicographic compositions and de Bruijn sequences", *J. Comb. Theory* **22** (1977), p. 17-30.

[9] C. F. Gauss, *Disquisitiones arithmeticae*, Yale University Press, 1966, xx+472 pages.

[10] T. Infomod, "Sunburst version `0`", available at `http://math.gsu.edu.tr/azeytin/infomod/node/3`, 2013.

[11] S. Katok & I. Ugarcovici, "Symbolic dynamics for the modular surface and beyond", *Bull. Am. Math. Soc.* **44** (2007), no. 1, p. 87-132.

[12] F. Klein, "Über die Transformation elfter Ordnung der elliptischen Functionen", *Clebsch Ann.* **XV** (1879), p. 533-555.

[13] R. S. Kulkarni, "An arithmetic-geometric method in the study of the subgroups of the modular group", *Am. J. Math.* **113** (1991), no. 6, p. 1053-1133.

[14] S. K. Lando & A. K. Zvonkin, *Graphs on surfaces and their applications*, Encyclopaedia of Mathematical Sciences, vol. 141, Springer, 2004, xv+455 pages.

[15] P. A. MacMahon, "Applications of a Theory of Permutations in Circular Procession to the Theory of Numbers", *Proc. Lond. Math. Soc.* **s1-23** (1891), no. 1, p. 305-318.

[16] M. Malik & M. Zafar, "Real quadratic irrational numbers and modular group action", *Southeast Asian Bull. Math.* **35** (2011), no. 3, p. 439-445.

[17] Y. I. Manin, "Real multiplication and noncommutative geometry (ein Alterstraum)", in *The legacy of Niels Henrik Abel*, Springer, 2004, p. 685-727.

[18] Q. Mushtaq, "Modular group acting on real quadratic fields", *Bull. Aust. Math. Soc.* **37** (1988), no. 2, p. 303-309.

[19] P. Sarnak, "Reciprocal geodesics", in *Analytic number theory. A tribute to Gauss and Dirichlet*, Clay Mathematics Proceedings, vol. 7, American Mathematical Society, 2007, p. 217-237.

[20] J. Sawada, "Generating Bracelets in Constant Amortized Time", *SIAM J. Comput.* **31** (2001), no. 1, p. 259-268.

[21] N. J. A. Sloane, "The On-Line Encyclopedia of Integer Sequences", published electronically at `http://oeis.org/`.

[22] The PARI Group, "PARI/GP version `2.5.0`", 2012, available at `http://pari.math.u-bordeaux.fr/`.

[23] A. M. Uludağ, "The modular group and its actions, Volume I", in *Handbook of group actions*, Advanced Lectures in Mathematics, vol. 31, International Press and Higher Education Press, 2015, p. 333-370.

[24] A. M. Uludağ & A. Zeytin, "A panorama of the fundamental group of the modular orbifold", in *Handbook of Teichmüller Theory, Vol. VI*, IRMA Lectures in Mathematics and Theoretical Physics, vol. 27, European Mathematical Society, 2016, p. 501-519.

[25] D. B. Zagier, *Zetafunktionen und quadratische Körper. Eine Einführung in die höhere Zahlentheorie*, Hochschultext, Springer, 1981, ix+144 pages.

[26] ———, "New points of view on the selberg zeta function", in *Proceedings of Japanese-German Seminar*, Ryushi-do, 2002, p. 1-10.
[27] A. Zeytin, "On reduction theory of binary quadratic forms", *Publ. Math.* **89** (2016), p. 203-221.
[28] A. Zeytin, H. Ayral & A. M. Uludağ, "InfoMod: A visual and computational approach to Gauss' binary quadratic forms", `https://arxiv.org/abs/1704.00902`, 2017.

A. Muhammed Uludağ
Department of Mathematics, Galatasaray University
Turkey
E-mail: `muludag@gsu.edu.tr`
URL: `http://math.gsu.edu.tr/uludag/`

Ayberk Zeytin
Department of Mathematics, Galatasaray University
Turkey
E-mail: `azeytin@gsu.edu.tr`
URL: `http://math.gsu.edu.tr/azeytin/`

Merve Durmuş
Department of Mathematics, Yeditepe University
Turkey
E-mail: `merve1988durmus@gmail.com`