CONGRUENCE AND NONCONGRUENCE SUBGROUPS OF $\Gamma(2)$ VIA GRAPHS ON SURFACES

DISSERTATION

Presented in Partial Fulfillment of the Requirements for the Degree Doctor of Philosophy in the Graduate School of the Ohio State University

By

erica j. Whitaker, M.Sci.

Graduate Program in Mathematics

The Ohio State University

2011

Dissertation Committee:

James W. Cogdell, Advisor

Thomas Kerler

Warren Mann Sinnott

ABSTRACT

There is an established bijection between finite-index subgroups Γ of $\Gamma(2)$ and bipartite graphs on surfaces, or, equivalently, triples of permutations. We utilize this relationship to study noncongruence subgroups in terms of the corresponding graphs. In particular, we will produce infinite families of noncongruence subgroups of $\Gamma(2)$ of every even level by constructing their associated graphs. Also, given a graph on a surface, we have a method to produce generators for the corresponding group Γ in terms of the generators of $\Gamma(2)$. Given generators for $\Gamma(2n)$, we show how to determine whether or not a graph of level $2n$ corresponds to a congruence subgroup. Finally we give an algorithm to find permutations and generators for groups of the form $\Gamma(2p)$ for p prime.

This thesis is dedicated to my husband John, and Jim Cogdell.

ACKNOWLEDGMENTS

I am grateful to the dozens of people who, though surely tempted, didn't strangle me in my sleep during this process.

More specifically, I would like to thank my committee members Warren Sinnott and Thomas Kerler for their time and attention. I am grateful to Cindy Bernlohr, our teaching coordinator, who always worked to give me assignments that would help me balance my time between teaching and studies. I appreciate our computer support staff, especially Dave Alden and Tim Winningham, for helping me obtain the software I needed and dealing with my panic when I couldn't get it to behave. I want to thank Justin Lynd for introducing me to the software GAP, which helped with many computations. I offer my thanks and apologies to the entire the sixth floor of the Mathematics Tower, who endured me wandering shoeless through the halls and making popcorn without offering to share. I especially thank my husband John, for his willingness to live in the frozen north for years and not complaining when my late nights meant he had no clean socks or company.

And finally, I thank my advisor Jim Cogdell. I cannot imagine how a human could be more patient and supportive, and without his guidance I would not be where I am today.

VITA

1993	BS in Mathematics, BA in Music, Birmingham-Southern College
1993-1997	Teaching Assistant, University of Texas at Austin
1997-1999	Instructor, Louisiana State University
2000-2002	Instructor, Wittenberg University
2004	MS in Mathematics, The Ohio State University
2002-Present	Graduate Teaching Associate, VIGRE Fellow, The Ohio State University

FIELDS OF STUDY

Major Field: Mathematics

Specialization: Graph Theory, Topology and Number Theory

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Graphs on surfaces have a wide range of applications in mathematics. In particular, the notion of a bipartite graph in which we have a cyclic ordering at each vertex proves surprisingly powerful. There is a well-known correspondence between these graphs and finite-index subgroups Γ of $\Gamma(2)$, which can be realized by considering how such groups act on the upper half-plane. The graphs are easy to describe and work with, even when the properties of the groups are not. One such property is that of congruence. Noncongruence subgroups of the modular group are of interest in number theory through the theory of modular forms and their connections with Galois representations. See for example the papers of Atkin and Swinnerton-Dyer [1], Li, Long, and Yang [6, 7] and Scholl [11]. While much is known about congruence subgroups, since one can describe them in terms of congruences on the entries, noncongruence subgroups are more mysterious. However, the correspondence between groups and graphs does not discriminate between congruence and noncongruence, so the graphs give a hands-on way to work with both. In this thesis we will try to understand as much as we can about noncongruence subgroups of $\Gamma(2)$ in terms of the associated graphs.

There are several existing tests and criteria for a subgroup to be congruence, such as those due to Hsu [5] and Larcher [9]. Using the correspondence between subgroups and graphs we reinterpret these criteria in terms of graphs in Chapter 3. Exploiting these criteria, and the fact that the graphs are easier to work with than the subgroups themselves, in Chapter 4 we construct examples of graphs corresponding to infinite families of noncongruence subgroups. We construct infinite families for every even level on a torus and we have families for (almost) every even level on a surface of genus 2.

In order to realize the noncongruence subgroups Γ coming from graphs more specifically as subgroups of $\Gamma(2)$, in Chapter 5 we develop a method to produce generators for Γ corresponding to a specific graph in terms of the standard generators for $\Gamma(2)$. To do so, we introduce the notion of a graph tiling for the associated surface. The graph tiling also allows us to give a method by which to determine if one group contains another, given the graph for the large group and generators for the smaller one in terms of the generators for $\Gamma(2)$, by determining if the corresponding graphs cover one another. Thus, given generators for $\Gamma(2n)$, we can determine if a graph corresponds to a congruence subgroup of level $2n$ by determining if the graph for $\Gamma(2n)$ covers the graph for Γ.

For this to be effective, we then need generators for the principal congruence subgroups $\Gamma(2n)$ in terms of the generators for $\Gamma(2)$. In Chapter 6 we give an algorithm which produces both the permutations and generators for the Hecke congruence groups $\Gamma_0(2p) \cap \Gamma(2)$ and $\Gamma_1(2p) \cap \Gamma(2)$ and the principal congruence group $\Gamma(2p)$, with p prime.

Many of the results were inspired by looking at countless examples, some of which are recorded in the Appendices. These include some of the graphs for the Hecke congruence groups.

CHAPTER 2

THE CORRESPONDENCE

In this chapter we will introduce some notation and terminology, some of which is standard in the literature, and others which are introduced for the purpose of this thesis. Section 2.1 will study certain subgroups of $PSL_2(\mathbb{Z})$ and their action on the upper half-plane. Section 2.2 will introduce equivalent ways to view the particular type of graph we are interested in. Section 2.3 will explain the established relationship between these objects.

2.1 Subgroups of $PSL_2(\mathbb{Z})$

We are working within the group $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\pm I$. When we use a matrix, it is always understood as an equivalence class in $PSL_2(\mathbb{Z})$.

Definition 2.1.1. The *principal congruence subgroup of level n* is the group

$$\Gamma(n) = \{\gamma \in PSL_2(\mathbb{Z}) \mid \gamma \equiv \pm I \pmod{n}\}.$$

We can also define some groups which contain $\Gamma(n)$:

$$\Gamma_0(n) = \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PSL_2(\mathbb{Z}) \middle| \, c \equiv 0 \pmod{n} \right\}$$

$$\Gamma_1(n) = \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(n) \middle| \, a \equiv d \equiv \pm 1 \pmod{n} \right\}$$

Similarly we can define $\Gamma^0(n)$ and $\Gamma^1(n)$ such that $b \equiv 0 \bmod n$, instead of $c \equiv 0 \bmod n$. These are examples of *congruence subgroups*: a subgroup $\Gamma \subset PSL_2(\mathbb{Z})$ is called *congruence* if it contains $\Gamma(n)$ for some n. For a congruence subgroup Γ, we define the *level* of Γ as the smallest n such that $\Gamma(n) \subset \Gamma$.

In fact we will be most concerned with finite-index subgroups of $\Gamma(2)$. $\Gamma(2)$ is freely generated by the elements $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$. Throughout this thesis, A and B will always stand for exactly those matrices.

We are working within $PSL_2(\mathbb{Z})$ instead of $SL_2(\mathbb{Z})$ because we are interested in these groups acting on the upper half-plane as linear-fractional transformations. Our preferred fundamental domain for $\Gamma(2)$, $\mathcal{D}$, is given in Figure 2.1. The dashed lines indicate that the arc from 0 to 1 and the arc from -1 to ∞ are not included, though in the future this won't be made explicit.

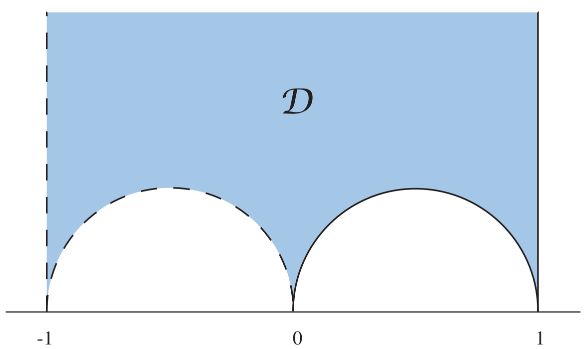

Figure 2.1: Fundamental domain for $\Gamma(2)$

Given a group $\Gamma \subset \Gamma(2)$ such that $[\Gamma(2) : \Gamma] = n < \infty$, we can find a fundamental domain for Γ consisting of n copies of the domain for $\Gamma(2)$. When we give such a domain we will usually show it as tiled by copies of $\mathcal{D}$, and label each tile by an element of $\Gamma(2)$ in terms of its generators A and B. When we are referring to a region in the upper half-plane instead of just a matrix, we will use the term *tile*. Thus, the *tile* A is the region of the upper half-plane consisting of the image of $\mathcal{D}$ under the matrix A. In general we can find the image of a matrix X by applying X to the elements of $\mathcal{D}$. Some sample tiles are labeled in Figure 2.2. Because we are now labeling the tiles with coset representatives, we will use I instead of $\mathcal{D}$ for the original domain of $\Gamma(2)$.

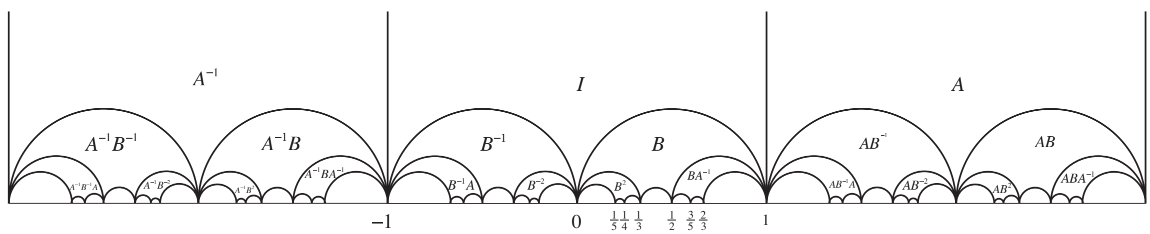

Figure 2.2: Images of $\mathcal{D}$ under some elements of $\Gamma(2)$

One of the challenges in viewing fundamental domains for groups of higher index is that the cusps become increasingly close together. To overcome this difficulty we will use the following approach: the $x-$values for the cusps will be shown equally spaced on the axis. This results in significant distortion of the regions, but the smallest regions are easier to see. Figure 2.3 shows the above tiles displayed in this manner.

The matrix $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ acts on $\mathcal{D}$ by translating to the right, which is equivalent to rotating counterclockwise about the cusp ∞. The matrix $B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ acts on $\mathcal{D}$ by rotating clockwise about the cusp 0. In general if we rotate clockwise about an image of 0, we find the adjacent tile by multiplying on the right by B. If we rotate counterclockwise about an image of ∞, we find the adjacent tile by multiplying on

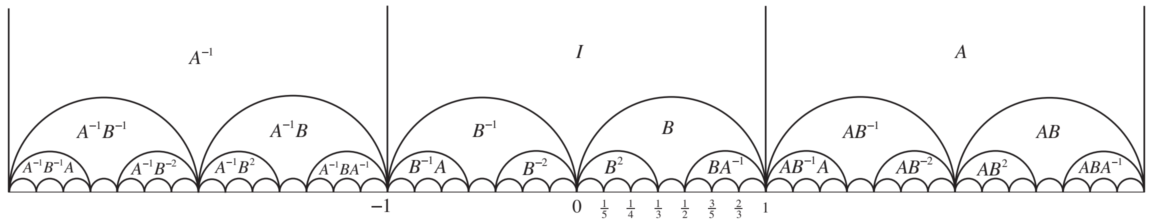

Figure 2.3: Images of $\mathcal{D}$ under some elements of $\Gamma(2)$, rescaled

the right by A. For example, consider the cusp at $-\frac{1}{2}$, which is the image of ∞ under the matrix B^{-1}. Rotating counterclockwise about $-\frac{1}{2}$, we pass from the tile B^{-1} to the tile $B^{-1}A$.

Example 2.1.2. Consider the group $\Gamma = \Gamma_0(6) \cap \Gamma(2)$.

Because $[\Gamma(2) : \Gamma] = 4$, we can form a fundamental domain for Γ from four copies of $\mathcal{D}$. (See the index formula in Lemma 6.1.1.) The matrices B, B^2 and BA^{-1} represent distinct cosets of Γ in $\Gamma(2)$. The tiles B and B^2 are found by rotating clockwise about the cusp at 0. Rotating clockwise about the cusp at $\frac{1}{2}$ we pass from the tile B to the tile BA^{-1}. This domain is pictured in Figure 2.4.

2.2 Graphs

We will be dealing with a special type of graph which can be described in several equivalent ways. Because these objects have a large variety of applications, these or their close relatives have been described (and named) in various ways in the literature. A few examples: One of the most notable is Grothendieck's term *dessins d'enfants*, or "children's drawings", which he introduced in his *Sketch of a Program*, [4]. Birch, in [2], referred to them as *drawings*. In Lando and Zvonkin's text [8] they are called *maps* (or *hypermaps* depending on the exact object used). Because these will be the

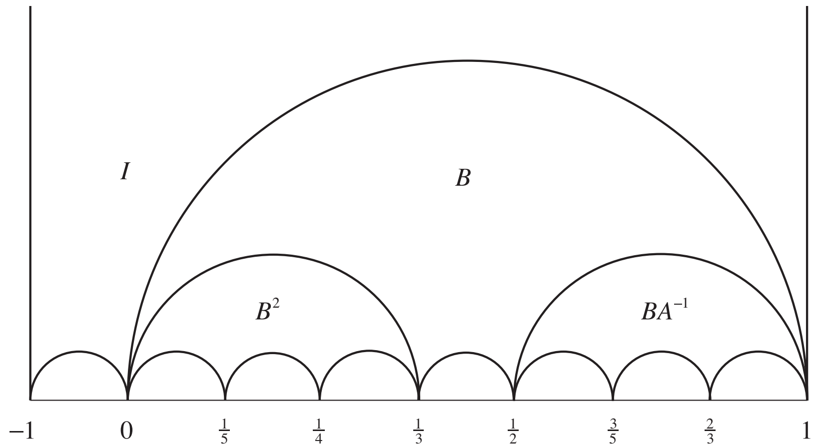

Figure 2.4: Fundamental domain for $\Gamma_0(6) \cap \Gamma(2)$

only type of graphs we are interested in, here they will be referred to simply (albeit imprecisely) as *graphs.* In this section we will examine these graphs and define other related terms.

Definition 2.2.1. A *graph* $\mathcal{G}$ will mean a connected bipartite graph G together with a cyclic ordering of the edges at each vertex.

Example 2.2.2. Let's consider two very basic examples, pictured in Figure 2.5.

Notice that if we were considering these as graphs in the usual way they would be equivalent: they each have five edges, one black vertex and three white vertices, all connected in the same pairs. However, we are also concerned with the cyclic ordering at each vertex. If we rotate counterclockwise about the black vertex and look down each edge, in graph (a) we see the white vertices in the order $W_2,\ W_2,\ W_1,\ W_1,\ W_3$; while in graph (b) the order is $W_2,\ W_1,\ W_2,\ W_1,\ W_3$. We will have a standard convention when labeling the edges: *from the viewpoint of a black vertex, the edge label will always lie on the left of the edge.*

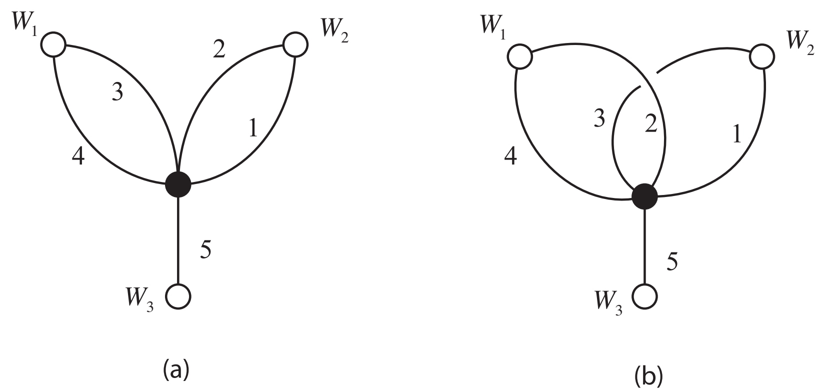

Figure 2.5: Two distinct graphs, each with five edges

Here is another way we can view the same objects. That these definitions are equivalent is a consequence of Theorem 2.3.1.

Definition 2.2.3. By the term *graph*, we mean a pair $\mathcal{G} = \{G, \Sigma\}$; where G is a connected bipartite graph on a compact orientable surface Σ, and such that the complement of the graph is a disjoint collection of 2-cells, called *faces*.

Thinking in these terms, we consider graph (a) to be on a sphere. Graph (b) cannot be placed on a sphere without changing the ordering of the edges. Instead, it can viewed on a torus; see Figure 2.6. While graph (b) can be embedded on a surface of higher genus, in doing so we would not satisfy the condition that the complement of the graph be a disjoint collection of 2-cells. At the end of this section we will discuss a way to calculate the appropriate genus of the surface for a given graph.

We refer to the *degree* of a vertex as the number of edges attached to it. For the faces we remember our convention of placing an edge label on the left side of an edge (from the viewpoint of a black vertex). We say a face *contains* an edge if the label for that edge is inside the face, and the *degree* of a face is the number of edges it

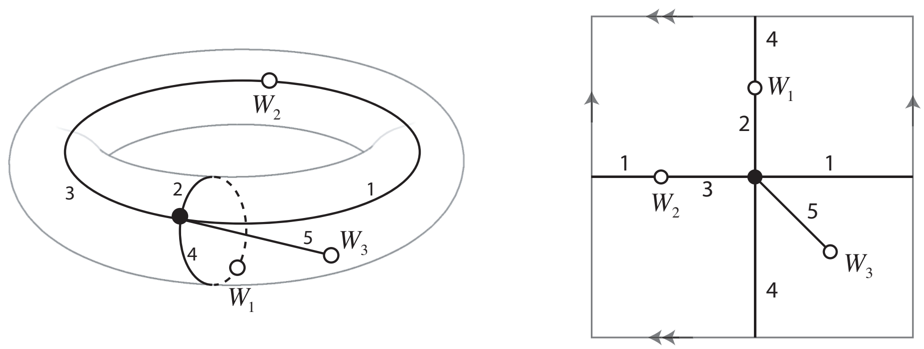

Figure 2.6: Graph (b) viewed on a torus

contains. We also have an ordering for each face: when standing at a face center, we rotate counterclockwise and record the edges.

In our examples, graph (a) has a black vertex of degree 5, two white vertices of degree 2, a white vertex of degree 1, two faces of degree 1, and a face of degree 3 with ordering 2, 5, 4. Compare this to graph (b): we see in Figure 2.6 that while the vertices have the same degrees as graph (a), there is only one face, which has degree 5 with ordering 1, 2, 3, 5, 4.

We can use these degrees to define another useful term. The *level* of a graph is twice the least common multiple of the degrees of all vertices and faces in the graph. Graph (a) has level $2 \cdot lcm(1, 2, 3, 5) = 60$, while graph (b) has level $2 \cdot lcm(1, 2, 5) = 20$. (This is related to the term *level* we defined in Section 2.1, as we will see in Section 3.2.)

For large graphs it isn't always practical to draw the pictures. Instead, it is enough to keep track of the vertices and the orderings of the edges at each. We can write these orderings as cycles in S_n where n the number of edges in the graph. This leads to another version of our definition, also equivalent because of Theorem 2.3.1.

Definition 2.2.4. By the term *graph*, we mean a pair of permutations in S_n: σ, in which each cycle corresponds to the cyclic ordering of the edges at a black vertex, and α, in which each cycle corresponds to the ordering of the edges at a white vertex. (Note that the trivial cycles of length 1 also correspond to vertices.) In order for the graph to be connected, we require that the group generated by σ and α be transitive on the n edges.

In graph (a), at the black vertex we see the permutation $(1, 2, 3, 4, 5)$, while the white vertices are represented by $(1, 2)(3, 4)(5)$. In graph (b) we have the same permutation for the black vertex, but the white vertices yield the permutation $(1, 3)(2, 4)(5)$.

If we have been careful with our conventions of where to label the edges and to rotate counterclockwise to read the cycles, we can notice this phenomenon: the product of the cycles for the black vertices and the white vertices will tell us about the faces of the graph. This is shown in Proposition 1.3.16 in [8]. For graph (a) we have the calculation

$$(1, 2, 3, 4, 5) \cdot (1, 2)(3, 4)(5) = (1)(2, 4, 5)(3); \tag{2.2.1}$$

for graph (b) we see

$$(1, 2, 3, 4, 5) \cdot (1, 3)(2, 4)(5) = (1, 4, 5, 3, 2). \tag{2.2.2}$$

Notice that these relate to the faces we found for each graph when drawn on its respective surface. If we choose a point in the center of each face, the inverse of each cycle corresponds to the edges we see rotating counterclockwise in that face. Thus, we can specify a graph by giving any two of the permutations for the black vertices, white vertices and faces.

In Figure 2.6 we showed graph (b) on a torus. In general each graph will properly embed on a surface of a particular genus. We can use the permutations associated to the vertices to find the genus of the surface for a given graph: we multiply the permutations for the vertices as above to find the permutation for the faces, and count the cycles to find the number of faces. Then we use the Euler characteristic to find the genus g of the surface,

$$\chi = V - E + F = 2 - 2g.$$

As an example we can find the genus of the surfaces for graphs (a) and (b) using only the calculations in 2.2.1 and 2.2.2. Graph (a) has four vertices, five edges and three faces, so $\chi = 4 - 5 + 3 = 2$, which agrees with our drawing on a sphere. Graph (b) has four vertices, five edges and one face, so $\chi = 4 - 5 + 1 = 0$, which justifies its belonging on a torus.

2.3 The Correspondence

Having introduced both finite-index subgroups of $\Gamma(2)$ and the graphs, we are now ready to understand the correspondence between them. This is found in many places in the literature; here we restate Theorem 1 from Birch [2].

Theorem 2.3.1 ([2]). *For each positive integer n, the following families of objects are in $1-1$ correspondence:*

1. *Triples $(\mathcal{R}, \phi, O)$ where $\mathcal{R}$ is an $n-$sheeted Riemann surface, $\phi : \mathcal{R} \to \overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ is a covering map branched at most above $\{\infty, 0, 1\}$, and O is a point of $\mathcal{R}$ above ∞.*

2. *Quadruples $(\beta, \sigma, \alpha; \star)$ where β, σ and α are permutations of S_n such that $\beta\sigma\alpha = id$ and such that the group generated by σ, α is transitive on the symbols permuted by S_n, and $\star$ is a marked cycle of β; all modulo equivalence corresponding to simultaneous conjugation by an element of S_n.*

3. *Subgroups $\Gamma \subset \Gamma(2)$ of index n, modulo conjugacy by translation.*

4. Drawings with n edges.

Item 2 corresponds with our Definition 2.2.4: given σ and α, we use the relation $\beta\sigma\alpha = id$ to compute the permutation β^{-1} of the faces. Then we mark one cycle (i.e., one face); marking a different face amounts to"simultaneous conjugation by an element of S_n". By "drawings" in item 4, he is referring to our Definition 2.2.1; thus this theorem verifies that these definitions are equivalent. In this section we will explore the relationship between these graphs and the groups in item 3. (Item 1 is of considerable interest, but we will not be venturing in this direction here.)

2.3.1 From a group to a graph

To understand the relationship between the finite-index subgroups of $\Gamma(2)$ and graphs we will look first at the domain $\mathcal{D}$ for $\Gamma(2)$ given in Figure 2.1. The arc from -1 to ∞ is identified with the arc from 1 to ∞ by the element $A \in \Gamma(2)$, while the arc from 0 to -1 is identified with the arc from 0 to 1 by the element $B \in \Gamma(2)$. When identified, we see a sphere with three points removed: the cusps at $1 = -1$, 0, and ∞. Next we will "fill the holes": at the cusp 0, we add a black vertex; we fill the cusp at 1 with a white vertex, and replace the cusp at infinity with a $*$ to represent a face center, so that we now have a sphere with three marked points. The arc from 0 to 1 will represent an edge; we use dashed lines between white vertices and corresponding face centers. In this way we can identify the group $\Gamma(2)$ with the graph on a sphere consisting of one black vertex, one white vertex, one edge, and one face. See Figure 2.7.

Now consider $\Gamma = \Gamma_0(6) \cap \Gamma(2)$, as in Example 2.1.2. We label 0 and its images under B, B^2, and BA^{-1} as black vertices; 1 and -1 and their images as white vertices, and ∞ and its images as face centers with a $*$. The images of the arc from 0 to 1 are now edges. We number the edges as shown in Figure 2.8.

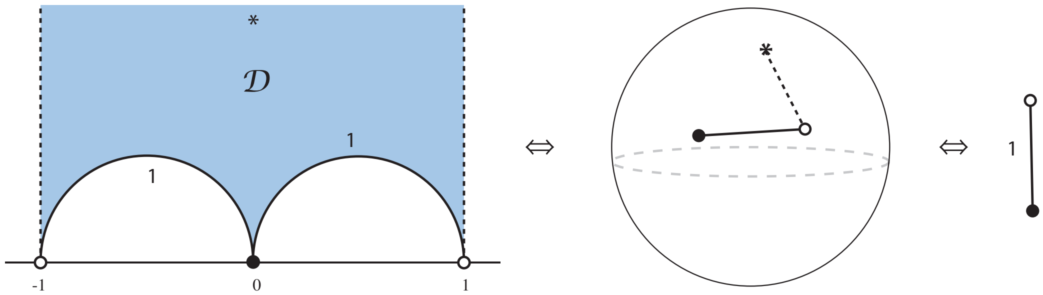

Figure 2.7: $\Gamma(2)$ as a graph

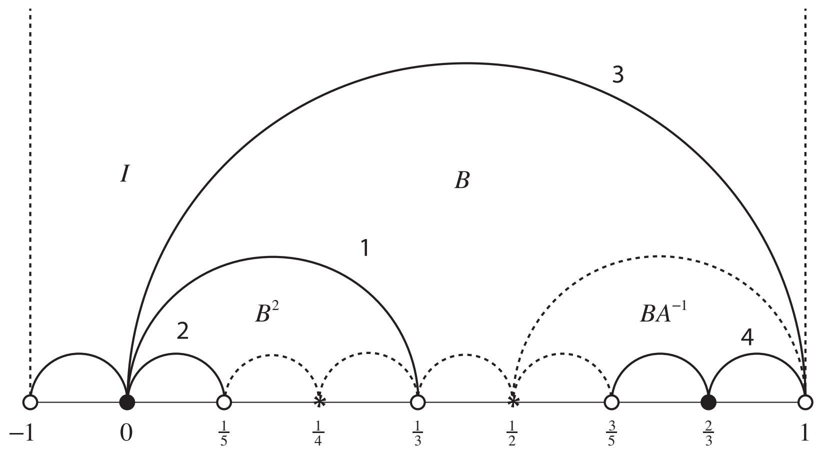

Figure 2.8: Domain for $\Gamma_0(6) \cap \Gamma(2)$, labeled as a graph

Notice that by numbering the edges, we have also numbered the tiles: we can associate edge 1 to the tile B, edge 2 to the tile B^2, edge 3 to the tile I, and edge 4 to the tile BA^{-1}.

At this point we have almost enough information to draw the corresponding graph. We need to be able to read the edge numbers as we rotate counterclockwise about each vertex. To do this we will need to find the side-pairing transformations that will turn our domain into a compact surface.

First consider the black vertex at 0. If we were to rotate counterclockwise, we would end up in the tile B^{-1}. We need to know which of our four tiles is equivalent to B^{-1} under an element of Γ. This amounts to finding a tile X so that there is a $g \in \Gamma$ with $gB^{-1} = X$. Among our choices this works for the tile B^2, because $gB^{-1} = B^2$ implies $g = B^3$, which is in Γ. As a result, we pair the edge from 0 to -1 with the edge from 0 to $\frac{1}{5}$. Now we can read the cycle for this vertex: the black vertex at 0 is associated with the cycle $(3, 2, 1)$.

Now consider the black vertex at $\frac{2}{3}$. Notice there is only one choice: on the boundary of our domain only one other arc represents an edge of the graph, so we plan to pair the arc from $\frac{2}{3}$ to 1 with the arc from $\frac{2}{3}$ to $\frac{3}{5}$. Let's verify that this is valid for Γ. Rotating counterclockwise about $\frac{2}{3}$ we find ourselves in the tile $BA^{-1}B^{-1}$. Then $gBA^{-1}B^{-1} = BA^{-1}$ implies $g = BA^{-1}BAB^{-1} = \begin{pmatrix} 13 & -8 \\ 18 & -11 \end{pmatrix}$, which is indeed in Γ. Thus the black vertex at $\frac{2}{3}$ is associated to the cycle (4).

Next we consider the face centers. Rotating counterclockwise about ∞ lands us in the tile A. This tile is equivalent to I under Γ, because $gI \cdot A = I$ implies $g = A^{-1}$, which is in Γ. This tells us to pair the two "vertical" edges of our domain. In rotating about ∞ we don't actually pass through an edge, but we remember that the edges are also labels for their corresponding tiles. Thus this face, of degree 1, is associated to the cycle (3).

For the face center at $\frac{1}{4}$, rotating counterclockwise from B^2 across the arc from $\frac{1}{4}$ to $\frac{1}{3}$ we arrive in the tile B^2A. We can see that B^2A is equivalent to BA^{-1} under Γ, because $gB^2A = BA^{-1}$ implies $g = BA^{-2}B^{-2} = \begin{pmatrix} 17 & -4 \\ 30 & -7 \end{pmatrix}$, which is in Γ. Thus we pair the arc from $\frac{1}{4}$ to $\frac{1}{3}$ with the arc from $\frac{1}{2}$ to $\frac{3}{5}$. Continuing in this manner, we pair the sides as shown in Figure 2.9. Because we have rotated through the tiles B^2, BA^{-1} and then B, the cycle associated to the resulting face is $(2, 4, 1)$.

Given the permutations we have found for the black vertices, $\sigma = (3, 2, 1)(4)$ and for the faces, $\beta = (1, 2, 4)(3)$, we can compute the permutation for the white vertices as a check. $\alpha = \sigma^{-1}\beta^{-1} = (1)(2,3,4)$. The diagram verifies that rotating counterclockwise about the white vertices according to the side-pairings, we see these cycles.

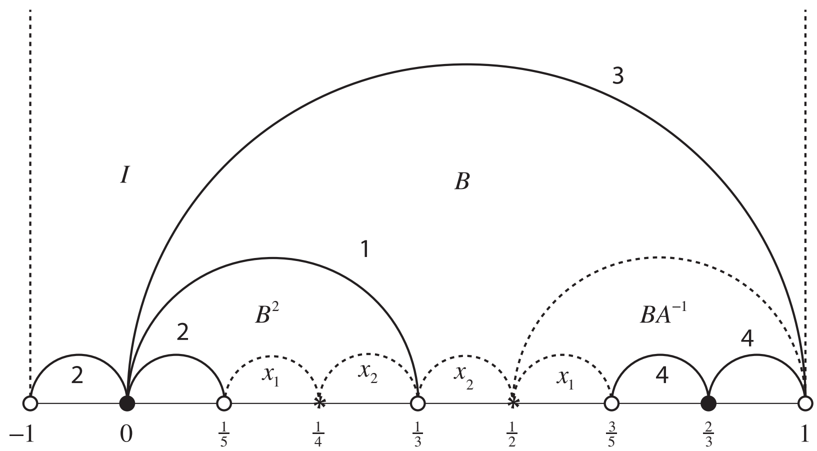

Figure 2.9: Domain for $\Gamma_0(6) \cap \Gamma(2)$ with side pairings

Now that we have the side-pairing transformations we can find the graph. We have two black vertices, two white vertices, two faces and four edges, so the Euler characteristic tells us the genus for this graph is 0 and the graph belongs on a sphere. Recall from Theorem 2.3.1 that we require a marked face $\star$ for our graph; by convention, we always mark the face which has its face center at the cusp ∞. (However, as our examples become more complicated, we will cease to indicate the marked face on the graph.) The graph is shown in Figure 2.10. In Section 6.2 we will find an algorithm to find the graphs for all $\Gamma_0(2p) \cap \Gamma(2)$.

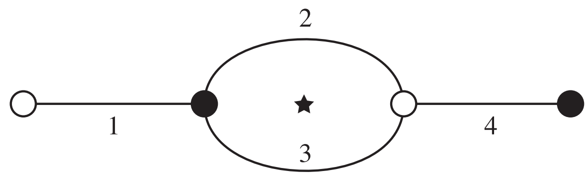

Figure 2.10: Graph associated to $\Gamma_0(6) \cap \Gamma(2)$

2.3.2 From a graph to a group

Next we will consider the other direction: given a graph, how do we find the corresponding subgroup of $\Gamma(2)$? First we must find a fundamental domain which corresponds to the graph, and then we find the side-pairing transformations, which generate the group. (See Ford [3], Theorem 19 in Section 28 or Theorem 10 in Section 32).

We first consider graph (b) of Example 2.2.2. It has five edges, so we need five copies of $\mathcal{D}$. This graph has only one face; we can choose ∞ to be its center. We rotate around ∞ by applying the matrix A, so we can use the tiles I, A, A^2, A^3 and A^4 as our domain. Rotating counterclockwise the cycle for the face is $(1, 2, 3, 5, 4)$; we number the edges in that order and identify the arc from -1 to ∞ with the arc from 9 to ∞. Now we proceed to use the cycle for the black vertex, $(1, 2, 3, 4, 5)$ to determine our edge pairings. For example, rotating counterclockwise about the cusp at 0 we go from edge 1 to edge 2, so we pair the arc from 0 to -1 with the arc from 2 to 3. See Figure 2.11. We can verify that with these pairings the cusps at 0, 2, 4 and 8 are all identified to form the black vertex in graph (b). We can also verify that rotating around the white vertices we see the cycles $(1, 3)(2, 4)(5)$.

The side-pairing transformations give us generators of the corresponding group Γ_b. We will have six generators: one for each edge, and also A^5, which identifies

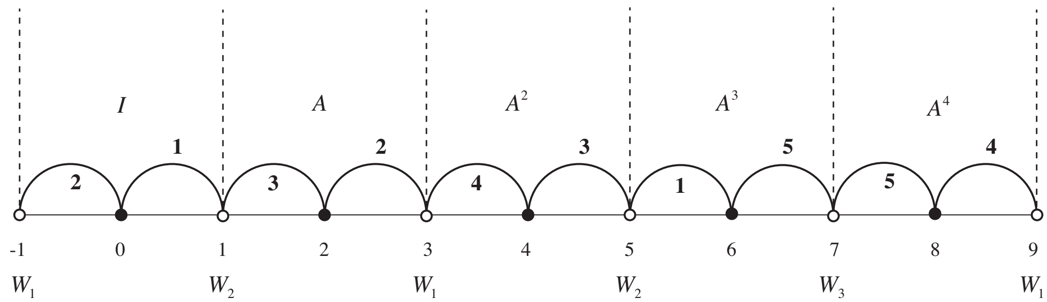

Figure 2.11: Domain for graph (b) from Example 2.2.2

the vertical arcs. For example, for edge 3, we rotate counterclockwise about the black vertex in A to arrive at A^2, so the generator g_3 satisfies $g_3 AB^{-1} = A^2$; thus $g_3 = A^2BA^{-1}$. Similarly we compute the others to get the group

$$\Gamma_b = \left\langle A^5,\ BA^{-3},\ AB,\ A^2BA^{-1},\ A^4BA^{-2},\ A^3BA^{-4} \right\rangle .$$

Let's do the same process for graph (a). We can choose the degree 3 face, $(2,5,4)$ to have its face center at ∞; we need three copies of $\mathcal{D}$ at ∞, so we can choose I, A and A^2 and label them as edges 2, 5, and 4 respectively. We identify the vertical arcs from -1 to ∞ and 5 to ∞, so the element A^3 is in the group Γ_a.

Now rotate counterclockwise about the black vertex at 0. The cycle for the black vertex is $(1,2,3,4,5)$, so rotating counterclockwise through edge 2 we need edge 3. Edge 3 doesn't yet appear in our domain, so we add the tile B^{-1} and label its edge as 3. After edge 3 we need edge 4, so we identify the arc from 0 to $\frac{1}{3}$ with the arc from 4 to 5, which appears in the tile A^2. Thus, the generator for edge 3 satisfies $g_3 B^{-1} \cdot B^{-1} = A^2$, so $g_3 = A^2B^2$. Next consider the cusp at 2: after edge 5 we need edge 1, which causes us to add the tile AB^{-1}. Finally we rotate through edge 1 to edge 2, so we identify the arc from 2 to $\frac{5}{3}$ with the arc from 0 to 2 to close the cycle.

Next consider the cusp at $-\frac{1}{2}$. The face with edge 3 has degree 1, so we will pair the arc from $-\frac{1}{2}$ to -1 with the arc from $-\frac{1}{2}$ to $-\frac{1}{3}$. The generator for this pairing satisfies $g_{x_1}B^{-1}A = B^{-1}$, so $g_{x_1} = B^{-1}A^{-1}B$. We continue to pair edges and solve for the corresponding generators to get the group

$$\Gamma_a = \langle A^3,\ B^2A^{-1},\ A^2B^2,\ ABA^{-2},\ B^{-1}A^{-1}B,\ AB^{-1}A^{-1}BA^{-1}\rangle$$

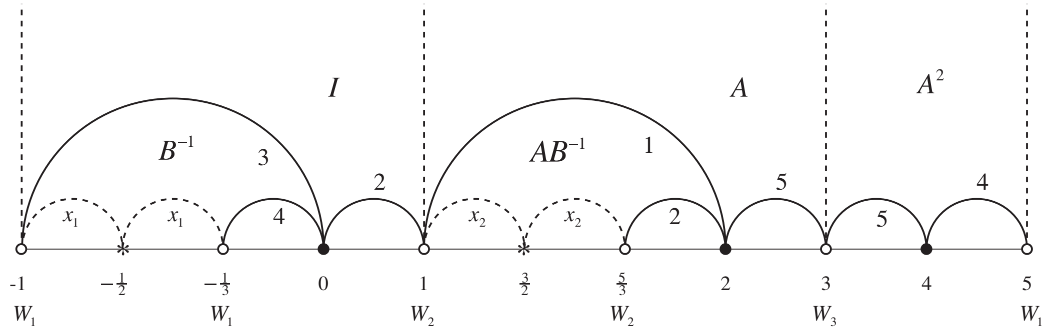

Figure 2.12: Domain for graph (a) from Example 2.2.2

The correspondence inspires the following terminology:

Definition 2.3.2. By a *(fundamental) domain of a graph*, we mean a connected fundamental domain of the corresponding group $\Gamma \subset \Gamma(2)$, tiled by copies of $\mathcal{D}$, and with the images of the arc from 0 to 1 labeled according to the edges of the graph. We label the images of 0 as black vertices, the images of 1 and -1 as white vertices, and images of ∞ as $*$ to represent a face center; when identified these form the black vertices, white vertices and face centers of the given graph.

Using this terminology, Figure 2.12 is a domain for graph (a), and Figure 2.11 is a domain for graph (b).

CHAPTER 3

TESTING FOR CONGRUENCE

Recall from Section 2.1 that a group $\Gamma \subset PSL_2(\mathbb{Z})$ is *congruence* if it contains $\Gamma(n)$ for some n. There are many existing tests for whether a given finite-index subgroup is congruence. In this section we want to explore ways to implement such tests for subgroups of $\Gamma(2)$ by looking at their graphs. For example, Tim Hsu in [5] has an algorithm to determine whether a group $\Gamma \subset PSL_2(\mathbb{Z})$ is congruence by using graphs similar to the ones we have developed; in Section 3.1 we will discuss how to convert the graphs we are using into ones for which his algorithm applies. In Section 3.2 we will look at a theorem of Wohlfahrt which will reconcile our definitions of the level of a group, and interpret his theorem in terms of our graphs. In Section 3.3 we will examine some criteria for congruence proven by Larcher [9], and discuss how they can be applied to our graphs.

3.1 Drawings for subgroups of $PSL_2(\mathbb{Z})$

The idea of looking at subgroups of $PSL_2(\mathbb{Z})$ in terms of drawings is not new. However, for the most part these versions of drawings differ from the graphs we have used. This arises from the fact that others are looking at subgroups of $\Gamma(1) = PSL_2(\mathbb{Z})$ which are not necessarily in $\Gamma(2)$.

In Figure 2.7 we showed how $\mathcal{D}$, the fundamental domain of $\Gamma(2)$, can be interpreted as a graph: the arc from 0 to 1 represents an edge, and the cusps at 0, 1 and ∞ represent a black vertex, white vertex, and face center, respectively. For subgroups of $\Gamma(2)$, the domains consisting of n copies of $\mathcal{D}$ correspond to graphs with n edges.

The fundamental domain $\mathcal{F}$ for $\Gamma(1)$ is pictured in Figure 3.1. The vertical arcs are identified under the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. The arc from i to $\rho = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ is identified with the arc from i to $-\bar{\rho}$ by the matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

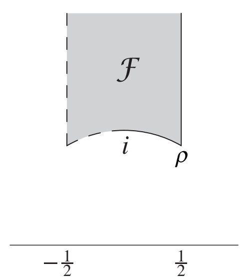

Figure 3.1: Fundamental domain for $PSL_2(\mathbb{Z})$

Unlike our domain for $\Gamma(2)$, the domain $\mathcal{F}$ has only one cusp (at ∞). It also has two *marked points*, that at i, which has an order 2 stabilizer in $PSL_2(\mathbb{Z})$, and ρ, whose stabilizer in $PSL_2(\mathbb{Z})$ has order 3. The natural way to associate a graph to this group is to mark the point ρ with a black vertex, i with a white vertex, and continue to mark the cusp ∞ with a $*$ to represent a face center. The graph associated to $\Gamma(1)$ itself is a single edge; see Figure 3.2.

Now consider the domain $\mathcal{D}$ we introduced for $\Gamma(2)$. Since $[\Gamma(1) : \Gamma(2)] = 6$ we can tile $\mathcal{D}$ with six copies of $\mathcal{F}$ (see Figure 3.3). In doing so we find a new way to draw a graph for $\Gamma(2)$: we lift the graph for $\Gamma(1)$ to the tiling of the fundamental domain

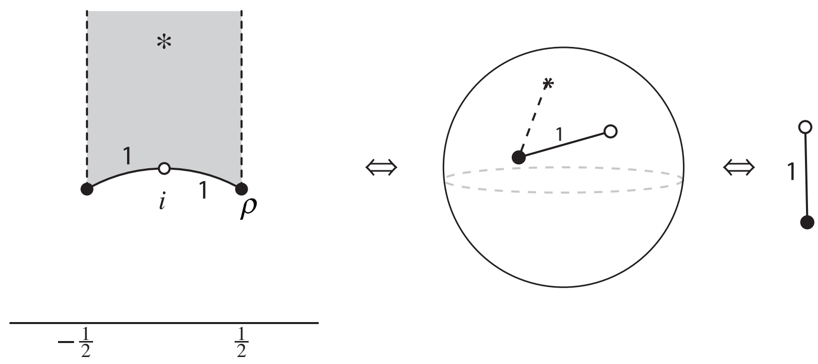

Figure 3.2: Fundamental domain for $PSL_2(\mathbb{Z})$ as a graph

for $\Gamma(2)$ by copies of $\mathcal{F}$, as shown in Figure 3.4. In general, for a group $\Gamma \subset \Gamma(2)$ of index n we have two distinct graphs: the type we obtained in Section 2.3 by tiling its domain with n copies of $\mathcal{D}$ and lifting the graph for $\Gamma(2)$ in Figure 2.7, and another by tiling its domain with $6n$ copies of $\mathcal{F}$ and lifting the graph for $\Gamma(1)$ in Figure 3.2. For this section we will distinguish these by referring to the $\Gamma(1)$-*graph* and the $\Gamma(2)$-*graph*, respectively, associated to group Γ. Notice that in the $\Gamma(1)$-graph the black vertices all have degree either 1 or 3, and the white vertices will have degree 1 or 2.

By computing a few examples one can begin to find the pattern in converting from a $\Gamma(2)$-graph to a $\Gamma(1)$-graph. In the domains for the graphs for $\Gamma(2)$ the vertices and face centers are all labeled at cusps. When tiled by copies of $\mathcal{F}$ these cusps are all images of ∞; thus when converting, every black vertex, white vertex and face center will appear as the center of a face on the new graph. As a way to get started, we can notice in Figure 3.4 that the original $\Gamma(2)$ edge, i.e., the arc from 0 to 1, now has a white vertex in its center which is connected to two black vertices; so for each edge in our $\Gamma(2)$-graph we can add a white vertex on top of it and two black vertices to the sides.

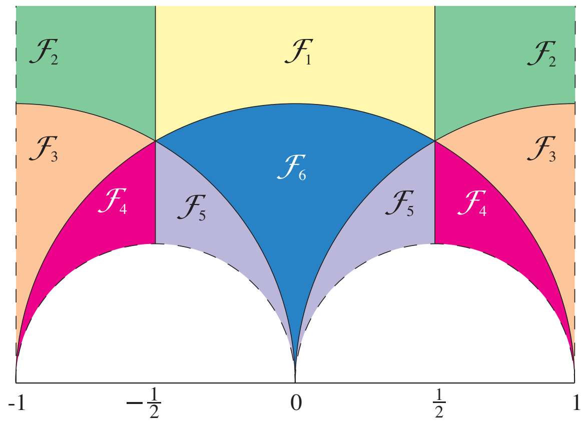

Figure 3.3: Fundamental domain for $\Gamma(2)$ tiled by the domain for $PSL_2(\mathbb{Z})$

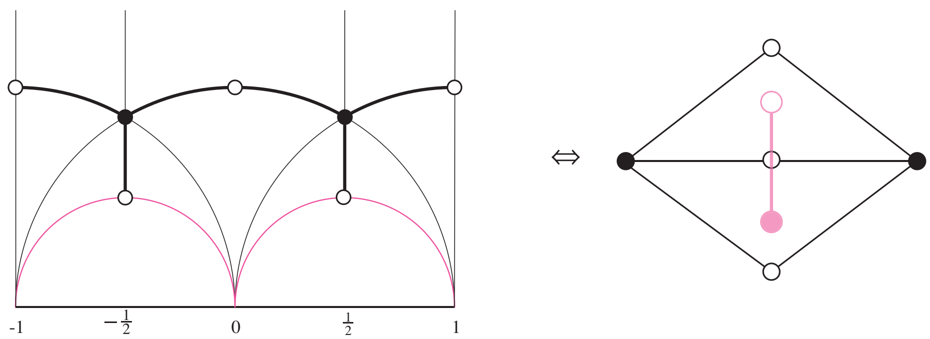

Figure 3.4: Drawing for $\Gamma(2)$ as a subgroup of $PSL_2(\mathbb{Z})$

As an example we consider the 3-star, a black vertex connected to three white vertices, considered as a $\Gamma(2)$-graph. In Figure 3.5 we see a domain for this graph tiled first by copies of $\Gamma(2)$ and then by copies of $\Gamma(1)$. When we identify sides to find the corresponding $\Gamma(1)$-graph, we discover the relationship in Figure 3.6. In Figure 3.7 we have another example of a $\Gamma(2)$-graph converted to its $\Gamma(1)$ counterpart.

Recall that in Definition 2.2.4 we had another way to specify a $\Gamma(2)$-graph: we could list a permutation σ in which the cycles correspond to the black vertices and a

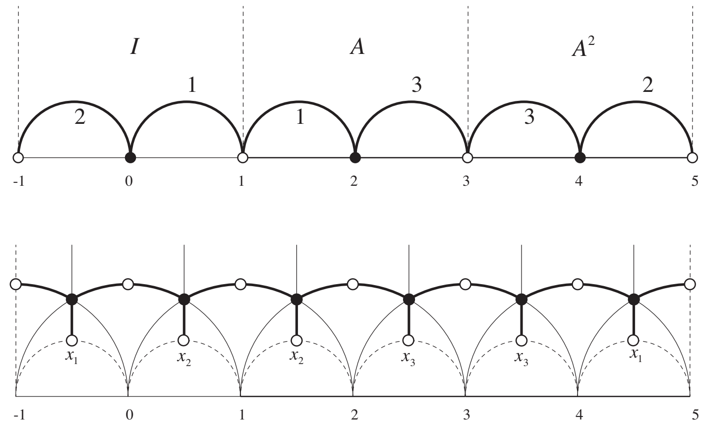

Figure 3.5: Domain for the 3-star, tiled first by $\mathcal{D}$ and then by $\mathcal{F}$

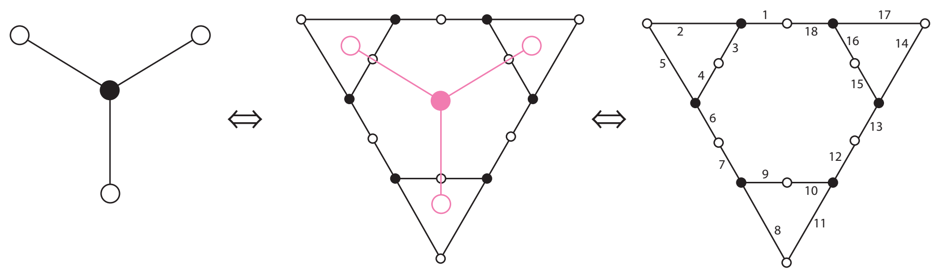

Figure 3.6: Converting the 3-star from a $\Gamma(2)$-graph to a $\Gamma(1)$-graph

permutation α in which the cycles correspond to the white vertices. The permutation $\beta = \alpha^{-1}\sigma^{-1}$ then gives a permutation in which the cycles correspond to the faces. We can do the same for the $\Gamma(1)$-graphs. For example, for the 3-star, the permutations as a $\Gamma(2)$ graph are $\sigma = (1, 2, 3)$, $\alpha = (1)(2)(3)$ and $\beta = (1, 3, 2)$. As a $\Gamma(1)$-graph we can refer to Figure 3.6 to obtain the following:

$$\sigma_1 = (1, 2, 3)(4, 5, 6)(7, 8, 9)(10, 11, 12)(13, 14, 15)(16, 17, 18)$$

$$\alpha_1 = (1, 18)(2, 5)(3, 4)(6, 7)(8, 11)(9, 10)(12, 13)(14, 17)(15, 16)$$

$$\beta_1 = (1, 17, 13, 11, 7, 5)(3, 6, 9, 12, 15, 18)(2, 4)(8, 10)(14, 16)$$

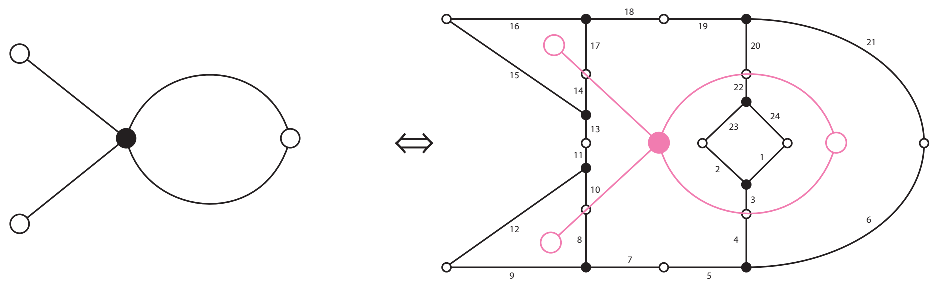

Figure 3.7: A fish in $\Gamma(2)$ becomes a spaceship in $\Gamma(1)$.

Notice that the order of σ_1 is 3; in a $\Gamma(1)$-graph all black vertices will have order either 1 or 3. The order of α_1 is 2, which agrees with the degrees of the white vertices. The cycle structure of β_1 tells us about the cycle structures of all of the vertices and faces for the $\Gamma(2)$-graph. In the above example, the first cycle of β_1 corresponds to the outside face of the 3-star; the second cycle of β_1 corresponds to the face of the $\Gamma(1)$-graph which contains the black vertex of the 3-star, and the last three cycles correspond to the faces of the $\Gamma(1)$-graph which contain the white vertices of the 3-star.

The advantage to converting our $\Gamma(2)$-graphs to their $\Gamma(1)$ versions is that there are many results available for subgroups of $PSL_2(\mathbb{Z})$. One example of such a result is an algorithm developed by Hsu to determine whether a group $\Gamma \subset PSL_2(\mathbb{Z})$ is congruence in terms of these permutations; see [5]. He specifies such a Γ by giving permutations σ_1 and α_1 as above, and his algorithm amounts to checking a list of relations. Thus, if we consider one of our $\Gamma(2)$-graphs, we can determine if the corresponding subgroup of $\Gamma(2)$ is congruence by first converting it to a $\Gamma(1)$-graph and then applying Hsu's algorithm. For example, in applying this algorithm it turns out that the group Γ which corresponds to the 3-star is noncongruence. One of the relations that fails amounts to checking that the cycle $\left(\beta_1^4(\alpha_1\sigma_1)^{-4}\beta_1^4\right)^4 \neq 1$.

In summary, it is true that every finite-index subgroup of $PSL_2(\mathbb{Z})$ can be viewed as a graph. In doing so, we only get restricted types of graphs due to the degree restrictions for the black and white vertices in these $\Gamma(1)$-graphs, but we can then apply known results for subgroups of $\Gamma(1)$ to these graphs.

However, there are advantages to working with our versions of the graphs even though they apply only to subgroups of $\Gamma(2)$. Firstly, the $\Gamma(2)$-graphs have six times fewer edges than their $\Gamma(1)$ counterparts, which simplifies computing and allows us to draw graphs for higher-index subgroups. Secondly, we are less restricted on which graphs can occur; in fact by parts 3 and 4 of Birch's Theorem 2.3.1 we can get any graph as a $\Gamma(2)$-graph, with no restrictions on the black and white vertices. We will see in Chapter 4 that this flexibility can allow us to find some interesting examples.

3.2 Wohlfahrt's Theorem

On page 9 we defined the level of a graph as twice the least common multiple of the degrees of all vertices and faces, while on page 4 we defined the level of a congruence subgroup $\Gamma \subset \Gamma(2)$ as the smallest n such that $\Gamma(n) \subset \Gamma$. In fact, due to a result of Wohlfahrt, for a congruence subgroup these definitions agree.

In [12], Wohlfahrt defines the level of a finite-index subgroup $\Gamma \subset \Gamma(1)$ as the least common multiple of the cusp widths (or amplitudes) for Γ. For the group $\Gamma(2)$ the cusp width of ∞ is 2, which is the width of its fundamental domain at ∞; the degree of the face in the graph for $\Gamma(2)$ is 1. In the graph for a group $\Gamma \subset \Gamma(2)$, a vertex or face of degree d will touch d copies of the domain for $\Gamma(2)$, and thus have cusp width $2d$. The least common multiple of the cusp widths is the least common multiple of twice each degree, and thus twice the least common multiple of the degrees.

Wohlfahrt then proves that for a group Γ of level n in his sense, Γ is congruence if and only if Γ contains $\Gamma(n)$, and so for congruence subgroups the two definitions agree. Thus, in order to check if a group of level n is congruence, we need check only whether it contains $\Gamma(n)$ for this particular value of n.

3.3 Interpreting some results of Larcher

In [9], Larcher proves some results about the cusp widths of congruence subgroups $\Gamma \subset PSL_2(\mathbb{Z})$. In this section we will restate two of these results in terms of our graphs for finite-index subgroups of $\Gamma(2)$.

Theorem 3.3.1 ([9])**.** *If Γ is a congruence subgroup of level m and d and e are the respective widths of ∞ and 0 in Γ then $de \equiv 0 \pmod{m}$.*

Recall that in Section 3.2 we saw that a vertex or face of degree d has cusp width $2d$. Thus, we can restate the theorem as follows:

Corollary 3.3.2 (Theorem 3.3.1, restated)**.** *Let $\Gamma \subset \Gamma(2)$ be a congruence subgroup of level $2n$. In the corresponding graph, let d and e be the respective degrees of the face corresponding to ∞ and the black vertex corresponding to 0. Then $(2d)(2e) \equiv 0 \pmod{2n}$, and thus $2de \equiv 0 \pmod{n}$.*

In Section 5.1 we will use graph coverings to generalize the above theorem; in fact the result holds for any face with any of its vertices.

Another powerful criteria for congruence:

Theorem 3.3.3 ([9])**.** *If Γ is a congruence subgroup of level m then Γ contains a cusp of width m.*

When interpreted for graphs the statement reads as follows:

Corollary 3.3.4 (Theorem 3.3.3, restated)**.** *If $\Gamma \subset \Gamma(2)$ is a congruence subgroup of level $2n$, then the graph corresponding to Γ has either a vertex or a face of degree n.*

These criteria provide necessary conditions for congruence. Consider the example in Figure 3.7: The fish has vertices of degrees 1, 2, and 4 and faces of degree 1 and 3, and thus the level of this graph is $2 \cdot lcm(1, 2, 3, 4) = 24$. Because the graph does not contain a vertex or face of degree 12, we immediately conclude that the corresponding group is noncongruence. By contrast, if we were to apply Hsu's algorithm as in the above section, we would need to work with the $\Gamma(1)$ version of the graph (the spaceship). This graph has permutations in S_{24} and the computations are lengthy by comparison.

However, the conditions are not sufficient: notice that while Hsu's algorithm showed us that the 3-star corresponds to a noncongruence subgroup, the graph does not violate Larcher's criteria above. We will have a an algorithm to determine congruence that depends only on graphs in Section 5.4.

CHAPTER 4

NONCONGRUENCE EXAMPLES

In this chapter we will construct infinite families of examples of noncongruence subgroups of $\Gamma(2)$ for every even level. Producing congruence subgroups of a given level is generally more approachable, because a congruence subgroup Γ of level $2n$ corresponds to a subgroup of $\Gamma(2n)\backslash\Gamma(2)$, which is a finite matrix group. For example, we have $\Gamma_0(2n)$ and $\Gamma_1(2n)$, as defined in Section 2.1.

Noncongruence subgroups are more difficult to work with because they are defined by what they are not: they do not contain $\Gamma(n)$ for any n. However, the correspondence between subgroups and graphs does not distinguish between congruence and noncongruence; we can construct a group simply by drawing a bipartite graph on a surface. The flexibility and concreteness of this approach will allow us to visually and immediately determine noncongruence for the majority of the examples.

The main strategy in their construction involves applying the criteria stated in Corollary 3.3.4: If Γ is a congruence subgroup of level $2n$, the corresponding graph has either a face or vertex of degree n. In other words, to produce a noncongruence subgroup of level $2n$ it suffices to find a graph in which the least common multiple of the degrees of the vertices and faces is n, but no particular vertex or face has degree n.

In Section 5.3 we will have a method to find generators for the group corresponding to a given graph, so these groups can be realized as subgroups of $\Gamma(2)$ specified by a finite set of generators.

4.1 Examples on a torus

In this section we will find infinite families of subgroups of level $2p_1^{n_1}p_2^{n_2}\dots p_k^{n_k}$, for the p_i distinct primes.

Example 4.1.1. Level $2p^n$, $p \neq 2$: The Waving Onion.

Let p be an odd prime. We begin with one black vertex and one white vertex, each of degree p^n. We will connect them in such a way that each face has degree 1 or degree p^n, each vertex we add has degree 1, and that the complement of the graph on the torus is a collection of 2-cells. An example of such a graph is shown in Figure 4.1. Notice that the right-most black vertex has degree p^n: it has edges connecting it

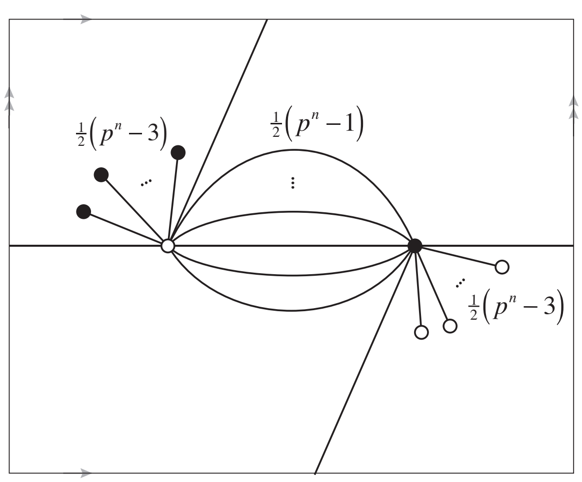

Figure 4.1: Noncongruence Subgroup of level $2p^n$, $p \neq 2$, $n > 1$

to $\frac{1}{2}(p^n - 3)$ white vertices of degree 1, and $2 + \frac{1}{2}(p^n - 1)$ edges connecting it to the degree p^n white vertex. The left-most white vertex has the same count. The outside face has degree p^n as well; it has $2 \cdot \frac{1}{2}(p^n - 3)$ edges connected to degree 1 vertices, and three edges between the black and white vertices of degree p^n. (Recall that we label an edge on the left side from the viewpoint of a black vertex, and we declare an edge to be "in a face" if its label is in that face.) All other vertices and faces have degree 1, so the least common multiple of the degrees is p^n, which confirms the graph is level $2p^n$. In all the graph has $p^n - 1$ vertices, $\frac{1}{2}(p^n - 1)$ faces, and $\frac{3}{2}(p^n - 1)$ edges; this confirms the Euler characteristic is 0, so the graph lies on a torus. This graph represents a noncongruence subgroup for $n > 1$; the proof of this is delayed until the end of the section. For now we need this as a building block for the other examples.

Notice that this process does not work for the case $p = 2$; the number of degree 1 faces is $\frac{1}{2}(p^n - 1)$, which is not an integer if $p = 2$. We address this case in the next example.

Example 4.1.2. Level 2^n: The Tree Frog.

To handle this case we can form the graph in Figure 4.2. A count reveals that the outside face has degree 2^{n-1}, as do the left-most white vertex and right-most black vertex. The "eyes" of the tree frog are vertices of degree 2, which do not change the least common multiple of the degrees and thus do not change the level. This graph has 2^{n-1} vertices, $3 \cdot 2^{n-2}$ edges and 2^{n-2} faces, so the Euler characteristic confirms that the graph belongs on a torus. This graph provides noncongruence subgroups for $n > 1$; the proof is again delayed until the end of the section.

In fact the above cases are the only ones in this section not immediately proven noncongruence by Corollary 3.3.4, but they will form the building blocks for what follows.

Example 4.1.3. Level $2p^nq^m$, for $p \neq q$ and $p, q \neq 2$.

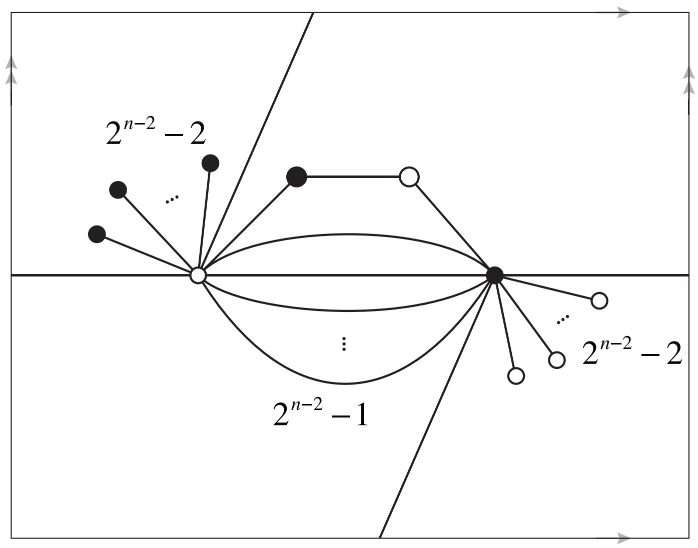

Figure 4.2: Noncongruence "tree frog" of level 2^n, $n > 1$

In Figure 4.3 we consider the case of level $2p^nq^m$, for p and q distinct odd primes. We can think of this as a tiling of two copies of Example 4.1.1. The middle strip has the same count of vertices and faces as our example for level $2p^n$; the top (and bottom) strip mimic the same example for level $2q^m$. Now the least common multiple of the degrees is p^nq^m, so the level is $2p^nq^m$. A count of vertices, edges and faces will confirm this graph lies on a torus. In this case we can immediately conclude that the corresponding subgroup is noncongruence using Corollary 3.3.4: the level is $2p^nq^m$, but there is no vertex or face with degree p^nq^m.

Example 4.1.4. Level $2p_1^{n_1}p_2^{n_2}\dots p_k^{n_k}$.

The previous example provides the structure for an arbitrary number of primes: we can produce a graph of level $2p_1^{n_1}p_2^{n_2}\dots p_k^{n_k}$, with $p_i \neq 2$, as in Figure 4.4. As in the above example, they will be noncongruence because of Corollary 3.3.4.

Notice that we can also produce an infinite family of graphs for each level: we can repeat the strips for any of the prime factors without changing the least common

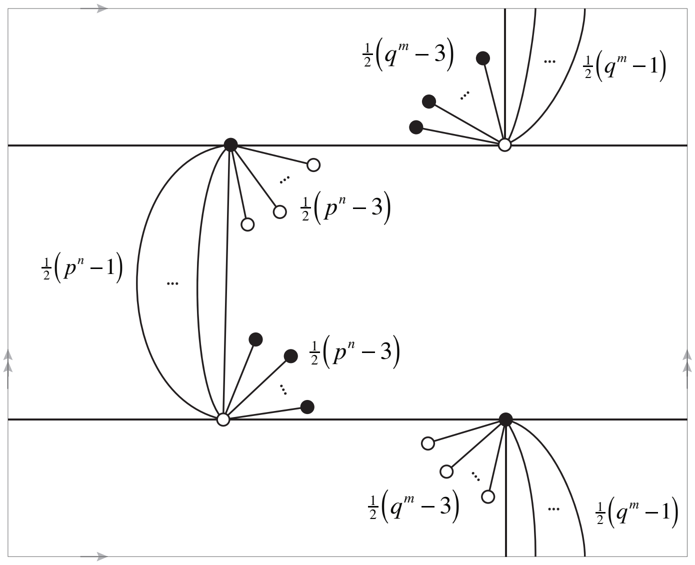

Figure 4.3: Noncongruence Subgroup of level $2p^nq^m$

multiple of the degrees, and thus without changing the level. If one of the $p_i = 2$, we can use the alternate strip shown in Figure 4.5, which is based on the "tree frog" in Example 4.1.2. This also allows us to produce noncongruence subgroups for level $2p^n$ with $n = 1$; we can repeat enough strips using the prime p so that the total number of edges in the graph exceeds the index of $\Gamma(2p)$ in $\Gamma(2)$. (In Example 4.1, the case $n = 1$ is the only case for which we are not guaranteed the corresponding group is congruence.)

Now we return to our "building blocks" in Examples 4.1.1 and 4.1.2 to show that they too represent noncongruence subgroups.

Proposition 4.1.5. *The graph shown in Figure 4.1 represents a noncongruence subgroup* Γ *of level* $2p^n$ *for* $n > 1$.

Proof. Suppose for contradiction that Γ represents a congruence subgroup. We have

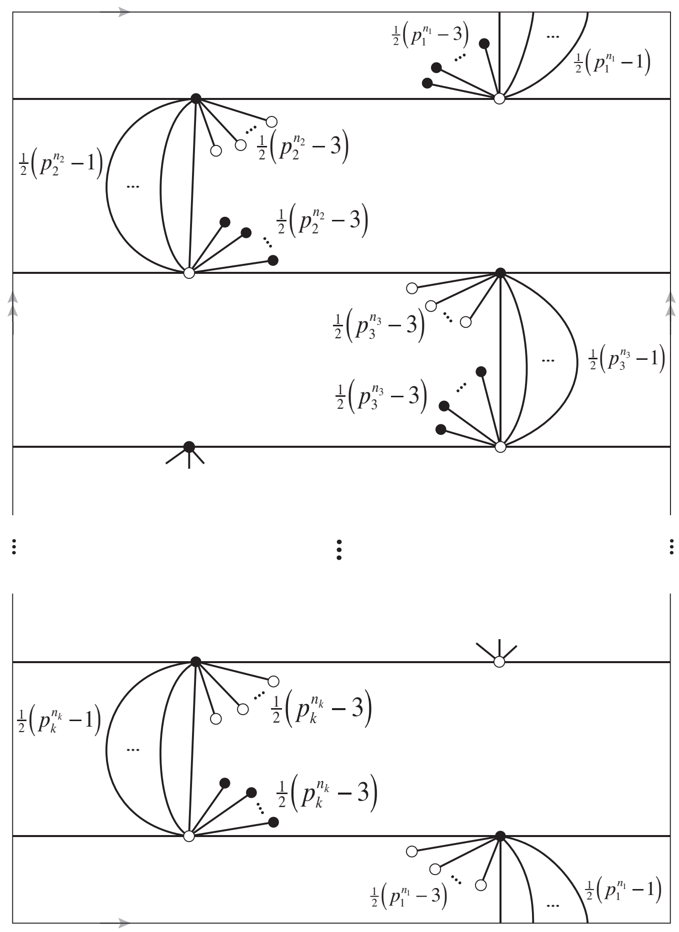

Figure 4.4: Noncongruence Subgroup of level $2p_1^{n_1}p_2^{n_2}\dots p_k^{n_k}$, $p_i \neq 2$

shown the graph to have level $2p^n$, so $\Gamma(2p^n) \subset \Gamma$, and we have

$$[\Gamma(2) : \Gamma(2p^n)] = [\Gamma(2) : \Gamma] \cdot [\Gamma : \Gamma(2p^n)].$$

This graph has $\frac{3}{2}(p^n - 1)$ edges, so $[\Gamma(2) : \Gamma] = \frac{3}{2}(p^n - 1)$. We can apply the index formula 6.1.1 to find that $[\Gamma(2) : \Gamma(2p^n)] = \frac{1}{2}p^{3n-2}(p^2 - 1)$. Division yields

$$[\Gamma : \Gamma(2p^n)] = \frac{p^{3n-2}(p^2 - 1)}{3(p^n - 1)}.$$

Case 1: Let $n > 2$. Notice that $(p^n - 1)$ is relatively prime to p, and so if this fraction

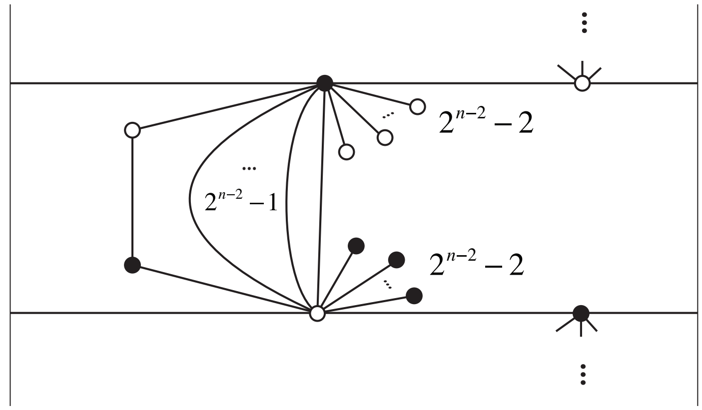

Figure 4.5: Tree frog strip for the case $p_i^n = 2^n$

is an integer, we have $(p^n - 1)$ dividing $(p^2 - 1)$. But since $n > 2$, we have $p^n - 1 > p^2 - 1$, which gives a contradiction.

Case 2: Let $n = 2$, and $p \neq 3$. The fraction becomes $\frac{1}{3}p^4$, and since $p \neq 3$, it is not an integer; again, we have a contradiction.

Case 3: Let $n = 2$ and $p = 3$. The resulting graph of level 18 can be checked using Tim Hsu's algorithm in [5]; it also represents a noncongruence subgroup.

$\square$

Proposition 4.1.6. *The graph shown in Figure 4.2 represents a noncongruence subgroup Γ of level 2^n for $n > 1$.*

Proof. Assume for contradiction that Γ is congruence of level 2^n. As above, we will consider the indices. The graph has $3 \cdot 2^{n-2}$ edges. The index formula 6.1.1 yields $[\Gamma(2) : \Gamma(2^n)] = 2^{3n-4}$. Thus division yields

$$[\Gamma : \Gamma(2^n)] = \frac{2^{3n-4}}{3 \cdot 2^{n-2}}.$$

This fraction is not an integer, so we arrive at a contradiction. $\square$

Notice that the argument for Proposition 4.1.5 does not apply for the case $n = 1$. In fact for the case $n = 1$ and $p = 3$, the graph represents a congruence subgroup of level 6. For $n = 1$ and $p = 5$, the graph as drawn corresponds to the (congruence) subgroup $\Gamma_0(10) \cap \Gamma(2)$. However, with only a small change we can produce a noncongruence subgroup: see Figure 4.6. The graph on the left corresponds to $\Gamma_0(10) \cap \Gamma(2)$,

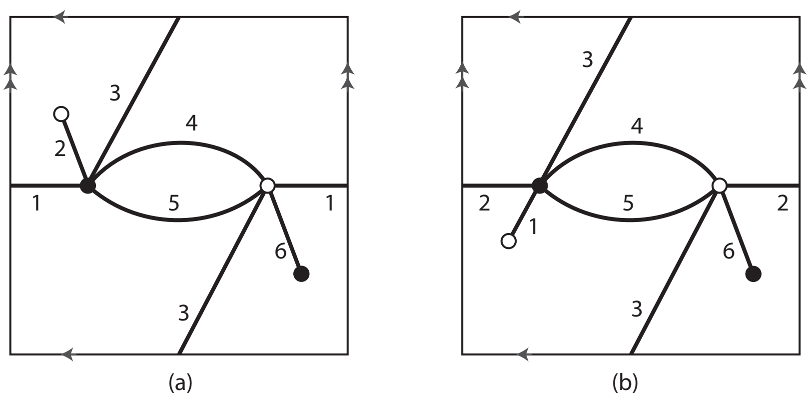

Figure 4.6: Two graphs of level 10

but the graph on the right represents a noncongruence subgroup of level 10. This can be shown using Tim Hsu's algorithm, or using the procedure described in Section 5.4. At first glance these graphs are remarkably similar; we see how delicate it can be to determine whether or not a graph corresponds to a congruence subgroup. (The fundamental domain for $\Gamma_0(10) \cap \Gamma(2)$ appears in Figure B.3 on page 99.)

4.2 Examples on a Genus 2 Surface

In this section we will see graphs on a genus 2 surface of level $2n$ for $n \geq 4$. (In fact it is not possible to have a graph of level 4 or 6 on a genus 2 surface; this will be shown at the end of the section in Proposition 4.2.8.) The examples are not as general: we have families of examples of every allowable even level, but they are not infinite families.

The constructions follow a similar pattern to those on the torus: we look first at "building blocks": graphs of level $2p^n$ and 2^n. We then construct a graph of level $2p^n q^m$ which is noncongruence by Corollary 3.3.4; and then graphs for noncongruence groups of arbitrary even level. All graphs are drawn on an octagon with opposite sides identified to create a genus 2 surface.

Example 4.2.1. Level $2p^n$, with p an odd prime such that $p^n \geq 5$.

We can construct a graph similar to that in Example 4.1.1. The graph in Figure

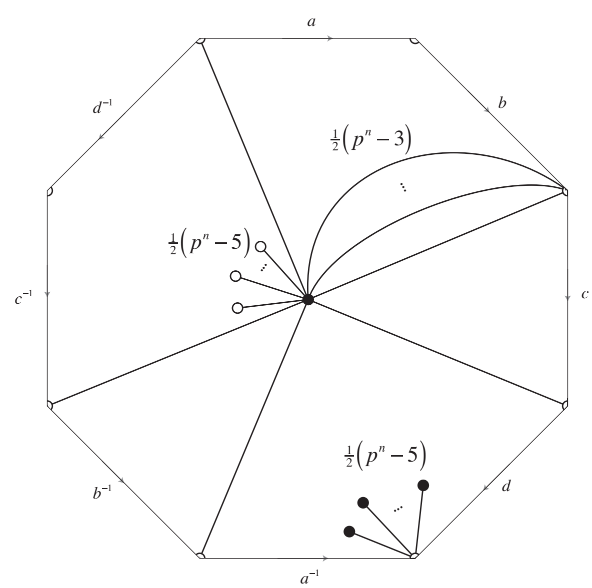

Figure 4.7: Level $2p^n$, $p^n \geq 5$ and $p \neq 2$

4.7 has a black vertex of degree p^n marked at the center, and a white vertex of degree

p^n which is marked at every corner of the octagon (when the sides of the octagon are identified, this becomes a single point). We can check these degrees with a count: the black vertex in the center has $\frac{1}{2}(p^n - 5)$ edges connected to degree 1 white vertices, and $4 + \frac{1}{2}(p^n - 3)$ edges to the degree p^n white vertex. The graph is symmetric with regard to the black and white vertices, so the white vertices have the same count. The outside face has degree p^n: it has $2 \cdot \frac{1}{2}(p^n - 5)$ edges connected to degree 1 vertices, and 5 edges connected between the degree p^n vertices. There are $\frac{1}{2}(p^n - 3) - 1$ faces of degree 1. The least common multiples of the degrees is p^n, so the level is $2p^n$. We can check that the graph belongs on a genus 2 surface; it is not quite so obvious as the case for the torus, since we must be sure the complement of the graph is a collection of 2-cells. In this case we have $2 + 2 \cdot \frac{1}{2}(p^n - 5)$ vertices, $\frac{1}{2}(p^n - 3)$ faces, and $\frac{1}{2}(3p^n - 5)$ edges, which gives an Euler characteristic of -2 as desired. Note that the $p^n \geq 5$ restriction arises from the $\frac{1}{2}(p^n - 5)$ black and white vertices of degree 1.

For these graphs we are able to show the corresponding groups are noncongruence for $n > 1$; the proof is delayed until the end of the section (see Proposition 4.2.7).

Example 4.2.2. Level 2^n, $n \geq 3$.

We have the same difficulty as before for $p = 2$; the degrees as marked in the above example are not integers. We can see in Figure 4.8 a version that works for level 2^n. As before, we can check the counts to see that all vertices and faces have degree 1, 2, or 2^{n-1}, so their least common multiple is 2^{n-1} and the graph is of level 2^n. The graph has $2^n - 2$ vertices, $2^{n-2} - 1$ faces, and $2^n + 2^{n-2} - 1$ edges, so the Euler characteristic is -2, which confirms the graph lies on a genus 2 surface. We check that the group Γ corresponding to such an example is noncongruence in the same manner as in Proposition 4.1.6: $[\Gamma(2) : \Gamma] = 2^n + 2^{n-2} - 1$ is odd, which does not divide $[\Gamma(2) : \Gamma(2^n)] = 2^{3n-4}$, and so Γ does not contain $\Gamma(2^n)$.

Example 4.2.3. Level $2p^n q^m$, with p and q odd primes such that $p^n \geq 7$.

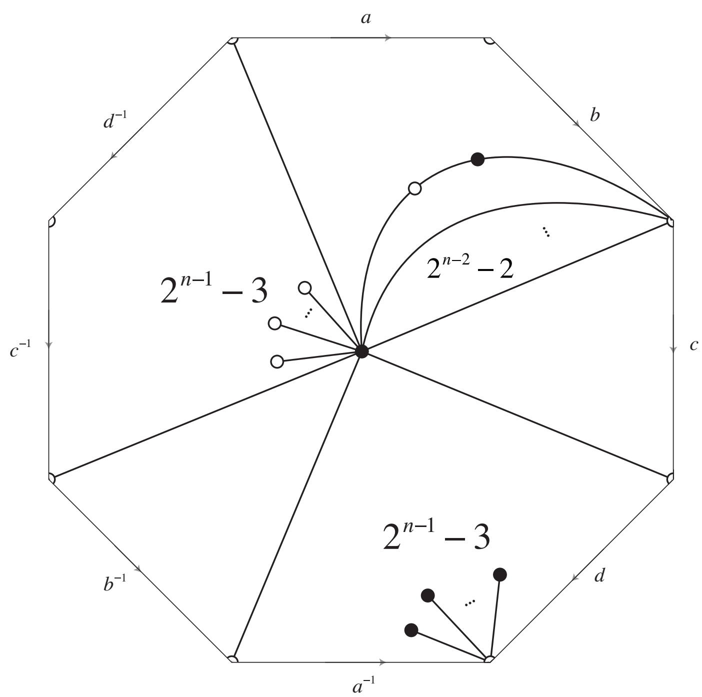

Figure 4.8: Level 2^n, $n \geq 3$

We can see a graph of level $2p^nq^m$ in Figure 4.9. For this graph the outside face has degree p^n, the inside face has degree q^m, and there are $\frac{1}{2}(3q^m + p^n - 6)$ faces of degree 1. For vertices, we see two of degree p^n, four of degree q^m, and $p^n + q^m - 10$ vertices of degree 1, so $p^n + q^m - 4$ vertices in all. (Note that we are no longer placing a vertex at the corners of the octagon.) There are $\frac{1}{2}(3p^n + 5q^m - 10)$ edges. This yields an Euler characteristic of -2 as desired.

Note that the least common multiple of the degrees is p^nq^m but there is no vertex or face with this degree. Thus, by Corollary 3.3.4, the graphs of this form represent noncongruence subgroups of level $2p^nq^m$.

Once again, we must consider separately the case where one of the primes is 2, level 2^mp^n.

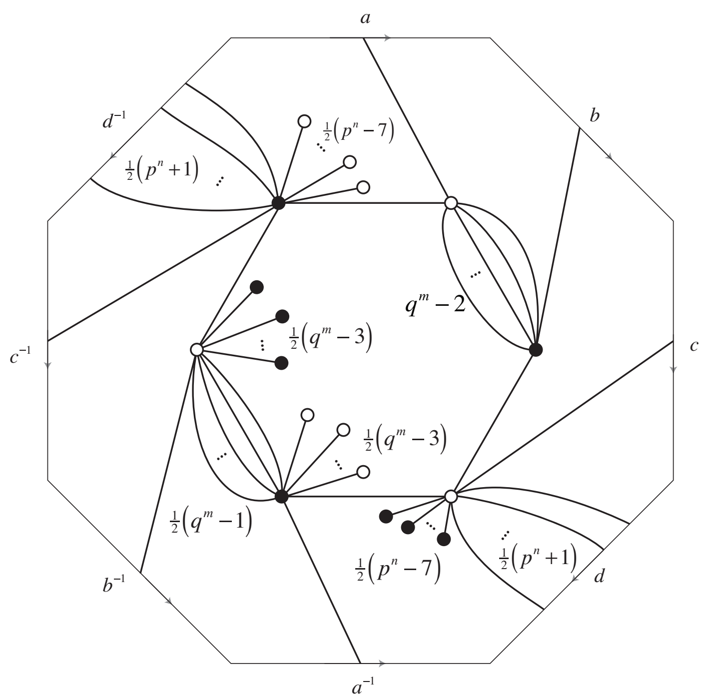

Figure 4.9: Noncongruence example of level $2p^nq^m$, with p, q odd primes and $p^n \geq 7$

Example 4.2.4. Level 2^mp^n, with p an odd prime.

We can construct these in several ways, each with their own limitations. In each case, Corollary 3.3.4 allows us to immediately conclude that the corresponding subgroups are noncongruence.

In the first method we make an adjustment to the inside face so that its degree is 2^{m-1}. Here we have the same restriction on p that we did in the previous example, that $p^n \geq 7$, and we require that $m \geq 3$. In the second version we instead make an adjustment to the outside face, so that its degree is 2^{m-1}. This does not restrict p, but does require that $m \geq 4$. These are pictured in Figure 4.10

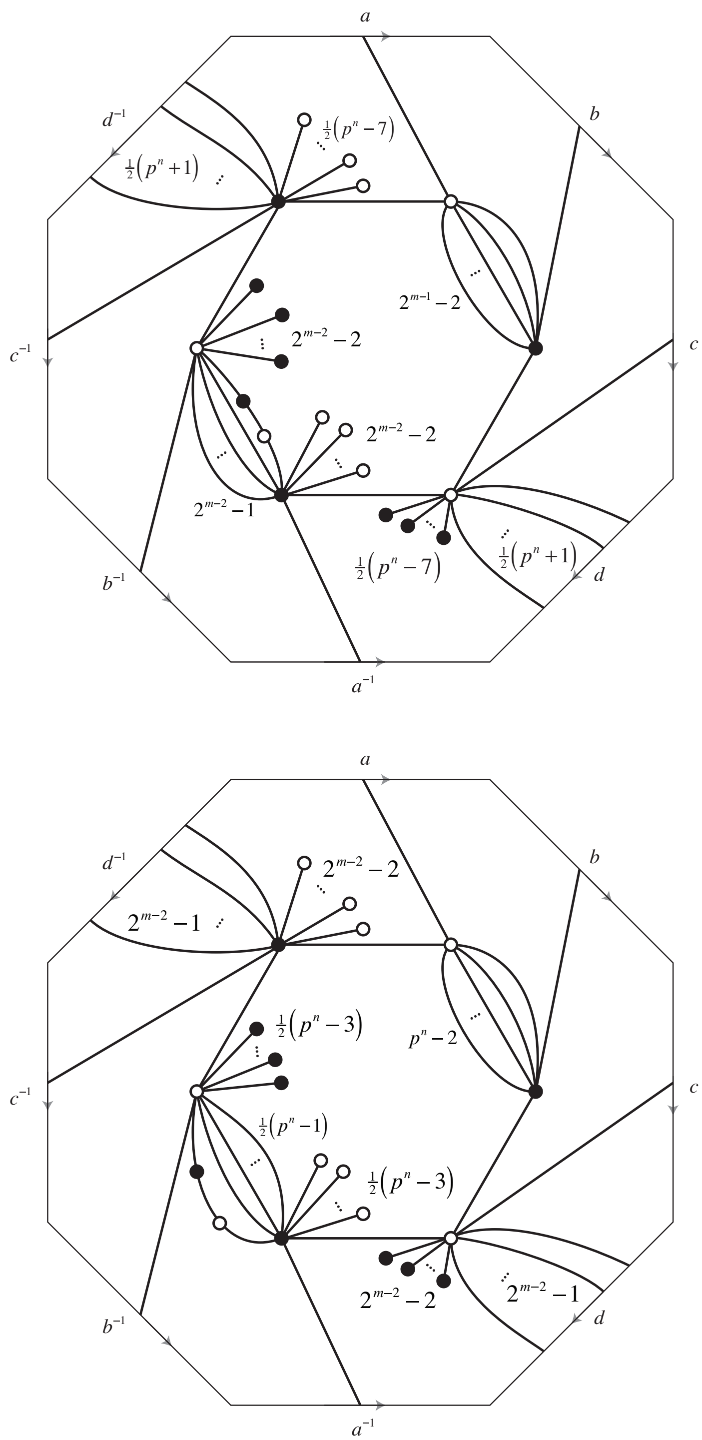

Figure 4.10: Noncongruence examples of level $2^m p^n$. Top version requires $p^n \geq 7$ and $m \geq 3$. Bottom version requires only that $m \geq 4$

.

Neither of these approaches produces a graph of level $4p^n$. To address this case we can construct the graph in Figure 4.11, which requires $p^n \geq 9$. By adding a black and white vertex "inside the onion" we create vertices and faces of degree 2.

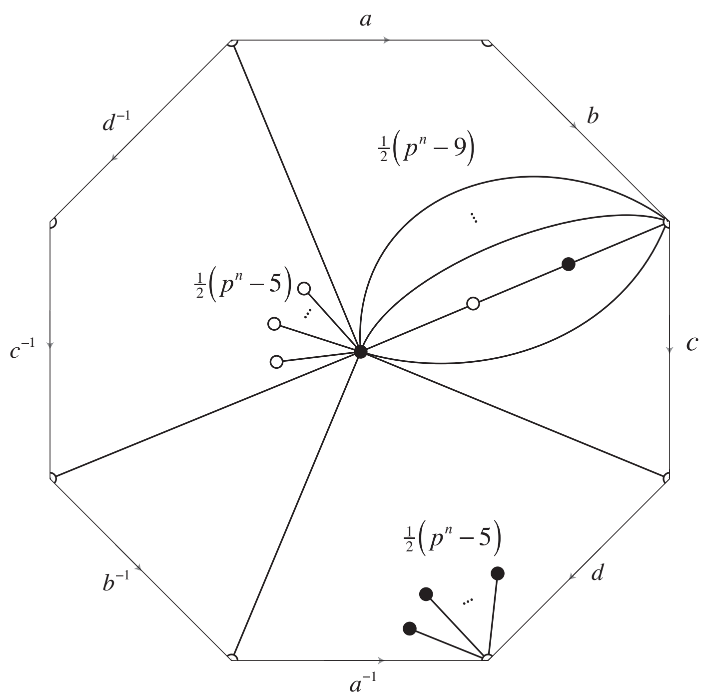

Figure 4.11: Noncongruence example of level $4p^n$, p an odd prime and $p^n \geq 9$

The example in Figure 4.11 inspires another class of examples of level $2^m p^n$ for $p^n \geq 9$: we can in fact add several degree 2 vertices, enough that the two adjacent faces each have degree 2^{m-1}. See Figure 4.12.

We are now ready to consider the general case. This is complicated by the fact that we can't simply "add strips" as we did for the torus examples and expect to remain on a genus 2 surface. Instead we take the approach of a construction similar to Example 4.2.3; we will have an "inside face" and an "outside face", and the remaining faces

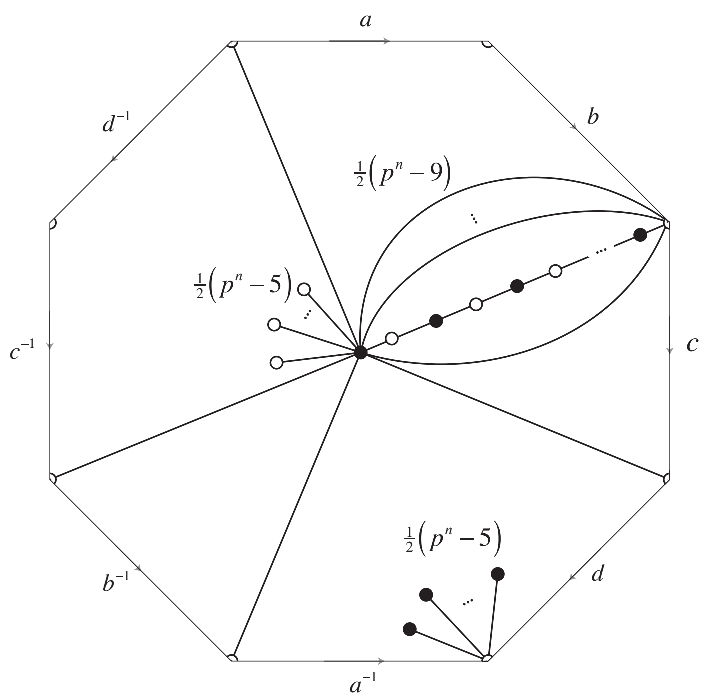

Figure 4.12: Noncongruence example of level $2^m p^n$, $p^n \geq 9$

will have degree 1. The degree of these faces are dependent on the number of prime factors k; thus we must consider separately the cases for k odd and k even.

Example 4.2.5. Level $2p_1^{n_1}p_2^{n_2}\dots p_k^{n_k}$ for k odd.

Consider the graph in Figure 4.13. This example is constructed so that the outside face has degree $p_1^{n_1}$ and the inside face has degree $p_2^{n_2}$. The polygon at the center has a pair of vertices for each prime factor; in each "onion" the degree of the black vertex and white vertex is $p_i^{n_i}$. Notice that we are allowed to use $p_i = 2$ as long as $i > 2$. However, we have some restrictions: we require $p_1^{n_1} \geq k + 4$ and $p_2^{n_2} \geq k$. In this construction we once again have no vertex or face of degree $p_1^{n_1}p_2^{n_2}\dots p_k^{n_k}$, so Corollary 3.3.4 guarantees the corresponding subgroup is noncongruence.

Example 4.2.6. Level $2p_1^{n_1}p_2^{n_2}\dots p_k^{n_k}$ for k even.

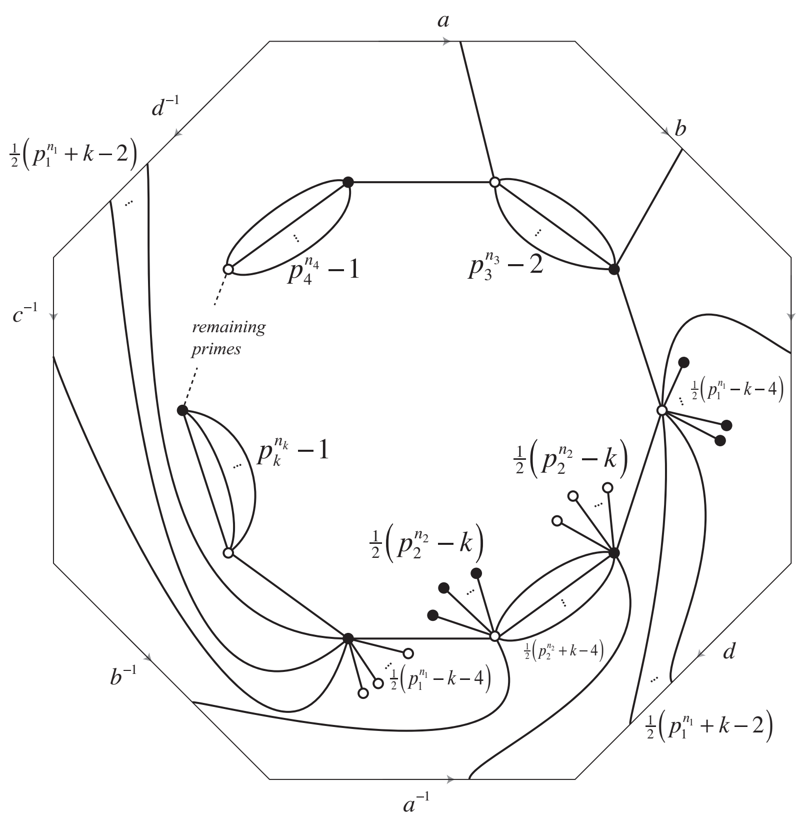

Figure 4.13: Noncongruence example of level $2p_1^{n_1}p_2^{n_2}\dots p_k^{n_k}$, with k odd

The above example does not work if k is even because, for example, $\frac{1}{2}(p_2^{n_2}-k)$ would not be an integer. We can overcome this by repeating one of the primes; we add one "onion" to the polygon of the central face. In Figure 4.14 we see such a graph; the repeated factor is $p_1^{n_1}$. In this case the restrictions are $p_1^{n_1} \geq k+5$ and $p_2^{n_2} \geq k+1$. Again, we are allowed to use $p_i = 2$ as long as $i > 2$.

For the examples in Figures 4.13 and 4.14 it is possible to increase the index for a given level. We can do so by repeating a prime factor in the manner we described for $p_1^{n_1}$ in the example for k even we saw above. However, there is a limitation: if we let k' be the number of prime factors including repeated factors, the polygon inside contributes k' edges to each of the inside and outside faces. Thus we require k' small

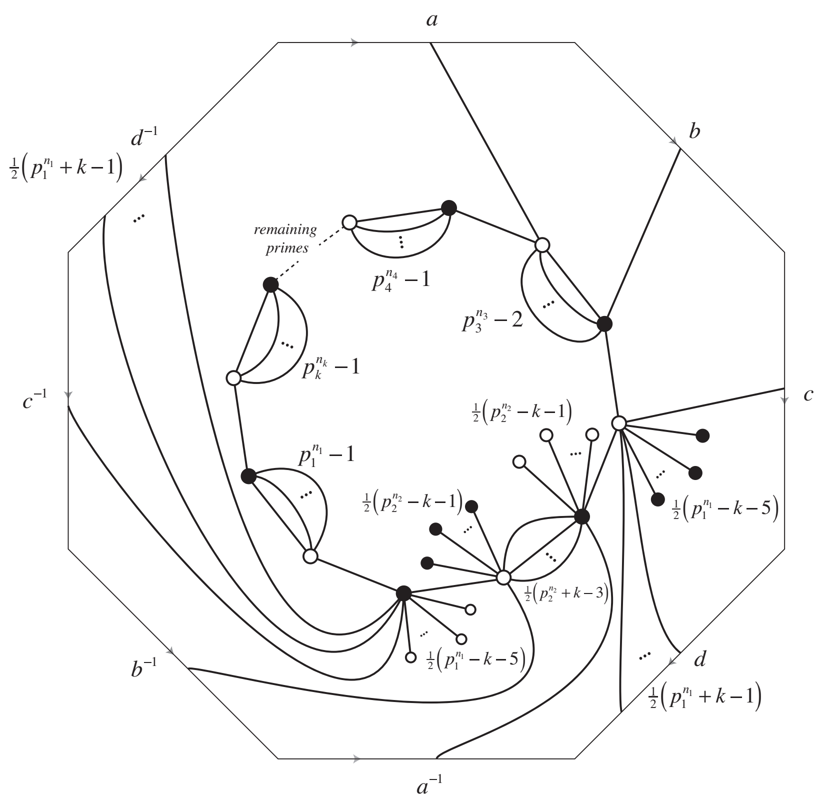

Figure 4.14: Level $2p_1^{n_1}p_2^{n_2}\dots p_k^{n_k}$, k even

enough that the restrictions listed for each case still hold for k'. So, in Example 4.13 we now have the restrictions $p_1^{n_1} \geq k' + 4$ and $p_2^{n_2} \geq k'$ as upper bounds on k'.

Now we return to the first example, the case of level $2p^n$.

Proposition 4.2.7. *The graph shown in Figure 4.7 represents a noncongruence subgroup* Γ *of level* $2p^n$ *for* $n > 1$.

Proof. The number of edges in this graph is $\frac{1}{2}(3p^n - 5)$, so $[\Gamma(2) : \Gamma] = \frac{1}{2}(3p^n - 5)$. Recall from Proposition 4.1.5 that $[\Gamma(2) : \Gamma(2p^n)] = \frac{1}{2}p^{3n-2}(p^2 - 1)$. Thus, if Γ were congruence of level $2p^n$, the covering degree must be an integer:

$$[\Gamma : \Gamma(2p^n)] = \frac{p^{3n-2}(p^2 - 1)}{3p^n - 5}.$$

Case 1: Suppose $p \neq 5$. In this case $3p^n - 5$ is relatively prime to p. Because $n > 1$ we have $3p^n - 5 > p^2 - 1$. Thus the fraction above is not an integer, and so $\Gamma(2p^n)$ is not contained in Γ.

Case 2: Let $p = 5$. In this case the fraction reduces to

$$\frac{5^{3n-3}(24)}{3 \cdot 5^{n-1} - 1}.$$

For $n \geq 3$, we see that the denominator is relatively prime to 5, and $3 \cdot 5^{n-1} - 1 > 24$. For $n = 2$ the fraction reduces to $\frac{1500}{7}$. Thus the fraction is not an integer, and so $\Gamma(2p^n)$ is not contained in Γ.

$\square$

Finally, we find the minimum level required for a graph to belong on a genus 2 surface. Figure 4.8 provides a graph of level 8. The following proposition shows we cannot have a graph of level 6; a similar argument shows the same for level 4.

Proposition 4.2.8. *It is not possible to have a graph of level 6 on genus 2 surface.*

Proof. Suppose for contradiction that we have such a graph. Because it is level 6, every vertex and face has degree either 1 or 3. Let b_1 and b_3 be the number of black vertices of degree 1 and 3 respectively, and let w_i and f_i be defined similarly. Each edge is associated to exactly one black vertex, one white vertex and one face, so we can count the number of edges, e, in three different ways:

$$e = b_1 + 3b_3 = w_1 + 3w_3 = f_1 + 3f_3.$$

Now consider the Euler characteristic; for a genus 2 surface we have $v - e + f = -2$. We know $v = b_1 + b_3 + w_1 + w_3$, and then using $e = b_1 + 3b_3$ and simplifying, the Euler characteristic calculation becomes

$$w_1 + w_3 + f_1 + f_3 = 2b_3 - 2. \tag{4.2.1}$$

We know there is at least one white vertex and at least one face, so the left-hand side is at least 2. Then $2b_3 - 2 \geq 2$ implies $b_3 \geq 2$. Redoing this with the other expressions for e, we also conclude $w_3 \geq 2$ and $f_3 \geq 2$, so $w_3 + f_3 \geq 4$. Now we look again at Equation 4.2.1: we conclude $b_3 \geq 3$; which in turn implies $w_3 \geq 3$ and $f_3 \geq 3$, and we can repeat the process again. Inductively, we must have $b_3 \geq n$ for all n; this is impossible, and so no such graph can exist. □

4.3 Future Projects

For the genus 2 examples, we first note that the proof for Proposition 4.2.7 does not address the case $n = 1$. We may be able to show these are noncongruence using another approach, or may be able to construct similar examples which are clearly noncongruence of level $2p$. Otherwise, we are missing examples for levels 12, 20, 24, 28, 30 and 40. We should either be able to construct examples for each of these particular levels, or perhaps find a new class of examples which includes graphs of these levels.

The examples in the genus 2 case are more complicated as we add more prime factors. There may be a way to construct examples that are more straightforward. In doing so, we hope to be able to construct infinite families of noncongruence subgroups of every even level on a genus 2 surface.

We would also like to find examples for every allowable even level on surfaces of higher genus, and eventually arbitrary genus.

And finally, we think they should all include frogs.

CHAPTER 5

USING GRAPHS TO DETERMINE CONGRUENCE

In this chapter we develop some tools that allow us to learn about a finite-index subgroup $\Gamma \subset \Gamma(2)$ by looking directly at its corresponding graph.

In the first section we generalize a result of Larcher which gives a property of congruence subgroups, which will give us more power in determining whether a graph corresponds to a congruence subgroup. The following sections develop an algorithm for determining whether Γ is congruence from the graph. In Section 5.2 we define a *graph tiling*; in Section 5.3 we use this to find generators for the group corresponding to a given graph. In Section 5.4 we use a graph tiling to determine whether a group Γ_2 is contained in the group Γ_1 associated to a given graph; as an application, letting $\Gamma_2 = \Gamma(2n)$ for the appropriate value of n will determine whether Γ is congruence.

5.1 Generalizing a result of Larcher

In Section 3.3 we stated results of Larcher which give properties of congruence subgroups, and interpreted them in terms of graphs. Recall the following restatement of one of Larcher's results:

Corollary 3.3.2 *Let $\Gamma \subset \Gamma(2)$ be a congruence subgroup of level $2n$. In the corresponding graph, let d and e be the respective degrees of the face corresponding to ∞ and the black vertex corresponding to 0. Then $2de \equiv 0 \pmod{n}$.*

We can generalize this result as follows:

Theorem 5.1.1. *Let $\Gamma \subset \Gamma(2)$ be a congruence subgroup of level $2n$. In the corresponding graph, for any face, let d be the degree of that face and e be the degree of any of its vertices. Then $2de \equiv 0 \pmod{n}$.*

Proof. Because we assumed Γ is congruence of level $2n$ we know $\Gamma(2n) \subset \Gamma$, and thus the graph associated to $\Gamma(2n)$ is a cover for the graph associated to Γ.

Let F be a face of Γ of degree d, and v be one of its vertices of degree e. Find a fundamental domain for the graph associated to Γ as described in Definition 2.3.2. We will see how we can conjugate by an element of $PSL_2(\mathbb{Z})$ to move the cusp associated to F to ∞, and then the cusp associated to v to zero. The resulting group, Γ', is congruence of level $2n$ if and only if Γ is congruence, since $\Gamma(2n) \lhd PSL_2(\mathbb{Z})$.

Recall from Theorem 2.3.1 that the correspondence between Γ and its graph requires a marked face, which we have chosen to be the face at ∞. The cusp that corresponds to the face center of F is the image of ∞ under an element $g \in \Gamma(2)$, and so conjugation by g moves the center of F to ∞. This will not change the graph itself, and will not change the degree of the face F; the only change is that F is now the marked face. Marking a different face will not change the fact that the graph for $\Gamma(2n)$ is a cover, so this face of degree d and the vertex at 0 must satisfy Larcher's congruence property above.

Now consider the vertex v, and let v' be its image under the conjugation in the previous step. Conjugation does not change the degree of a vertex, so the degree of v' is e. Notice that because the face F is now centered at ∞ it is tiled by translates of $\mathcal{D}$ under A, and so the cusps corresponding to black vertices are found at even integers, while the cusps corresponding to the white vertices are found at odd integers. First suppose that the vertex v is a black vertex. Translation by the appropriate power of A will fix ∞ and move v' to 0. Recall from part 3 of Theorem 2.3.1 the correspondence between groups and graphs is modulo conjugacy by translation: applying powers of A will not change the graph or the face which is marked, and so the graph is still covered by $\Gamma(2n)$. Hence, Larcher's congruence property is still satisfied.

Suppose instead that v is a white vertex; in this case we can move v' to 0 by conjugating by an odd power of $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. On the level of the graph this has the effect of switching the colors of the black and white vertices. The resulting group Γ' is congruence if and only if Γ is congruence, because $\Gamma(2n) \lhd PSL_2(\mathbb{Z})$, and so Larcher's congruence property holds. $\square$

5.2 Graph tilings

In Section 2.3.2 when we discussed a way to go from a graph to a group, we first found a fundamental domain for the graph. The fundamental domain for a graph $\mathcal{G}$ with n edges consists of n copies of $\mathcal{D}$, our fundamental domain for $\Gamma(2)$. In what follows we will need to keep track of not only the edges of $\mathcal{G}$, but the sides of the n tiles themselves as they appear on the surface; we will call this the *graph tiling of* $\mathcal{G}$. In this section we will describe how to find this tiling without drawing the fundamental domain as an intermediate step.

To do so, we start by reexamining our graph and fundamental domain $\mathcal{D}$ for $\Gamma(2)$. We will care about not just the arc from 0 to 1 and the arc from 0 to -1, but the entire quadrilateral that composes $\mathcal{D}$. We label the face center at ∞ as a $*$, and use dotted lines to indicate the arc from 1 to ∞ and the arc from -1 to ∞. Notice that crossing the arc from 1 to ∞ corresponds to applying the generator A to $\mathcal{D}$, while crossing the arc from 0 to 1 corresponds to applying B to $\mathcal{D}$. It will prove helpful for us to indicate these operations in the quadrilateral. See Figure 5.1.

Suppose we have a graph $\mathcal{G}$ drawn on a surface. In order to form our graph tiling for $\mathcal{G}$, we first label each face with a $*$ at its center. Next we draw dotted lines from

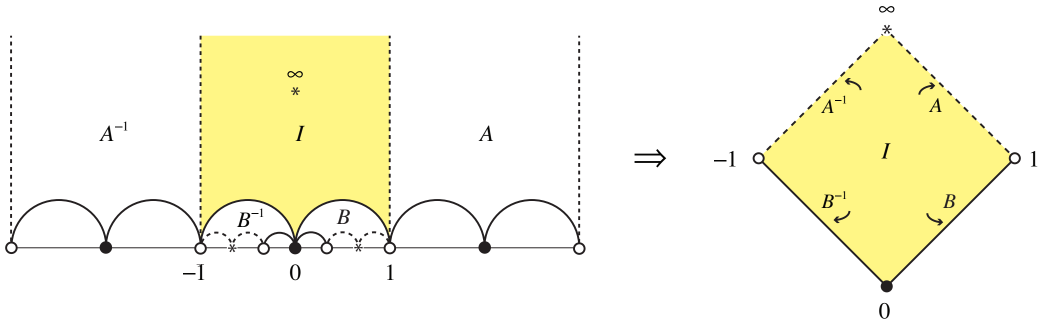

Figure 5.1: Labeling a tile

the white vertices to the $*$; at each white vertex we now alternate between solid lines (the edges to black vertices) and dotted lines (to the face center). This has the effect of doubling the degree of each white vertex. Recall from part 2 of Theorem 2.3.1 that specifying a graph involves marking one face with a $\star$; this marking will play a role in what follows. We have several examples: In Figure 5.2 we see this process applied to the graph corresponding to $\Gamma(2)$ itself. Figure 5.3 shows the graph tiling of the

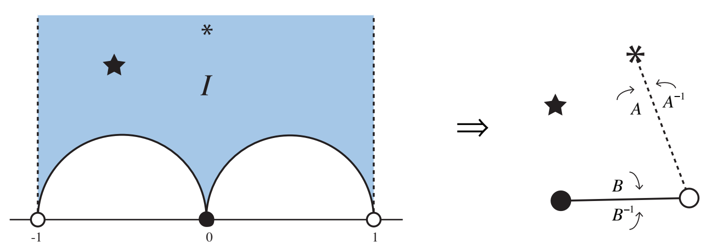

Figure 5.2: Graph tiling for $\Gamma(2)$

3-star. Notice that the 3-star has only one face (which is necessarily the marked face) but three tiles. When we label the quadrilaterals the marking will be in one of them, which we can declare to be the tile associated to I. We can refer to the fundamental domain for the 3-star (pictured in Figure 3.5 on page 23): we see that, beginning in the marked face $\star$, crossing the dotted line labeled A in the graph will bring us from the tile I to the tile A in the domain. Crossing the edge labeled B in the graph amounts to crossing edge 1 in the domain; this edge is identified with the the edge in tile A, and so the result is consistent. In other words, we can extend the notion of applying the generators A and B to the graph itself, which justifies the labelings we have added to the tiles on the graph.

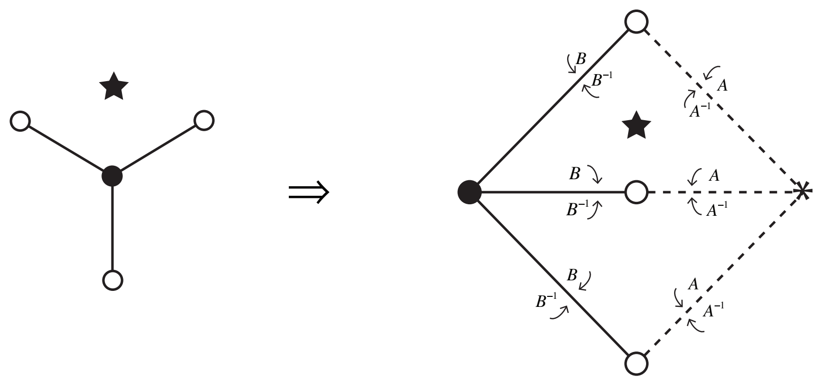

Figure 5.3: Graph tiling of 3-star

In Figure 5.4 we see an example of a tiling for a graph with five edges and two faces, with the face of degree 3 chosen as the marked face. Figure 5.5 shows an example of a graph tiling for a graph with four edges which lies on a torus.

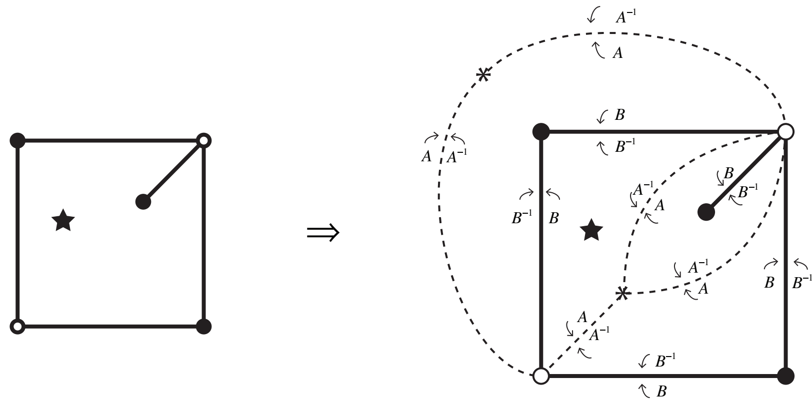

Figure 5.4: Graph tiling for a graph with 5 edges on the sphere

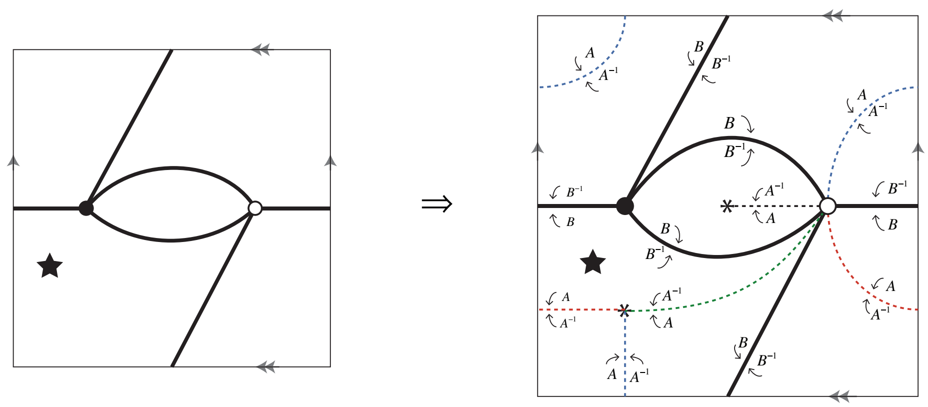

Figure 5.5: Graph tiling for a graph with 4 edges on a torus

5.3 Generators from a graph

The correspondence theorem guarantees a bijection between our graphs and finite-index subgroups of $\Gamma(2)$, and we have seen in Section 5.1 that we can realize properties of a group directly from the graph. In this section we will discuss how to use a graph $\mathcal{G}$ to read generators for the corresponding group $\Gamma \subset \Gamma(2)$ in terms of A and B.

We begin by finding the graph tiling for $\mathcal{G}$ as in Section 5.2. Next we will add several loops, each using the $\star$ of the marked face as a base point. For a graph on a sphere, we must add loops around all but one of the vertices and face centers. For a graph on a surface of higher genus we also add loops corresponding to generators of the fundamental group of the surface. Next, we follow each loop; as we cross each dotted or solid line, we read the label A, A^{-1}, B or B^{-1} and form a word by multiplying the labels on the left. In Proposition 5.3.1 we will see that this word corresponds to a generator of the corresponding group Γ. The direction we choose to follow each loop is irrelevant, because if g is in a generating set for Γ, we can replace g with g^{-1} without changing Γ.

Figure 5.6 shows this process applied to the graph for $\Gamma(2)$ itself. Notice that as we follow the top loop in the counterclockwise direction we find the generator A, and following the bottom loop in the clockwise direction produces the generator B. This agrees with our knowledge that $\Gamma(2)$ is generated by the elements A and B.

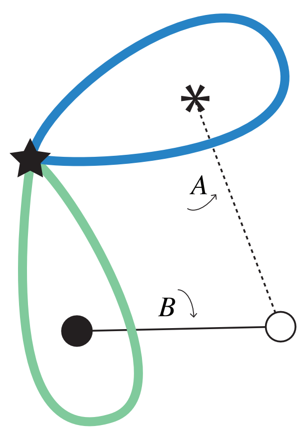

Figure 5.6: Reading generators for $\Gamma(2)$ from its graph

Now consider the 3-star; we found the graph tiling in Figure 5.3. In Figure 5.7 we see this graph with loops added. We can find the generators by following each loop counterclockwise: the top loop gives BA^{-1}; the loop on the right gives $A^{-1}B$, the bottom loop gives $B^{-1}A^{-1}B^2$, and the loop on the left gives B^{-3}. Thus, the group associated to the 3-star is $\Gamma = \langle BA^{-1},\ A^{-1}B,\ B^{-1}A^{-1}B^2,\ B^{-3}\rangle$.

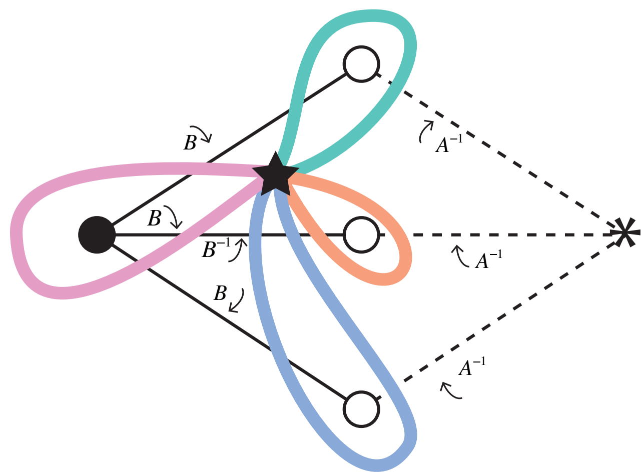

Figure 5.7: Finding generators for the group associated to the 3-star

Next we find loops for the graph in Figure 5.4. Notice that we have a choice of which cusp to omit when forming loops; in this graph it is natural to avoid the white vertex in the upper-right because it has the highest degree. We have six loops; beginning with the top-most loop and working our way clockwise, we find the group associated to this graph:

$$\Gamma = \left\langle B^{-1}A^2B,\ B^2,\ ABA^{-1},\ A^3, A^{-1}B^2A,\ B^{-1}AB^{-1}A \right\rangle.$$

Finally we look at the graph on a torus from Figure 5.5. In Figure 5.9 we see three loops around cusps, and two loops (vertical and horizontal) which generate the fundamental group of a torus. Reading generators from the vertical loop, horizontal

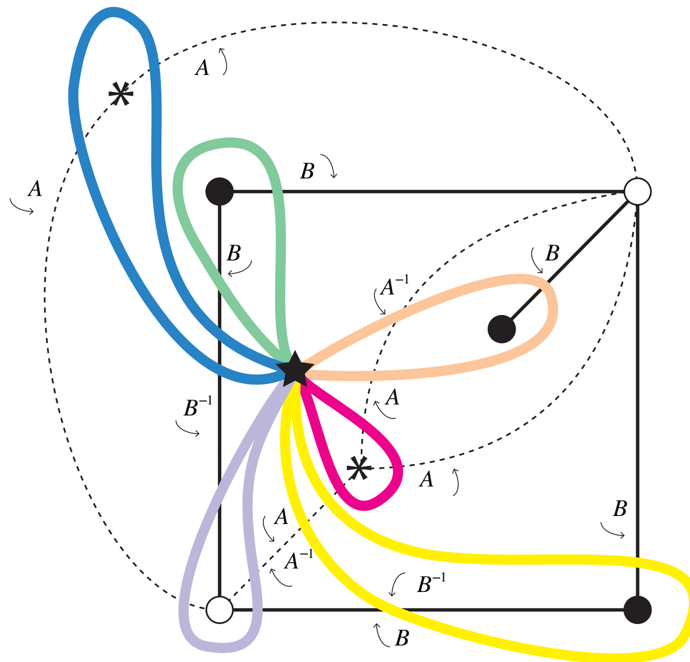

Figure 5.8: Finding generators for the graph in Figure 5.4

loop, and then the three loops around the cusps (top, middle, bottom), we find the group:

$$\Gamma = \left\langle B^{-1}A^2,\ AB^{-1}A,\ B^4,\ BAB^{-1},\ A^3 \right\rangle .$$

Having seen several examples, we now justify our prodcedure:

Proposition 5.3.1. *Generators for a finite-index subgroup* $\Gamma \subset \Gamma(2)$ *can be found from the loops drawn as above for its associated graph.*

Proof. We see this by understanding the group Γ associated to a graph $\mathcal{G}$ in two different ways.

Refer to Section 2.3.1: given a group Γ, we find the associated graph by first finding a fundamental domain for Γ, and then finding side-pairing transformations to form a punctured surface Σ'. Notice that the punctures are at the vertices and

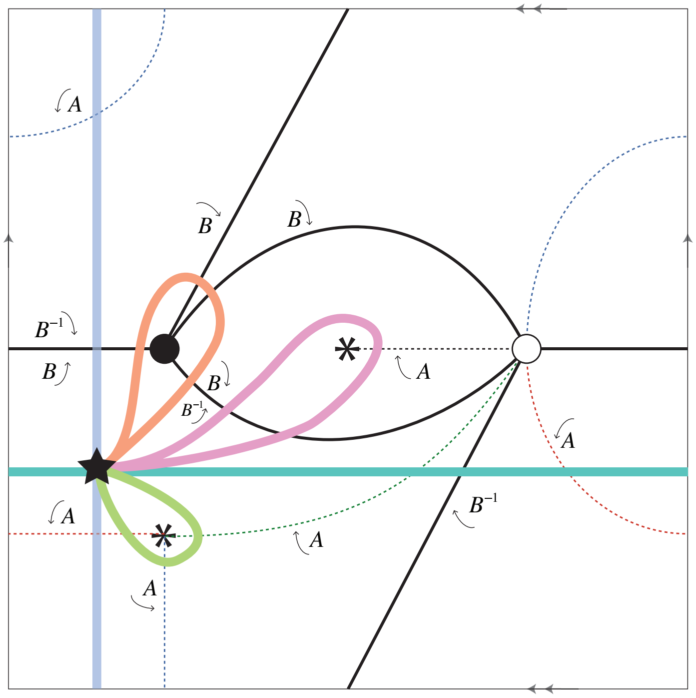

Figure 5.9: Finding generators for the graph in Figure 5.5

face centers of the graph. The side-pairing transformations generate Γ, which is the fundamental group of this punctured surface because $\Sigma' \simeq \Gamma\backslash\mathbb{H}^+$, with Γ acting freely on the upper-half plane $\mathbb{H}^+$.

We can also compute the fundamental group of Σ' using algebraic topology. Given a surface Σ' of genus g with r punctures, $\pi_1(\Sigma')$ is a free group on $2g+r-1$ generators. The generators are homotopy classes of loops; $2g$ for the genus of the surface, and loops around all but one of the punctures. We can interpret these loops as words in A, A^{-1}, B and B^{-1} using the graph tiling we found in Section 5.2. We begin each loop ℓ at $\star$; following the loop, each time we cross a side from one tile to another it corresponds to applying one of the $A^{\pm 1}$ or $B^{\pm 1}$ to our tiling. Since these motions correspond to applying these to images of $\mathcal{D}$ in $\mathbb{H}^+$, we build from right to left an element γ_ℓ of Γ corresponding to the loop ℓ. The fundamental group of the surface is then generated by the collection of γ_ℓ for our loops. Since we know this fundamental group is in fact Γ, the γ_ℓ generate Γ. Thus, though the generators we have found might not directly correspond to side-pairing transformations of a fundamental domain for Γ, they still generate the fundamental group of the same punctured surface. $\square$

5.4 Using graphs to determine congruence

Suppose we have a graph $\mathcal{G}$ corresponding to a finite-index subgroup Γ_1 of $\Gamma(2)$. Now suppose we have another finite-index subgroup $\Gamma_2 \subset \Gamma(2)$ for which we know generators in terms of A and B. In this section we will show how to determine whether $\Gamma_2 \subset \Gamma_1$. One useful application of this result is to determine whether a group is congruence: if Γ_1 has level $2n$ and we know generators for $\Gamma(2n)$, we can determine whether $\Gamma(2n) \subset \Gamma_1$. We note in Remark 6.4.4 that the algorithms in Chapter 6 to find permutations for $\Gamma(2p)$ for p prime also produce such generators.

The procedure is as follows: Find the graph tiling for $\mathcal{G}$ as we did in Section 5.2. Let γ be a generator for Γ_2 expressed as a word in $A^{\pm 1}$ and $B^{\pm 1}$. We will form the path in $\mathcal{G}$ beginning at $\star$ which follows γ by reversing of the process in Proposition 5.3.1: reading from right to left, we apply $A^{\pm 1}$ or $B^{\pm 1}$ to cross the corresponding edge of the tile. If the path ends in the same tile as $\star$ we have formed a loop ℓ on Σ', and thus $\gamma = \gamma_\ell$ is an element of $\pi_1(\Sigma') = \Gamma_1$. If we do not return to the tile with $\star$, the generator γ is not in Γ_1. If every element of our generating set for Γ_2 forms a loop, we have $\Gamma_2 \subset \Gamma_1$.

As an example, consider the 3-star. As we discussed in Section 3.1, this graph does not violate the necessary conditions in Larcher's statements, but the algorithm of Tim Hsu shows the corresponding group Γ is noncongruence. We will see how to apply the test in this section to come to the same conclusion. This graph is level 6, so if Γ is to be congruence it must contain $\Gamma(6)$. We begin by finding a set of generators for $\Gamma(6)$.

In Appendix B, Figure B.1 shows a fundamental domain for $\Gamma(6)$; the side-pairing transformations yield the generators. For example, the generator corresponding to x_1 is $ABA^{-2}B^{-2}$. This corresponds to the path shown in Figure 5.10, which is not a loop. Thus $\Gamma(6)$ is not in Γ, so the 3-star does not represent a congruence subgroup.

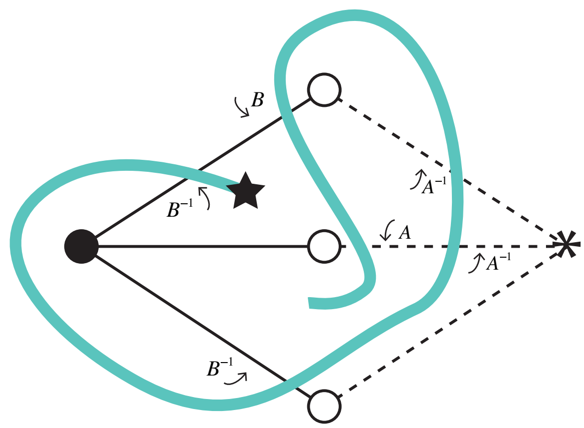

Figure 5.10: The 3-star represents a noncongruence subgroup

5.5 Future Projects

The results of Larcher discussed in Section 5.1 are quite natural to interpret in terms of graphs, though his proofs in [9] are based entirely in number theory. It may be possible to reprove these using properties of the graphs, and in doing so we may discover other necessary conditions for congruence.

Also, Section 5.4 provides a way to determine whether or not the group associated to a given a graph is noncongruence. For a more complicated graph it would be useful to work directly with the permutations which define the graph without having to draw the picture. It would be of interest to reformulate the results of this Chapter in terms of the permutations (if possible). This might yield a test for congruence similar to that of Hsu in [5].

CHAPTER 6

ALGORITHMS

In this section we focus on finding the permutations associated to the group $\Gamma(2p)$ and two of its subgroups, the Hecke groups $\Gamma_0(2p) \cap \Gamma(2)$ and $\Gamma_1(2p) \cap \Gamma(2p)$, for p prime. Our motivation is two-fold. First of all, knowing the permutations is equivalent to knowing their graphs; in the case of $\Gamma_0(2p) \cap \Gamma(2)$ we can immediately draw the associated graph, and in the case of $\Gamma_1(2p) \cap \Gamma(2p)$ there is a clear pattern we hope to formalize in the future. Secondly, in the course of finding these permutations we also find a fundamental domain and side-pairing transformations. The side-pairing transformations generate the corresponding groups (see Ford [3]), so they provide generators in terms of the generators of $\Gamma(2)$. We saw in Chapter 5 that these are of use in proving whether a group is congruence by looking directly at its graph.

The algorithms depend on finding first the permutations for $\Gamma_0(2p) \cap \Gamma(2)$ and then $\Gamma_1(2p) \cap \Gamma(2)$. The calculations to implement the algorithms require only basic mod p arithmetic. The group $\Gamma_0(2p) \cap \Gamma(2)$ for the case $p = 3$ was discussed in Section 2.3. In this chapter we will use the example $p = 7$ throughout, which proved small enough to be tractable but still large enough to illustrate the various cases we might encounter. The appendices show all or part of the examples for $p = 3, 5, 11$ and 13.

6.1 Index formulae

We will need to make use of a few elementary index formulae. These are found by beginning with known index formulae for subgroups of $PSL_2(\mathbb{Z})$ (see, for example, [10]) and modifying them to apply to subgroups of $\Gamma(2)$.

Lemma 6.1.1.

$$[\Gamma(2) : \Gamma_0(2n) \cap \Gamma(2)] = n \prod_{\substack{p|n \\ p \neq 2}} (1 + \tfrac{1}{p})$$

Proof. Let $\Gamma(1)$ denote $PSL_2(\mathbb{Z})$. We know

$$[\Gamma(1) : \Gamma_0(N)] = N \prod_{p|N} (1 + \tfrac{1}{p}).$$

Consider the following diagram:

$$\begin{tikzcd}
1 \arrow[r] & \Gamma(2) \arrow[r] & \Gamma(1) \arrow[r, "mod\ 2"] & SL_2(\mathbb{Z}/2\mathbb{Z}) \arrow[r] & 1 \\
1 \arrow[r] & \Gamma_0(2n) \cap \Gamma(2) \arrow[r] \arrow[u] & \Gamma_0(2n) \arrow[r, "mod\ 2"] \arrow[u] & B \arrow[r] \arrow[u] & 1
\end{tikzcd}$$

where $B = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in SL_2(\mathbb{Z}/2\mathbb{Z}) \right\}$ and the vertical arrows are the natural injections. Applying a standard index formula we find

$$[SL_2(\mathbb{Z}/2\mathbb{Z}) : B] \cdot [\Gamma(2) : \Gamma_0(2n) \cap \Gamma(2)] = [\Gamma(1) : \Gamma_0(2n)].$$

By counting elements we find that $[SL_2(\mathbb{Z}/2\mathbb{Z}) : B] = 3$. Thus,

$$\begin{aligned}
[\Gamma(2) : \Gamma_0(2n) \cap \Gamma(2)] &= \tfrac{1}{3}(2n) \prod_{p|2n} (1 + \tfrac{1}{p}) \\
&= \tfrac{2}{3} n (1 + \tfrac{1}{2}) \prod_{\substack{p|n \\ p \neq 2}} (1 + \tfrac{1}{p}) \\
&= n \prod_{\substack{p|n \\ p \neq 2}} (1 + \tfrac{1}{p})
\end{aligned}$$

□

Lemma 6.1.2.

$$[\Gamma_1(2n) \cap \Gamma(2) : \Gamma(2n)] = n$$

Proof. We use a similar argument to the one above. We know that

$$[\Gamma_1(N) : \Gamma(N)] = N.$$

Consider the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Gamma_1(2n) \cap \Gamma(2) & \longrightarrow & \Gamma_1(2n) & \xrightarrow{mod\ 2} & B & \longrightarrow & 1 \\ & & \big\uparrow & & \big\uparrow & & \big\uparrow & & \\ 1 & \longrightarrow & \Gamma(2n) & \longrightarrow & \Gamma(2n) & \xrightarrow{mod\ 2} & 1 & \longrightarrow & 1 \end{array}$$

Because the order of B is 2, this yields

$$2[\Gamma_1(2n) \cap \Gamma(2) : \Gamma(2n)] = [\Gamma_1(2n) : \Gamma(2n)]$$

and thus $[\Gamma_1(2n) \cap \Gamma(2) : \Gamma(2n)] = \frac{1}{2}(2n) = n$. $\square$

Lemma 6.1.3.

$$[\Gamma_0(2n) \cap \Gamma(2) : \Gamma_1(2n) \cap \Gamma(2)] = \tfrac{1}{2}\varphi(2n)$$

where φ is the Euler φ-function.

Proof. We know that

$$[\Gamma(1) : \Gamma(N)] = \begin{cases} \dfrac{N^3}{2} \displaystyle\prod_{p|N} \left(1 - \tfrac{1}{p^2}\right) & \text{if } \ N > 2 \\ 6 & \text{if } \ N = 2 \end{cases}$$

Since $[\Gamma(1) : \Gamma(2)] = 6$ we have

$$\begin{aligned} [\Gamma(2) : \Gamma(2n)] &= \tfrac{1}{6} \cdot \tfrac{(2n)^3}{2} \prod_{p|2n} \left(1 - \tfrac{1}{p^2}\right) \\ &= \tfrac{n^3}{2} \prod_{\substack{p|n \\ p \neq 2}} \left(1 - \tfrac{1}{p^2}\right). \end{aligned} \tag{6.1.1}$$

Recall

$$\varphi(2n) = n \prod_{\substack{p|n \\ p \neq 2}} \left(1 - \tfrac{1}{p}\right).$$

Applying Lemmas 6.1.1 and 6.1.2, we divide to find the desired result. $\square$

6.2 $\Gamma_0(2p) \cap \Gamma(2)$

This section gives an algorithm to find the permutations for the graph associated to $\Gamma_0 = \Gamma_0(2p) \cap \Gamma(2)$. Lemma 6.1.1 tells us that $[\Gamma(2) : \Gamma_0] = p + 1$, so the graph associated to Γ_0 has $p + 1$ edges.

Algorithm 6.2.1. Permutations for $\Gamma_0(2p) \cap \Gamma(2)$.

STEP 1 The permutation for the black vertices is given by $\sigma = (p, p-1, \cdots, 2, 1)(p+1)$.

STEP 2 The faces give a permutation of the form $\beta = (\varphi_1, \varphi_2, \cdots, \varphi_p)(p)$, where we can define the φ_i recursively as follows:

(a) Let $\varphi_1 = 1$.

(b) For the (unique) i such that $1+4\varphi_i$ is not invertible mod p, let $\varphi_{i+1} = p+1$ and choose $\varphi_{i+2} \in \{2, \ldots, p-1\}$ so that $\varphi_{i+2} \equiv -\varphi_i \pmod{p}$.

(c) Otherwise, choose $\varphi_{i+1} \in \{2, \ldots, p-1\}$ so that $\varphi_{i+1} \equiv \varphi_i(1 + 4\varphi_i)^{-1} \pmod{p}$.

Example 6.2.2. We compute the permutations associated to $\Gamma_0(14) \cap \Gamma(2)$.

The black vertices give the permutation $\sigma = (7, 6, 5, 4, 3, 2, 1)(8)$.

For the faces, let $\varphi_1 = 1$. Then we have

$$\begin{aligned}
\varphi_2 &\equiv 1(1+4)^{-1} \pmod{7} &&= 3 \\
\varphi_3 &\equiv 3(1+12)^{-1} \pmod{7} &&= 4 \\
\varphi_4 &\equiv 4(1+16)^{-1} \pmod{7} &&= 6 \\
\varphi_5 &\equiv 6(1+24)^{-1} \pmod{7} &&= 5
\end{aligned}$$

Since $(1+20)$ is not invertible mod 7, we let $\varphi_6 = 8$ and $\varphi_7 \equiv -5 \pmod{7} = 2$. Then φ_8 would be $2(1+8)^{-1} \pmod{7} = 1$, so we have completed the cycle. The faces have permutation $\beta = (1, 3, 4, 6, 5, 8, 2)(7)$.

The white vertices have permutation $\alpha = \sigma^{-1}\beta^{-1} = (1, 8, 5, 4, 6, 7, 2)(3)$.

The graph is shown in Figure 6.1. We see an octagon with sides identified according to the graph edges in such a way as to produce an orientable surface of genus 2. The corresponding fundamental domain is shown in the appendix, Figure B.7.

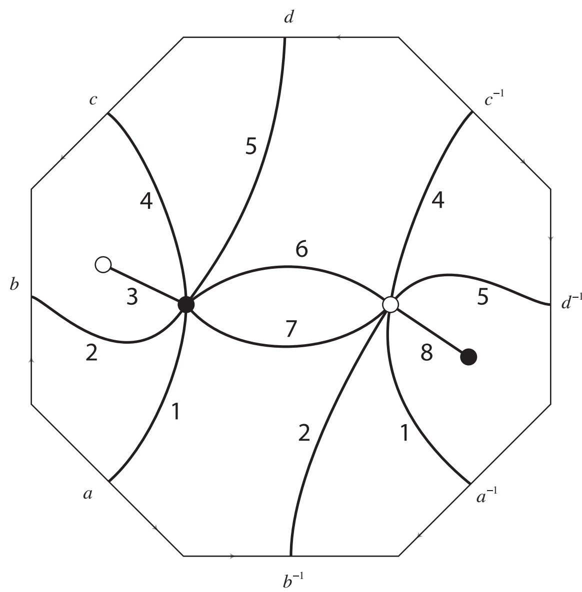

Figure 6.1: Graph for $\Gamma_0(14) \cap \Gamma(2)$

Theorem 6.2.3. *The above steps compute the permutations for the graph associated to* $\Gamma_0(2p) \cap \Gamma(2)$.

Proof. Let $\Gamma_0 = \Gamma_0(2p) \cap \Gamma(2)$. We will construct a fundamental domain for Γ_0 from I, B, B^2, …, B^{p-1} and X (to be determined below). Note that for $i \neq j$, $1 \leq i, j < p$, $B^i \cdot (B^j)^{-1} = B^{i-j}$ is not in Γ_0, so we know the B^i represent distinct cosets of Γ_0 in $\Gamma(2)$. Label the tiles so that the graph edge in B^i is i and the graph edge in I is p

(see Figure 6.2). In doing so we have associated the permutation $\alpha = (p, p-1, \ldots, 1)$ to the black vertex at 0.

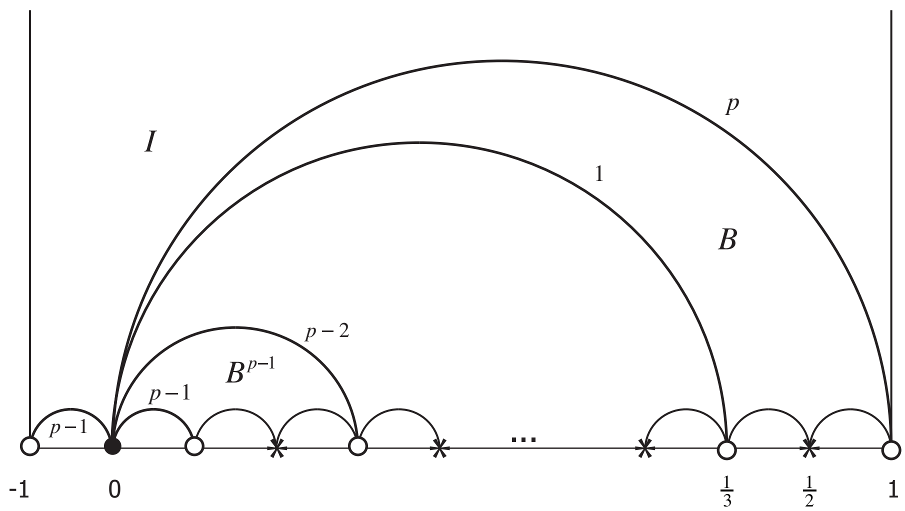

Figure 6.2: Degree p black vertex for $\Gamma_0(2p) \cap \Gamma(2)$

In order to determine the permutation for the faces and discover an appropriate choice for X, we will begin to find the side-pairing transformations for the fundamental domain. We can rotate counterclockwise about a face center from the tile B^m to the tile B^k by finding $g \in \Gamma_0$ so that $gB^mA \equiv B^k \pmod{2p}$.

In this case we have

$$g = B^k A^{-1} B^{-m} = \begin{pmatrix} 1+4m & -2 \\ 2k-2m+8mk & 1-4k \end{pmatrix},$$

and g is in Γ_0 when $2k - 2m + 8mk \equiv 0 \pmod{2p}$. Thus, if $1+4m$ is invertible mod p, then $k \equiv m(1+4m)^{-1} \pmod{p}$. We now see Step 2(c) of the algorithm: when $1+4m$ is invertible mod p, the tile labeled m is glued to the tile labeled $m(1+4m)^{-1} \pmod{p}$.

In the case where $1+4m$ is not invertible mod p, the tile B^mA is not equivalent to one of the form B^k under Γ_0. Thus we find our choice of X: let $X = B^mA$, and label its corresponding graph edge as $p+1$ (see Figure 6.3).

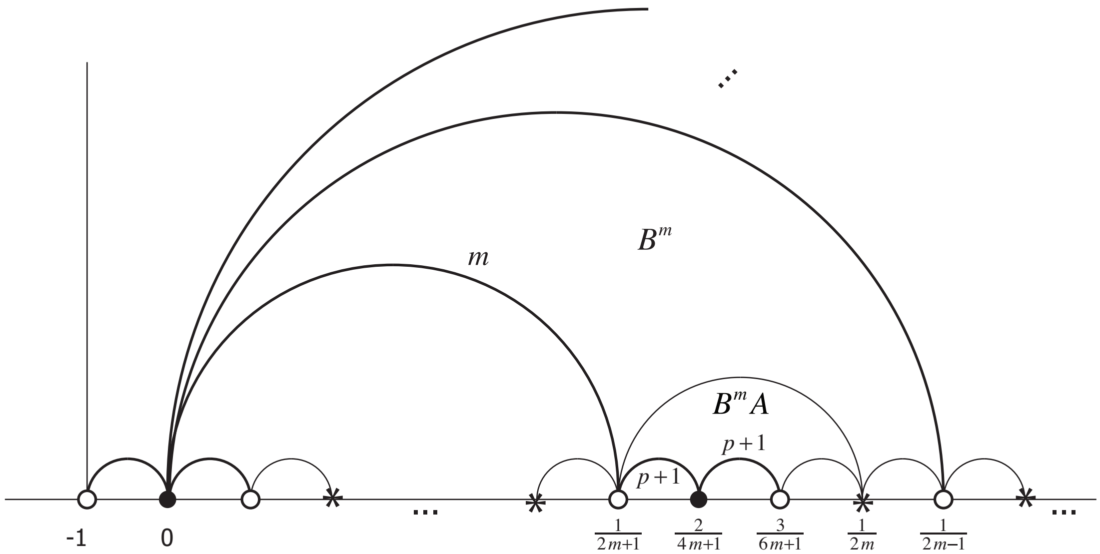

Figure 6.3: Degree 1 black vertex for $\Gamma_0(2p) \cap \Gamma(2)$

To verify this is an appropriate choice we need to check that its edges will pair with others in our domain. First, we will see that this tile contributes a degree 1 black vertex at $\frac{2}{4m+1}$. Rotating counterclockwise about this black vertex, we check that there is $g \in \Gamma_0$ with $gB^mAB^{-1} \equiv B^mA \pmod{2p}$. In this case we have

$$g = B^mABA^{-1}B^{-m} = \begin{pmatrix} 16m+5 & -8 \\ 2(1+4m)^2 & -16m-3 \end{pmatrix}. \tag{6.2.1}$$

Since we have chosen m in the case that $1+4m$ is a multiple of p, this g is indeed in Γ_0.

Now we look at the remaining side of the tile X. Rotating counterclockwise around the face center $\frac{1}{2m}$ we have passed from the tile B^m labeled m to the tile $X = B^m A$ labeled $p+1$. From there we seek a value k so that $gB^m A \cdot A \equiv B^k \pmod{2p}$. In this case we have

$$g = B^k A^{-2} B^{-m} = \begin{pmatrix} 1+8m & -4 \\ 2k-2m+16mk & 1-8k \end{pmatrix} \tag{6.2.2}$$

which is in Γ_0 when $2k - 2m + 16mk \equiv 0 \pmod{2p}$, i.e., $k \equiv m(1+8m)^{-1} \pmod{p}$. Because $1+4m$ is a multiple of p, we find that $1+8m \equiv -1 \pmod{p}$ (and is therefore invertible mod p). This explains Step 2(b) of the algorithm: if $\varphi_i = m$ with $1+4m$ not invertible mod p, then $\varphi_{i+1} = p+1$ and $\varphi_{i+2} \equiv m(1+8m)^{-1} \equiv -m \pmod{p}$

Thus, we have produced a fundamental domain for $\Gamma_0(2p) \cap \Gamma(2)$ from the $p+1$ tiles $I, B, \ldots, B^{p-1}$ and $X = B^m A$ with all sides identified by elements of $\Gamma_0(2p) \cap \Gamma(2)$, and assigned the labels in such a way as to produce the permutations given in the algorithm.

$\square$

6.3 $\Gamma_1(2p) \cap \Gamma(2)$

Having found permutations for $\Gamma_0 = \Gamma_0(2p) \cap \Gamma(2)$, we can use these to build the permutations for $\Gamma_1 = \Gamma_1(2p) \cap \Gamma(2)$. Using the index formula in Lemma 6.1.3, let $n = [\Gamma_0 : \Gamma_1] = \frac{1}{2}(p-1)$. The graph for Γ_1 will have $n(p+1)$ edges.

Algorithm 6.3.1. Permutations for $\Gamma_1(2p) \cap \Gamma(2)$.

STEP 1 The black vertices give the following $2n$ cycles:

$$(p, p-1, \ldots, 2, 1)(p+1)$$
$$(2p+1, 2p, \ldots, p+2)(2p+2)$$
$$(3p+2, 3p+1, \ldots, 2p+3)(3p+3)$$
$$\vdots$$
$$(np+n-1, np+n-2, \ldots, np+n-p)(np+n)$$

STEP 2 The n faces of degree 1 are given by the cycles $(p)(2p+1)(3p+2)\cdots(np+n-1)$.

STEP 3 Each face of degree p gives a cycle of the form $\Psi_i = (\psi_{i_1}, \psi_{i_2}, \cdots, \psi_{i_p})$, where we can define the ψ_{i_j} as follows:

(a) Find the cycle for the degree p face of $\Gamma_0(2p) \cap \Gamma(2)$, $\Phi = (\varphi_1, \varphi_2, \cdots, \varphi_p)$, with $\varphi_1 = 1$.

(b) To each φ_i associate u_i: For the (unique) i such that $1+4\varphi_i$ is not invertible mod p, let $u_i = 1$ and $u_{i+1} = -1$. Otherwise, let $u_i = (1+4\varphi_i)^{-1} \pmod{p}$.

(c) We find the first p-cycle Ψ_1 as follows: Set $c_1 = 1$. For $i \geq 2$, choose $c_i \in \{1, 3, 5, \ldots, p-1\}$ such that

$$c_i \equiv \pm \prod_{j=1}^{i-1} u_j \pmod{2p}. \tag{6.3.1}$$

Let $\psi_{1_i} = \varphi_i + \frac{1}{2}(c_i - 1)(p+1)$. The resulting $\Psi_1 = (\psi_{1_1}, \psi_{1_2}, \cdots, \psi_{1_p})$ is the cycle for a face in the graph.

(d) Given p-cycles corresponding to degree p faces $\Psi_1, \ldots, \Psi_k$, we can find Ψ_{k+1}: Find a number e, $1 < e < np+n$, that does not appear in any of the cycles $\Psi_1, \ldots, \Psi_k$. Cyclically permute the cycle Φ and relabel the φ_i (and their corresponding u_i from (b)) so that $\Phi = (\varphi_1, \varphi_2, \cdots, \varphi_p)$ with

$\varphi_1 \equiv e \pmod{p+1}$. Now proceed exactly as in (c) to find Ψ_{k+1}. (Note that we always begin this step by setting $c_1 = 1$.)

Example 6.3.2. We compute the permutations associated to $\Gamma_1(14) \cap \Gamma(2)$.

The permutation for the six black vertices is given by

$$\sigma = (7,6,5,4,3,2,1)(8)(15,14,13,12,11,10,9)(16)(23,22,21,20,19,18,17)(24)$$

The cycles for the faces of degree 1 are (7)(15)(23).

For the faces of degree 7, we first refer to Example 6.2.2 to find that the cycle for the degree 7 face of $\Gamma_0(14) \cap \Gamma(2)$ is $\Phi = (1,3,4,6,5,8,2)$.

Next we find the u_i, calculating each mod 14:

$$\begin{array}{lllr}
\varphi_1 = 1 & u_1 = (1+4)^{-1} & = & 3 \\
\varphi_2 = 3 & u_2 = (1+12)^{-1} & = & -1 \\
\varphi_3 = 4 & u_3 = (1+16)^{-1} & = & 5 \\
\varphi_4 = 6 & u_4 = (1+24)^{-1} & = & -5 \\
\varphi_5 = 5 & u_5 & = & 1 \\
\varphi_6 = 8 & u_6 & = & -1 \\
\varphi_7 = 2 & u_7 = (1+8)^{-1} & = & -3
\end{array}$$

Now we find each of the three 7-cycles.

The first 7-cycle, Ψ_1:

$$\begin{array}{r|rrrrrrr}
\varphi_i & 1 & 3 & 4 & 6 & 5 & 8 & 2 \\
u_i & 3 & -1 & 5 & -5 & 1 & -1 & -3 \\
c_i & 1 & 3 & 3 & 1 & 5 & 5 & 5 \\
\hline
\psi_{1_i} & 1 & 11 & 12 & 6 & 21 & 24 & 18
\end{array}$$

The second 7-cycle, Ψ_2:

φ_i	2	1	3	4	6	5	8
u_i	-3	3	-1	5	-5	1	-1
c_i	1	3	5	5	3	1	1
ψ_{2_i}	2	9	19	20	14	5	8

The third 7-cycle, Ψ_3:

φ_i	3	4	6	5	8	2	1
u_i	-1	5	-5	1	-1	-3	3
c_i	1	1	5	3	3	3	3
ψ_{3_i}	3	4	22	13	16	10	17

Thus the faces give the permutation

$$\beta = (1, 11, 12, 6, 21, 24, 18)(2, 9, 19, 20, 14, 5, 8)(3, 4, 22, 13, 16, 10, 17)(7)(15)(23)$$

The white vertices are given by $\alpha = \sigma^{-1}\Psi^{-1}$, which yields

$$\alpha = (1, 8, 5, 12, 22, 23, 10)(2, 17, 24, 21, 4, 14, 15)(6, 7, 18, 9, 16, 13, 20)(3)(11)(19)$$

The graph is shown in Figure 6.4, with the faces shown in different colors. We identify the 24 sides of the polygon according to the edge labels to form an orientable surface of genus 4. The corresponding fundamental domain is shown in the appendix, Figure B.8

An example for the case $p = 11$ is worked out in the Appendices, Section C.2.

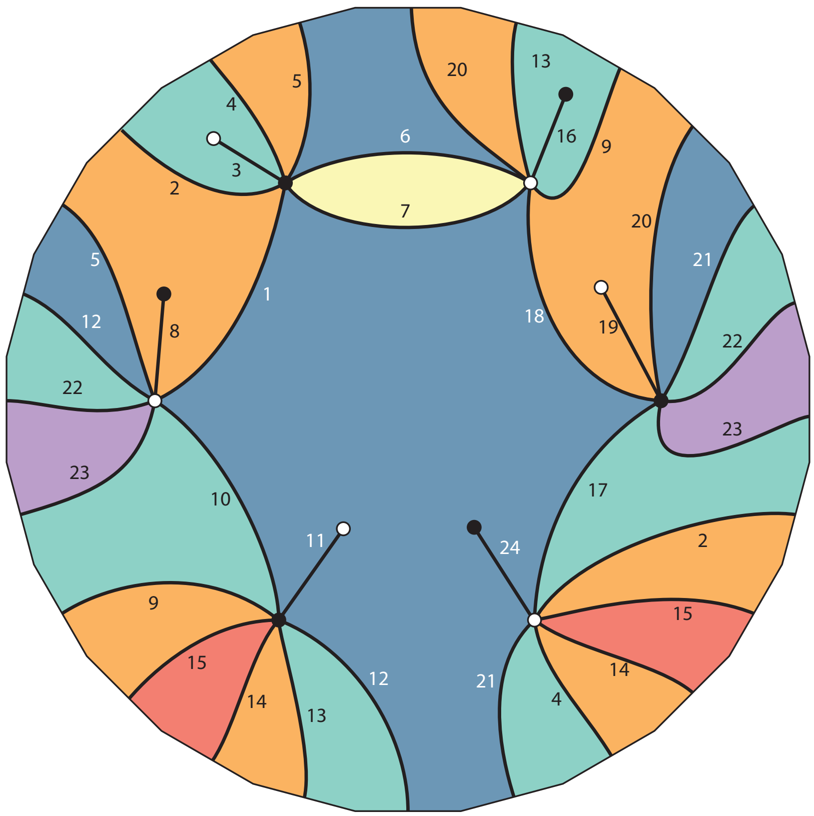

Figure 6.4: Graph for $\Gamma_1(14) \cap \Gamma(2)$

Theorem 6.3.3. *The above steps compute the permutations for the graph associated to* $\Gamma_1(2p) \cap \Gamma(2)$.

Proof. Let $\mathcal{F}_0$ be the fundamental domain for $\Gamma_0 = \Gamma_0(2p) \cap \Gamma(2)$ we constructed in Theorem 6.2.3, consisting of the tiles I, B, B^2, $\ldots$, B^{p-1} and $X = B^m A$ (where $1+4m$ is not invertible mod p). We construct a fundamental domain $\mathcal{F}_1$ for Γ_1 from $n = \frac{1}{2}(p-1)$ copies of $\mathcal{F}_0$. To do so we will find matrices $C(j) \in \Gamma_0 \setminus \Gamma_1$ so that the domain for Γ_1 is $\mathcal{F}_0, C(1)\mathcal{F}_0, \ldots, C(n-1)\mathcal{F}_0$. (For consistency in notation, define $C(0) = I$.)

We desire our domain to be connected, so we will take each $C(j)$ to be of the form $B^k A^{-1} B^{-m}$ with $1 \leq k, m < p$. We know these matrices have the form

$$\begin{pmatrix} 1+4m & -2 \\ 2k-2m+8mk & 1-4k \end{pmatrix}.$$

For j odd, let $m = \frac{1}{2}(j+p)$; for even j, let $m = \frac{1}{2}j$. Choose k so that $k \equiv m(1+4m)^{-1}$ (mod $2p$). This results in $C(j)$ with

$$C(j) \equiv \begin{pmatrix} 2j+1 & -2 \\ 0 & (2j+1)^{-1} \end{pmatrix} \pmod{2p}.$$

(Since $2j+1 \leq p-2$, we know $2j+1$ is invertible mod p.) Apply the $C(j)$ to $\mathcal{F}_0$. Label the edges in $C(0)\mathcal{F}_0$ as they were for Γ_0. For each edge x in $C(0)\mathcal{F}_0$, label the corresponding edge in $C(j)\mathcal{F}_0$ as $x + j(p+1)$.

The labels are assigned in a way to produce the cycles for the black vertices of degree p given in Step 1. For the degree 1 black vertices, we need to check that the black vertex contributed by the tile X and all of its images under the $C(j)$ are still of degree 1. In the proof for Theorem 6.2.3, we found that when rotating counterclockwise about the black vertex in X there is $g \in \Gamma_0$ with $gB^m AB^{-1} \equiv B^m A$ (mod $2p$). Note the upper-left entry in the matrix (6.2.1). Because $1 + 4m = \lambda p$

for some λ, we see that $16m + 5 \equiv 1 \pmod{2p}$, so this matrix is also in Γ_1. Thus, the black vertex in the tile X is represented by the cycle $(p+1)$ for both Γ_0 and Γ_1. For the images of X under the $C(j)$, consider g such that $gC(j)XB^{-1} \equiv C(j)X \pmod{2p}$. The matrix $g = C(j)(XBX^{-1})C(j)^{-1}$ has upper-left entry $(2j+1)(16m+5)(2j+1)^{-1} = 16m + 5 \equiv 1 \pmod{2p}$. Thus each of these matrices is in Γ_1, so each corresponding tile contributes a black vertex of degree 1.

Similarly, we consider the faces of degree 1. For Γ_0, the tile I contributes the degree 1 face (p): We checked that when rotating about the face center ∞, there is a $g \in \Gamma_0$ with $gIA = I$. The matrix $g = A^{-1}$ is also in Γ_1, so the cycle (p) represents a degree 1 face for Γ_1 as well. The images of I under the $C(j)$ also contribute faces of degree 1, because $gC(j)A = C(j)$ implies $g = C(j)A^{-1}C(j)^{-1}$, which is in Γ_1.

Finally, we consider the faces of degree p. We will find their permutations by seeing how they cover the degree p face of Γ_0.

Consider any $\phi_i = m$ and $\phi_{i+1} = k$ such that $1 \leq m, k < p$ with $g = B^k A^{-1} B^{-m} \in \Gamma_0$. Then in Φ, the permutation for the degree p face for Γ_0, edge k follows edge m. Now choose j with $0 \leq j < n$. Because the graph for Γ_1 covers the graph for Γ_0, the edge $m + j(p+1)$ will be followed by an edge of the form $k + j'(p+1)$. We seek a j' for which there is a $g \in \Gamma_1$ with $gC(j)B^m A = C(j')B^k$. In this case,

$$\begin{aligned} g &= C(j')B^k A^{-1} B^{-m} C(j)^{-1} \\ &\equiv \begin{pmatrix} c(j')c(j)^{-1}(1+4m) & * \\ 0 & c(j')^{-1}c(j)(1-4k) \end{pmatrix} \pmod{2p} \end{aligned} \tag{6.3.2}$$

where $c(j) = 2j+1$ and $c(j') = 2j'+1$ are the upper-left entries of $C(j)$ and $C(j')$, and the value of $*$ is unimportant for now. That the lower-left entry is 0 follows from the fact that $B^k A^{-1} B^{-m}$ is in Γ_0. For g to be in Γ_1 we require the diagonal entries to be congruent to ± 1 mod $2p$; i.e., $c(j') \equiv \pm c(j)(1+4m)^{-1} \pmod{2p}$. Given

$C(j)$, m and k we have determined $c(j')$ and $C(j')$, and the corresponding edge is $k + \frac{1}{2}(c(j') - 1)(p + 1)$.

To continue, suppose that in Φ edge $\ell = \phi_{i+2}$ follows edge $k = \phi_{i+1}$, with $g = B^{\ell}A^{-1}B^{-k} \in \Gamma_0$ We want to find the j'' so that the edge $\ell + \frac{1}{2}(c(j'') - 1)(p + 1)$ follows the edge $k + \frac{1}{2}(c(j') - 1)(p + 1)$. Thus we seek a j'' so there is a $g \in \Gamma_1$ with $gC(j')B^kA = C(j'')B^{\ell}$. Then $g = C(j'')B^{\ell}A^{-1}B^{-k}C(j')^{-1}$ has upper-left entry $c(j'')c(j')^{-1}(1 + 4k)$, so we require $c(j'') \equiv c(j')(1 + 4k)^{-1} \pmod{2p}$. Since $c(j') \equiv c(j)(1 + 4m)^{-1} \pmod{2p}$, we have $c(j'') \equiv c(j)(1 + 4m)^{-1}(1 + 4k)^{-1} \pmod{2p}$. If we find the edge ψ_i in the tile $C(j_i)\mathcal{F}_0$, we set $C_i = C(j_i)$ and let c_i be its upper-left entry. Thus, other than considering the case where $1 + \varphi_i$ is not invertible mod p, we can see Step 2(c) of the algorithm as an induction: C_{i+1} is found by multiplying the previous c_i by $u_i = (1 + 4\varphi_i)^{-1}$.

Finally we look at what happens in the case where $1 + 4m = 1 + 4\varphi_i$ is not invertible mod p. When rotating counterclockwise about the face center in B^m we pass through X with the edge $p+1$ without changing the copy of $C(j)\mathcal{F}_0$. The value of c_i will be the same as before, so we set the corresponding $u_i = 1$. Rotating further we needed k so that there is a g in Γ_0 with $gXA = B^k$. Recall the calculation in 6.2.2: the upper-left entry of the matrix is $1 + 8m \equiv -1 \pmod{p}$, so we let $u_{i+1} = -1$.

This concludes the process: we have found a fundamental domain $\mathcal{F}_1$ for Γ_1, labeled the edges in such a way as to produce the cycles for the black vertices listed in the algorithm, and identified the sides of the domain by elements of Γ_1 in such a way as to produce the cycles for the faces given in the algorithm.

$\square$

6.4 $\Gamma(2p)$

Next we use the permutations we found for $\Gamma_1 = \Gamma_1(2p) \cap \Gamma(2)$ to construct those for $\Gamma(2p)$. Let $n = [\Gamma_0(2p) \cap \Gamma(2) : \Gamma_1] = \frac{1}{2}(p-1)$. Let $\nu = [\Gamma(2) : \Gamma_1] = \frac{1}{2}(p^2-1)$ be the number of edges in the graph for Γ_1. Let Φ, φ_i, u_i, C_i and c_i be defined as they were for the Γ_1 algorithm above.

Algorithm 6.4.1. Permutations for $\Gamma(2p)$.

STEP 1 Let $(b_1, b_2, \ldots, b_p)$ be the p-cycle a degree p black vertex of Γ_1. Then, for all $0 \le i < p$, $(b_1 + i\nu, b_2 + i\nu, \ldots, b_p + i\nu)$ is the cycle for a black vertex of $\Gamma(2p)$.

STEP 2 Let (x) be the cycle for a degree 1 black vertex of Γ_1. Note that $x = (p+1) + j(p+1)$ for some $0 \le j < n$. For $1 \le i < p$, set $r_i \equiv 4(i-1)(2j+1)^2 \pmod p$ with $0 \le r_i < p$. Then $(x + r_1\nu, \ldots, x + r_p\nu)$ is the cycle for a black vertex of $\Gamma(2p)$.

STEP 3 Let (f) be the cycle for a degree 1 face of Γ_1. Note that $f = p + j(p+1)$ for some $0 \le j < n$. For $1 \le i < p$, set $r_i \equiv (i-1)(2j+1)^2 \pmod p$ with $0 \le r_i < p$. Then $(f + r_1\nu, \ldots, f + r_p\nu)$ is the cycle for the corresponding face of $\Gamma(2p)$.

STEP 4 Let $\Psi = (\psi_1, \psi_2, \ldots, \psi_p)$ be the cycle for a degree p face of Γ_1. Choose r_1 with $0 \le r_1 < p$. (Each such choice will give a distinct face of $\Gamma(2p)$.) Given r_i, find r_{i+1}, $0 \le r_{i+1} < p$ as follows:

(a) If $1 + 4\varphi_i$ is not invertible mod p, let $r_{i+1} = r_i$, and $r_{i+2} \equiv r_{i+1} - 2(c_{i+1})^2 \pmod p$.

(b) Suppose $1 + 4\varphi_i$ is invertible mod p.

i. If $c_i \ne 1$ and $c_i \ne 1$, choose $r_{i+1} \equiv r_i - c_i + u_i c_i^2 + c_{i+1} \pmod p$.

ii. If $c_i = 1$ and $c_{i+1} \ne 1$, chose $r_{i+1} \equiv r_i + u_i + c_{i+1} \pmod p$.

iii. If $c_i \neq 1$ and $c_{i+1} = 1$, choose $r_{i+1} \equiv r_i + u_i^{-1} - c_i \pmod p$.

iv. If $c_i = c_{i+1} = 1$, choose $r_{i+1} \equiv r_i \pmod p$.

Then $(\psi_1 + r_1\nu, \ldots, \psi_p + r_p\nu)$ is the cycle for the corresponding face of $\Gamma(2p)$.

Example 6.4.2. We compute the permutations associated to $\Gamma(14)$.

First, we compute the cycles arising from the degree 1 black vertices of Γ_1. Note that $\nu = 24$.

The first cycle is (8), with $j = 0$, so $r_i \equiv 4(i-1) \pmod 7$.

r_i	0	4	1	5	2	6	3
$r_i\nu$	0	96	24	120	48	144	72
(8)	8	104	32	128	56	152	80

The next cycle, (16), has $j = 1$, so $r_i \equiv 4(i-1) \cdot 3^2 \equiv i - 1 \pmod 7$.

r_i	0	1	2	3	4	5	6
$r_i\nu$	0	24	48	72	96	120	144
(16)	16	40	64	88	112	136	160

The cycle (24) has $j = 2$, so $r_i \equiv 4(i-1) \cdot 5^2 \equiv 2(i-1) \pmod 7$.

r_i	0	2	4	6	1	3	5
$r_i\nu$	0	48	96	144	24	72	120
(24)	24	72	120	168	48	96	144

Each degree 7 black vertex of $\Gamma_1(14) \cap \Gamma(2)$ will contribute seven vertices to $\Gamma(14)$. For example, the cycle $(7, 6, 5, 4, 3, 2, 1)$ contributes itself as well as $(31, 30, \ldots, 25)$, $(55, 54, \ldots, 49)$, and so on.

Thus, the cycles associated to the black vertices of $\Gamma(14)$ are

$(7, 6, 5, 4, 3, 2, 1)$	$(15, 14, 13, 12, 11, 10, 9)$	$(23, 22, 21, 20, 19, 18, 17)$
$(31, 30, 29, 28, 27, 26, 25)$	$(39, 38, 37, 36, 35, 34, 33)$	$(47, 46, 45, 44, 43, 42, 41)$
$(55, 54, 53, 52, 51, 50, 49)$	$(63, 62, 61, 60, 59, 58, 57)$	$(71, 70, 69, 68, 67, 66, 65)$
$(79, 78, 77, 76, 75, 74, 73)$	$(87, 86, 85, 84, 83, 82, 81)$	$(95, 94, 93, 92, 91, 90, 89)$
$(103, 102, 101, 100, 99, 98, 97)$	$(111, 110, 109, 108, 107, 106, 105)$	$(119, 118, 117, 116, 115, 114, 113)$
$(127, 126, 126, 124, 123, 122, 121)$	$(135, 134, 133, 132, 131, 130, 129)$	$(143, 142, 141, 140, 139, 138, 137)$
$(151, 150, 149, 148, 147, 146, 145)$	$(159, 158, 157, 156, 155, 154, 153)$	$(167, 166, 165, 164, 163, 162, 161)$
$(8, 104, 32, 128, 56, 152, 80)$	$(16, 40, 64, 88, 112, 136, 160)$	$(24, 72, 120, 168, 48, 96, 144)$

Next we compute the cycles arising from the degree 1 faces of Γ_1.

The cycle (7) has $j = 0$, so $r_i = i - 1$.

r_i	0	1	2	3	4	5	6
$r_i\nu$	0	24	48	72	96	120	144
(7)	7	31	55	79	103	127	151

The cycle (15) has $j = 1$, so $r_i \equiv (i-1) \cdot 3^2 \equiv 9(i-1) \pmod 7$.

r_i	0	2	4	6	1	3	5
$r_i\nu$	0	48	96	144	24	72	120
(15)	15	63	111	159	39	87	135

The cycle (23) has $j = 2$, so $r_i \equiv 25(i-1) \pmod 7$.

r_i	0	4	1	5	2	6	3
$r_i\nu$	0	96	24	120	48	144	72
(23)	23	119	47	143	71	167	95

Finally, we can compute the cycles for the faces of $\Gamma(2p)$ which cover the degree 7 faces of $\Gamma_1(14)$. Here we will show two examples. For the first, begin with $\Psi_1 = (1, 11, 12, 6, 21, 24, 18)$ and set $r_1 = 0$. We get

ψ_{1_i}	1	11	12	6	21	24	18
u_i	3	-1	5	-5	1	-1	-3
c_i	1	3	3	1	5	5	5
r_i	0	6	4	4	4	4	3
$\psi_i + r_i\nu$	1	155	108	102	117	120	90

so the cycle for the corresponding face of $\Gamma(14)$ is $(1, 155, 108, 102, 117, 120, 90)$. We repeat this computation beginning with each choice of r_1 to construct the cycles for seven different faces of $\Gamma(14)$.

Another example, this time using $\Psi_2 = (2, 9, 19, 20, 14, 5, 8)$ and setting $r_1 = 4$.

ψ_{2_i}	2	9	19	20	14	5	8
u_i	-3	3	-1	5	-5	1	-1
c_i	1	3	5	5	3	1	1
r_i	4	4	5	1	5	6	6
$\psi_i + r_i\nu$	98	105	139	44	134	149	152

and thus the corresponding cycle is $(98, 105, 139, 44, 134, 149, 152)$.

Theorem 6.4.3. *The above steps compute the permutations for the graph associated to* $\Gamma(2p)$.

Proof. The proof will follow a pattern similar to the proof for the $\Gamma_1(2p) \cap \Gamma(2)$ algorithm above: We will choose a fundamental domain for $\Gamma(2p)$, label the edges appropriately, and show that we can pair the edges by elements of $\Gamma(2p)$.

Let $\mathcal{F}_1$ be the fundamental domain we constructed for $\Gamma_1 = \Gamma_1(2p) \cap \Gamma(2)$, consisting of n copies of the domain for Γ_0. We can construct a domain $\mathcal{F}$ for $\Gamma(2p)$ as p copies of $\mathcal{F}_1$ by translating $\mathcal{F}_1$ by powers of A, so the domain for $\Gamma(2p)$ will be $A^0\mathcal{F}_1$, $\ldots$, $A^{p-1}\mathcal{F}_1$. We label the ν edges in $A^0\mathcal{F}_1$ as they were for Γ_1. For each edge x in $A^0\mathcal{F}_1$, label the corresponding edge in $A^i\mathcal{F}_1$ as $x + i\nu$. This choice of labeling will yield the cycles for the black vertices of $\Gamma(2p)$ described in Step 1.

Moving on to Step 2, we will now construct the cycles for the black vertices of $\Gamma(2p)$ that cover the degree 1 cycles of Γ_1. Consider first the cycle $(p+1)$. This edge is found in the tile $X = B^m A$, where $1 + 4m$ is not invertible mod p. We showed previously that this vertex has degree 1 for the graphs of both Γ_0 and Γ_1, because $gXB^{-1} = X$ implies $g \in \Gamma_1$. However, this vertex will not have degree 1 in the graph for $\Gamma(2p)$. Recall the calculation in 6.2.1:

$$g = XBX^{-1} = \begin{pmatrix} 16m+5 & -8 \\ 2(1+4m)^2 & -16m-3 \end{pmatrix} \equiv \begin{pmatrix} 1 & -8 \\ 0 & 1 \end{pmatrix} \pmod{2p}.$$

Instead, the vertex represented by $(x) = (p+1)$ in Γ_1 will be covered by a degree p vertex for $\Gamma(2p)$. The edge labeled x is in the tile $A^{r_1}X$ with $r_1 = 0$; we will find r_2 so that this tile is glued to the tile $A^{r_2}X$. More generally, given the edge labeled $x + r_i\nu$ in the tile $A^{r_i}X$, we will find r_{i+1} so that the next edge in the cycle is $x + r_{i+1}\nu$. This happens when there is a $g \in \Gamma(2p)$ with $gA^{r_i}XB^{-1} = A^{r_{i+1}}X$. In this case we have

$$\begin{aligned} g &= A^{r_{i+1}}XBX^{-1}A^{-r_i} \\ &\equiv \begin{pmatrix} 1 & 2r_{i+1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -8 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -2r_i \\ 0 & 1 \end{pmatrix} \pmod{2p} \\ &\equiv \begin{pmatrix} 1 & -2r_i - 8 + 2r_{i+1} \\ 0 & 1 \end{pmatrix} \pmod{2p} \end{aligned} \tag{6.4.1}$$

so we see that $g \in \Gamma(2p)$ when $r_{i+1} \equiv r_i + 4 \pmod{p}$. Since we begin with $r_1 = 0$, we see inductively that $r_i \equiv 4(i-1) \pmod 2$. Thus, for these choices of r_i, the cycle $(x+r_1\nu, x+r_2\nu, \ldots, x+r_p\nu)$ represents a black vertex of $\Gamma(2p)$ which covers the cycle (x) of Γ_1.

Now we consider the black vertices of $\Gamma(2p)$ that cover the other degree 1 black vertices of Γ_1. Consider the case of a black vertex in the tile $C(j)X$ with $1 \le j < n$, which is represented by the cycle $(x) = ((p+1) + j(p+1))$. We found that these vertices have degree 1 for Γ_1 because, rotating counterclockwise about x, there is a $g \in \Gamma_1$ with $gC(j)XB^{-1} = C(j)X$. Suppose we have the corresponding vertex in the tile $A^{r_i}C(j)X$. Again, we must find r_{i+1} so that there is a $g \in \Gamma(2p)$ with $gA^{r_i}C(j)XB^{-1} = A^{r_{i+1}}C(j)X$. In this case we have

$$\begin{aligned} g &= A^{r_{i+1}}C(j)XBX^{-1}C(j)^{-1}A^{-r_i} \\ &\equiv \begin{pmatrix} 1 & 2r_{i+1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -2c(j)^2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -2r_i \\ 0 & 1 \end{pmatrix} \pmod{2p} \\ &\equiv \begin{pmatrix} 1 & -2r_i - 8c(j)^2 + 2r_{i+1} \\ 0 & 1 \end{pmatrix} \pmod{2p} \end{aligned} \tag{6.4.2}$$

which is in $\Gamma(2p)$ when $r_{i+1} \equiv r_i + 4c(j)^2 \pmod p$. Again, beginning with $r_1 = 0$, we see inductively that $r_i \equiv 4(i-1)c(j)^2 \pmod p$.

Note that because we assigned $C(0) = I$, we have $c(0) = 1$, so we have a consistent result with the previous case: in general, if we let $(x) = ((p+1) + j(p+1))$ with $0 \le j < n$, we can construct the cycle for a black vertex of $\Gamma(2p)$ which covers (x) as $(x + r_1\nu, \ldots, x + r_p\nu)$ where $r_i \equiv 4(i-1)c(j)^2 \pmod p$.

We now proceed to Step 3, where we consider the faces which cover the degree 1 faces of Γ_1. We checked that when rotating about the face center ∞ there is a $g \in \Gamma_1$ with $gIA = I$. The matrix $g = A^{-1}$ is not in $\Gamma(2p)$, so this face will be covered by a p cycle. If we start with the edge x in the tile A^{r_i}, we find r_{i+1} so that there is $g \in \Gamma(2p)$ with $gA^{r_i} \cdot A = A^{r_{i+1}}$. This yields $g = A^{r_{i+1}-r_i-1}$, which is in $\Gamma(2p)$ when $r_{i+1} \equiv r_i + 1 \pmod{p}$. Beginning with $r_1 = 0$, we find inductively that $r_i \equiv i \pmod{p}$, which produces the cycle $(p, p+\nu, \ldots, p+(p-1)\nu)$.

The other degree 1 faces of Γ_1 are found in the tiles $C(j) \cdot I$. Beginning with the edge f in the tile $A^{r_i}C(j)$ above such a face, we seek r_{i+1} so there is a $g \in \Gamma(2p)$ with $gA^{r_i}C(j)A = A^{r_{i+1}}C(j)$. In this case we have

$$\begin{aligned} g &= A^{r_{i+1}}C(j)A^{-1}C(j)^{-1}A^{-r_i} \\ &\equiv \begin{pmatrix} 1 & -2r_i - 2c(j)^2 + 2r_{i+1} \\ 0 & 1 \end{pmatrix} \pmod{2p} \end{aligned}$$

which is in $\Gamma(2p)$ when $r_{i+1} \equiv r_i + c(j)^2 \pmod{p}$. Starting with $r_1 = 0$ we find inductively that $r_i \equiv ic(j)^2 \pmod{2p}$. Again, because we have defined $C(0) = I$, this is consistent with the previous result; if we let $(f) = (p + j(p+1))$ with $0 \le j < n$, we can construct the cycle for a face of $\Gamma(2p)$ above (f) as $(f + r_1\nu, \ldots, f + r_p\nu)$ where $r_i \equiv (i-1)c(j)^2 \pmod{p}$.

Now we will consider the faces computed in Step 4. Let $\Phi = (\varphi_1, \ldots, \varphi_p)$ denote the cycle for the degree p face of Γ_0, and let $\Psi = (\psi_1, \ldots, \psi_p)$ be the cycle for one of the degree p faces of Γ_1: We will construct a the cycle for a face of $\Gamma(2p)$ of the form $(\psi_1 + r_1\nu, \ldots, \psi_p + r_p\nu)$. Select a value of r_1, with $0 \le r_i < p$. Given r_i, our goal is to find r_{i+1} so that there is a $g \in \Gamma(2p)$ with $gA^{r_i}C_iB^{\varphi_i}A = A^{r_{i+1}}C_{i+1}B^{\varphi_{i+1}}$.

First consider the general case in Step 4(b), where $1 + 4\varphi_i$ is invertible mod p, and let $u_i = (1 + 4\varphi_i)^{-1}$ as in the algorithm for the Γ_1 permutations. Recall from 6.3.2 that in this case we have $g \in \Gamma_1$ with $gC_iB^{\varphi_i}A = C_{i+1}B^{\varphi_{i+1}}$, so

$$\begin{aligned} g &= C_{i+1}B^{\varphi_{i+1}}A^{-1}B^{-\varphi_i}C_i^{-1} \\ &\equiv \begin{pmatrix} c_{i+1}c_i^{-1}u_i^{-1} & * \\ 0 & (c_{i+1})^{-1}c_iu_i \end{pmatrix} \pmod{2p} \end{aligned}$$

We know $g \in \Gamma_1$, so $c_{i+1}c_i^{-1}u_i^{-1} = \pm 1$ and $*$ is even. Let $\kappa = c_{i+1}c_i^{-1}u_i^{-1} = (c_{i+1})^{-1}c_i u_i$ and denote $*$ as $-2\kappa e_{i+1}$; factoring out κ, the above matrix becomes

$$\kappa \begin{pmatrix} 1 & -2e_{i+1} \\ 0 & 1 \end{pmatrix} \pmod{2p} \tag{6.4.3}$$

To consider edges in $\Gamma(2p)$ which cover these edges, we want $g \in \Gamma(2p)$ with

$$gA^{r_i}C_iB^{\varphi_i}A = A^{r_{i+1}}C_{i+1}B^{\varphi_{i+1}}.$$

In this case

$$\begin{aligned} g &= A^{r_{i+1}}C_{i+1}B^{\varphi_{i+1}}A^{-1}B^{-\varphi_i}C_i^{-1}A^{-r_i} \\ &\equiv \kappa \begin{pmatrix} 1 & 2r_{i+1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -2e_{i+1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -2r_i \\ 0 & 1 \end{pmatrix} \pmod{2p} \\ &\equiv \kappa \begin{pmatrix} 1 & -2r_i - 2e_{i+1} + 2r_{i+1} \\ 0 & 1 \end{pmatrix} \pmod{2p} \end{aligned}$$

Thus, for g to be in $\Gamma(2p)$, we require $r_{i+1} \equiv r_i + e_{i+1} \pmod{p}$.

Next we must determine the value of e_{i+1} in 6.4.3. This will depend on whether one or both of the C_i are I.

Case 1. Suppose $C_i, C_{i+1} \neq I$. Then we have

$$\begin{aligned} C_{i+1}B^{\varphi_{i+1}}A^{-1}B^{-\varphi_i}C_i^{-1} &\equiv \begin{pmatrix} c_{i+1} & -2 \\ 0 & (c_{i+1})^{-1} \end{pmatrix} \begin{pmatrix} u_i^{-1} & -2 \\ 0 & u_i \end{pmatrix} \begin{pmatrix} c_i^{-1} & 2 \\ 0 & c_i \end{pmatrix} \pmod{2p} \\ &\equiv \begin{pmatrix} \kappa & -2(-c_{i+1}u_i^{-1} + c_ic_{i+1} + u_ic_i) \\ 0 & \kappa \end{pmatrix} \pmod{2p} \end{aligned}$$

So $e_{i+1} = \frac{1}{\kappa}(-c_{i+1}u_i^{-1} + c_ic_{i+1} + u_ic_i) = -c_i + u_ic_i^2 + c_{i+1}$.

Case 2. Suppose $C_i = I$, but $C_{i+1} \neq I$. Then we have

$$\begin{aligned}
C_{i+1}B^{\varphi_{i+1}}A^{-1}B^{-\varphi_i}C_i^{-1} &\equiv \begin{pmatrix} c_{i+1} & -2 \\ 0 & (c_{i+1})^{-1} \end{pmatrix} \begin{pmatrix} u_i^{-1} & -2 \\ 0 & u_i \end{pmatrix} \pmod{2p} \\
&\equiv \begin{pmatrix} c_{i+1}u_i^{-1} & -2(c_{i+1}+u_i) \\ 0 & (c_{i+1})^{-1}u_i \end{pmatrix} \pmod{2p} \\
&\equiv \begin{pmatrix} \kappa & -2(c_{i+1}+u_i) \\ 0 & \kappa \end{pmatrix} \pmod{2p}
\end{aligned}$$

where $\kappa = c_{i+1}u_i^{-1} = (c_{i+1})^{-1}u_i$. Then $e_{i+1} = \frac{1}{\kappa}(c_{i+1}+u_i) = u_i + c_{i+1}$.

Case 3. Suppose $C_i \neq I$, but $C_{i+1} = I$. Then we have

$$\begin{aligned}
C_{i+1}B^{\varphi_{i+1}}A^{-1}B^{-\varphi_i}C_i^{-1} &\equiv \begin{pmatrix} u_i^{-1} & -2 \\ 0 & u_i \end{pmatrix} \begin{pmatrix} c_i^{-1} & 2 \\ 0 & c_i \end{pmatrix} \pmod{2p} \\
&\equiv \begin{pmatrix} c_i^{-1}u_i^{-1} & -2(-u_i^{-1}+c_i) \\ 0 & u_ic_i \end{pmatrix} \pmod{2p} \\
&\equiv \begin{pmatrix} \kappa & -2(-u_i^{-1}+c_i) \\ 0 & \kappa \end{pmatrix} \pmod{2p}
\end{aligned}$$

where $\kappa = c_i^{-1}u_i^{-1} = u_ic_i$. Then $e_{i+1} = \frac{1}{\kappa}(-u_i^{-1}+c_i) = -c_i + u_i^{-1}$.

Case 4. Suppose $C_{i+1} = C_i = I$. Then

$$C_{i+1}B^{\varphi_{i+1}}A^{-1}B^{-\varphi_i}C_i^{-1} \equiv \begin{pmatrix} u_i^{-1} & -2 \\ 0 & u_i \end{pmatrix}$$

Then $\kappa = u_i^{-1}$ and $e_{i+1} = \frac{1}{u_i^{-1}} = u_i$.

The above cases constitute Step 4(b) of the algorithm.

Finally we consider Step 4(a), the case where $1 + 4\varphi_i$ is not invertible. Rotating around the face center we encounter the edge of the fundamental domain in the tile

C_iX, and so $u_i = 1$, $C_{i+1} = C_i$, and $r_{i+1} = r_i$. From there, we require $g \in \Gamma(2p)$ so that $gA^{r_{i+1}}C_{i+1}B^{\varphi_i}A^2 = A^{r_{i+2}}C_{i+2}B^{\varphi_{i+2}}$, and thus

$$g = A^{r_{i+2}}C_{i+2}B^{\varphi_{i+1}}A^{-2}B^{-\varphi_i}(C_{i+1})^{-1}A^{-r_{i+1}}.$$

Recall also that in this case $u_{i+1} = -1$. Because $c_{i+2} = u_{i+1}c_{i+1}$, and the c_i are defined only up to sign, we have $c_{i+2} = c_i$. Using these and referring to 6.2.2 and the lines that follow, we have, for the case $C_i \neq I$,

$$\begin{aligned} C_{i+2}B^{\varphi_{i+1}}A^{-2}B^{-\varphi_i}(C_{i+1})^{-1} &\equiv \begin{pmatrix} c_i & -2 \\ 0 & c_i^{-1} \end{pmatrix} \begin{pmatrix} -1 & -4 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} c_i^{-1} & 2 \\ 0 & c_i \end{pmatrix} \pmod{2p} \\ &\equiv \begin{pmatrix} -1 & -4c_i^2 \\ 0 & -1 \end{pmatrix} \pmod{2p} \end{aligned}$$

Thus $\kappa = -1$ and $e_{i+1} = -2c_i^2$.

In the case $C_i = I$, we have

$$C_{i+2}B^{\varphi_{i+1}}A^{-2}B^{-\varphi_i}(C_{i+1})^{-1} \equiv \begin{pmatrix} -1 & -4 \\ 0 & -1 \end{pmatrix}$$

and thus $e_{i+1} = -2$, which is consistent with the above result.

Thus, we have Step 4 of the algorithm: using these values for e_{i+1}, and letting $r_{i+1} = r_i + e_{i+1}$, we have the cycle for a face of $\Gamma(2p)$ as $(\psi_1 + r_1\nu, \ldots, \psi_p + r_p\nu)$.

This concludes the process: we have found a fundamental domain $\mathcal{F}$ for $\Gamma(2p)$, labeled the edges in such a way as to produce the cycles for the black vertices listed in the algorithm, and identified the sides of the domain by elements of $\Gamma(2p)$ in such a way as to produce the cycles for the faces given in the algorithm. $\square$

Remark 6.4.4. The algorithms in this chapter have produced the permutations associated to $\Gamma_0(2p)$, $\Gamma_1(2p)$, and $\Gamma(2p)$. Notice that in the course of the proofs we have also found the side-pairing transformations for their fundamental domains; by

Theorem 19 in Section 28 of Ford [3], these generate the groups. Thus, we have also found generators for each of these groups in terms of A and B.

6.5 Future Projects

We have described permutations for the case of $\Gamma(2p)$; it is hopeful that these methods could be employed to work with $\Gamma(2n)$ for general n. Cases currently being considered are $\Gamma(2^k)$ and $\Gamma(2pq)$. The difficulty in working with $\Gamma(2n)$ with the above methods arises because as we increase the number of prime factors in $2n$, we increase both the difficulty of the calculations and the complexity of the fundamental domain for $\Gamma_0(2n) \cap \Gamma(2)$.

Also, in Section 5.4 we made use of the generators for $\Gamma(2n)$ in terms of A and B. These are found for $\Gamma(2p)$ as a consequence of the proofs in this section, but it would be useful to have a more direct computation to find such generators.

Finally, we can see immediately a way to visually display a graph for $\Gamma_0(2p) \cap \Gamma(2)$ given the permutations. There is a clear pattern in the graphs for $\Gamma_1(2p) \cap \Gamma(2)$ that can probably be formalized. Though it would be impractical for all but the smallest values of p, there may be a way to sketch graphs for $\Gamma(2p)$ as well.

Appendix A

EXAMPLES OF GRAPHS OF HECKE GROUPS

In this section we provide the graphs corresponding to several of the Hecke congruence groups, ordered by level. Refer to the "List of Figures" beginning on page x as a guide for this section. For some of these examples, the corresponding fundamental domains can be found in Appendix B. Some graphs for such groups have appeared as examples in the body of the thesis; these include $\Gamma_0(6) \cap \Gamma(2)$ on page 16, $\Gamma_0(10) \cap \Gamma(2)$ on page 35, $\Gamma_0(14) \cap \Gamma(2)$ on page 65, and $\Gamma_1(14) \cap \Gamma(2)$ on page 72. Graphs for $\Gamma_0(22) \cap \Gamma(2)$ and $\Gamma_1(22) \cap \Gamma(2)$ appear in Appendix C.2.

These examples were created primarily by first constructing a fundamental domain for the underlying group, finding side-pairing transformations to discover the permutations, calculating the genus on which the graph lies, and then attempting to arrange the vertices and edges into a recognizable pattern. The graphs and domains for levels 10 and 26 can be constructed using the algorithms in Chapter 6. For the other levels the construction is similar but is complicated by the additional number of prime factors.

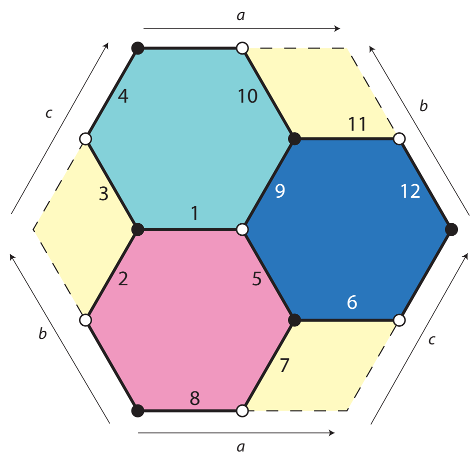

Figure A.1: Graph for $\Gamma(6)$; domain appears in Figure B.1

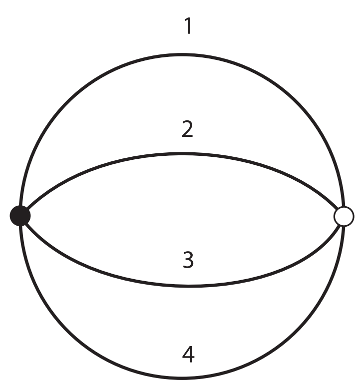

Figure A.2: Graph for $\Gamma_0(8) \cap \Gamma(2)$

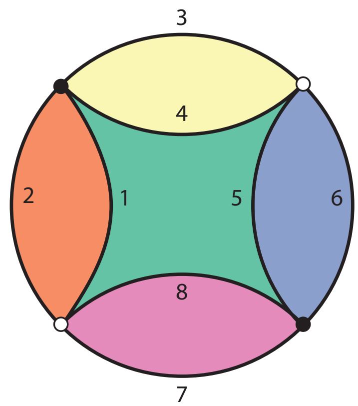

Figure A.3: Graph for $\Gamma_1(8) \cap \Gamma(2)$; domain appears in Figure B.2

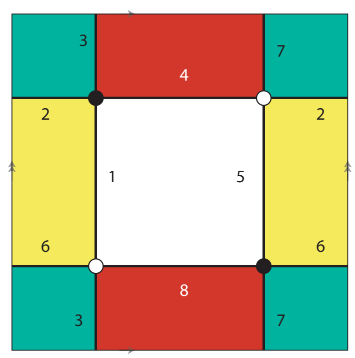

Figure A.4: Graph for $\Gamma_0(8) \cap \Gamma(4)$

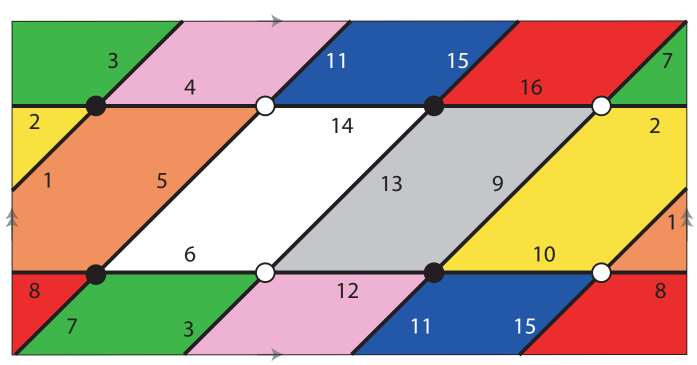

Figure A.5: Graph for $\Gamma_1(8) \cap \Gamma(4)$

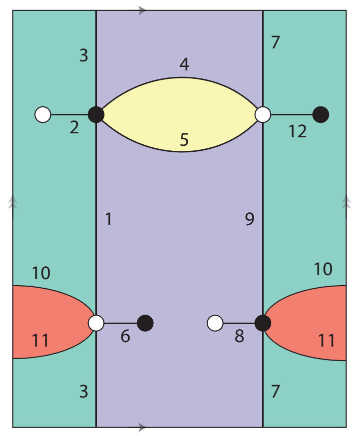

Figure A.6: Graph for $\Gamma_1(10) \cap \Gamma(2)$; domain appears in Figure B.4

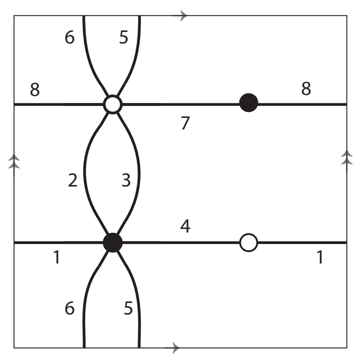

Figure A.7: Graph for $\Gamma_0(12) \cap \Gamma(2)$

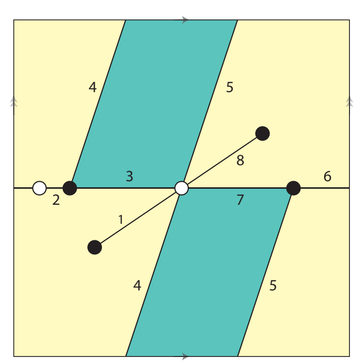

Figure A.8: Graph for $\Gamma^0(12) \cap \Gamma(2)$; domain appears in Figure B.5

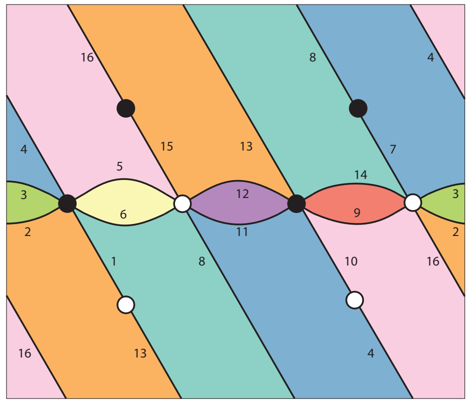

Figure A.9: Graph for $\Gamma_1(12) \cap \Gamma(2)$; domain appears in Figure B.6

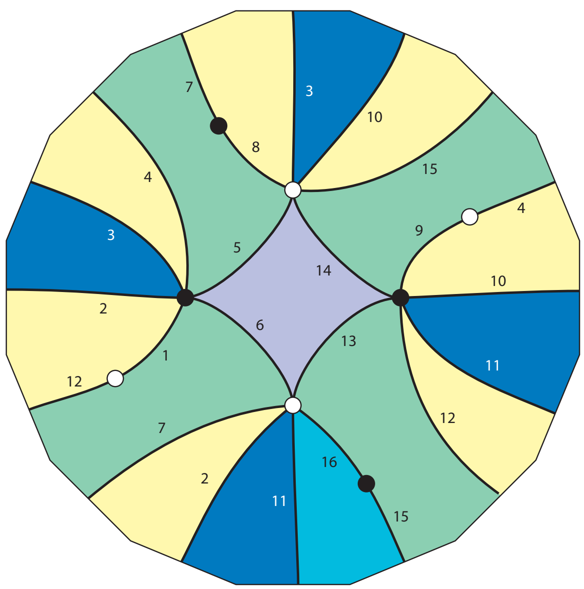

Figure A.10: Graph for $\Gamma_0(12) \cap \Gamma(4)$

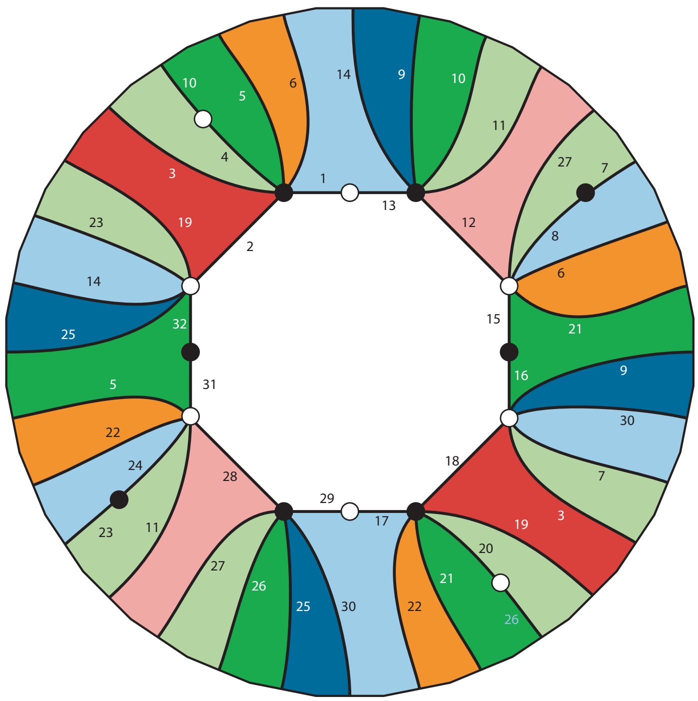

Figure A.11: Graph for $\Gamma_1(12) \cap \Gamma(4)$

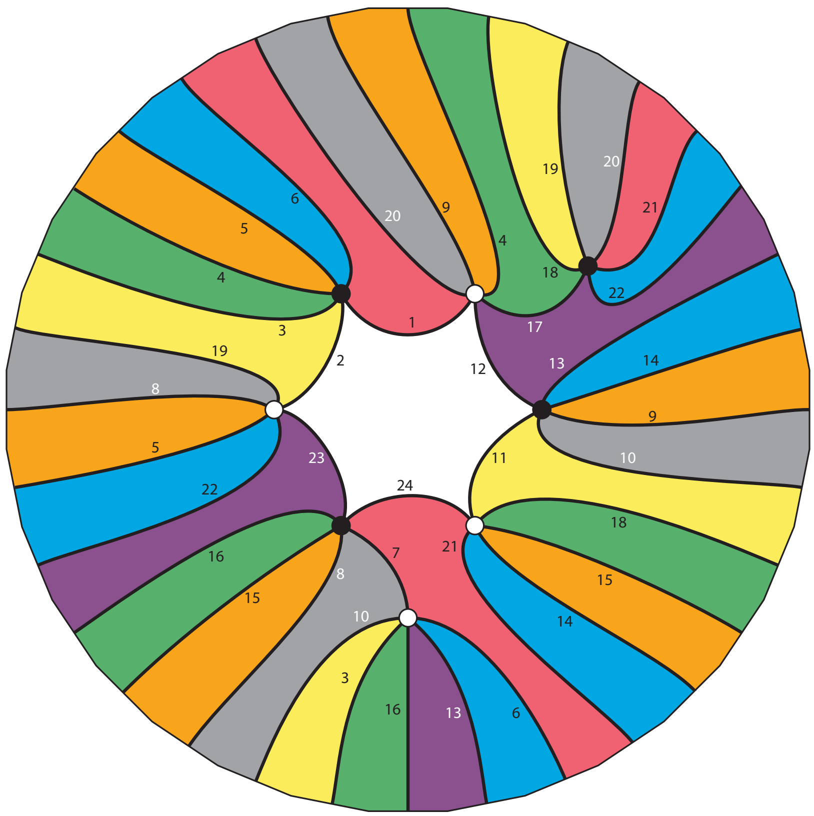

Figure A.12: Graph for $\Gamma_0(12) \cap \Gamma(6)$

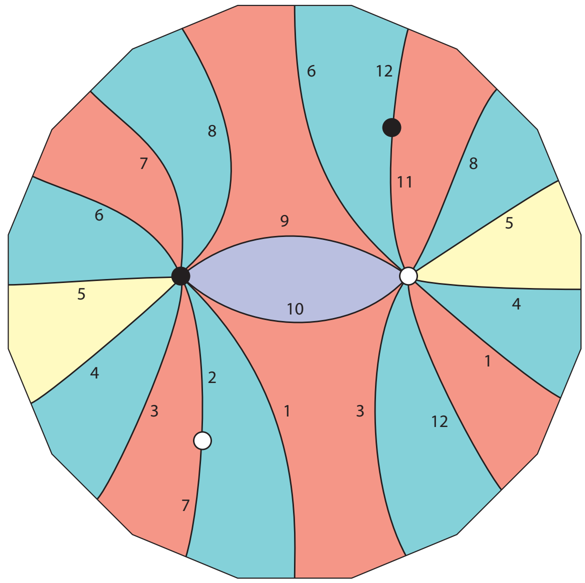

Figure A.13: Graph for $\Gamma_0(20) \cap \Gamma(2)$

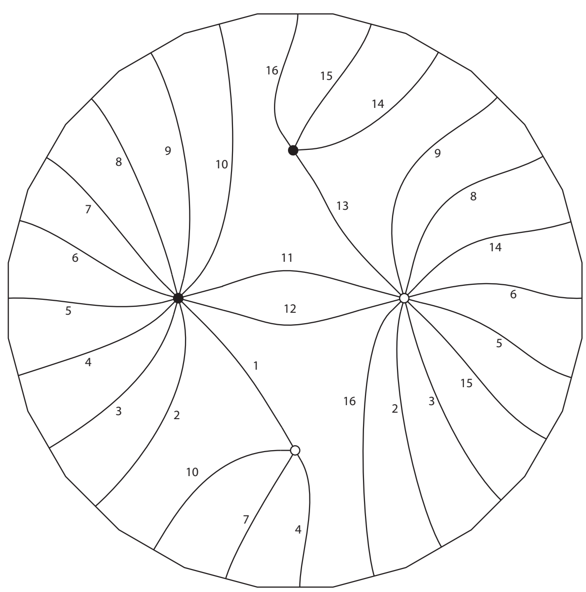

Figure A.14: Graph for $\Gamma_0(24) \cap \Gamma(2)$

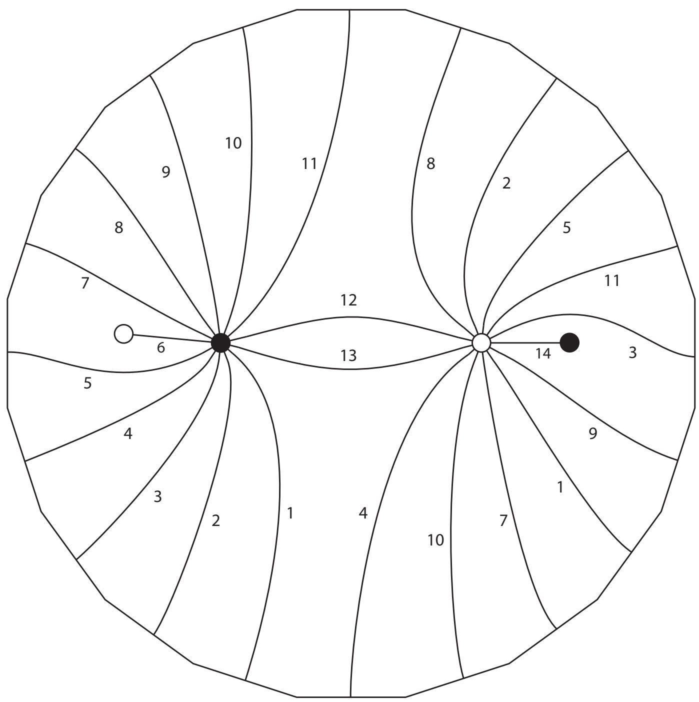

Figure A.15: Graph for $\Gamma_0(26) \cap \Gamma(2)$

Appendix B

EXAMPLES OF FUNDAMENTAL DOMAINS

In this section we provide examples of fundamental domains for Hecke groups in the manner described in Definition 2.3.2. The corresponding graphs are referred to in the captions below each graph; for graphs shown in color the colors are consistent with those in the corresponding domain. The edges of the graph are labeled in the domain with the same numbering; for example, the edge labeled 1 in a graph will be labeled as $e1$ in the corresponding domain. The other paired sides are labeled on the real axis as x_i. Most of the graphs shown in the thesis were created by first finding the domains shown in this section. Several domains had to be omitted because of their size; they would not be readable if displayed on a single page and would be more confusing if spread over several pages.

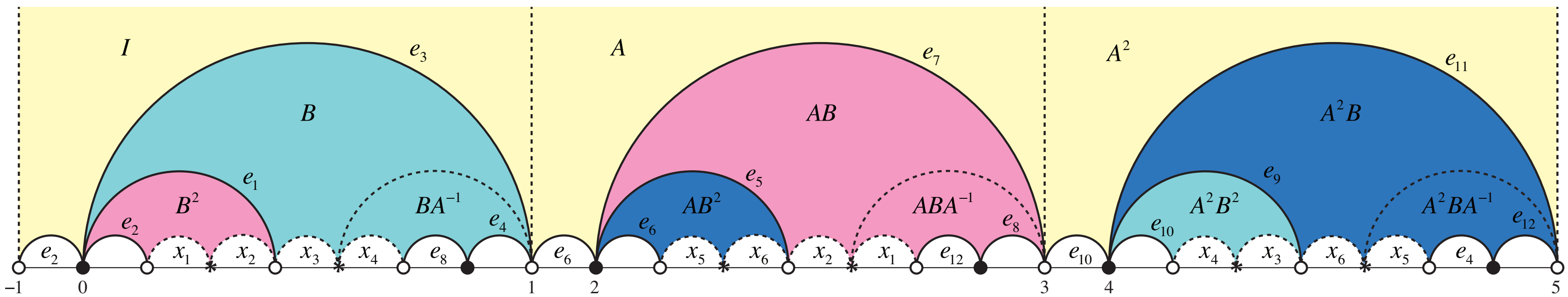

Figure B.1: Fundamental domain for $\Gamma(6)$; graph in Figure A.1

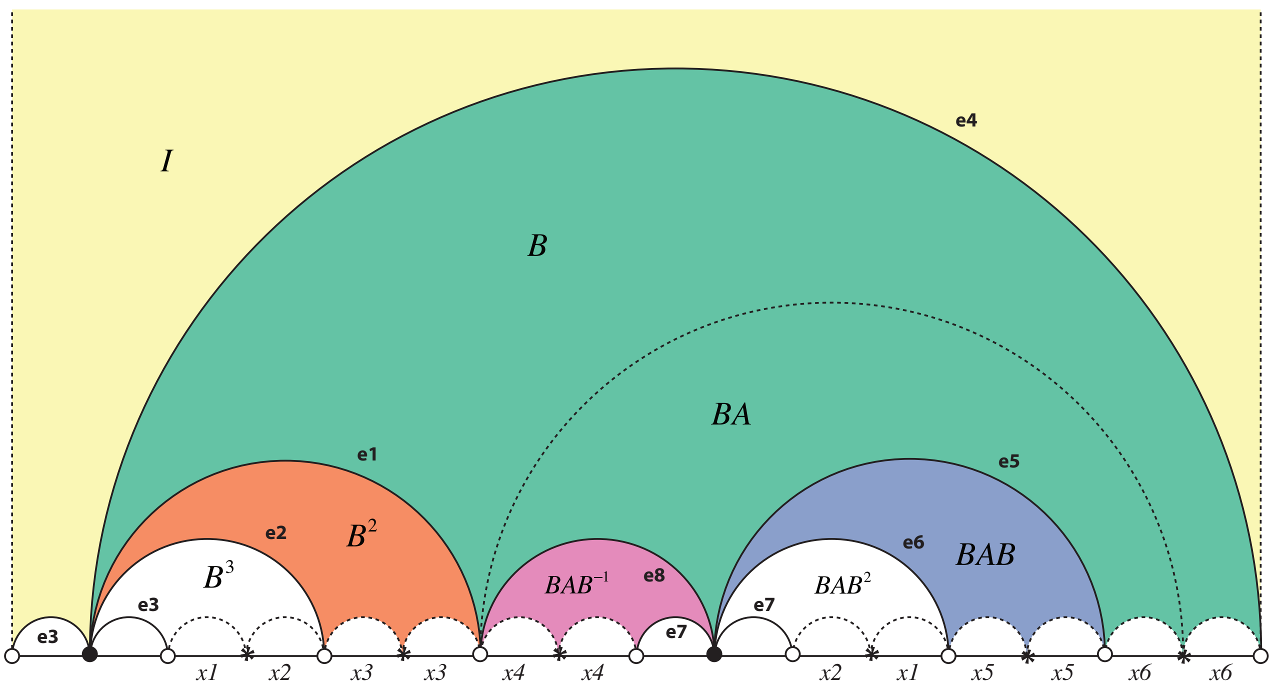

Figure B.2: Fundamental domain for $\Gamma_1(8) \cap \Gamma(2)$; graph in Figure A.3

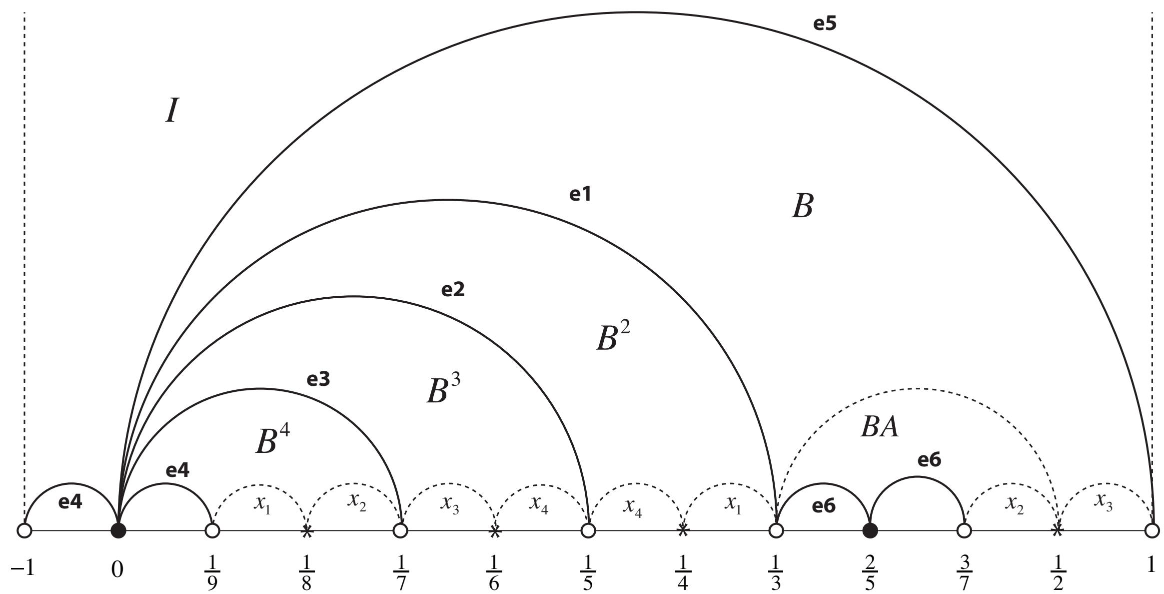

Figure B.3: Fundamental domain for $\Gamma_0(10) \cap \Gamma(2)$; graph in Figure 4.6

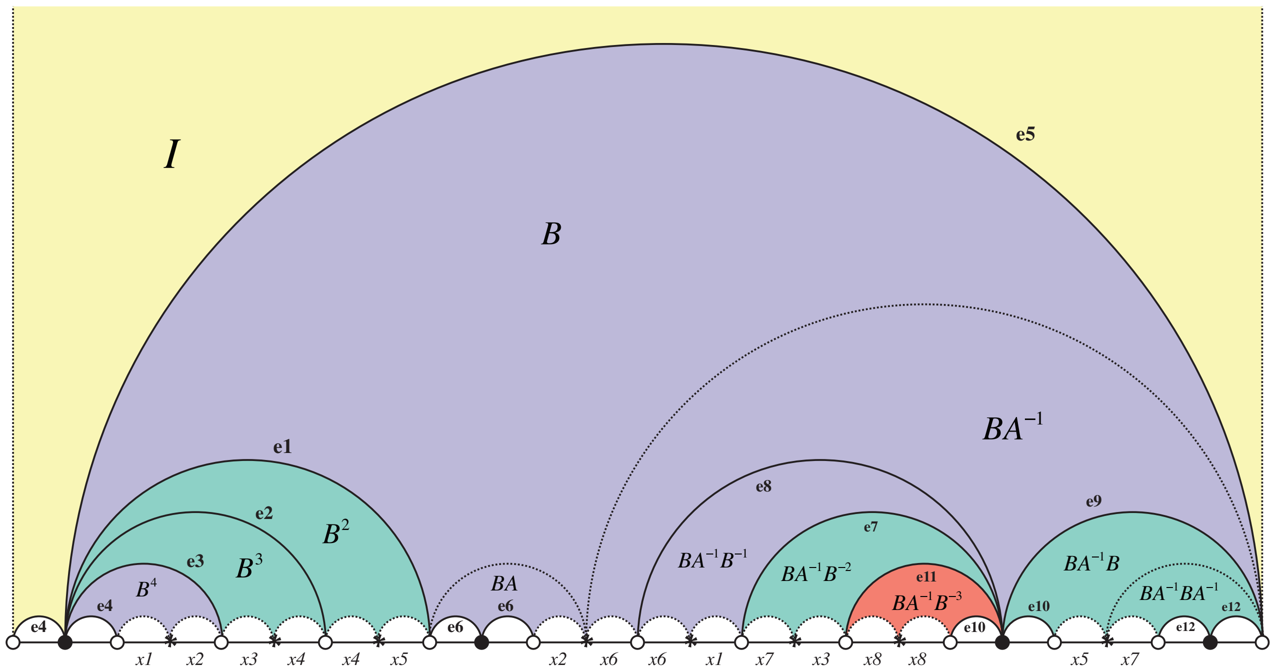

Figure B.4: Fundamental domain for $\Gamma_1(10) \cap \Gamma(2)$; graph in Figure A.6

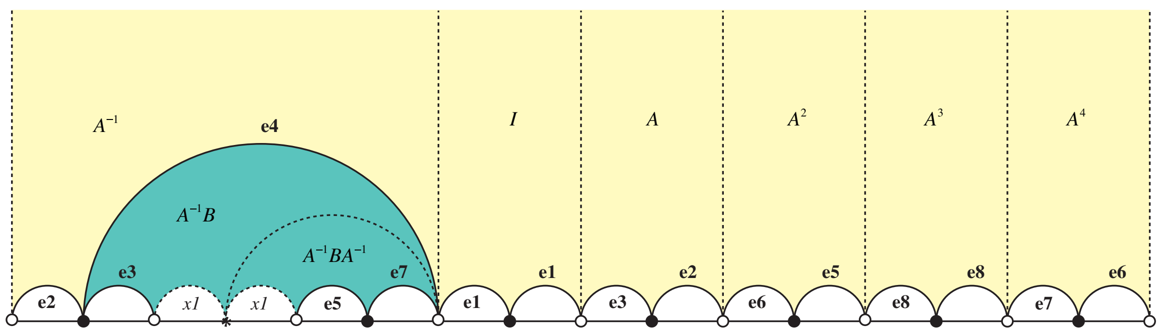

Figure B.5: Fundamental domain for $\Gamma^0(12) \cap \Gamma(2)$; graph in Figure A.8

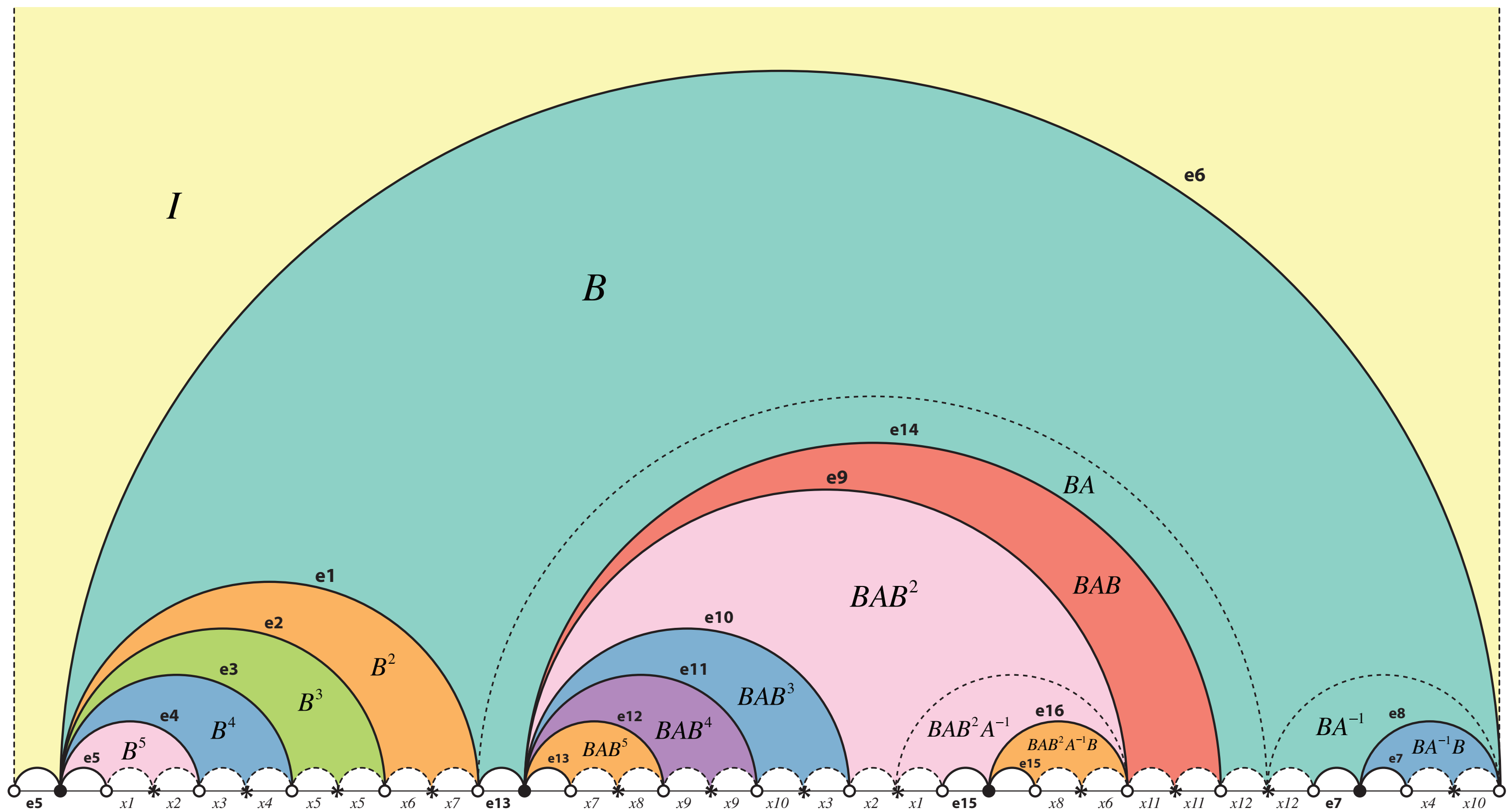

Figure B.6: Fundamental domain for $\Gamma_1(12) \cap \Gamma(2)$; graph in Figure A.9

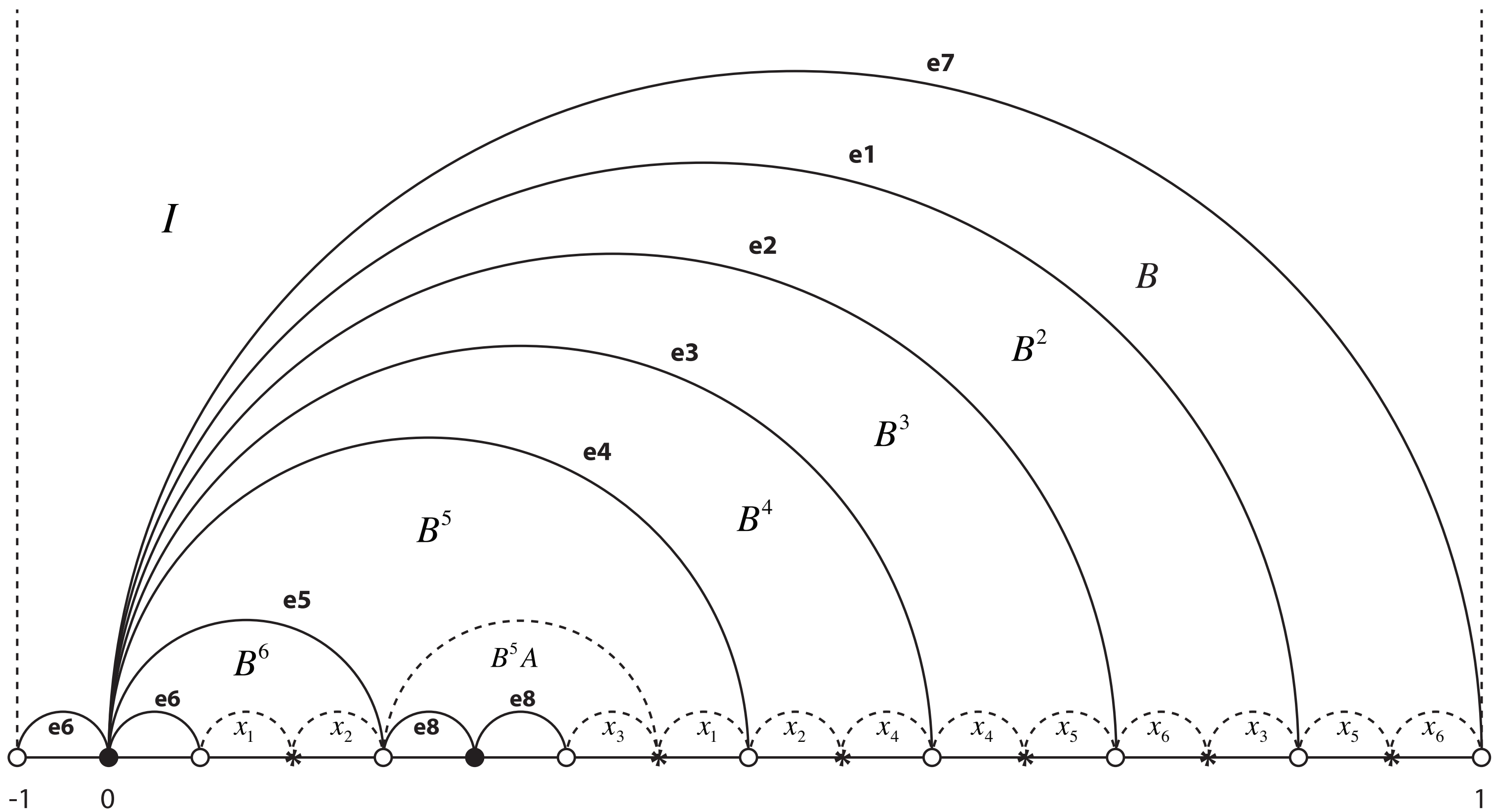

Figure B.7: Fundamental domain for $\Gamma_0(14) \cap \Gamma(2)$; graph in Figure 6.1

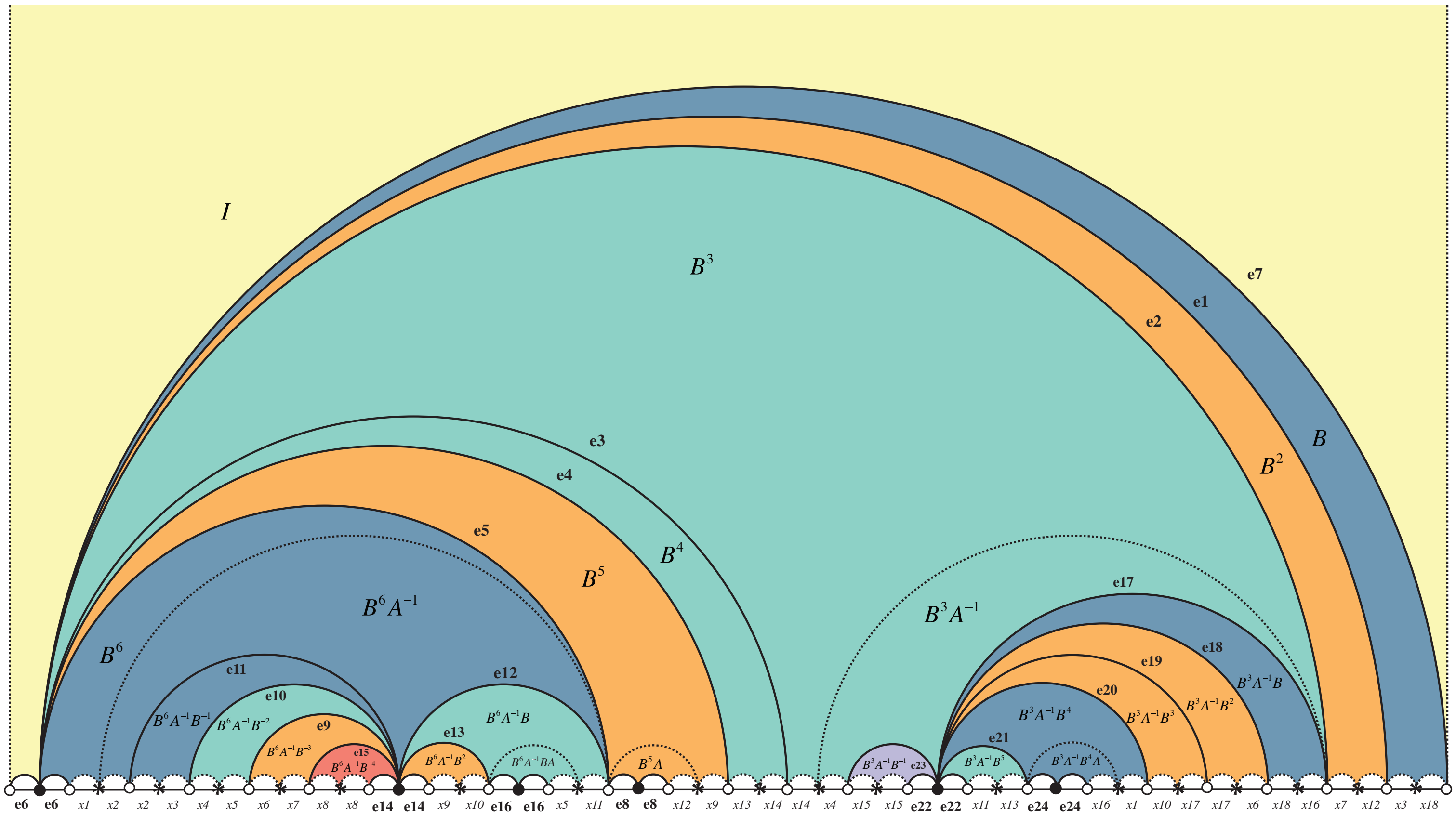

Figure B.8: Fundamental domain for $\Gamma_1(14) \cap \Gamma(2)$; graph in Figure 6.4

Appendix C

EXAMPLES OF PERMUTATIONS

C.1 Principal Congruence Subgroups

In this section we record permutations which correspond to the principal congruence subgroups up to level 12. These were computed by hand, by first finding a fundamental domain for the group, finding the side-pairing transformations and then recording the edges found by rotating counterclockwise about each vertex. For the most part these were computed before the algorithms for level $2p$ were fully developed, and so unfortunately the numbering is not consistent with the output of the algorithms in these cases.

C.1.1 $\Gamma(4)$

Black vertices: $(1,2)(3,4)$. White vertices: $(1,4)(2,3)$. Faces: $(1,3)(2,4)$.

C.1.2 $\Gamma(6)$

Black vertices: $(3,2,1)(7,6,5)(11,10,9)(4,8,12)$;

White vertices: $(1,5,9)(2,11,12)(3,4,6)(7,8,10)$;

Faces: $(1,10,4)(2,8,5)(3,7,11)(6,12,9)$

C.1.3 $\Gamma(8)$

Black vertices: $(1,2,3,4)(5,6,7,8)\dots(29,30,31,32)$

White vertices:

$(1,28,15,6)$	$(2,21,16,11)$	$(3,26,13,8)$	$(4,23,14,9)$
$(5,32,27,18)$	$(7,30,25,20)$	$(10,29,24,19)$	$(12,31,22,17)$

Faces:

$(1,5,17,21)$	$(2,10,18,26)$	$(3,7,19,23)$	$(4,12,20,28)$
$(6,14,22,30)$	$(8,16,24,32)$	$(9,13,25,29)$	$(11,15,27,31)$

C.1.4 $\Gamma(10)$

Black vertices: $(1,2,3,4,5)(6,7,8,9,10)\dots(56,57,58,59,60)$

White vertices:

$(1,55,60,18,27)$	$(2,9,44,59,13)$	$(3,23,33,43,53)$	$(4,29,38,32,7)$
$(5,15,19,37,21)$	$(6,24,39,48,42)$	$(8,54,14,28,22)$	$(10,34,49,58,52)$
$(11,56,46,36,26)$	$(12,51,45,50,17)$	$(16,57,41,35,40)$	$(20,47,31,25,30)$

Faces:

$(1,26,40,34,9)$	$(2,12,16,39,23)$	$(3,52,57,20,29)$	$(4,6,41,56,15)$
$(5,25,35,45,55)$	$(7,31,46,60,54)$	$(8,21,36,50,44)$	$(10,51,11,30,24)$
$(13,58,48,38,28)$	$(14,53,42,47,19)$	$(17,49,33,22,27)$	$(18,59,43,32,37)$.

C.1.5 $\Gamma(12)$

Black vertices: $(1,2,3,4,5,6)(7,8,9,10,11,12)\ldots(91,92,93,94,95,96)$.

White vertices:

$(1,90,48,81,68,37)$ $(2,58,50,82,74,10)$ $(3,23,96,83,18,28)$

$(4,87,45,84,71,40)$ $(5,55,53,79,77,7)$ $(6,20,93,80,15,25)$

$(8,17,61,54,22,33)$ $(9,92,39,49,30,44)$ $(11,14,64,51,19,36)$

$(12,95,42,52,27,47)$ $(13,85,78,24,69,56)$ $(16,88,75,21,72,59)$

$(26,70,62,94,86,34)$ $(29,67,65,91,89,31)$ $(32,41,73,66,46,57)$

$(35,38,76,63,43,60)$

Faces:

$(1,42,94,61,16,58)$ $(2,9,43,62,69,23)$ $(3,27,51,63,75,87)$

$(4,39,91,64,13,55)$ $(5,12,46,65,72,20)$ $(6,30,54,66,78,90)$

$(7,76,37,67,28,17)$ $(8,32,56,68,80,92)$ $(10,73,40,70,25,14)$

$(11,35,59,71,83,95)$ $(15,79,52,41,31,88)$ $(18,82,49,38,34,85)$

$(19,50,57,45,86,93)$ $(21,74,81,47,26,33)$ $(22,53,60,48,89,96)$

$(24,77,84,44,29,36)$

C.2 Level 22

In this section we work out an example of the algorithm for $\Gamma_1(2p)\cap\Gamma(2)$ in Section 6.3 for the case $p=11$.

The permutation for the ten black vertices is given by

$$(11,10,9,8,7,6,5,4,3,2,1)(12)$$

$$(23,22,21,20,19,18,17,16,15,14,13)(24)$$

$$(35,34,33,32,31,30,29,28,27,26,25)(36)$$

$$(47,46,45,44,43,42,41,40,39,38,37)(48)$$

$$(59,58,57,56,55,54,53,52,51,50,49)(60)$$

The cycles for the faces of degree 1 are (11)(23)(35)(47)(59).

For the faces of degree 11, we first use the algorithm for the degree 11 face of $\Gamma_0(22)\cap\Gamma(2)$ to find $\Phi = (1, 9, 5, 6, 2, 10, 4, 8, 12, 3, 7)$. Next we find the u_i, calculating each mod 22:

$$
\begin{aligned}
u_1 &= (1+4)^{-1} &&= 9 \\
u_2 &= (1+36)^{-1} &&= 3 \\
u_3 &= (1+20)^{-1} &&= -1 \\
u_4 &= (1+24)-1 &&= -7 \\
u_5 &= (1+8)^{-1} &&= 5 \\
u_6 &= (1+40)^{-1} &&= 7 \\
u_7 &= (1+16)^{-1} &&= -9 \\
u_8 & &&= 1 \\
u_9 &= (1+65)^{-1} &&= -1 \\
u_{10} &= (1+12)^{-1} &&= -5 \\
u_{11} &= (1+28)^{-1} &&= -3
\end{aligned}
$$

Now we find each of the five 11-cycles.

The first 11-cycle, Ψ_1:

φ_i	1	9	5	6	2	10	4	8	12	3	7
u_i	9	3	-1	-7	5	7	-9	1	-1	-5	-3
v_i	1	9	5	5	9	1	7	3	3	3	7
ψ_{1_i}	1	21	29	30	14	10	52	44	48	39	55

The second 11-cycle, Ψ_2:

φ_i	2	10	4	8	12	3	7	1	9	5	6
u_i	5	7	-9	1	-1	-5	-3	9	3	-1	-7
v_i	1	5	3	9	9	9	3	5	1	7	7
ψ_{2_i}	2	34	16	56	60	51	19	25	9	41	42

Continuing as above, we find the cycles for all ten of the faces:

$$(1, 21, 29, 30, 14, 10, 52, 44, 48, 39, 55)(11)$$

$$(2, 34, 16, 56, 60, 51, 19, 25, 9, 41, 42)(23)$$

$$(3, 31, 49, 45, 17, 18, 38, 58, 28, 8, 12)(35)$$

$$(4, 20, 24, 15, 7, 37, 33, 53, 54, 26, 46)(47)$$

$$(5, 6, 50, 22, 40, 32, 36, 27, 43, 13, 57)(59)$$

The white vertices are given by $\alpha = \sigma^{-1}\Psi^{-1}$, (where α is the permutation from the black vertices and Ψ is the permutation for the faces), which yields

$$(1, 42, 27, 58, 59, 31, 40, 9, 14, 24, 20)(5)$$

$$(2, 12, 8, 25, 54, 39, 22, 23, 43, 52, 33)(17)$$

$$(3, 46, 47, 7, 28, 21, 50, 60, 56, 13, 30)(29)$$

$$(4, 57, 38, 48, 44, 49, 6, 15, 34, 35, 19)(41)$$

$$(10, 11, 55, 16, 45, 26, 36, 32, 37, 18, 51)(53)$$

The graphs for $\Gamma_0(22) \cap \Gamma(2)$ and $\Gamma_1(22) \cap \Gamma(2)$ are shown in Figures C.1 and C.2. $\Gamma_0(22) \cap \Gamma(2)$ appears on a polygon with 16 sides, which when identified form a surface of genus 4. The graph for $\Gamma_1(22) \cap \Gamma(2)$ is drawn on a polygon with 80 sides (shown as alternating black and gray so we can distinguish them). We identify the sides to form an orientable surface of genus 16.

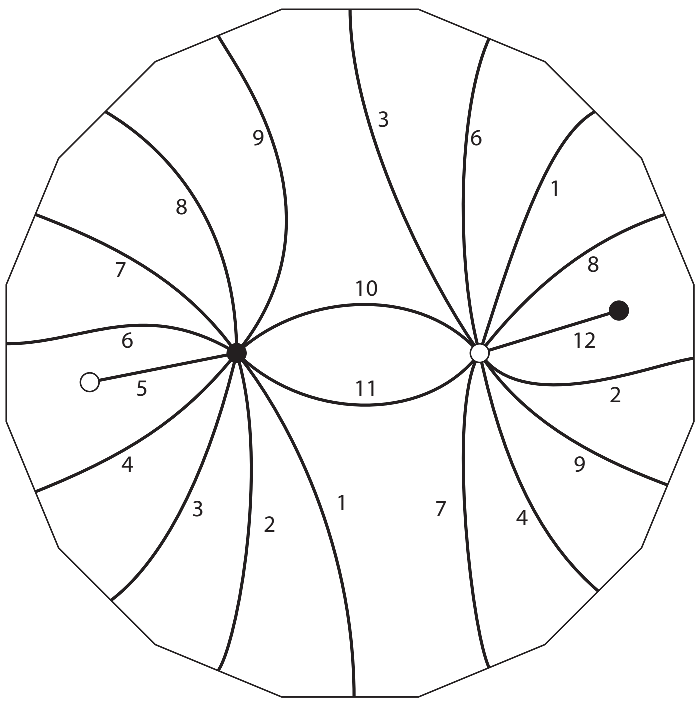

Figure C.1: Graph for $\Gamma_0(22) \cap \Gamma(2)$

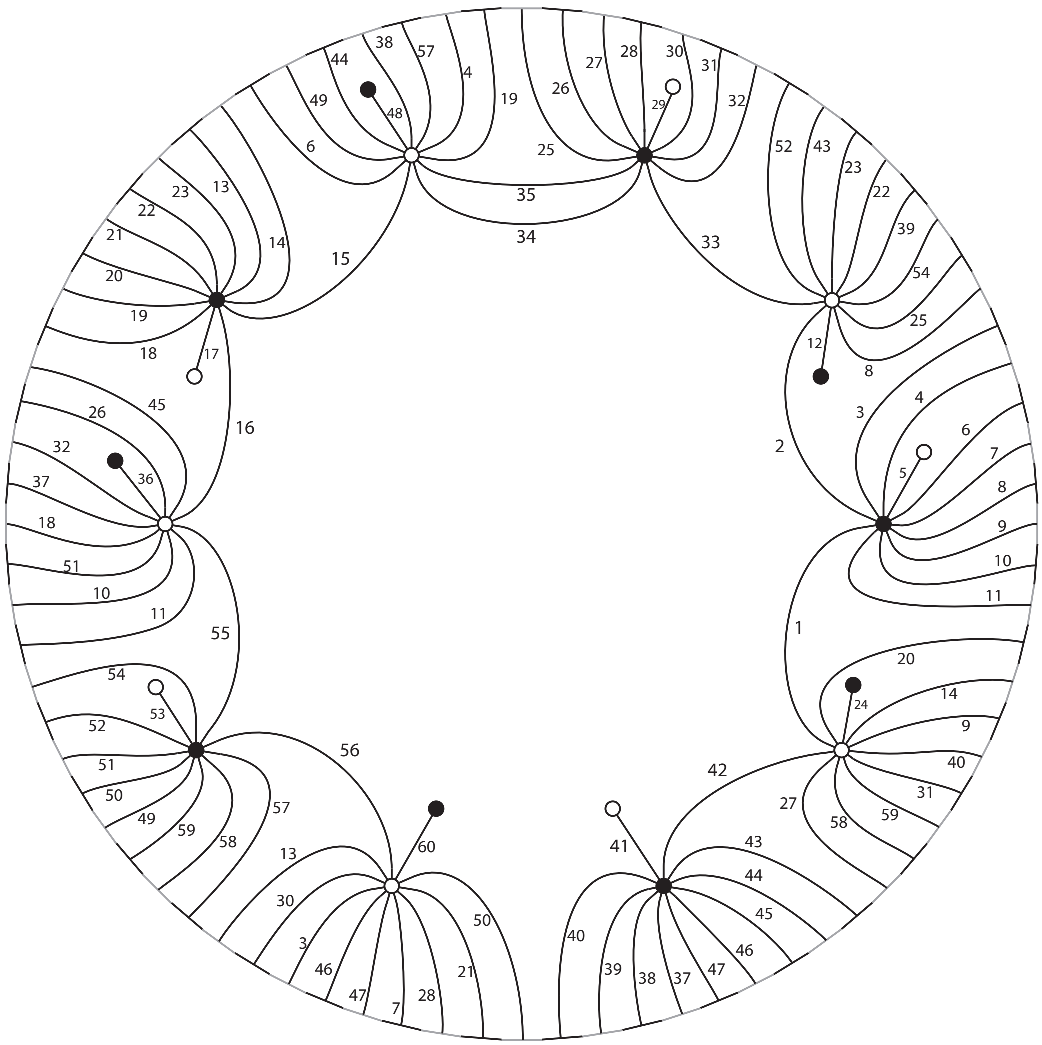

Figure C.2: Graph for $\Gamma_1(22) \cap \Gamma(2)$

BIBLIOGRAPHY

[1] A. O. L. Atkin and H. P. F. Swinnerton-Dyer, Modular forms on noncongruence subgroups. *Combinatorics, Proc. Sympos. Pure Math.* **XIX** Amer. Math. Soc., 1971, 1–25.

[2] B. Birch, Noncongruence subgroups, covers and drawings. *The Grothendieck Theory of Dessins d'Enfants, London Math. Soc. Lecture Note Ser.* **200** (1994), 25–45.

[3] L.R. Ford, *Automorphic Functions.* Chelsea Publishing Co., New York, 1951.

[4] A. Grothendieck, Sketch of a program (English translation). *Geometric Galois Actions, 1, London Math. Soc. Lecture Note Ser.* **242** Cambridge Univ. Press, 1997, 243–283.

[5] T. Hsu, Identifying Congruence Subgroups of the Modular Group. *Proc. Amer. Math. Soc.* **124** (1996), 1351–1359.

[6] W.C. Li, L. Long, and Z. Yang, Modular forms for noncongruence subgroups. *Quarterly Journal of Pure and Applied Mathematics* **1** (2005), 205–221.

[7] ——-, On Atkin and Swinnerton-Dyer congruence relations. *J. of Number Theory* **113** (2005), 117–148.

[8] S. Lando and A. Zvonkin, *Graphs on Surfaces and Their Applications.* Encyclopaedia of Mathematical Sciences **141**. Springer-Verlag, Berlin, 2004.

[9] H. Larcher, The Cusp Amplitudes of the Congruence Subgroups of the Classical Modular Group. *Illinois J. Math.* **26** (1982), 164–172.

[10] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions.* Iwanami Shoten and Princeton University Press, 1971.

[11] A. J. Scholl, The ℓ-adic representations attached to a certain noncongruence subgroup. *J. Reine Angew. Math* **392** (1988), 1–15.

[12] K. Wohlfahrt, An extension of F. Klein's level concept. *Illinois J. Math.* **8** (1964), 529–535.