MONODROMY GROUPS OF DESSINS D'ENFANT ON RATIONAL POLYGONAL BILLIARDS SURFACES

RICHARD A. MOY

Lee University
rmoy@leeuniversity.edu

JASON SCHMURR

Lee University
jschmurr@leeuniversity.edu

JAPHETH VARLACK

Wake Forest University
varlja22@wfu.edu

ABSTRACT. A *dessin d'enfant*, or *dessin*, is a bicolored graph embedded into a Riemann surface, and the monodromy group is an algebraic invariant of the dessin generated by rotations of edges about black and white vertices. A *rational polygonal billiards surface* is a Riemann surface that arises from the dynamical system of billiards within a rational-angled polygon. In this paper, we compute the monodromy groups of dessins embedded into rational polygonal billiards surfaces and identify all possible monodromy groups arising from rational triangular billiards surfaces.

1. Introduction

Monodromy groups of dessins d'enfant have been studied extensively [1, 2, 6, 5, 7]. In [14], the authors investigated the connection between rational triangular billiards surfaces and dessins d'enfant and classified the monodromy groups of dessins drawn on these surfaces. In this paper, we generalize the main result in [14] by computing the monodromy groups of *dessins d'enfant* drawn on billiard surfaces of *k-gons* with $k \geq 3$.

We show that all such monodromy groups can be expressed as the semidirect product $N \rtimes C_k$, where N is isomorphic to the column span of a circulant matrix over $\mathbb{Z}/n\mathbb{Z}$ for an appropriate integer n (Theorem 1 and Lemma 4) and C_k is the cyclic group of order k.

In Section 4, we show how to use the Smith Normal Form to explicitly compute the monodromy group of any given rational billiards surface (Theorem 2).

Next, for the case when $n = p$ for some prime p, we establish a correspondence between k-gons modulo p and elements of $\mathbb{F}_p[x]$ which has the useful property that the monodromy group of the k-gon is completely determined by the greatest common divisor of the polynomial and $x^k - 1$(Proposition 6). This correspondence allows us to complete the classification of all monodromy groups of polygonal billiard surfaces for *k-gons* when $n = p$ is prime and $p > k$ (Theorem 4). Showing this correspondence requires proving the existence of polynomials over $\mathbb{F}_p$ with all non-zero coefficients that have the appropriate greatest common divisor with $x^k - 1$.

2000 *Mathematics Subject Classification.* Primary 14H57; Secondary 11C08, 11R09, 15B05, 37C83.

Finally, in Section 9, we provide some preliminary results for composite n which are sufficient to give a complete classification for triangles and an analogue of the main result in [14] for quadrilaterals.

Throughout this paper, we will reference many well known algebraic and number theoretic results. See any introductory graduate abstract algebra book, such as [3], or number theory book, such as [12], for a reference.

2. Background

2.1. ***The Rational Billiard Surface Construction.*** A rational billiards surface is constructed by gluing together copies of a polygon that result from consecutive reflections across the sides. This name is motivated by the task of examining the paths of balls that bounce around the interior of a billiard table. When a ball hits a side of the table, the resulting bounce is instead represented by gluing a reflection of the table across that side and continuing the billiard path in the reflected copy in the same direction. This way, the path of a ball is represented by a single geodesic on a flat surface instead of a jagged path that may cross back on itself. Equipped with this intuition, a rational billiards surface is constructed from all of the reflections required to account for every possible path a ball could take.

More formally, a rational billiard surface can be constructed from a k-gon P whose angles are rational multiples of π, in the following way. Label the sides of P as $e_0, \dots e_{k-1}$, in consecutive counterclockwise order around P. Label the angles of P as $\theta_i = \dfrac{a_i\pi}{n}$, where θ_i is the internal angle formed by sides e_i and e_{i+1} and $n \in \mathbb{N}$ is the least common denominator for the various $\dfrac{a_i}{n}$. Let Γ be the dihedral group generated by the reflections $r_0, \dots, r_{k-1}$ across lines through the origin parallel to the corresponding sides of P. This group consists of $2n$ elements [4], consisting of n Euclidean rotations and n Euclidean reflections. The rotation subgroup of Γ is generated by rotation by the angle $\dfrac{2\pi}{n}$. Hence we may label the rotations using the notation ρ_m for rotation by an angle of $\dfrac{2m\pi}{n}$. Let $\mathscr{P} = \{\gamma(P) : \gamma \in \Gamma\}$. For each $\gamma(P) \in \mathscr{P}$ and each r_i, we glue together $\gamma(P)$ and $\gamma r_i(P)$ along their copies of e_i. The resulting object X is a Riemann surface called a *translation surface*. This is because, if we let $\tilde{X}$ be the be the flat surface obtained by puncturing all singularities of X, then all transition functions of $\tilde{X}$ are translations. See [17] and [18] for a detailed description of the rational billiards construction.

2.2. ***Defining a Monodromy Group on the Surface.*** Next, we draw a graph on this surface by placing a vertex in the center of each copy of P and labeling it with the corresponding element of Γ. We draw an edge between two vertices α and β precisely when $\alpha = \beta r_i$ for some i. This graph is the Cayley graph for Γ with generating set $r_0, \dots, r_{k-1}$. See [16] for a more in-depth exposition on this graph.

Since the generating set consists of reflections, this graph is bipartite, where one partite vertex set is the set of Euclidean rotations in Γ and the other partite vertex set is the set of Euclidean reflections in Γ.

We will define a labeling scheme, introduced in [14], for the edges of the graph in following way. Take an arbitrary edge of the graph; one endpoint will be a vertex labeled ρ_m and the other endpoint will be $\rho_m r_i$, for integers m and i. We label this edge with the ordered pair $(m,i) \in C_n \times C_k$ where $C_n \times C_k$ is viewed as a set and not a group. (Here, C_n represents the cyclic group of order n.) In fact this defines a bijection between the edge set of the graph and $C_n \times C_k$.

We can define a *dessin d'enfant* on the surface by assigning a color to each of the partite sets (say, black for rotation and white for reflection) and by defining a cyclic ordering of the edges (oriented counterclockwise) around each vertex [11]. The ordering around a black vertex ρ_m is $(m,0),(m,1),\dots,(m,k-1)$, and the ordering around a white vertex $\rho_m r_i$ is $(m,i),(m-a_{i-1},i-1),(m-a_i-a_{i-1},i-2),\dots,(m+a_{i+1},i+1)$. See Figure 1.

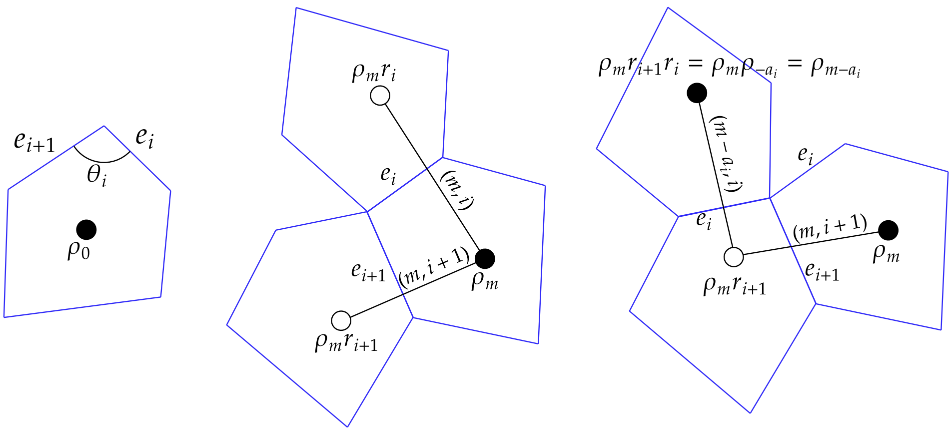

FIGURE 1

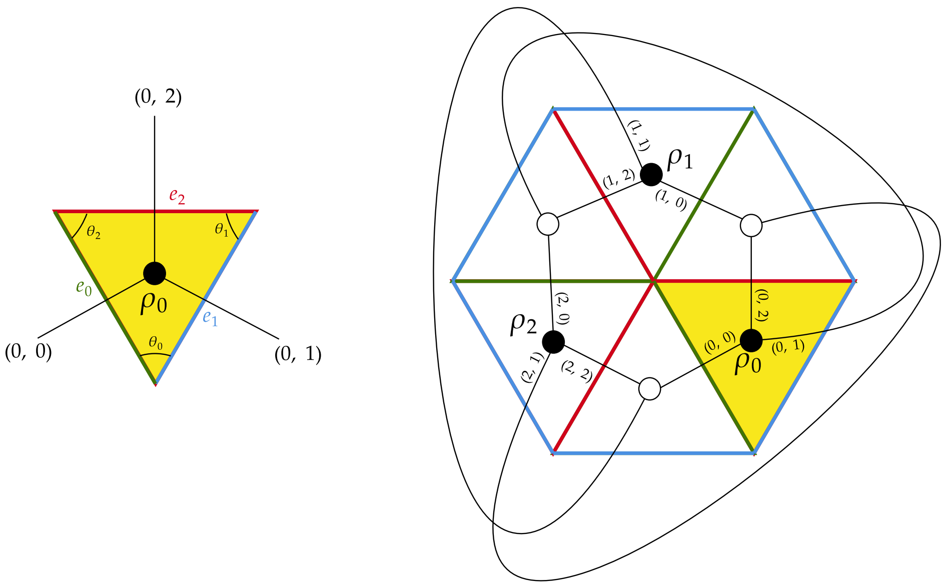

FIGURE 2

The ordering around a black vertex is apparent from our labeling scheme. To justify the ordering around a white vertex, observe that $r_{i+1}r_i = \rho_{-a_i}$ and $\rho_a\rho_b = \rho_{a+b}$, by basic facts about the composition of Euclidean reflections and rotations [16]. See Figure 2 for an example of this construction for the equilateral triangle, and see [14] for further exposition on triangular billiards surfaces.

The *monodromy group* of this dessin is a group $\langle \sigma_0, \sigma_1 \rangle$ of permutations of the edges generated by two permutations σ_0 and σ_1. We define σ_0 to be the permutation that takes each edge to the next edge in the cyclic ordering about its black vertex. Similarly, we define σ_1 to be the permutation that takes each edge to the next edge in the cyclic ordering about its white vertex.

Therefore, we have that for any edge (m,i),

$$\sigma_0[(m,i)] = (m,i+1) \tag{1}$$

and

$$\sigma_1[(m,i)] = (m-a_{i-1}, i-1). \tag{2}$$

2.3. *Representing Polygons by k-tuples.* Let P be a rational polygon with consecutive internal angles $\frac{a_i\pi}{n}$, where $a_0 + \ldots + a_{k-1} = (k-2)n$ and $\gcd(a_0, \ldots, a_{k-1}, n) = 1$. We shall use the notation $[a_0, a_1, \dots, a_{k-1}]$ to represent P. Although this notation does not uniquely define P up to geometric similarity when $k > 3$, it does uniquely define the dessin drawn on P up to graph isomorphism. This motivates the following definition.

Definition 1. If $k, n \in \mathbb{N}$ with $k \geq 3$, then an ordered k-tuple of positive integers $[a_0, \dots, a_{k-1}]$ *represents a geometric polygon, or geometric k-gon, modulo* n when $a_0 + \cdots + a_{k-1} = (k-2)n$ and $a_i < 2n$, $a_i \neq n$ for all i and $\gcd(a_0, \dots, a_{k-1}, n) = 1$. Throughout this paper, we will regularly use the term *k-gon* to refer to a geometric k-gon.

Remark. The angles of a k-gon represented by $[a_0, \dots, a_{k-1}]$ modulo n are $\frac{a_0}{n}\pi, \dots, \frac{a_{k-1}}{n}\pi$.

It is not obvious that every k-tuple $[a_0, \dots, a_{k-1}]$ that represents a polygon modulo n corresponds to a polygon in the plane with zero crossings. However, it is in fact true.

Proposition 1 (Theorem 1, [9])**.** Suppose that $\theta_0, \dots, \theta_{k-1}$ is a sequence of angles (in radians) in the set $(0, \pi) \cup (\pi, 2\pi)$. If $\theta_0 + \cdots + \theta_{k-1} = (k-2)\pi$, then there exists a polygon in the plane with no crossings with angles $\theta_0, \dots, \theta_{k-1}$ in that sequence.

Using this same convention, if the polygon P is represented by $[a_0, a_1, \dots, a_{k-1}]$ then we will use the notation $X(a_0, \dots, a_{k-1})$ for the rational billiards surface arising from P and $D(a_0, \dots, a_{k-1})$ to represent the dessin drawn on $X(a_0, \dots, a_{k-1})$. Finally, we will use $G(a_0, \dots, a_{k-1})$ to represent the monodromy group of that dessin.

3. Semidirect Product Structure of the Monodromy Group

The goal of this section is to describe the monodromy groups as semidirect products of abelian groups.

Theorem 1. Let $[a_0, \dots, a_{k-1}]$ represent a k-gon modulo n. Let $G(a_0, \dots, a_{k-1}) = \langle \sigma_0, \sigma_1 \rangle$ be the monodromy group of the dessin $D(a_0, \dots, a_{k-1})$ drawn on the rational polygonal billiards surface $X(a_0, \dots, a_{k-1})$. Setting $N = \langle \sigma_0^x \sigma_1^x : 0 < x < k \rangle$ and $H = \langle \sigma_0 \rangle$, we have $G(a_0, \dots, a_{k-1}) = N \rtimes H$.

Lemma 1. The permutations $\sigma_0^x \sigma_1^x$ and $\sigma_0^y \sigma_1^y$ commute.

Proof. Let $(m, i) \in C_n \times C_k$ be an arbitrary edge of the dessin.

From (1) and (2) we have that

$$\sigma_0^x \sigma_1^x [(m,i)] = \sigma_0^x \left[\left(m - \sum_{j=1}^{x} a_{i-j}, i - x \right) \right] = \left(m - \sum_{j=i-x}^{i-1} a_j, i \right). \tag{3}$$

The lemma follows from a modest computation. $\square$

Definition 2. Let $N = \langle \sigma_0^x \sigma_1^x : 0 < x < k \rangle$. Observe that $\sigma_1^y \sigma_0^y = (\sigma_0^{k-y} \sigma_1^{k-y})^{-1}$.

Now we proceed with the proof of Theorem 1.

Proof of Theorem 1. To prove that $N \triangleleft G(a_0, \dots, a_{k-1})$, observe that this is equivalent to proving the following statements:

(1) $\sigma_1 (\sigma_0^x \sigma_1^x) \sigma_1^{-1} \in N$
(2) $\sigma_0 (\sigma_0^x \sigma_1^x) \sigma_0^{-1} \in N$

To prove 1, observe that

$$\sigma_1 (\sigma_0^x \sigma_1^x) \sigma_1^{-1} = (\sigma_1 \sigma_0)(\sigma_0^{x-1} \sigma_1^{x-1}) = (\sigma_0^{k-1} \sigma_1^{k-1})^{-1} (\sigma_0^{x-1} \sigma_1^{x-1}) \in N.$$

To prove 2, observe that

$$\sigma_0 (\sigma_0^x \sigma_1^x) \sigma_0^{-1} = (\sigma_0^{x+1} \sigma_1^{x+1})(\sigma_1^{k-1} \sigma_0^{k-1}) = (\sigma_0^{x+1} \sigma_1^{x+1})(\sigma_0 \sigma_1)^{-1} \in N.$$

To prove that $N \cap H = \{id\}$, suppose instead that the intersection of these groups is not trivial. Then there is an element in N that is equal to σ_0^ℓ for some $0 < \ell < k$. Observe that $\sigma_0^\ell (m, i) = (m, i + \ell)$ and thus does not fix the second component of the edge labels. However, N

is generated by elements that fix the second component of the edge labels (3). Hence, we have reached a contradiction.

Finally, to prove that $NH = G(a_0,\dots,a_{k-1})$, observe that since $N \lhd G(a_0,\dots,a_{k-1})$ and $H \le G(a_0,\dots,a_{k-1})$, we know that $NH \le G(a_0,\dots,a_{k-1})$. Observe that $\sigma_0 \in NH$ and $\sigma_1 = (\sigma_0^{k-1}\sigma_1^{k-1})^{-1}\sigma_0^{-1} \in NH$. Because NH contains the generators of $G(a_0,\dots,a_{k-1})$, we conclude that $NH = G(a_0,\dots,a_{k-1})$.

Now we may conclude that $G(a_0,\dots,a_{k-1})$ is a semidirect product of subgroups N and H. □

Remark. The action of H on N in the semidirect product is via conjugation by elements of H.

4. Computing the Structure of N

In this section, we prove several properties about the subgroup $N \lhd G(a_0,\dots,a_{k-1})$, introduced in Definition 2, to provide more precise information about the structure of N and, by extension, $G(a_0,\dots,a_{k-1})$.

Let $S = \{\sigma_1^{-j}(\sigma_0^{-1}\sigma_1^{-1})\sigma_1^{j} : 0 \le j < k\}$. We first show that one can generate N using the elements of S.

Lemma 2. The subgroup N is precisely the subgroup of $G(a_0,\dots,a_{k-1})$ that fixes the second component of the coordinates (m,i).

Proof. Let N' be the collection of elements in $G(a_0,\dots,a_{k-1})$ that fix the second component of (m,i). Clearly the identity is an element of N'. If $g,h \in N'$ then gh and g^{-1} also fix the second component of (m,i). Hence, N' is a subgroup of $G(a_0,\dots,a_{k-1})$ and the formula for $\sigma_0^x\sigma_1^x$ in (3) shows that $\sigma_0^x\sigma_1^x \in N'$. Since $\sigma_0^x\sigma_1^x$ generate N as x ranges from 1 to $k-1$, we see that $N \le N'$.

Every element in $G(a_0,\dots,a_{k-1})$ (and thus in N') can be written as a product $g = (\sigma_0^{x_1}\sigma_1^{y_1})\dots(\sigma_0^{x_t}\sigma_1^{y_t})$ of t pairs of the form $\sigma_0^{x_i}\sigma_1^{y_i}$ where $x_i, y_i \in \mathbb{Z}$. We will show that $N' \le N$ by induction on t. If $g = \sigma_0^{x_1}\sigma_1^{y_1}\dots\sigma_0^{x_t}\sigma_1^{y_t} \in N'$, we know that $\sum x_i \equiv \sum y_i \mod k$ by (1) and (2).

Base Case: $t = 1$ In this case, we see that $x_1 \equiv y_1 \mod k$. Since the orders of σ_0 and σ_1 are both k, we can assume $x_1 = y_1$. Furthermore, we can also assume that $0 \le x_1 < k$. Hence, $g \in N$.

Induction Step: Suppose our theorem is true for $t \ge 1$ and consider $t+1$. That is, suppose $g = \sigma_0^{x_1}\sigma_1^{y_1}\dots\sigma_0^{x_{t+1}}\sigma_1^{y_{t+1}} \in N'$. Consider

$$g' = (\sigma_0^{x_1}\sigma_1^{x_1})^{-1}g(\sigma_0^{y_{t+1}}\sigma_1^{y_{t+1}})^{-1} = \sigma_1^{y_1-x_1}\sigma_0^{x_2}\sigma_1^{y_2}\dots\sigma_0^{x_t}\sigma_1^{y_t}\sigma_0^{x_{t+1}-y_{t+1}}$$

Since $g \in N'$ then $g' \in N'$ and $(g')^{-1} \in N'$. Let $z_1 = y_{t+1} - x_{t-1}, z_2 = -x_t, \dots, z_t = -x_2$ and $w_1 = -y_t, \dots, w_{t-1} = -y_2, w_t = x_1 - y_1$. Observe that $(g')^{-1} = \sigma_0^{z_1}\sigma_1^{w_1}\dots\sigma_0^{z_t}\sigma_1^{w_t}$. Thus by the induction hypothesis, $(g')^{-1} \in N$. Hence, $g' \in N$ and $g \in N$. By induction, we have proven the desired result. □

Lemma 3. The subgroup N is generated by S.

Proof. Recall that $N = \langle \sigma_0^x\sigma_1^x : \ 0 < x < k \rangle$. Let $S = \{\sigma_1^{-j}(\sigma_0^{-1}\sigma_1^{-1})\sigma_1^{j} : 0 \le j < k\}$. We claim $\langle S \rangle = N$. Using (1) and (2), we see that $\sigma_1^{-j}(\sigma_0^{-1}\sigma_1^{-1})\sigma_1^{j}$ fixes the second component of the coordinates (m,i) and is thus an element of N by Lemma 2. Hence, $\langle S \rangle \le N$.

We will prove that $\sigma_0^j\sigma_1^j \in \langle S \rangle$ using induction. Observe that $\sigma_1^{-1}(\sigma_0^{-1}\sigma_1^{-1})\sigma_1^{1} = (\sigma_0\sigma_1)^{-1}$. Hence, $\sigma_0\sigma_1 \in \langle S \rangle$.

Suppose $\sigma_0^{j-1}\sigma_1^{j-1} \in \langle S \rangle$. Observe that $\sigma_1^{-j}(\sigma_0^{-1}\sigma_1^{-1})\sigma_1^{j} = (\sigma_0^j\sigma_1^j)^{-1}\sigma_0^{j-1}\sigma_1^{j-1}$ which implies $\sigma_0^j\sigma_1^j \in \langle S \rangle$. Thus, $\sigma_0^j\sigma_1^j \in \langle S \rangle$ for all $j > 0$ and hence $N \le \langle S \rangle$. □

As we observed in Lemma 2, the subgroup N is precisely the subgroup of $G(a_0,\dots,a_{k-1})$ which fixes the second component of the edge (m,i). Hence, we may view any element $g \in N$ as a column vector $\begin{bmatrix} x_0 \\ \vdots \\ x_{k-1} \end{bmatrix} \in (\mathbb{Z}/n\mathbb{Z})^k$, where $g(m,i) = (m + x_i, i)$ and x_i depends only on i

and not on m. It follows from equations (1) and (2) that $\sigma_1^{-j}(\sigma_0^{-1}\sigma_1^{-1})\sigma_1^j(m,i) = (m+a_{i-j},i)$. Therefore the set $S = \{\sigma_1^{-j}(\sigma_0^{-1}\sigma_1^{-1})\sigma_1^j : 0 \le j < k\}$ can be identified with the columns of the matrix

$$C = \begin{bmatrix} a_0 & a_{k-1} & \dots & a_2 & a_1 \\ a_1 & a_0 & a_{k-1} & & a_2 \\ \vdots & a_1 & a_0 & \ddots & \vdots \\ a_{k-2} & & \ddots & \ddots & a_{k-1} \\ a_{k-1} & a_{k-2} & \dots & a_1 & a_0 \end{bmatrix} \tag{4}$$

in $M_k(\mathbb{Z}/n\mathbb{Z})$ where $M_k(\mathbb{Z}/n\mathbb{Z})$ is the set of $k\times k$ matrices with entries in $\mathbb{Z}/n\mathbb{Z}$. We make this statement more formal in the following lemma.

Lemma 4. The subgroup N is isomorphic to the span of the columns of C.

Proof. From (1), (2), and Lemma 2, we see that an arbitrary element $g \in N$ has the form $g(m,i) = (m+x_i,i)$ where $\mathbf{x} = \begin{bmatrix} x_0 \\ \vdots \\ x_{k-1} \end{bmatrix} \in (\mathbb{Z}/n\mathbb{Z})^k$. We define a homomorphism $\varphi : N \to (\mathbb{Z}/n\mathbb{Z})^k$ via $\varphi(g) = \mathbf{x}$. It is easy to check that φ is a well-defined map with $\varphi(g_1g_2) = \varphi(g_1)+\varphi(g_2)$.

It is also easy to see that φ is injective. If $\varphi(g) = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$, then g fixes every edge of the dessin. Hence, g is the identity element since the monodromy group acts faithfully on the edges of the dessin. Thus, we may conclude that φ maps N bijectively onto $\varphi(N)$.

Since the elements of the set S generate N, we conclude that the set of vectors of the form $\varphi(\sigma_1^{-j}(\sigma_0^{-1}\sigma_1^{-1})\sigma_1^j) = \begin{bmatrix} a_{k-j} \\ \vdots \\ a_{k-j-1} \end{bmatrix}$ where $0 \le j < k$ spans $\varphi(N)$. And thus, N is isomorphic to the span of the columns of C. □

Remark. It is worth noting that when viewing N as a set of vectors in $(\mathbb{Z}/n\mathbb{Z})^k$, there is a natural group action of $C_k \cong H$ on N which is the cyclic permutation of the vector entries. That is, the homomorphic image of H in $\mathrm{Aut}(N)$ is precisely the subgroup of cyclic permutations of vector entries.

In order to determine the group structure of N, we will use row and column operations on the matrix C.

4.1. ***Smith Normal Form.*** In previous sections we establish that the monodromy group $G(a_0,\dots,a_{k-1})$ can be expressed as the semidirect product of C_k and some finite abelian subgroup N, where N has a natural $\mathbb{Z}/n\mathbb{Z}$-module structure. In this section we explore the explicit computation of N. This can be done via the *Smith Normal Form*. See [3] or [15] for a reference.

Definition 3. The *Smith Normal Form* of a matrix A with entries from a ring R is a factorization $A = UDV$ where

- $D = \begin{bmatrix} d_1 & & \\ & \ddots & \\ & & d_k \end{bmatrix}$ is a diagonal matrix
- $d_i | d_{i+1}$ for all i
- U and V are square matrices with determinant ± 1

Consider the R-module M, which is a submodule of R^k, generated by the columns of A. Then as a group, M is isomorphic to the direct product

$$d_1R \times \dots \times d_kR.$$

The elements $d_1 \dots, d_k$ are called the *elementary divisors* of M. In [10], Kaplansky defines an *elementary divisor ring* R to be a ring over which all matrices have a Smith Normal Form. It is well-known (see [10]) that all PID's are elementary divisor rings. However, not all elementary divisor rings are domains. Indeed, it follows from Corollary 2.3 of [13] that $\mathbb{Z}/n\mathbb{Z}$ is an elementary divisor ring. Hence, we can always compute the group structure of one of our particular monodromy groups by computing the Smith Normal Form of the associated circulant matrix.

In practice, algorithms exist for computing the Smith Normal Form of a matrix over $\mathbb{Z}$. Therefore, to compute the Smith Normal Form of a matrix over $\mathbb{Z}/n\mathbb{Z}$, it is convenient to compute the Smith Normal Form of an associated matrix over $\mathbb{Z}$ and then apply the standard ring homomorphism to reduce modulo n.

Since the matrices U and V in Definition 3 are invertible over $\mathbb{Z}$, their reductions modulo n (call them $\overline{U}$, $\overline{V}$) are invertible over $\mathbb{Z}/n\mathbb{Z}$. Therefore, the transformation $x \mapsto \overline{U}^{-1} \cdot x$ is an isomorphism from $(\mathbb{Z}/n\mathbb{Z})^k \mapsto (\mathbb{Z}/n\mathbb{Z})^k$.

Hence, the $\mathbb{Z}/n\mathbb{Z}$ submodule generated by $v_0\overline{V}^{-1}, \dots, v_{k-1}\overline{V}^{-1}$ is isomorphic to the $\mathbb{Z}/n\mathbb{Z}$ submodule generated by the columns of D which are

$$\overline{U}^{-1}\overline{v_1}\overline{V}^{-1} = \begin{bmatrix} d_1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \dots, \overline{U}^{-1}\overline{v_k}\overline{V}^{-1} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ \overline{d_k} \end{bmatrix}.$$

Hence, N is isomorphic to $\overline{d}_1\mathbb{Z}/n\mathbb{Z} \oplus \cdots \oplus \overline{d}_k\mathbb{Z}/n\mathbb{Z}$ where $\overline{d}_i$ is the reduction of d_i modulo n. And therefore,

$$N \cong \bigoplus_{i=1}^{k} \mathbb{Z}/\delta_i\mathbb{Z}$$

where $\delta_i = \frac{n}{\gcd(d_i,n)}$. We summarize these results with the following theorem, combining the results from Theorem 1.

Theorem 2. Let C be the matrix defined in (4) and let $d_1, \dots, d_k$ be the elementary divisors of C coming from its Smith Normal Form when viewing C as a matrix over $\mathbb{Z}$. Then

$$G(a_0, \dots, a_{k-1}) = \left(\bigoplus_{i=1}^{k} C_{\delta_i} \right) \rtimes C_k$$

where $\delta_i = \frac{n}{\gcd(d_i,n)}$.

Note that some of the δ_i may equal 1, in which case the group C_{δ_i} is trivial.

Example 1. Consider the quadrilateral with angles $(\frac{2}{5}\pi, \frac{2}{5}\pi, \frac{2}{5}\pi, \frac{4}{5}\pi)$. This gives the billiards surface $X(2,2,2,4)$ and dessin $D(2,2,2,4)$. To calculate the monodromy group $G(2,2,2,4)$ of the dessin, we compute the smith normal form for the circulant matrix

$$C = \begin{bmatrix} 2 & 4 & 2 & 2 \\ 2 & 2 & 4 & 2 \\ 2 & 2 & 2 & 4 \\ 4 & 2 & 2 & 2 \end{bmatrix} = UDV = \begin{bmatrix} -11 & -12 & -14 & -3 \\ -11 & -12 & -13 & -3 \\ -7 & -8 & -9 & -2 \\ -11 & -13 & -14 & -3 \end{bmatrix} \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 10 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 4 \\ -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & -3 \end{bmatrix}$$

where U and V are unimodular. This gives us

$$\delta_1 = \delta_2 = \delta_3 = \frac{5}{\gcd(2,5)} = 5, \quad \delta_4 = \frac{5}{\gcd(10,5)} = 1.$$

Then we have

$$G(2,2,2,4) = (C_5 \times C_5 \times C_5) \rtimes C_4.$$

As a consequence of Theorem 2, one can quickly compute the monodromy groups of any rational triangular billiards surfaces.

Corollary 1 (Theorem 1, [14])**.** Let $[a_0,a_1,a_2]$ represent a triangle modulo n. Let $G(a_0,a_1,a_2) = \langle\sigma_0,\sigma_1\rangle$ be the monodromy group of the dessin $D(a_0,a_1,a_2)$ drawn on the triangular billiards surface $X(a_0,a_1,a_2)$. Setting $N = \langle\sigma_0\sigma_1,\sigma_0^2\sigma_1^2\rangle$ and $H = \langle\sigma_0\rangle$, we have $G(a_0,a_1,a_2) = N \rtimes H$. Furthermore, if $n = a_0+a_1+a_2$ and $\alpha = \gcd(n, a_0a_1 - a_2^2)$, then

$$G(a_0,a_1,a_2) \cong (C_n \times C_{\frac{n}{\alpha}}) \rtimes C_3.$$

One can easily compute that $\gcd(n,a_0a_1-a_2^2) = \gcd(n,a_0a_2-a_1^2) = \gcd(n,a_1a_2-a_0^2)$ and thus α in the above Corollary does not depend on the order of a_0, a_1, and a_2.

Proof. Consider the arbitrary rational triangle with angles $\left(\frac{a_0\pi}{n},\frac{a_1\pi}{n},\frac{a_2\pi}{n}\right)$, where the a_i are positive integers, $a_0+a_1+a_2 = n$, and $\gcd(a_0,a_1,a_2,n) = 1$. Observe that it follows that $\gcd(a_0,a_1,n) = 1$ as well. The normal subgroup N of the associated monodromy group is represented by the column span of $C = \begin{bmatrix} a_0 & a_1 & a_2 \\ a_1 & a_2 & a_0 \\ a_2 & a_0 & a_1 \end{bmatrix}$ over $\mathbb{Z}/n\mathbb{Z}$.

Since $\gcd(a_0,a_1,n) = 1$, there exist integers s, t, and u such that $sa_0+ta_1+un = 1$, and hence $sa_0+ta_1 \equiv 1 \mod n$.

Using elementary row and column operations modulo n, we obtain the following factorization:

$$C = \begin{bmatrix} a_0 & a_1 & a_2 \\ a_1 & a_2 & a_0 \\ a_2 & a_0 & a_1 \end{bmatrix} = \begin{bmatrix} a_0 & -t & 0 \\ a_1 & s & 0 \\ -a_0-a_1 & -s+t & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & -a_1^2+a_0a_2 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & sa_1+ta_2 & -sa_1-ta_2-1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}.$$

One easily checks that the diagonalizing matrices are unimodular. It then follows from Theorem 2 that the monodromy group of the (a_0,a_1,a_2) triangle is

$$(C_n \times C_{n/\alpha}) \rtimes C_3,$$

where $\alpha = \gcd(n, a_0a_2 - a_1^2)$. ☐

The following corollary follows from Theorem 2 after a short computation.

Corollary 2 (Corollary to Theorem 2)**.** The monodromy group of the dessin drawn on the rational billiards surface of the regular k-gon is $C_{\frac{k}{\gcd(k,2)}} \times C_k$.

5. Algebraic Polygons

In this section, we introduce the notion of an *algebraic polygon* and develop the relevant theory with the goal of proving results about actual polygons. We arrive at the concept of an algebraic polygon by relaxing the constraints on polygons modulo n slightly:

Definition 4. If $k,n \in \mathbb{N}$ with $k \geq 2$, then an ordered k-tuple of nonnegative integers $[a_0,\ldots,a_{k-1}]$ *represents an algebraic polygon, or k-gon, modulo n* if $a_0+\cdots+a_{k-1} \equiv 0 \mod n$ and $\gcd(a_0,\ldots,a_{k-1},n) = 1$. Observe that $[0,\ldots,0]$ is not an algebraic k-gon.

Every geometric polygon modulo n is also an algebraic polygon modulo n. We shall define a "monodromy group" for any algebraic polygon in a natural way which coincides with the monodromy groups associated to geometric polygons described in Section 4. It turns out that it is relatively easy to classify the possible monodromy groups for all algebraic polygons modulo a prime p (we do this in Theorem 3). The challenge is to determine when, for a given monodromy group G of an algebraic polygon, there exists a *geometric* polygon with a monodromy group isomorphic to G. Lemmas 5 and 6 show that this is always possible if none of the entries in the algebraic polygon are zero modulo n. This motivates work in Section 8 to produce algebraic polygons with nonzero entries.

Remark. Note that the definition of an algebraic polygon allows for an algebraic 2-gon even though no geometric 2-gons exist. Despite this fact, algebraic 2-gons can be used to produce geometric k-gons via Proposition 3.

5.1. *Results About Algebraic Polygons.*

Definition 5. We say that two algebraic polygons, $[a_0,\dots,a_{k-1}]$ and $[b_0,\dots,b_{k-1}]$ modulo n are *associates* if there exists $c \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $b_i \equiv ca_i \pmod{n}$ for all i.

Remark. Our definition of associate algebraic polygons coincides with the definition of associate triangles from Aurell and Itzykson [4].

Observe that reflex angles lead to interesting associate polygons. For example, the (algebraic) polygons $[3,5,11,1]$ and $[3,15,1,1]$ are associates modulo 10.

Proposition 2. Suppose that $[a_0,\dots,a_{k-1}]$ represents an algebraic polygon modulo n. Further suppose that $0 < a_i < 2n, a_i \neq n$ for all i and $a_0+\cdots+a_{k-1} \le (k-2)n$. Then there exists an associate polygon $[b_0,\dots,b_{k-1}]$. Consequently, there exists a polygon in the plane with consecutive angles $\frac{b_0}{n}\pi,\dots,\frac{b_{k-1}}{n}\pi$ and zero crossings.

Observe that Proposition 2 produces a geometric polygon, not simply an algebraic polygon.

Proof. If $a_0+\cdots+a_{k-1} = (k-2)n$, then, letting $a_i = b_i$, $[a_0,\dots,a_{k-1}] = [b_0,\dots,b_{k-1}]$ represents an associate polygon modulo n. If $a_0+\cdots+a_{k-1} < (k-2)n$, then let $d = \frac{(k-2)n-(a_0+\cdots+a_{k-1})}{n}$. We can find $a_{i_1},\dots,a_{i_d}$ with $i_1,\dots,i_d$ distinct such that $a_{i_j} < n$. Add n to each of these a_{i_j} to obtain $b_{i_j} = a_{i_j}+n \equiv a_{i_j} \mod n$. Let $b_i = a_i$ for all other indices $i \neq i_j$. Thus, $[b_0,\dots,b_{k-1}]$ represents an associate k-gon modulo n. By Proposition 1, there exists a geometric polygon in the plane with consecutive angles $\frac{b_0}{n}\pi,\dots,\frac{b_{k-1}}{n}\pi$ and zero crossings. □

Example 2. Consider the algebraic polygon $[1,2,2,7]$ modulo 12. Using the procedure in Proposition 2, we produce the associate geometric polygon $[13,2,2,7]$.

We will use the following lemma many times to verify that an algebraic k-gon satisfies the hypotheses of Proposition 2.

Lemma 5. Suppose that $[a_0,\dots,a_{k-1}]$ is an algebraic polygon modulo n with $a_i \not\equiv 0 \mod n$ for all i. Then, $[a_0,\dots,a_{k-1}]$ has an associate k-gon $[b_0,\dots,b_{k-1}]$ that is a polygon modulo n. If $n = p$ is a prime and $p \ge k-1$, then there exists an associate *convex* k-gon $[b_0,\dots,b_{k-1}]$ that is a polygon modulo p.

Proof. Let $\overline{a_i}$ denote the reduction of a_i modulo n. Since $a_i \not\equiv 0 \mod n$ for all i, we see that $0 < \overline{a_i} < n$ for all i. Since $a_0+\cdots+a_{k-1} \equiv 0 \mod n$, we see that $\overline{a_0}+\cdots+\overline{a_{k-1}} \equiv 0 \mod n$. Combining this fact with the fact that $\overline{a_0}+\cdots+\overline{a_{k-1}} \le k\cdot(n-1)$, we conclude that $\overline{a_0}+\cdots+\overline{a_{k-1}} \le (k-1)\cdot n$. The case where $\overline{a_0}+\cdots+\overline{a_{k-1}} \le (k-2)\cdot n$ has already been addressed in Proposition 2.

Consider the case where $\overline{a_0}+\cdots+\overline{a_{k-1}} = (k-1)n$. Let $a'_i = -a_i$ for all i. Observe that $\overline{a_i}+\overline{a'_i} = n$ for all i. Therefore, $\overline{a'_0}+\dots\overline{a'_{k-1}} = kn-(\overline{a_0}+\cdots+\overline{a_{k-1}}) = n \le (k-2)n$. Using Proposition 2, we obtain the desired $[b_0,\dots,b_{k-1}]$.

Now consider the case where $n = p$ is a prime and $p \ge k-1$. Since $a_i \not\equiv 0 \mod p$ for all i, the reduction of a_i modulo p can be chosen so that $0 < \overline{a_i} < p$ for all i. Since $[a_0,\dots,a_{k-1}]$ is an algebraic polygon, we know that $a_0+\cdots+a_{k-1} \equiv 0 \mod p$. Therefore, $\overline{a_0}+\cdots+\overline{a_{k-1}} = cp$ where $0 < c < k$. Choose $c' \in \mathbb{Z}/p\mathbb{Z}$ so that $c'\cdot c \equiv k-2 \mod p$. We see that $c'\cdot\frac{\overline{a_0}+\cdots+\overline{a_{k-1}}}{p} \equiv c'\cdot c \equiv k-2 \mod p$. Hence, $\overline{c'a_0}+\dots\overline{c'a_{k-2}} = (k-2)p$ and thus, letting $b_i = \overline{c'a_i}$, $[b_0,\dots,b_{k-1}]$ is a k-gon modulo p. Since $0 < b_i < p$ for all i, we see that $[b_0,\dots,b_{k-1}]$ represents a convex polygon. □

5.2. *Monodromy Groups of Algebraic Polygons.*

The purpose of introducing algebraic polygons is to understand monodromy groups of actual polygons. Therefore, we must associate to each algebraic polygon a monodromy group that coincides with the monodromy group in Section 2 for geometric polygons.

Definition 6. The *monodromy group* associated with an algebraic k-gon $[a_0,\ldots,a_{k-1}]$ modulo n is the group $N \rtimes C_k$ where N is the additive group generated by the columns of the matrix

$$C = \begin{bmatrix} a_0 & a_{k-1} & \ldots & a_2 & a_1 \\ a_1 & a_0 & a_{k-1} & & a_2 \\ \vdots & a_1 & a_0 & \ddots & \vdots \\ a_{k-2} & & \ddots & \ddots & a_{k-1} \\ a_{k-1} & a_{k-2} & \ldots & a_1 & a_0 \end{bmatrix}$$

in the $\mathbb{Z}/n\mathbb{Z}$ module $(\mathbb{Z}/n\mathbb{Z})^k$. The group C_k acts on the columns of C by cyclicly permuting the entries of a vector.

The monodromy groups that arose in Section 2 were monodromy groups of dessins d'enfant drawn on rational billiards surfaces. Although these surfaces and dessins do not exist for algebraic polygons, associating a monodromy group with them will still prove quite useful theoretically.

Remark. If $[a_0,\ldots,a_{k-1}]$ is a k-gon modulo n, then its monodromy group above is the same as the monodromy group of $D(a_0,\ldots,a_{k-1})$ drawn on the rational polygonal billiards surface $X(a_0,\ldots,a_{k-1})$. See Sections 2 and 4 for reference.

The following lemma illustrates that the monodromy group of associate algebraic polygons are isomorphic.

Lemma 6. Fix $n \in \mathbb{N}$. If $[a_0,\ldots,a_{k-1}]$ and $[b_0,\ldots,b_{k-1}]$ are associate algebraic polygons, then their monodromy groups are the same.

Proof. Since $[a_0,\ldots,a_{k-1}]$ and $[b_0,\ldots,b_{k-1}]$ are associates, there exists $c \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $b_i \equiv ca_i$ for all i. Let C' and C'' be the corresponding circulant matrices for $[b_0,\ldots,b_{k-1}]$ and $[a_0,\ldots,a_{k-1}]$ respectively. Therefore, $C' \equiv c \cdot C'' \mod n$. Since C' and C'', are scalar multiples of each other by a unit, the spans of their columns are equal. The result follows. □

Proposition 3. Suppose that $[a_0,\ldots,a_{k-1}]$ and $[b_0,\ldots,b_{k-1}]$ represent algebraic k-gons modulo n_1 and n_2 respectively where $\gcd(n_1,n_2) = 1$. Suppose their respective monodromy groups are $N_1 \rtimes C_k$ and $N_2 \rtimes C_k$. Then there exists an algebraic k-gon $[c_0,\ldots,c_{k-1}]$ modulo n_1n_2 with monodromy group $(N_1 \times N_2) \rtimes C_k$. Furthermore, if $a_i \not\equiv 0 \mod n_1$ or $b_i \not\equiv 0 \mod n_2$ for every i, then $c_i \not\equiv 0 \mod n_1n_2$ for all i.

Proof. By the Chinese Remainder Theorem, there exist unique integers c_i with $0 < c_i < n_1n_2$ such that $c_i \equiv a_i \mod n_1$ and $c_i \equiv b_i \mod n_2$ for all i. Since $c_i \equiv a_i \mod n_1$, we see that $c_0 + \cdots + c_{k-1} \equiv 0 \mod n_1$ and $\gcd(c_0,\ldots,c_{k-1},n_1) = 1$. A similar argument shows that $c_0 + \cdots + c_{k-1} \equiv 0 \mod n_2$ and $\gcd(c_0,\ldots,c_{k-1},n_2) = 1$. Hence, $c_0 + \cdots + c_{k-1} \equiv 0 \mod n_1n_2$ and $\gcd(c_0,\ldots,c_{k-1},n_1n_2) = 1$ since $\gcd(n_1,n_2) = 1$.

Now, we will will compute the monodromy group of $[c_0,\ldots,c_{k-1}]$ which is $N \rtimes C_k$ where N is an abelian group and submodule of $(\mathbb{Z}/n_1n_2\mathbb{Z})^k$. Let C' and C'' be the circulant matrices associated to $[c_0,\ldots,c_{k-1}]$ and $[a_0,\ldots,a_{k-1}]$ respectively. Since $c_i \equiv a_i \mod n_1$ for all i , we see that $C' \equiv C'' \mod n_1$.

Let $d_1,\ldots,d_k$ be the elementary divisors of C'. They are the same modulo n_1 as the elementary divisors of C''. By Theorem 2, we know the monodromy group of $[c_0,\ldots,c_{k-1}]$ is

$$\bigoplus_{i=1}^{k} C_{\delta_i} = \bigoplus_{i=1}^{k} C_{\frac{n_1n_2}{\gcd(d_i,n_1n_2)}} = \bigoplus_{i=1}^{k} C_{\frac{n_1}{\gcd(d_i,n_1)}} \oplus C_{\frac{n_2}{\gcd(d_i,n_2)}} \tag{5}$$

since $\gcd(n_1,n_2) = 1$. Thus, the monodromy group of $[a_0,\ldots,a_{k-1}]$ is $N_1 = \bigoplus_{i=1}^{k} C_{\frac{n_1}{\gcd(d_i,n_1)}}$. Therefore, $N_1 \cong n_2N \cong N/n_1N$. If N_2 is the monodromy group of $[b_0,\ldots,b_{k-1}]$, then a similar argument shows that $N_2 \cong n_1N \cong N/n_2N$. We conclude that $N \cong N_1 \times N_2$ and the main result follows. □

Remark. In essence, Proposition 3 allows one to combine two algebraic k-gons $[a_0,\dots,a_{k-1}]$ and $[b_0,\dots,b_{k-1}]$ with coprime moduli n_1 and n_2 and create a new algebraic k-gon $[c_0,\dots,c_{k-1}]$. Suppose the monodromy groups of $[a_0,\dots,a_{k-1}]$ and $[b_0,\dots,b_{k-1}]$ are $N_1 \rtimes C_k$ and $N_2 \rtimes C_k$ respectively. Then the monodromy group of $[c_0,\dots,c_{k-1}]$ is equal to $(N_1 \times N_2) \rtimes C_k$ which is a restricted product $\prod_i'(v_i, j_i)$ where the restriction requires $j_1 = j_2$. In other words, you can combine two elements $(v_1, j_1) \in N_1 \rtimes C_k$ and $(v_2, j_2) \in N_2 \rtimes C_k$ if $j_1 = j_2$ to obtain $(v_3, j_1) = (v_3, j_2)$ where v_3 is a vector in $\mathbb{Z}/n_1n_2\mathbb{Z}$ that equals v_1 when reduced modulo n_1 and equals v_2 when reduced modulo n_2.

Example 3. One can actually combine two algebraic k-gons with no k-gon associates to create an algebraic k-gon with a k-gon associate. Consider the algebraic 3-gon $[0,1,1]$ modulo 2 with monodromy group $C_2^2 \rtimes C_3$ and the algebraic 3-gon $[1,0,4]$ modulo 5 with monodromy group $C_5^2 \rtimes C_3$. Neither of these algebraic 3-gons have a polygonal associate. However, if we combine them using Proposition 3, we obtain the algebraic 3-gon $[6,5,9]$ modulo 10. This algebraic 3-gon has a 3-gon associate $[4,5,1]$ modulo 10 obtained by scaling by $9 \mod 10$. The 3-gon $[4,5,1]$ has monodromy group $(C_2^2 \times C_5^2) \rtimes C_3 \cong C_{10}^2 \rtimes C_3$.

Proposition 4. Suppose that $[c_0,\dots,c_{k-1}]$ is an algebraic k-gon modulo n_1n_2 with $n_1, n_2 > 1$ and with monodromy group $N \rtimes C_k$. Then there exists an algebraic k-gon $[a_0,\dots,a_{k-1}]$ modulo n_1 with monodromy group $(n_2N) \rtimes C_k$. Furthermore, if $\gcd(n_1,n_2) = 1$, then the monodromy group $(n_2N) \rtimes C_k \cong (N/n_1N) \rtimes C_k$.

Proof. Observe that $c_i \not\equiv 0 \mod n_1$ for some i. If $n_1 | c_i$ for all i, then $\gcd(c_0,\dots,c_{k-1},n_1n_2) > 1$, a contradiction with the definition of an algebraic polygon.

Choose $a_i \equiv c_i \mod n_1$ for all i. We see that $a_0 + \dots + a_{k-1} \equiv 0 \mod n_1$ since $c_0 + \dots + c_{k-1} \equiv 0 \mod n_1n_2$. Suppose that the monodromy group of $[a_0,\dots,a_{k-1}]$ is $N_1 \rtimes C_k$. By basic abelian group theory computations, we conclude that $N_1 \cong n_2N$.

Now suppose $\gcd(n_1,n_2) = 1$. Using (5), we see that the monodromy group of $[c_0,\dots,c_{k-1}]$ has the form $N \rtimes C_k$ where

$$N = \bigoplus_{i=1}^{k} C_{\delta_i} = \bigoplus_{i=1}^{k} C_{\frac{n_1}{\gcd(d_i,n_1)}} \oplus C_{\frac{n_2}{\gcd(d_i,n_2)}}$$

Observe that $n_2N \cong \bigoplus_{i=1}^{k} C_{\frac{n_1}{\gcd(d_i,n_1)}}$ and $n_1N \cong \bigoplus_{i=1}^{k} C_{\frac{n_2}{\gcd(d_i,n_2)}}$. Thus, $n_2N \cong N/n_1N$. $\square$

Remark. If n_1 and n_2 are coprime in Proposition 4, then $N_1 \cong N/n_1N$. However, this is not the case when n_1 and n_2 have a non-trivial gcd. We illustrate this phenomenon in the following example.

Example 4. Consider the 4-gon $[1,2,24,23]$ modulo 25. The monodromy group is $N \rtimes C_4$ where $N \cong C_{25} \times C_5$. If we apply Proposition 4 when $n_1 = 5$, we obtain the k-gon $[1,2,4,3]$ which has monodromy group $N_1 \rtimes C_4$ where $N_1 \cong C_5 \cong 5N \not\cong N/5N$.

The following proposition allows us to lift an algebraic k-gon modulo n to an algebraic ℓ-gon modulo n if $k|\ell$.

Proposition 5. Suppose that $k, \ell \in \mathbb{N}$ and $k|\ell$. Further suppose that $[a_0,\dots,a_{k-1}]$ is an algebraic k-gon modulo n with monodromy group $N \rtimes C_k$. Then there exists an algebraic ℓ-gon $[c_0,\dots,c_{\ell-1}]$ modulo n with monodromy group $N \rtimes C_\ell$.

Proof. Let $c_i = a_j$ where j is the least nonnegative integer satisfying $i \equiv j \mod k$. In essence,

$$[c_0,\dots,c_{\ell-1}] = [a_0,\dots,a_{k-1},a_0,\dots,a_{k-1},a_0,\dots,a_{k-1}]$$

where the pattern $a_0,\dots,a_{k-1}$ repeats itself $\frac{\ell}{k}$ times. Let C and C' be circulant matrices associated to $[a_0,\dots,a_{k-1}]$ and $[c_0,\dots,c_{\ell-1}]$ respectively. Observe that C' is a $\frac{\ell}{k} \times \frac{\ell}{k}$ block matrix in which the matrix C repeats $\frac{\ell}{k}$ times in each row and column. Therefore, the group generated by the columns of C' is isomorphic to the group generated by the columns of C and thus the monodromy group of $[c_0,\dots,c_{\ell-1}]$ is $N \rtimes C_\ell$. $\square$

The following example illustrates how Proposition 5 is used to lift an algebraic k-gon to an algebraic ℓ-gon.

Example 5. Let $k=2$, $\ell=4$ and consider the algebraic 2-gon $[3,4]$ modulo $n=7$. Using Proposition 5, lift $[3,4]$ to the algebraic 4-gon $[3,4,3,4]$ modulo 7. The monodromy group of $[3,4]$ is $C_7 \rtimes C_2$ and the monodromy group of $[3,4,3,4]$ is $C_7 \rtimes C_4$.

A quick lemma about semidirect products is needed to complete our series of results about combining algebraic polygons to form new algebraic polygons. The following lemma follows from an easy elementary group theory argument.

Lemma 7. Suppose that N_1,H_1,N_2,H_2 are finite groups. If $G_1 \cong N_1 \rtimes H_1$ and $G_2 \cong N_2 \rtimes H_2$ then $G_1 \times G_2 \cong (N_1 \times N_2) \rtimes (H_1 \times H_2)$.

Now, let us combine the results from Propositions 3 and 5 to obtain the following corollary.

Corollary 3. Fix $n_1,n_2,k,\ell \in \mathbb{N}$ with $k,\ell \geq 2$. Suppose that $\gcd(n_1,n_2)=1$ and $\gcd(k,\ell)=1$. If $[a_0,\dots,a_{k-1}]$ is an algebraic k-gon modulo n_1 with monodromy group $N_1 \rtimes C_k$ and $[b_0,\dots,b_{\ell-1}]$ is an algebraic ℓ-gon modulo n_2 with monodromy group $N_2 \rtimes C_\ell$, then there exists an algebraic $k\ell$-gon $[c_0,\dots,c_{k\ell-1}]$ modulo n_1n_2 with monodromy group $(N_1 \times N_2) \rtimes C_{\ell k} \cong (N_1 \rtimes C_k) \times (N_2 \rtimes C_\ell)$.

Proof. Combining Propositions 3 and 5 give us the desired algebraic $k\ell$-gon $[c_0,\dots,c_{k\ell-1}]$ with monodromy group $(N_1 \rtimes N_2) \rtimes C_{k\ell}$. Since $\gcd(k,\ell)=1$, $C_{k\ell} \cong C_k \times C_\ell$. Thus, by Lemma 7, $(N_1 \rtimes N_2) \rtimes C_{k\ell} \cong (N_1 \rtimes C_k) \times (N_2 \rtimes C_\ell)$. $\square$

The following example illustrates how to use Corollary 3.

Example 6. Let $k=3$, $\ell=4$, $n_1=7$ and $n_2=5$. Let $[1,2,4]$ be our algebraic 3-gon modulo 7 and let $[2,3,3,2]$ be our algebraic 4-gon modulo 5. The monodromy group of group of $[1,2,4]$ is $C_7 \rtimes C_3$ and the monodromy group of $[2,3,3,2]$ is $C_5^2 \rtimes C_4$. Using Proposition 5, we lift $[1,2,4]$ to $[1,2,4,1,2,4,1,2,4,1,2,4]$ and we lift $[2,3,3,2]$ to $[2,3,3,2,2,3,3,2,2,3,3,2]$. Using Proposition 3, we combine these algebraic 12-gons to obtain $[22,23,8,22,2,18,8,2,32,8,23,32]$ modulo 35 which has monodromy group $(C_7 \times C_5^2) \rtimes C_{12} \cong (C_7 \rtimes C_3) \times (C_5^2 \rtimes C_4)$.

6. Results about Circulant Matrices

The following results on circulant matrices will be needed to compute monodromy groups of polygons modulo p when p is prime. The results are well known over $\mathbb{C}$, and we provide the proofs for the corresponding results over finite fields for completeness.

Definition 7. A $k \times k$ *circulant* matrix C has the following form

$$C = \begin{bmatrix} a_0 & a_{k-1} & \cdots & a_2 & a_1 \\ a_1 & a_0 & a_{k-1} & & a_2 \\ \vdots & a_1 & a_0 & \ddots & \vdots \\ a_{k-2} & & \ddots & \ddots & a_{k-1} \\ a_{k-1} & a_{k-2} & \cdots & a_1 & a_0 \end{bmatrix}.$$

For the purposes of this paper, the entries c_i are integers or integers modulo n.

Definition 8. We call the polynomial $f(x)=a_0+a_1x+\cdots+a_{k-1}x^{k-1}$ the *associated polynomial* of the circulant matrix C.

The following result can be found in any introductory text about circulant matrices such as [8].

Lemma 8. The rank of a $k \times k$ circulant matrix C over a field $\mathbb{F}$ which has an algebraic extension with k distinct kth roots of unity is equal to $k-d$ where d is the degree of $\gcd(f(x),x^k-1)$.

Lemma 9. Suppose p_1 and p_2 are distinct prime integers and p_1 is a generator for the cyclic group $\mathbb{F}_{p_2}^{\times}$. Then $x^{p_2-1}+\cdots+x+1$ is irreducible over $\mathbb{F}_{p_1}$.

Proof. Let ω be a primitive p_2th root of unity of $\mathbb{F}_{p_1}$. The group $\mathrm{Gal}(\mathbb{F}_{p_1}(\omega)/\mathbb{F}_{p_1})$ is generated by the Frobenius automorphism $\phi : x \mapsto x^{p_1}$ [3, Proposition 5.8, page 445]. Since p_1 generates $\mathbb{F}_{p_2}^{\times}$, we see that $|\phi| = p_2 - 1$. Thus, $[\mathbb{F}_{p_1}(\omega) : \mathbb{F}_{p_1}] = p_2 - 1$ and $x^{p_2-1}+\cdots+x+1$ is irreducible over $\mathbb{F}_{p_1}$. □

Corollary 4. Let p_1 and p_2 be primes such that p_1 is a generator for the cyclic group $\mathbb{F}_{p_2}^{\times}$. Suppose that C is a $p_2 \times p_2$ circulant matrix with entries in $\mathbb{F}_{p_1}$. Then $\mathrm{rank}(C) = 0,\ 1,\ p_2 - 1$, or p_2.

Proof. By Lemma 9, we know that $x^{p_2-1}+\cdots+x+1$ is irreducible over $\mathbb{F}_{p_1}$. Hence $x^{p_2}-1$ factors as $(x-1)(x^{p_2-1}+\cdots+x+1)$ over $\mathbb{F}_{p_1}$. By Lemma 8, we see that $d = 0,\ 1,\ p_2-1$, or p_2 from which our result follows. □

7. Results for $n = p$ Prime

In Section 4.1, we gave a description of the monodromy group in terms of the elementary divisors of a particular circulant matrix. Although this result (Theorem 2) allows one to easily compute the monodromy group, the result is not explicit. We will prove several results below in the special case when n is equal to a prime p. In other words, $[a_0,\ldots,a_{k-1}]$ represents an algebraic k-gon modulo a prime p. In this case, the group N can be viewed as a $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ module and is thus a vector space. In this section, $\mathbb{F}_p$ will denote the finite field with p elements and $\mathbb{F}_p^{\times}$ will denote its group of units.

Proposition 6. Suppose that $[a_0,\ldots,a_{k-1}]$ represents an algebraic k-gon modulo a prime p. Let $f(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1}$ and let d be the degree of $\gcd(f(x), x^k - 1)$. Then the monodromy group of $[a_0,\ldots,a_{k-1}]$ is $G(a_0,\ldots,a_{k-1}) = C_p^{k-d} \rtimes C_k$.

Proof. Let C be the circulant matrix associated to $[a_0,\ldots,a_{k-1}]$. By Lemma 8, we know that the rank of C is equal to $k-d$ where d is the degree of $\gcd(f(x), x^k-1)$. The rank of a subspace of a vector space determines the group structure and the result follows. □

This allows us to translate the problem of finding the rank of a matrix to that of a degree of a gcd. The following corollary shows how we can use this connection to compute the monodromy groups of a large collection of dessins on rational billiards surfaces.

Corollary 5. Suppose p_2 is a prime number and p_1 is a prime number that generates the cyclic group $(\mathbb{F}_{p_2})^{\times}$. Suppose that $[a_0,\ldots,a_{p_2-1}]$ represents an algebraic p_2-gon modulo p_1 with monodromy group $G(a_0,\ldots,a_{p_2-1})$. Let $f(x) = a_0 + a_1x + \cdots + a_{p_2-1}x^{p_2-1}$, then $G(a_0,\ldots,a_{p_2-1}) \cong C_{p_1}^{p_2-1} \rtimes C_{p_2}$.

Proof. By Corollary 4, the rank of the appropriate matrix C is $0,\ 1,\ p_2-1$, or p_2. Since $f(1) \equiv 0 \mod p_1$, we know $x - 1 | f(x)$ and thus $\mathrm{rank}(C) \le p_2 - 1$. Since $x^{p_2-1}+\cdots+x+1$ is irreducible over $\mathbb{F}_{p_1}$ by Lemma 9, the $\deg(\gcd(f(x), x^{p_2}-1)) = 1$ or p_2. If $\deg(\gcd(f(x), x^{p_2}-1)) = p_2$ then $a_0 = \cdots = a_{p_2-1} = 0$ since $\deg(f) \le p_2 - 1$, which is a contradiction. Hence, $\deg(\gcd(f(x), x^{p_2}-1)) = 1$ and the result follows. □

Example 7. Choose $p_2 = 17$. Observe that $p_1 = 41$ generates the multiplicative group $\mathbb{F}_{17}^{\times}$. Hence, any algebraic 17-gon modulo 41 has monodromy group $C_{41}^{16} \rtimes C_{17}$.

7.1. *Possible Monodromy Groups.*

Now, let's prove a general theorem that lists all possible monodromy groups for polygons $[a_0,\ldots,a_{k-1}]$ modulo p.

Proposition 7. Suppose that $[a_0,\ldots,a_{k-1}]$ represents an algebraic polygon modulo a prime p. Let $f(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1}$ and suppose $x^k - 1 = \prod g_i(x)$ where the $g_i(x)$ are irreducible over $\mathbb{F}_p$. Further suppose that $\gcd(f(x), x^k - 1) = \prod_{j=1}^{\ell} g_{i_j}(x)$. Then the monodromy group of $[a_0, \ldots, a_{k-1}]$ is $G(a_0, \ldots, a_{k-1}) = C_p^{k-d} \rtimes C_k$ where $d = \sum_{j=1}^{m} \deg(g_{i_j}(x))$.

In essence, Proposition 7 gives a list of all potential monodromy groups of *algebraic* k-gons modulo p. If $[a_0, \ldots, a_{k-1}]$ is an algebraic k-gon modulo p with monodromy group $C_p^{k-d} \rtimes C_k$ then d must be equal to the sum of degrees of distinct irreducible factors of $x^k - 1$ in $\mathbb{F}_p$. The factor $x - 1$ must be one of these factors. If there is no way to add up to d the degrees $\deg(g_{i_j}(x))$ of a subset of the irreducible factors $g_i(x)$ of $x^k - 1$ in $\mathbb{F}_p$, then such a monodromy group *cannot* occur.

Example 8. Consider $k = 3$ and $p = 5$. We see that $x^3 - 1$ factors as $(x-1)(x^2+x+1)$ modulo 5. Since $x - 1$ is required to be a factor of $\gcd(f(x), x^k - 1)$, we see that this gcd *cannot* have degree two. Therefore, the monodromy group $C_5^{3-2} \rtimes C_3$ is not achieved by any algebraic 3-gon modulo 5.

Proof of Proposition 7. By Proposition 6, we know that d is the degree of $\gcd(f(x), x^k - 1)$. Since the gcd must be a product of some subset of $\{g_i(x)\}$, we see that d is the sum of the degrees of some subset of $\{g_i(x)\}$. The theorem follows.

Observe that $\ell \geq 1$ because $f(1) = a_0 + \ldots a_{k-1} \equiv 0 \mod p$ implies $x - 1$ divides $f(x)$. □

Theorem 3. Fix a prime $p \nmid k$. Suppose $x^k - 1 = \prod g_i(x)$ where the $g_i(x)$ are irreducible over $\mathbb{F}_p$. Let $d = \sum_{j=1}^{\ell} \deg(g_{i_j}(x))$. Further suppose that $g_{i_j} = x - 1$ for some i_j. Then there exists an *algebraic* k-gon $[a_0, \ldots, a_{k-1}]$ modulo p with monodromy group $G(a_0, \ldots, a_{k-1}) \cong C_p^{k-d} \rtimes C_k$.

Proof. Let $f(x) = \prod g_{i_j}(x)$. We see that $\deg(\gcd(f(x), x^k - 1)) = d$. If $f(x) = a_0 + \cdots + a_{k-1}x^{k-1}$ then $a_0 + \cdots + a_{k-1} \equiv 0 \mod p$ since $(x-1) | f(x)$.

Since $f(x)$ is not the zero polynomial over $\mathbb{F}_p$, we see that $\gcd(a_0, \ldots, a_{k-1}, p) = 1$. Therefore, $[a_0, \ldots, a_{k-1}]$ is an algebraic k-gon with monodromy group $G(a_0, \ldots, a_{k-1}) \cong C_p^{k-d} \rtimes C_k$ by Proposition 6.

Since $\deg(f(x)) = d$, then $a_{k-1} = 0$ when $d < k - 1$. This is allowed since the associated polynomial $f(x)$ for an *algebraic* k-gon may have degree $d < k - 1$. □

Theorem 3 proves that all possible monodromy groups from Proposition 7 are achieved by algebraic polygons modulo p for a fixed prime p. Therefore, it is natural to ask which groups can occur for *k-gons* modulo p. The following theorem shows that for primes $p > k$, all possible monodromy groups from Proposition 7 are achieved by *k-gons* modulo p.

Theorem 4. Fix a prime $p > k \geq 3$. Suppose $x^k - 1 = g_1(x) \cdots g_\ell(x)$ where the $g_i(x)$ are irreducible over $\mathbb{F}_p$. Let $d = \sum_{j=1}^{m} \deg(g_{i_j}(x))$ where m is a positive integer less than ℓ and $1 \leq i_1 < \cdots < i_m \leq \ell$. Further suppose that $g_{i_j} = x - 1$ for some i_j. Then there exists a k-gon $[a_0, \ldots, a_{k-1}]$ modulo p with monodromy group $G(a_0, \ldots, a_{k-1}) \cong C_p^{k-d} \rtimes C_k$.

Remark. We only consider primes $p > k$ in Theorem 4, because $p \nmid k$ in this case. The polynomial, $x^k - 1$, has no repeated factors over $\mathbb{F}_p$ when $p \nmid k$ which implies that there is an algebraic extension of $\mathbb{F}_p$ with k distinct kth roots of unity. Furthermore, Theorem 4 is not true for primes $p \leq k$ in its current formulation. Consider $k = 3$ and $p = 3$. Since $x^3 - 1 = (x-1)^3$ modulo 3, Theorem 4 would predict the existence of 3-gons with monodromy groups $C_3^2 \rtimes C_3$ and $C_3 \rtimes C_3$. However, the only 3-gon is $[1,1,1]$, and thus the only possible monodromy group of a 3-gon modulo 3 is $C_3 \rtimes C_3$.

8. Proving Theorem 4

Here we lay out the basic strategy and supporting lemmas we will use to prove Theorem 4.

8.1. *Strategy for Proving Theorem 4.* Recall that Lemmas 8 and 9 allow us to construct a geometric polygon with monodromy group G if we can find an algebraic polygon with all nonzero entries that has an isomorphic monodromy group. To control the number of nonzero entries in an algebraic polygon, we define:

Definition 9. For a polynomial $f(x) = a_n x^n + \cdots + a_1 x + a_0$ with $a_n \neq 0$, let $w(f(x))$ be the maximum number of consecutive coefficients of $f(x)$ that are zero. For example, if $g(x) = x^7 - x^3 + 1$, then $w(g(x)) = 3$ since $a_6 = a_5 = a_4 = 0$ while $a_3, a_7 \neq 0$.

Now, our strategy for proving Theorem 4 is the following:

(1) For a given monodromy group $G \cong C_p^{k-d} \rtimes C_k$ described in Theorem 4, find an appropriate polynomial $g(x)$ satisfying $g(x)|x^k - 1$, $x - 1|g(x)$, and $\deg(g(x)) = d$.
(2) Using Proposition 8, multiply $g(x)$ by a series of linear polynomials to produce a polynomial $f(x)$, each of which reduces the value of the w function but leaves $\gcd(f(x), x^k - 1) = g(x)$. Repeat until $g(x)$ has been transformed into a polynomial $f(x) = \sum b_i x^i$ of degree $k-1$ with $w(f(x)) = 0$ and $\gcd(f(x), x^k - 1) = g(x)$.
(3) Use Lemmas 5 and 6 to transform $[b_0, \ldots, b_{k-1}]$ into a geometric polygon with monodromy group G.

Remark. The proofs of Theorem 5 and Proposition 11 follow the above approach. However, the proof of Proposition 12 differs slightly.

In the following proposition, we show that if we choose α appropriately, then $w((x-\alpha) \cdot f(x)) = \max(w(f(x)) - 1, 0)$.

Proposition 8. Let $\mathbb{F}$ be a field. Suppose that $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}[x]$ with $a_0, a_n \neq 0$. If $\{\alpha_0, \ldots, \alpha_n\}$ are distinct non-zero elements of $\mathbb{F}$, then there exists at least one α_i such that $w(f(x) \cdot (x - \alpha_i)) = \max(w(f(x)) - 1, 0)$.

Proof. Consider the coefficients of $f(x) \cdot (x - \alpha_i) = b_{n+1} x^{n+1} + b_n x^n + \cdots + b_1 x + b_0$. Observe that $b_0, b_{n+1} \neq 0$. Further observe that for $0 < j < n+1$, $b_j = a_{j-1} - \alpha_i a_j$. If $b_j = 0$ then one of three situations must arise:

(a) $a_{j-1} = a_j = 0$
(b) $a_{j-1} = \alpha_i = 0$
(c) $\alpha_i = \frac{a_{j-1}}{a_j}$ and $a_j \neq 0$

Situation (b) cannot arise, because α_i is chosen from non-zero elements of $\mathbb{F}$. By the pigeon hole principle, there exists at least one α_i in $\{\alpha_0, \ldots, \alpha_n\}$ such that $\alpha_i \neq \frac{a_{j-1}}{a_j}$ for all $0 \leq j \leq n$. Our choice of α_i prevents situation (c) from arising. Since situation (a) cannot occur if $w(f(x)) = 0$ then $w(f(x) \cdot (x - \alpha_i)) = 0$ in this case.

Now we consider the case where $w(f(x)) > 0$. By our choice of α_i, $b_j = 0$ implies $a_j = a_{j-1} = 0$. Assume that $w(f(x)) = d + 1$ which implies there exist $a_\ell, \ldots, a_{\ell+d}$, which are 0, with $a_{\ell-1} \neq 0$ and $a_{\ell+d+1} \neq 0$. We see that $b_\ell \neq 0$ and $b_{\ell+d+1} \neq 0$ and $b_{\ell+1}, \ldots, b_{\ell+d} = 0$. Hence, we have shown that $w(f(x) \cdot (x - \alpha_i)) = w(f(x)) - 1$. ☐

Now, we prove a useful result about the gcd of collections of polynomials with $x^k - 1$.

Lemma 10. Let $\mathbb{F}$ be a field and let $f(x) = a_d x^d + \cdots + a_1 x + a_0 \in \mathbb{F}[x]$. Then $\gcd(f(x), x^k - 1) = \gcd(x \cdot f(x) - a_{k-1}(x^k - 1), x^k - 1)$. Furthermore, $\gcd(f(x), x^k - 1) = \gcd(x^t \cdot f(x) - (a_{k-1} x^{t-1} + \cdots + a_{k-t+1} x + a_{k-t}) \cdot (x^k - 1)$ for any positive integer $t < k$.

Proof. Observe that $\gcd(f(x), x^k - 1) = \gcd(x \cdot f(x), x^k - 1)$ since x does not divide $x^k - 1$. It is clear that $\gcd(x \cdot f(x), x^k - 1)$ divides $\gcd(x \cdot f(x) - a_{k-1}(x^k - 1), x^k - 1)$. If $h(x) = \gcd(x \cdot$

$f(x)-a_{k-1}(x^k-1),x^k-1)$, then $h(x)$ divides $x\cdot f(x)-a_{k-1}(x^k-1)+a_{k-1}(x^k-1)=x\cdot f(x)$. Hence, $\gcd(f(x),x^k-1)=\gcd(x\cdot f(x)-a_{k-1}(x^k-1),x^k-1)$.

The result $\gcd(f(x),x^k-1)=\gcd(x^t\cdot f(x)-(a_{k-1}x^{t-1}+\cdots+a_{k-t+1}x+a_{k-t})\cdot(x^k-1)$ follows directly from using this same approach t times. ☐

Example 9. Consider the field $\mathbb{F}_2$. Let $f(x)=x^5+x^2+x+1$. Using Lemma 10 with $t=2$, we deduce that

$$\gcd(x^5+x^2+x+1,x^7-1)=\gcd(x^4+x^3+x^2+1,x^7-1)$$

In the following proposition, we prove a result about the maximum value of $w(f(x))$ for polynomials $f(x)$ dividing x^k-1.

Proposition 9. *Let $\mathbb{F}$ be a field and let $f(x)=a_dx^d+\ldots a_1x+a_0\in\mathbb{F}[x]$. Suppose that $f(x)$ is a non-zero polynomial with $\deg(f(x))=d$ and $f(x)|x^k-1$. Then $w(f(x))<k-d$.*

Proof. If $k-d\geq d=\deg(f(x))$, then the result is trivial. Otherwise, suppose that $w(f(x))\geq k-d$. This implies that $f(x)$ has $k-d$ consecutive coefficients equal to zero. For the purposes of this proof, assume $a_\ell,\ldots,a_{\ell+k-d-1}=0$ for some $\ell<d$.

Use Lemma 10 with $t=k-(\ell+k-d-1)=d-\ell$. That is, consider

$$g(x)=x^{d-\ell}f(x)-(a_{k-1}x^{d-\ell-1}+a_{k-2}x^{d-\ell-2}+\cdots+x\cdot a_{\ell+k-d+1}+a_{\ell+k-d})(x^k-1)$$

which can be rewritten as

$$g(x)=\sum_{i=d}^{k-1}a_{i-d+\ell}x^i+\sum_{i=d-\ell}^{d-1}a_{i-d+\ell}x^i+\sum_{i=0}^{d-\ell-1}a_{i+k-d+\ell}x^i.$$

Lemma 10 states that $\gcd(g(x),x^k-1)=\gcd(f(x),x^k-1)$. Since the first summation above is equal to zero, we see that $\deg(g(x))\leq d-1$. This implies that $\deg(\gcd(g(x),x^k-1))<d$ which is a contradiction since $\gcd(f(x),x^k-1)=f(x)$ and $\deg(f(x))=d$. ☐

8.2. *Proving Theorem 4 for* $p>k+1$.

In this section, we prove Theorem 4 in the case where $p>k+1$.

Proposition 10. *Fix an integer $k\geq 3$. Suppose that $d|k$ and $d<k$. For primes $p>k$, there exists a k-gon $[a_0,\ldots,a_{k-1}]$ modulo p with monodromy group $G(a_0,\ldots,a_{k-1})\cong C_p^{k-d}\rtimes C_k$.*

Proof. Consider $f(x)=(x^d-1)^{\frac{k}{d}-1}(x^{d-1}+\cdots+x+1)=b_0+b_1x+\cdots+b_{k-1}x^{k-1}$. Since $p>k$, the binomial coefficients in the expansion of $(x^d-1)^{\frac{k}{d}-1}$ are nonzero modulo p, and thus $b_i\not\equiv 0 \mod p$ for $0\leq i\leq k-1$. Further observe that x^k-1 has no repeated factors since $p\nmid k$. Since $x^{d-1}+\cdots+x+1$ divides x^d-1 and x^d-1 divides x^k-1, we deduce that $\gcd(f(x),x^k-1)=x^d-1$. Therefore, $[b_0,\ldots,b_{k-1}]$ is an algebraic k-gon modulo p.

By Lemma 5, Lemma 6, Proposition 2, and Proposition 6, $[b_0,\ldots,b_{k-1}]$ has a k-gon associate $[a_0,\ldots,a_{k-1}]$ modulo p with monodromy group $G(a_0,\ldots,a_{k-1})\cong C_p^{k-d}\rtimes C_k$. ☐

The following theorem is crucial in the proof of Theorem 4.

Theorem 5. *Let $k\geq 3$ be an integer, and let $p>k$ be a prime. Suppose $x^k-1=\prod g_i(x)$ where the $g_i(x)$ are irreducible over $\mathbb{F}_p$. Let $d=\sum_{j=1}^{\ell}\deg(g_{i_j}(x))$. Let M equal the number of roots of $\frac{x^k-1}{\prod g_{i_j}}$ in $\mathbb{F}_p$. Further suppose that $g_{i_j}=x-1$ for some i_j. If $p>k+M$, there exists a k-gon $[a_0,\ldots,a_{k-1}]$ modulo p with monodromy group $G(a_0,\ldots,a_{k-1})=C_p^{k-d}\rtimes C_k$.*

Proof. Let $g(x)=\prod g_{i_j}(x)$ which implies $\deg(g(x))=d$. By Proposition 9, $w(g(x))<k-d$. To produce a degree $k-1$ polynomial $f(x)$ with $\gcd(f(x),x^k-1)=g(x)$, we will use Proposition 8 exactly $k-d-1$ times. The result of this process will be a new polynomial $f(x)$ equal to $g(x)$ times $k-d-1$ linear polynomials, and $f(x)$ will have the property that $w(f(x))=0$.

To use Proposition 8, we must have at least k distinct nonzero $\alpha \in \mathbb{F}_p$. Furthermore, these α cannot be roots of $\frac{x^k-1}{g(x)}$. If α were a root of $\frac{x^k-1}{g(x)}$, then $\gcd((x-\alpha)\cdot g(x), x^k-1)$ would have degree greater than d. Since $\mathbb{F}_p$ has $p-1$ nonzero elements, we need $p-1 \geq k+M$ to satisfy the assumptions of Proposition 8 and thus we need $p > k+M$.

The result of using Proposition 8 exactly $k-d-1$ times is a degree $k-1$ polynomial $f(x) = b_{k-1}x^{k-1} + \cdots + b_1x + b_0$ with $b_{k-1}, \ldots, b_0 \not\equiv 0 \mod p$. Observe that $b_0 + \cdots + b_{k-1} \equiv 0 \mod p$ since $x-1 | f(x)$. By Lemma 5, Lemma 6, and Proposition 6, there exists a k-gon $[a_0, \ldots, a_{k-1}]$ modulo p with monodromy group $G(a_0, \ldots, a_{k-1}) \cong C_p^{k-d} \rtimes C_k$. □

Theorem 5 proves Theorem 4 for most k and p as illustrated in the following corollary.

Corollary 6. Fix an integer $k \geq 3$. Theorem 4 is true for primes $p > k+1$.

Proof. Fix $p > k+1$. Suppose that $\gcd(p-1, k) = d$. We claim that $\mathbb{F}_p^\times$ contains exactly d distinct kth roots of unity. Observe that $\mathbb{F}_p^\times \cong C_{p-1} \cong \mathbb{Z}/(p-1)\mathbb{Z}$. Finding the number of kth roots of unity in $\mathbb{F}_p^\times$ is equivalent to finding the number of solutions to $kx \equiv 0 \mod p-1$ in $\mathbb{Z}/(p-1)\mathbb{Z}$. Since $\gcd(\frac{k}{d}, p-1) = 1$, we see that the number of solutions to $kx = \frac{k}{d}(dx) \equiv 0 \mod p-1$ is the same as the number of solutions to $dx \equiv 0 \mod p-1$. Since $d | p-1$, there are d solutions to $dx \equiv 0 \mod p-1$ and thus $\mathbb{F}_p^\times$ contains exactly d distinct kth roots of unity. The remaining kth roots of unity lie in an algebraic extension of $\mathbb{F}_p$.

In Theorem 5, $M \leq d-1$ since the factor $g_{i_j} = x-1$ for some i_j. Since $p \neq k+1$ and $\gcd(p-1, k) = d$, we deduce that $p > k+d > k+M$. Thus, Theorem 4 is true when $p > k+1$. □

Remark. To prove Theorem 4, one need only verify it for integers $k \geq 3$ where $p = k+1$ is prime.

8.3. *Proving Theorem 4 for* $p = k+1$.

In this section, we prove Theorem 4 in the remaining cases in which $p = k+1$.

Remark. If $p = k+1$ then $x^k - 1$ splits completely into linear terms over $\mathbb{F}_p$ since $x^p - x = x(x^k-1)$ is the polynomial whose roots are the elements of $\mathbb{F}_p$.

Lemma 11. Suppose $p = k+1$ is an odd prime. Let $d | k$ with $d > 1$. There exists a polynomial $x^d - a \in \mathbb{F}_p[x]$ with no roots in $\mathbb{F}_p$.

Proof. Since $\mathbb{F}_p^\times$ is a cyclic group under multiplication, let a be a generator of this cyclic group. We claim $x^d - a$ has no roots in $\mathbb{F}_p$. Suppose $x^d - a$ had a root in $\mathbb{F}_p$. This would imply that there exists an element $b \in \mathbb{F}_p$ satisfying $b^d = a$. However, this would imply that $a^{k/d} = (b^d)^{k/d} = b^k = 1$, a contradiction with the fact that the order of a under multiplication is k. □

Proposition 11. Suppose $p = k+1$ is an odd prime. Further suppose $0 < d < \frac{k}{2}$. There exists a k-gon $[a_0, \ldots, a_{k-1}]$ modulo p with monodromy group $G(a_0, \ldots, a_{k-1}) = C_p^{k-d} \rtimes C_k$.

Proof. By Lemma 11, there exists a polynomial $x^{k/2} - a$ that has no linear factors in $\mathbb{F}_p$. Thus, $\gcd(x^{k/2} - a, x^k - 1) = 1$. We need to produce a polynomial $g(x)$ of degree $\frac{k}{2} - 1$ so that $w(g(x)) = 0$ and the $\gcd(g(x), x^k - 1)$ has degree d. If we can find such a $g(x)$, then $h(x) = (x^{k/2} - a) \cdot g(x)$ has degree $k-1$, the $\gcd(h(x), x^k - 1)$ has degree d, and $w(h(x)) = 0$.

Consider $(x-1)^{k/2-d}$ whose coefficients are nonzero modulo p. We need to find a sequence of distinct elements $\alpha_i \in \mathbb{F}_p$ so that if we set $g(x) = (x-1)^{k/2-d} \prod_{i=1}^{d-1} (x - \alpha_i)$ then $w(g(x)) = 0$. We proceed by induction. Suppose we have already found j distinct elements $\alpha_i \in \mathbb{F}_p$ so that $\tilde{g}(x) = (x-1)^{k/2-d} \prod_{i=1}^{j} (x - \alpha_i)$ and $w(\tilde{g}(x)) = 0$. How many choices for α_{j+1} are there? By Proposition 8, since $\deg(\tilde{g}) = \frac{k}{2} - d + j$, we need more than $\frac{k}{2} - d + j$ choices to select α_{j+1} so that $w(\tilde{g}\cdot(x-\alpha_{j+1}))=0$. We also remove j possible nonzero elements of $\mathbb{F}_p$ from consideration when we choose α_{j+1} to ensure all α_i are distinct. Since $j<d<\frac{k}{2}$, we see that $\frac{k}{2}-d+j<k-j$. Thus, by the pigeon hole principle, there exists a nonzero α_{j+1} so that the α_i are distinct for $1\le i\le j+1$ and $w(\tilde{g}\cdot(x-\alpha_{j+1}))=0$.

By induction, we have shown there exists a polynomial $g(x)=(x-1)^{k/2-d}\prod_{i=1}^{d-1}(x-\alpha_i)$ where the α_i are distinct and $w(g(x))=0$. Now, let $h(x)=g(x)\cdot(x^{k/2}-a)$. We see that $\deg(h(x))=k-1$, the $\gcd(h(x),x^k-1)$ has degree d, and $w(h(x))=0$.

By Lemma 5, Lemma 6, and Proposition 6, there exists a k-gon $[a_0,\ldots,a_{k-1}]$ modulo p with monodromy group $G(a_0,\ldots,a_{k-1})\cong C_p^{k-d}\rtimes C_k$. □

Proposition 12. Suppose $k\ge 3$ and $p=k+1$ is prime. Further suppose $\frac{k}{2}<d<k$. There exists a k-gon $[a_0,\ldots,a_{k-1}]$ modulo p with monodromy group $G(a_0,\ldots,a_{k-1})=C_p^{k-d}\rtimes C_k$.

Proof. Since k is even, observe that $x^{k/2}+1$ divides x^k-1. Let S be the set of roots of $x^{k/2}+1$ in $\mathbb{F}_p$. Choose a set $T=\{\alpha_1,\ldots,\alpha_{d-k/2}\}\subset\mathbb{F}_p^{\times}$ so that the α_i are distinct, $\alpha_1=1$, and $\alpha_i\notin S$ for all i.

Setting $\tilde{g}(x)=\prod_{i=1}^{d-k/2}(x-\alpha_i)$, observe that $\tilde{g}(x)$ divides $x^{k/2}-1$. By Proposition 9, we see that $w(\tilde{g}(x))<\frac{k}{2}-(d-\frac{k}{2})=k-d<\frac{k}{2}$. Now, we want to use Proposition 8 exactly $k-d-1$ times to find β_j in $\mathbb{F}_p$ so that $g(x)=\prod_{i=1}^{d-k/2}(x-\alpha_i)\cdot\prod_{j=1}^{k-d-1}(x-\beta_j)$ and $w(g(x))=0$ and each $\beta_j\in S\cup T$. If we have at least $\frac{k}{2}$ eligible distinct nonzero elements of $\mathbb{F}_p$, we can use Proposition 8 exactly $k-d-1$ times. Since there are d nonzero elements in $S\cup T$ and $d>\frac{k}{2}$, we can use Proposition 8 to select our β_j. The result of using Proposition 8 these $k-d-1$ times is the polynomial $g(x)=\prod_{i=1}^{d-k/2}(x-\alpha_i)\cdot\prod_{j=1}^{k-d-1}(x-\beta_j)$ which has the properties that $w(g(x))=0$ and each $\beta_j\in S\cup T$.

Now, let $h(x)=g(x)\cdot(x^{k/2}+1)$. We see that $\deg(h(x))=k-1$, and that $\gcd(h(x),x^k-1)=\tilde{g}(x)\cdot(x^{k/2}+1)$ has degree d, and that $w(h(x))=0$. By Lemma 5, Lemma 6, and Proposition 6, there exists a k-gon $[a_0,\ldots,a_{k-1}]$ modulo p with monodromy group $G(a_0,\ldots,a_{k-1})\cong C_p^{k-d}\rtimes C_k$. □

Now, we proceed with the proof of Theorem 4.

Proof of Theorem 4. The case where $p>k+1$ was proven in Corollary 6. Now consider the case when $p=k+1$ is an odd prime. If $1\le d\le k-1$, we claim there exists a k-gon modulo p with monodromy group $C_p^{k-d}\rtimes C_k$. The case where $d<\frac{k}{2}$ was proven in Proposition 11 and the case where $d>\frac{k}{2}$ was proven in Proposition 12. The case where $d=\frac{k}{2}$ is a consequence of Proposition 10 because $\frac{k}{2}$ divides k. Thus, the proof of Theorem 4 is complete. □

9. Results for Composite n

In this section, we will prove several results about monodromy groups when n is composite relying heavily on the theory of algebraic polygons from Section 5. This first proposition shows that you can combine k-gons with relatively prime moduli to create a new k-gon whose monodromy group is closely related to the monodromy groups of the initial k-gons.

Proposition 13. Suppose that $[a_0,\ldots,a_{k-1}]$ and $[b_0,\ldots,b_{k-1}]$ represent k-gons modulo n_1 and n_2 respectively where $\gcd(n_1,n_2)=1$. Suppose their respective monodromy groups are $N_1\rtimes C_k$ and $N_2\rtimes C_k$. Then there exists a k-gon $[c_0,\ldots,c_{k-1}]$ modulo n_1n_2 with monodromy group $(N_1\times N_2)\rtimes C_k$.

Proof. This proposition is an immediate consequence of Proposition 3, Lemma 5, and Lemma 6. □

Here is an example of the use of Proposition 13.

Example 10. Consider the quadrilateral $[a_0,a_1,a_2,a_3] = [1,4,4,1]$ which has modulus $n_1 = 5$. The monodromy group of $D(1,4,4,1)$ is $C_5^2 \rtimes C_4$. Also consider the quadrilateral $[b_0,b_1,b_2,b_3] = [2,3,4,3]$ which has modulus $n_2 = 6$. The monodromy group of $D(2,3,4,3)$ is $C_6^2 \rtimes C_4$. We can solve a system of four congruences modulo $5 \cdot 6 = 30$. Observe that if we set $[c_0,c_1,c_2,c_3] = [26,9,4,21]$ then we have $c_i \equiv a_i \mod 5$ and $c_i \equiv b_i \mod 6$. We see that $c_0+c_1+c_2+c_3 = 2 \cdot 30$. If this had not been the case, we could have modified the coefficients using Lemma 5 and Lemma 6 without changing the monodromy group. Finally, by Proposition 13, the monodromy group of $D(26,9,4,21)$ is $C_{30}^2 \rtimes C_4 \cong (C_5^2 \times C_6^2) \rtimes C_4$.

You can use Proposition 4 to project a k-gon modulo $n_1 n_2$ to an *algebraic* k-gon modulo n_1. However, this proposition does *not* guarantee that the new algebraic k-gon will have a k-gon associate, as illustrated in the following example.

Example 11. Consider the polygon $[c_0,c_1,c_2] = [1,1,4]$ modulo 6 which has monodromy group $(C_6 \times C_2) \rtimes C_3$. Consider the reduction $c_i \equiv a_i \mod 2$ to obtain $[a_0,a_1,a_2] = [1,1,0]$. The monodromy group of $[1,1,0]$ modulo 2 is $C_2^2 \rtimes C_3$. However, there do not exist any 3-gons modulo 2.

The above example illustrates how we must understand monodromy groups of algebraic polygons, and not polygons, in order to classify all possible monodromy groups for k-gons modulo composite n.

Proposition 14. Fix an abelian group N and a positive integer $n = \prod p_j^{x_j}$ where the p_j are distinct primes. There exists a k-gon $[c_0,\dots,c_{k-1}]$ modulo n with monodromy group $N \rtimes C_k$ if and only if there exist algebraic k-gons $[a_0^{(j)},\dots,a_{k-1}^{(j)}]$ modulo $p_j^{x_j}$ with monodromy groups $(N/p_j^{x_j}N) \rtimes C_k$ and for every $0 \le i \le k-1$ there exists some j for which $a_i^{(j)} \not\equiv 0 \mod p_j^{x_j}$.

Proof. If $[c_0,\dots,c_{k-1}]$ is a k-gon with the desired monodromy group $N \rtimes C_k$, then the forward direction of the proof follows immediately from Proposition 4 and the fact that $c_i \not\equiv 0 \mod n$ for all i.

Suppose there exist algebraic k-gons $[a_0^{(j)},\dots,a_{k-1}^{(j)}]$ modulo $p_j^{x_j}$ with monodromy groups $(N/p_j^{x_j}N) \rtimes C_k$ and for every $0 \le i \le k-1$ there exists some j for which $a_i^{(j)} \not\equiv 0 \mod p_j^{x_j}$. The reverse direction of the proof follows from Proposition 3, Lemma 5, and Lemma 6. □

Remark. The condition that $a_i^{(j)} \not\equiv 0 \mod p_j^{x_j}$ in Proposition 14 is satisfied if at least one of the algebraic k-gons $[a_0^{(j)},\dots,a_{k-1}^{(j)}]$ is an actual k-gon. This is sufficient but not necessary.

Proposition 14 translates the problem of understanding the monodromy groups of all algebraic k-gons to the problem of understanding monodromy groups for algebraic k-gons with prime power moduli.

Example 12. There does not exist a 3-gon modulo 35 with monodromy group $N \rtimes C_3$ where $N \cong C_{35}$ or where $N \cong C_{35} \times C_7$. Suppose there were such a 3-gon $[c_0,c_1,c_2]$ modulo 35. Then the projection of $[c_0,c_1,c_2]$ modulo 5 (using Proposition 4) would have monodromy group $7N \rtimes C_3 \cong (N/5N) \rtimes C_3$ which is isomorphic to $C_5 \rtimes C_3$ in both the case where $N \cong C_{35}$ and $N \cong C_{35} \times C_7$. However, $C_5 \rtimes C_3$ is not a possible monodromy group for any algebraic 3-gon modulo 5 by Proposition 7.

9.1. ***Triangular Billiards Surfaces.*** One well-known property of the Smith Normal Form for $\mathbb{Z}$ is summarized in the following lemma.

Lemma 12 (Proposition 8.1, [15]). If $d_1,\ldots,d_k$ are the elementary divisors of the Smith Normal Form of a matrix A over $\mathbb{Z}$, then $d_1\cdots d_j$ is equal to the gcd of the determinants of all $j\times j$ minors of the matrix A.

This property allows us to reprove Corollary 1 using a method that will extend to the higher k-gons.

Proof of Corollary 1. Consider the arbitrary rational triangle with angles $\left(\frac{a_0\pi}{n},\frac{a_1\pi}{n},\frac{a_2\pi}{n}\right)$, where the a_i are positive integers, $a_0+a_1+a_2=n$, and $\gcd(a_0,a_1,a_2,n)=1$. The normal subgroup N of the associated monodromy group is represented by the column span of $C=\begin{bmatrix}a_0 & a_1 & a_2\\ a_1 & a_2 & a_0\\ a_2 & a_0 & a_1\end{bmatrix}$ over $\mathbb{Z}/n\mathbb{Z}$. Observe that

$$C=\begin{bmatrix}a_0 & a_1 & a_2\\ a_1 & a_2 & a_0\\ a_2 & a_0 & a_1\end{bmatrix}=\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ -1 & -1 & 1\end{bmatrix}\begin{bmatrix}a_0 & a_1 & 0\\ a_1 & a_2 & 0\\ 0 & 0 & 0\end{bmatrix}\begin{bmatrix}1 & 0 & -1\\ 0 & 1 & -1\\ 0 & 0 & 1\end{bmatrix}.$$

The elementary divisors of C are the same as the elementary divisors of $C'=\begin{bmatrix}a_0 & a_1 & 0\\ a_1 & a_2 & 0\\ 0 & 0 & 0\end{bmatrix}$.
Using Lemma 12, we deduce that $d_1=\gcd(a_0,a_1,a_2,n)=1$. By looking at the 2×2 minors of C', we further deduce that $d_1d_2=d_2=\gcd(a_0a_2-a_1^2,n)$. It then follows from Theorem 2 that the monodromy group of the $[a_0,a_1,a_2]$ triangle is

$$(C_n\times C_{n/\alpha})\rtimes C_3,$$

where $d_2=\alpha=\gcd(n,a_0a_2-a_1^2)$. □

Although Corollary 1 gives a formula for computing the monodromy group of the dessin drawn on a triangular billiards surface, it does not specify which monodromy groups can arise. The following theorem classifies the monodromy groups of all rational triangular billiards surfaces modulo n.

Theorem 6. Fix $n\in\mathbb{N}$ with $n>3$. The set of possible monodromy groups for triangles modulo n includes precisely those groups of the form $(C_n\times C_{n/\alpha})\rtimes C_3$ where $\alpha|n$ and $\alpha=3^i\prod_j p_j^{n_j}$ where the p_j are primes congruent to 1 modulo 3, $i\in\{0,1\}$, and $n_j\geq 0$. If $n=3$, the only possible monodromy group is $C_3\rtimes C_3$.

The proof of this theorem utilizes results from algebraic number theory. Use any introductory graduate book on the topic, such as [12], as a reference.

Proof. Recall that the monodromy group associated to the triangle $[a_0,a_1,a_2]$ modulo n is $(C_n\times C_{n/\alpha})\rtimes C_3$ where $\alpha=\gcd(a_0a_2-a_1^2,n)$. What values can $a_0a_2-a_1^2$ take modulo n?

Observe that $a_2\equiv -a_0-a_1 \pmod n$. Hence, $a_0a_2-a_1^2\equiv a_0(-a_0-a_1)-a_1^2\equiv -(a_0^2+a_0a_1+a_1^2) \mod n$. Further observe that $a_0^2+a_0a_1+a_1^2=N(a_0-a_1\zeta_3)$ where ζ_3 is a third root of unity and N is the norm map from $\mathbb{Z}[\zeta_3]$ to $\mathbb{Z}$. So we can answer the question about the possible values of α by asking what values are in the image of the norm map. However, there are some restrictions on a_0 and a_1. Since $\gcd(a_0,a_1,a_2,n)=1$ and $a_0+a_1+a_2=n$, we deduce that $\gcd(a_0,a_1,n)=1$. Hence, if a_0 and a_1 have a common factor greater than 1, that factor does not divide n. Therefore, to find a triangle modulo n with monodromy group $(C_n\times C_{n/\alpha})\rtimes C_3$, we must find an ideal $(a_0-a_1\zeta_3)$ in $\mathbb{Z}[\zeta_3]$ with the properties that $\gcd(N(a_0-a_1\zeta_3),n)=\alpha$ and $\gcd(a_0,a_1,n)=1$. Note that every ideal has a generator since $\mathbb{Z}[\zeta_3]$ is a PID.

The fact that the norm map is multiplicative will allow us to answer the question by examining ideals with norm of prime power order. Since ideals factor uniquely as products of prime ideals in $\mathbb{Z}[\zeta_3]$, suppose the ideal $(a_0-a_1\zeta_3)=\prod\mathfrak{p}_j^{n_j}$ where the $\mathfrak{p}_j$ are distinct prime ideals in $\mathbb{Z}[\zeta_3]$. If $\mathfrak{p}_j=(b_0-b_1\zeta_3)$ then $\gcd(b_0,b_1,n)=1$. If $\gcd(b_0,b_1,n)\neq 1$, then $\gcd(a_0,a_1,n)\neq 1$. Secondly, if $p^{n_j}|\gcd(N(a_0-a_1\zeta_3),n)$ one of the following three situations must arise:

(1) $\mathfrak{p}^{n_j/2} = (p)^{n_j/2}$ is in the factorization of the ideal $(a_0 - a_1\zeta)$ if $\mathfrak{p}$ is an inert prime with $N(\mathfrak{p}) = p^2$.
(2) $\mathfrak{p}_1^x \mathfrak{p}_2^{n_j - x}$ is in the factorization of the ideal $(a_0 - a_1\zeta_3)$ if $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are the two primes above (p) in $\mathbb{Z}[\zeta_3]$. In this case, $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$.
(3) $\mathfrak{p}^{n_j}$ is in the factorization of the ideal $(a_0 - a_1\zeta)$ if $\mathfrak{p}$ is a ramified prime with $N(\mathfrak{p}) = p$.

To summarize, we want to know if, when p is a prime dividing n, does there exist an ideal $(b_0 - b_1\zeta_3)$ satisfying $N(b_0 - b_1\zeta_3) = p^{n_j}$ with $p^{n_j}|n$ and $\gcd(b_0, b_1, n) = 1$?

First consider a prime $p \equiv 2 \mod 3$. Observe that the ideal $(p) \subset \mathbb{Z}[\zeta_3]$ is an inert prime ideal that has norm p^2. Hence, p is not in the range of the norm map. If $b_0 - b_1\zeta_3 \in \mathbb{Z}[\zeta_3]$ has norm p^{n_j} then the ideal generated by $b_0 - b_1\zeta_3$ has the property $(b_0 - b_1\zeta_3) = (p^{n_j/2})$ since ideals factor uniquely as products of prime ideals in $\mathbb{Z}[\zeta_3]$. Hence, p divides b_0 and b_1, which implies $p \nmid n$. Hence, $p \not\equiv 2 \mod 3$.

Now consider a prime $p \equiv 1 \mod 3$. There is a prime ideal $(y - z\zeta_3)$ of norm p since the ideal (p) splits in $\mathbb{Z}[\zeta_3]$. Note that $\gcd(y, z) = 1$ since $N(y - z\zeta_3) = y^2 + yz + z^2 = p$. Set $(y - z\zeta_3)^{n_j} = (b_0 - b_1\zeta_3)$. Observe that the ideal $(b_0 - b_1\zeta_3)$ is an ideal with norm p^{n_j}. Now, we deduce $\gcd(b_0, b_1) = 1$ from the fact that ideals factor uniquely in $\mathbb{Z}[\zeta_3]$. Since $N(b_0 - b_1\zeta_3) = p^{n_j}$, the only factor they could have in common is p. But if $p|b_0$ and $p|b_1$ then the ideal (p) would divide $(y - z\zeta_3)^{n_j}$, which is a contradiction since the ideal (p) factors as a product of two distinct prime ideals of norm p, namely $(y - z\zeta_3)$ and $(y - z\zeta_3^2)$. Clearly, $(y - z\zeta_3^2)$ is not in the unique factorization of $(y - z\zeta_3)^{n_j}$. Hence, $\gcd(b_0, b_1) = 1$. Therefore, if $p \equiv 1 \mod 3$ is a prime dividing n, then there exist b_0, b_1 with $\gcd(b_0, b_1) = 1$ and $N(b_0 - b_1\zeta_3) = p^{n_j}$.

Now consider the case when $p = 3$. The unique prime ideal of norm 3 in $\mathbb{Z}[\zeta_3]$ is $(1 - \zeta_3)$. If $N(b_0 - b_1\zeta_3) = 3^i$ where $i > 1$ then the ideal (3) would divide $(b_0 - b_1\zeta_3)$ since the ideal $(1 - \zeta_3)^2 = (3)$. Since ideals have unique prime ideal factorizations in $\mathbb{Z}[\zeta_3]$, we would have $3|b_0$ and $3|b_1$, a contradiction. Hence, when $p = 3$, the only ideal $(b_0 - b_1\zeta_3)$ satisfying $N(b_0 - b_1\zeta_3) = 3^i$ with $3^i|n$ and $\gcd(b_0, b_1, n) = 1$ occurs when $i \in \{0, 1\}$.

Using the multiplicative property of the norm map, if $\alpha = 3^i \prod_j p_j^{n_j}$ divides n where the p_j are primes congruent to 1 modulo 3, $i \in \{0, 1\}$, and $n_j \geq 0$, then there exist positive integers a_0, a_1 with $\gcd(a_0, a_1, n) = 1$, and $\gcd(a_0 a_2 - a_1^2, n) = \alpha$ if $a_2 = n - a_0 - a_1$. To use Lemma 5, we must verify that $a_0, a_1, a_2 \not\equiv 0 \mod n$.

Assume $\alpha \neq 1$. By way of contradiction, assume one of the $a_i \equiv 0 \mod n$. Without loss of generality, assume $a_2 \equiv 0$. In this case, $a_0 \equiv -a_1 \mod n$. Thus, $a_0^2 + a_0 a_1 + a_1^2 \equiv a_0^2 \mod n$. Hence, $\gcd(N(a_0 - a_1\zeta_3), n) = \gcd(a_0^2 + a_0 a_1 + a_1^2, n) = \gcd(a_0^2, n)$. Since, $\gcd(a_0, a_1, n) = \gcd(a_0, -a_0, n) = 1$, then $\gcd(N(a_0 - a_1\zeta_3), n) = \gcd(a_0^2, n) = 1$, a contradiction.

Thus, if $\alpha \neq 1$, we can use Lemma 5 to adjust $[a_0, a_1, a_2]$ so that it is a geometric 3-gon modulo n without altering the gcd's above. Thus by Corollary 1, we have obtained the required monodromy group when $\alpha \neq 1$.

Now consider the case when $\alpha = 1$. Instead of showing $a_i \not\equiv 0 \mod n$ in the above construction, we instead find explicit geometric triangles with monodromy group $(C_n \times C_n) \rtimes C_3$. If $3 \nmid n$, then consider the triangle $[1, 1, n-2]$. Observe that $\gcd(a_0^2 + a_0 a_1 + a_2^2, n) = \gcd(3, n) = 1$. Thus, $[1, 1, n-2]$ has monodromy group $(C_n \times C_n) \rtimes C_3$ when $3 \nmid n$. Now consider the case when $3|n$. Consider the triangle $[\frac{n}{3} - 1, \frac{n}{3}, \frac{n}{3} + 1]$. This is a geometric triangle when $n > 3$. Observe that $a_0^2 + a_0 a_1 + a_1^2 = (\frac{n}{3} - 1)^2 + (\frac{n}{3} - 1)\frac{n}{3} + (\frac{n}{3})^2 = 1 - n + \frac{n^2}{3}$. Since $3|n$, we see that $a_0^2 + a_0 a_1 + a_1^2 \equiv 1 \mod n$. Thus $\gcd(a_0^2 + a_0 a_1 + a_1^2, n) = 1$ and the monodromy group of $[\frac{n}{3} - 1, \frac{n}{3}, \frac{n}{3} + 1]$ is $(C_n \times C_n) \rtimes C_3$. In the case when $n = 3$, there is only one geometric triangle, $[1, 1, 1]$, which has monodromy group $C_3 \rtimes C_3$. □

The following example illustrates how Theorem 6 can be used to classify the possible monodromy groups modulo a composite number n.

Example 13. If $n = 81$, there are only two possible monodromy groups. The triangle $[1, 2, 78]$ has associated monodromy group $(C_{81} \times C_{81}) \rtimes C_3$ and the triangle $[1, 1, 79]$ has associated monodromy group $(C_{81} \times C_{27}) \rtimes C_3$. However, there does not exist a triangle with associated monodromy group $(C_{81} \times C_9) \rtimes C_3$ or $(C_{81} \times C_3) \rtimes C_3$ or $(C_{81}) \rtimes C_3$.

9.2. *Quadrilateral Billiards Surfaces.* One can also use Lemma 12 to produce an analogue of Corollary 1 in the quadrilateral case.

Proposition 15. Suppose that $[a_0, a_1, a_2, a_3]$ represents a 4-gon modulo n. Let $G(a_0, a_1, a_2, a_3)$ be the monodromy group of the dessin $D(a_0, a_1, a_2, a_3)$ drawn on the quadrilateral billiards surface $X(a_0, a_1, a_2, a_3)$. Then

$$G(a_0, a_1, a_2, a_3) \cong (C_n \times C_{\frac{n}{d_2}} \times C_{\frac{n}{d_3}}) \rtimes C_4.$$

where

$$d_2 = \gcd(a_0a_2 - a_3^2, a_0a_1 - a_2a_3, a_0^2 - a_2^2, a_1a_3 - a_2^2, a_0a_3 - a_1a_2, a_0a_2 - a_1^2, n)$$

and

$$d_3 = \begin{cases} \gcd(\frac{(a_0+a_2)((a_0+a_1)^2+(a_1+a_2)^2)}{d_2}, n) & if\ d_2 \neq n \\ n & if\ d_2 = n. \end{cases}$$

Proof. The normal subgroup N of the associated monodromy group is represented by the column span of $C = \begin{bmatrix} a_0 & a_1 & a_2 & a_3 \\ a_1 & a_2 & a_3 & a_0 \\ a_2 & a_3 & a_0 & a_1 \\ a_3 & a_0 & a_1 & a_2 \end{bmatrix}$ over $\mathbb{Z}/n\mathbb{Z}$. Let $\tilde{a}_3 = -a_0 - a_1 - a_2$. Consider the matrix $C' = \begin{bmatrix} a_0 & a_1 & a_2 & \tilde{a}_3 \\ a_1 & a_2 & \tilde{a}_3 & a_0 \\ a_2 & \tilde{a}_3 & a_0 & a_1 \\ \tilde{a}_3 & a_0 & a_1 & a_2 \end{bmatrix}$. Observe that $C \equiv C' \mod n$ and thus they have the same elementary divisors modulo n. We will proceed by finding the elementary divisors of C' over $\mathbb{Z}$ and then reducing them modulo n to get the elementary divisors of C'. Let d_1, d_2, d_3, d_4 be the elementary divisors of C and let $\tilde{d_1}, \tilde{d_2}, \tilde{d_3}, \tilde{d_4}$ be the elementary divisors of C'. Since $\gcd(a_0, a_1, a_2, \tilde{a}_3, n) = \gcd(a_0, a_1, a_2, a_3, n) = 1$, the gcd of the one by one minors is 1. Hence, $d_1 = \tilde{d_1} = 1$ by Lemma 12.

Observe that

$$C' = \begin{bmatrix} a_0 & a_1 & a_2 & \tilde{a}_3 \\ a_1 & a_2 & \tilde{a}_3 & a_0 \\ a_2 & \tilde{a}_3 & a_0 & a_1 \\ \tilde{a}_3 & a_0 & a_1 & a_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} a_0 & a_1 & a_2 & 0 \\ a_1 & a_2 & \tilde{a}_3 & 0 \\ a_2 & \tilde{a}_3 & a_0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Thus the elementary divisors of C' are the same modulo n as the elementary divisors of

$$C'' = \begin{bmatrix} a_0 & a_1 & a_2 & 0 \\ a_1 & a_2 & \tilde{a}_3 & 0 \\ a_2 & \tilde{a}_3 & a_0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Hence, $d_4 = \tilde{d_4} = 0$. To compute d_2, we compute the gcd of the 2 by 2 minors of C'' of which there are only 9 that are nonzero. Three of the minors are duplicates, thus leaving us with 6. These minors are $\{a_0a_2 - \tilde{a}_3^2, a_0a_1 - a_2\tilde{a}_3, a_0^2 - a_2^2, a_1\tilde{a}_3 - a_2^2, a_0\tilde{a}_3 - a_1a_2, a_0a_2 - a_1^2\}$. Using Lemma 12, we obtain $d_2 = \gcd(\tilde{d_2}, n) = \gcd(a_0a_2 - a_3^2, a_0a_1 - a_2a_3, a_0^2 - a_2^2, a_1a_3 - a_2^2, a_0a_3 - a_1a_2, a_0a_2 - a_1^2, n)$.

Lastly, $\tilde{d_3}$ will be equal to the third elementary divisor of C' which is the same as the third elementary divisor of $\begin{bmatrix} a_0 & a_1 & a_2 \\ a_1 & a_2 & \tilde{a}_3 \\ a_2 & \tilde{a}_3 & a_0 \end{bmatrix}$. By Lemma 12, we know that $\tilde{d_2}\tilde{d_3} = \det \begin{bmatrix} a_0 & a_1 & a_2 \\ a_1 & a_2 & \tilde{a}_3 \\ a_2 & \tilde{a}_3 & a_0 \end{bmatrix} = a_0^2a_2 + 2a_1a_2\tilde{a}_3 - a_2^3 - a_0\tilde{a}_3^2 - a_0a_1^2 = -(a_0+a_2)((a_0+a_1)^2 + (a_1+a_2)^2)$. Hence, $\tilde{d_3} = \frac{(a_0+a_2)((a_0+a_1)^2+(a_1+a_2)^2)}{\tilde{d_2}}$

provided $\tilde{d}_2 \neq 0$. If $\tilde{d}_2 = 0$ then $\tilde{d}_3 = 0$. Therefore, $d_3 = \gcd(\tilde{d}_3, n) = \gcd(\frac{(a_0+a_2)((a_0+a_1)^2+(a_1+a_2)^2)}{d_2}, n)$ unless $d_2 = n$ in which case $d_3 = n$. □

10. Future Directions

There are many questions that naturally arose in the study of monodromy groups of dessin drawn on rational billiards surfaces. Here are some possible future questions to investigate.

Question 1. Throughout this paper, we used Proposition 2, Lemma 5, and Lemma 6 many times to produce a polygon with the same monodromy group as a particular algebraic polygon. Using Lemma 5, we can produce an associate *convex* polygon in the case where the modulus $n = p$ is prime and $p \geq k$. It is natural to ask if G is the monodromy group of a k-gon modulo n, is it the monodromy group of a convex k-gon modulo n?

Question 2. How can one generalize Theorem 4 to primes $p \leq k$? For $p \leq k$, a monodromy group attained by an algebraic k-gon may not be attainable by a k-gon. For example, $x^6 - 1 = (x-1)^2(x^2+x+1)^2$ modulo 2. Thus, there exist algebraic 6-gons modulo 2 with monodromy groups $C_2 \rtimes C_6$, $C_2^2 \rtimes C_6$, $C_2^3 \rtimes C_6$, $C_2^4 \rtimes C_6$, and $C_2^5 \rtimes C_6$. However, there is only one 6-gon modulo 2, namely $[3,1,1,1,1,1]$, which has monodromy group $C_2 \rtimes C_6$.

Question 3. Can one generalize Proposition 15 to k-gons where $k > 4$?

Question 4. In Theorem 6, we classified which groups appear as the monodromy group of a triangle. Can one prove an analogous result for the monodromy groups that arise for an arbitrary k-gon?

References

[1] N. M. Adrianov, Yu. Yu. Kochetkov, and A. D. Suvorov. Plane trees with exceptional primitive edge rotation groups. *Fundam. Prikl. Mat.*, 3(4):1085–1092, 1997.
[2] N. M. Adrianov, A. Zvonkin, and F. Pakovich. *Davenport-Zannier polynomials and Dessins d'enfants*. American Mathematical Society, 2020.
[3] P. Aluffi. *Algebra: Chapter 0*. American Mathematical Society, 2009.
[4] E. Aurell and C. Itzykson. Rational billiards and algebraic curves. *Journal of Geometry and Physics*, 5(2):191–208, 1988.
[5] Z. Batterman, I. Chung-Halpern, J. M. Clark, E. H. Goins, and E. Semere. Monodromy groups of Belyĭ Lattès maps. PRiME REU, 2022. https://pages.pomona.edu/~ehga2017/prime/previousresearch.html.
[6] J. A. Bond. *On the computation and composition of Belyĭ maps and dessins d'enfants*. PhD thesis, ProQuest Dissertations amp; Theses, 2018.
[7] N. Cameron, M. Kemp, S. Maslak, G. Melamed, R. A. Moy, J. Pham, and A. Wei. Shabat polynomials and monodromy groups of trees uniquely determined by ramification type. *Involve, a Journal of Mathematics*, 12(5):791–812, 2019.
[8] Philip J. Davis. *Circulant matrices*. John Wiley Sons, 1979.
[9] A. Efrat, R. Fulek, S. Kobourov, and C. D. Tóth. Polygons with prescribed angles in 2d and 3d. *Lecture Notes in Computer Science*, page 135–147, 2020.
[10] I. Kaplansky. Elementary divisors and modules. *Transactions of the American Mathematical Society*, 66(2):464–491, 1949.
[11] S. K. Lando and A. K. Zvonkin. *Graphs on surfaces and their applications*. Springer, 2004.
[12] S. Lang. *Algebraic Number Theory*. Springer, 2014.
[13] M. D. Larsen, W. J. Lewis, and T. S. Shores. Elementary divisor rings and finitely presented modules. *Transactions of the American Mathematical Society*, 187:231–248, 1974.
[14] M. Mabe, R. A. Moy, J. Schmurr, and J. Varlack. Monodromy groups of dessins d'enfant on rational triangular billiards surfaces. *Involve, a Journal of Mathematics*, 16(1):49–58, 2023.
[15] A. Miller and V. Reiner. Differential posets and smith normal forms. *Order*, 26(3):197–228, 2009.
[16] J. Schmurr, J. L. McCartney, and J. Grzegrzolka. Cayley graphs on billiard surfaces. *Involve, a Journal of Mathematics*, 2024. Forthcoming.
[17] Y. B. Vorobets. Planar structures and billiards in rational polygons: the veech alternative. *Russian Mathematical Surveys*, 51(5):779, 1996.

[18] A. N. Zemlyakov and A. B. Katok. Topological transitivity of billiards in polygons. *Mathematical Notes of the Academy of Sciences of the USSR*, 18(2):760–764, 1975.