

# Fundamental domains for genus-zero and genus-one congruence subgroups

C. J. Cummins

## ABSTRACT

In this paper, we compute Ford fundamental domains for all genus-zero and genus-one congruence subgroups. This is a continuation of previous work, which found all such groups, including ones that are not subgroups of  $\mathrm{PSL}(2, \mathbb{Z})$ . To compute these fundamental domains, an algorithm is given that takes the following as its input: a positive square-free integer  $f$ , which determines a maximal discrete subgroup  $\Gamma_0(f)^+$  of  $\mathrm{SL}(2, \mathbb{R})$ ; a decision procedure to determine whether a given element of  $\Gamma_0(f)^+$  is in a subgroup  $G$ ; and the index of  $G$  in  $\Gamma_0(f)^+$ . The output consists of: a fundamental domain for  $G$ , a finite set of bounding isometric circles; the cycles of the vertices of this fundamental domain; and a set of generators of  $G$ . The algorithm avoids the use of floating-point approximations. It applies, in principle, to any group commensurable with the modular group. Included as appendices are: MAGMA source code implementing the algorithm; data files, computed in a previous paper, which are used as input to compute the fundamental domains; the data computed by the algorithm for each of the congruence subgroups of genus zero and genus one; and an example, which computes the fundamental domain of a non-congruence subgroup.

## 1. Introduction

The modular group  $\mathrm{PSL}(2, \mathbb{Z}) := \mathrm{SL}(2, \mathbb{Z}) / \{\pm 1_2\}$  is a discrete subgroup of  $\mathrm{PSL}(2, \mathbb{R}) := \mathrm{SL}(2, \mathbb{R}) / \{\pm 1_2\}$ . The principal congruence subgroup of level  $N$  of  $\mathrm{SL}(2, \mathbb{Z})$  is

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}. \quad (1.1)$$

A subgroup  $G$  of  $\mathrm{SL}(2, \mathbb{Z})$  that contains some principal congruence subgroup is known as a congruence subgroup. If  $G$  is a congruence subgroup, then the level of  $G$  is the smallest  $N$  such that  $\Gamma(N) \subseteq G$ . Congruence subgroups of  $\mathrm{PSL}(2, \mathbb{Z})$  are defined similarly.

Study of the modular group and its congruence subgroups was given renewed impetus with the discovery of ‘monstrous moonshine’ [2, 5, 15, 21, 24, 25, 27]. The groups that appear in this context are discrete subgroups of  $\mathrm{PSL}(2, \mathbb{R})$  whose intersections with  $\mathrm{PSL}(2, \mathbb{Z})$  are congruence subgroups. They are not, however, necessarily subgroups of  $\mathrm{PSL}(2, \mathbb{Z})$ . Thus, it is convenient to define a congruence subgroup of  $\mathrm{PSL}(2, \mathbb{R})$  to be a discrete subgroup of  $\mathrm{PSL}(2, \mathbb{R})$  that contains some principal congruence subgroup.

The genus of a congruence subgroup is defined to be the genus of a certain Riemann surface, which arises from the group’s action on the complex upper half-plane (see Section 2 for details). The groups that occur in ‘moonshine’ are congruence subgroups of genus zero. It is known that there are infinitely many genus-zero subgroups of the modular group; see, for example, [18]. However, Rademacher conjectured that there are only finitely many genus-zero congruence subgroups of  $\mathrm{PSL}(2, \mathbb{Z})$ . This problem was studied by Knopp and Newman [19], McQuillan [22, 23] and Dennin [10–12]. Thompson [28] proved a more general result, motivated by the groups appearing in ‘monstrous moonshine’. His result is that, up to

---

Received 31 January 2008; revised 4 March 2010.

2000 Mathematics Subject Classification 20H05 (primary), 11F30, 11F22, 20H10 (secondary).

This work was supported in part by the NSERC of Canada.

conjugation, there are only finitely many congruence subgroups of  $\text{PSL}(2, \mathbb{R})$  of fixed genus. Zograf’s bound from [29] gives another proof of this result; see below. Cox and Parry [6, 7], independently of Thompson, showed that there are only finitely many congruence subgroups of  $\text{PSL}(2, \mathbb{Z})$  of fixed genus. Their work applies only to subgroups of  $\text{PSL}(2, \mathbb{Z})$ , but for this case they gave explicit bounds, which they then used to find the list of all congruence subgroups of  $\text{PSL}(2, \mathbb{Z})$  of genus zero.

In [8, 9], all subgroups of  $\text{PSL}(2, \mathbb{R})$  of genus zero or one were computed up to conjugacy, by making use of Zograf’s bound. This paper is a sequel to [8], and its aim is to find fundamental domains of all the genus-zero and genus-one congruence subgroups. To this end, in Sections 2 and 3 the necessary background on congruence subgroups and Ford fundamental domains is given. We include proofs of the required properties of Ford fundamental domains. Although many of these properties are well known, a detailed treatment does not seem to be available in the literature. In Section 4, the algorithm for computing the fundamental domains is discussed. In outline, given a group  $G$ , the algorithm proceeds by constructing a sequence of sets of isometric circles of  $G$  that (potentially) form part of the boundary of a Ford fundamental domain of  $G$ . An area computation using the Gauss–Bonnet theorem is used to determine when the algorithm terminates. Isometric circles are removed from the set if it is determined that they cannot form part of the boundary. Section 5 explains in detail the procedure used for finding hyperbolic areas. Finally, Section 6 gives a representative example, and explains the format and conventions of the data files.

Appendix 1 contains complete MAGMA [3] source code implementing the algorithm. Appendix 2 contains the data files from [8] which are used as input to compute the fundamental domains. Appendix 3 contains the data computed by the algorithm for each of the genus-zero and genus-one congruence subgroups. As the algorithm applies to any group commensurable with the modular group, Appendix 4 contains example code for computing the fundamental domain of a non-congruence subgroup.

## 2. Subgroups of $\text{PSL}(2, \mathbb{R})$

From a computational point of view, it is easier to work with subgroups of  $\text{SL}(2, \mathbb{Z})$  and  $\text{SL}(2, \mathbb{R})$  than with subgroups of  $\text{PSL}(2, \mathbb{Z})$  and  $\text{PSL}(2, \mathbb{R})$ . There is a one-to-one correspondence between the subgroups of  $\text{PSL}(2, \mathbb{R})$  and the subgroups of  $\text{SL}(2, \mathbb{R})$  that contain  $-1_2$ . Thus, in this paper, we work with subgroups of  $\text{SL}(2, \mathbb{R})$  that contain  $-1_2$ , rather than their images in  $\text{PSL}(2, \mathbb{R})$ . If  $G$  is a subgroup of  $\text{SL}(2, \mathbb{R})$ , then  $\overline{G}$  will denote its image in  $\text{PSL}(2, \mathbb{R})$ .

Congruence subgroups of  $\text{PSL}(2, \mathbb{R})$  are examples of subgroups that are commensurable with  $\text{PSL}(2, \mathbb{Z})$ , where two subgroups are commensurable if their intersection has finite index in both. If  $\overline{G}$  is a subgroup of  $\text{PSL}(2, \mathbb{R})$ , then  $\overline{G}$  acts on the complex upper half-plane  $\mathcal{H}$  by fractional linear transformations. If, moreover,  $\overline{G}$  is commensurable with  $\text{PSL}(2, \mathbb{Z})$ , then  $\overline{G}$  acts on the extended upper half-plane  $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$  by fractional linear transformations. In fact,  $\mathbb{Q} \cup \{\infty\}$  is the set of parabolic fixed points of  $\overline{G}$ ; see Shimura [26, Proposition 1.30]. The orbit space  $\mathcal{H}^*/\overline{G}$  can be given the structure of a compact Riemann surface, and the genus of  $\overline{G}$  is defined to be the genus of this Riemann surface; see [26, Section 1.3]. If  $G$  is a subgroup of  $\text{SL}(2, \mathbb{R})$ , then, in this paper, by the geometric invariants, such as the genus or cusp number of  $G$ , we shall mean the corresponding invariants of  $\overline{G}$ .

We next make the following definitions.

DEFINITION 2.1.

$$\Gamma_0(f) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z}) \mid c \equiv 0 \pmod{f} \right\};$$

$$\Gamma_0(f)^+ = \left\{ e^{-1/2} \begin{pmatrix} ae & b \\ cf & de \end{pmatrix} \in \text{SL}(2, \mathbb{R}) \mid a, b, c, d, e \in \mathbb{Z}, e > 0, e \parallel f, ade^2 - bcf = e \right\}.$$

In this definition,  $e \parallel f$  means that  $e$  divides  $f$  and  $\gcd(e, f/e) = 1$ . If  $f$  is square-free, then the group  $\Gamma_0(f)^+$  is the normalizer of  $\Gamma_0(f)$  in  $\mathrm{SL}(2, \mathbb{R})$ . The importance of these ‘Helling groups’ is illustrated by the following theorem.

**THEOREM 2.2** (Helling [16, 17]; see also [4]). *If  $G$  is a subgroup of  $\mathrm{SL}(2, \mathbb{R})$  that is commensurable with  $\mathrm{SL}(2, \mathbb{Z})$ , then  $G$  is conjugate to a subgroup of  $\Gamma_0(f)^+$  for some square-free  $f$ .*

For  $\Gamma_0(f)^+$ , the definition of the level of a subgroup is as follows. Let

$$G(n, f) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}) \mid a - 1 \equiv d - 1 \equiv b \equiv 0 \pmod{n}, c \equiv 0 \pmod{fn} \right\}. \tag{2.1}$$

It is easily verified that  $G(n, f)$  is a normal subgroup of  $\Gamma_0(f)^+$  and that  $G(n, 1) = \Gamma(n)$ . We then define the level of a congruence subgroup  $G$  of  $\Gamma_0(f)^+$  to be the smallest  $n$  such that  $G(n, f)$  is a subgroup of  $G$ .

Let  $\mathrm{Area}(G)$  and  $g(G)$  be the hyperbolic area and genus of  $\mathcal{H}^*/\overline{G}$ , respectively. Recall that

$$\frac{1}{2\pi} \mathrm{Area}(G) = 2(g(G) - 1) + m + \sum_{i=1}^k \left( 1 - \frac{1}{e_i} \right), \tag{2.2}$$

where  $m$  is the number of inequivalent parabolic fixed points of  $G$  (the cusp number),  $k$  is the number of inequivalent elliptic fixed points of  $G$  and  $e_i, i = 1, \dots, k$ , are the orders of these points; see, for example, [26, Theorem 2.20].

We then have the following theorem, due to Zograf.

**THEOREM 2.3** (Zograf [29]). *Let  $K$  be any subgroup of  $\mathrm{SL}(2, \mathbb{R})$  that is commensurable with  $\mathrm{SL}(2, \mathbb{Z})$ ; then for any congruence subgroup  $G$  of  $K$  we have*

$$g(G) + 1 > \frac{3}{128\pi} \mathrm{Area}(K) \mathrm{Index}(K : G). \tag{2.3}$$

As a corollary to his result, Zograf notes that it implies Thompson’s theorem as follows. Let  $K = G = \Gamma_0(f)^+$ , with  $f$  square-free. Then  $\mathrm{Area}(\Gamma_0(f)^+) = (\pi/3) \prod_{p|f} ((1+p)/2)$ , where  $p$  is prime. Writing  $g$  for  $g(\Gamma_0(f)^+)$ , we have, by Theorem 2.3,

$$\prod_{\substack{p|f \\ p \text{ prime}}} \frac{1+p}{2} < 128(g+1). \tag{2.4}$$

This bounds the possible values of  $f$  for a given genus. If  $k$  is the number of prime factors of  $f$ , then  $2^{k-2} < f/2^k < \prod_{p|f} (1+p)/2 < 128(g+1)$ , where  $p$  is prime. This bounds  $k$  and hence  $f$ . It follows that the set

$$H(g) = \{ \Gamma_0(f)^+ \mid f \text{ square-free, } \mathrm{genus}(\Gamma_0(f)^+) \leq g \}$$

is finite. By Theorem 2.2, any congruence subgroup  $G$  that is commensurable with  $\mathrm{SL}(2, \mathbb{Z})$  is conjugate to a subgroup of  $\Gamma_0(f)^+$  for some square-free  $f$ . By the Riemann–Hurwitz formula, any subgroup of  $\Gamma_0(f)^+$  has genus equal to, or larger than, the genus of  $\Gamma_0(f)^+$ . So if  $G$  has genus  $g$ , then it is conjugate to a subgroup of bounded index of at least one of the groups in  $H(g)$ . As there are only finitely many such subgroups, Thompson’s theorem follows.

The results of [8] give a tabulation of the genus-zero and genus-one congruence subgroups up to conjugacy in  $\Gamma_0(f)^+$  for those square-free  $f$  such that  $\Gamma_0(f)^+$  has genus zero or one. The condition that the groups contain  $-1_2$  is also assumed. The output of the computation gives each group as a union of cosets over some  $G(n, f)$ . One aim of the present paper is to compute a standard set of generators and a fundamental domain for each of these groups.

The next section gives the necessary background information on fundamental domains, in particular Ford fundamental domains.

### 3. Fundamental domains

In this section we summarize the necessary facts concerning fundamental domains of Fuchsian groups. This material is mostly standard and is contained, for example, in Beardon [1] or Lehner [20]. We do, however, give proofs of the properties of Ford fundamental domains that we need, as there seems to be no convenient reference; we shall make use of these properties in subsequent sections. We assume in this section that the group  $G$  is a finitely generated Fuchsian group of the first kind. The results are easier to state in this case, and the groups we wish to consider are all of this type. Towards the end of this section, it will be necessary to make the restriction to subgroups of  $\Gamma_0(f)^+$ , in order to obtain more precise information about the structure of the boundary of the Ford fundamental domain.

A *fundamental set* for  $G$  is defined to be a subset of  $\mathfrak{H}$  that contains exactly one point from each orbit of  $G$ . A *fundamental domain* is a domain (that is, an open and connected subset of  $\mathfrak{H}$ ) whose closure in  $\mathfrak{H}$  contains a fundamental set.

DEFINITION 3.1. A subset  $D$  of  $\mathfrak{H}$  is a fundamental domain for  $G$  if and only if:

- (i)  $D$  is a domain;
- (ii) there is a fundamental set  $F$  of  $G$  such that  $D \subset F \subset \tilde{D}$ , where  $\tilde{D}$  is the closure of  $D$  in  $\mathfrak{H}$ ;
- (iii)  $\text{Area}(\partial D) = 0$ , where  $\partial D$  is the boundary of  $D$ .

Without imposing further restrictions, fundamental domains may have certain undesirable properties. Beardon, in [1, Example 9.2.5], gives an example of a fundamental domain that is a convex, five-sided polygon but for which the natural map from  $\tilde{D}/G$  to  $\mathcal{H}/G$  is not a homeomorphism. This possibility can be avoided by considering fundamental domains that are both convex (with respect to the hyperbolic metric) and locally finite, the latter term being defined as follows.

DEFINITION 3.2. A fundamental domain  $D$  of  $G$  is said to be locally finite if and only if every compact subset of  $\mathcal{H}$  has non-empty intersection with only finitely many  $G$ -images of  $D$ .

In order to list the properties of convex, locally finite, fundamental domains, it is convenient to introduce the notions of sides and vertices of fundamental domains.

DEFINITION 3.3. A *side* of a fundamental domain  $D$  is a geodesic segment of positive (hyperbolic) length that has the form  $\tilde{D} \cap g(\tilde{D})$  for some  $g$  in  $G$ . A *vertex*  $v$  of  $D$  is a point of  $\mathcal{H}$  such that  $\{v\} = \tilde{D} \cap g\tilde{D} \cap h\tilde{D}$ , for some  $g$  and  $h$  in  $G$  which are distinct and not equal to the identity element.

Let  $S(D)$  be the set of sides of  $D$ , and let  $P(D)$  be the set of elements  $g$  in  $G$  such that  $\tilde{D} \cap g\tilde{D}$  is a side of  $D$ . We then have the following result.

THEOREM 3.4. Let  $D$  be a convex, locally finite, fundamental domain for  $G$ , a finitely-generated Fuchsian group of the first kind. Then the following properties hold.

- (i)  $\text{Area}(D) < \infty$ , where  $\text{Area}(D)$  is the hyperbolic area of  $D$ .
- (ii)  $D$  has only finitely many sides.
- (iii) The boundary of  $D$  is the union of the sides of  $D$ .
- (iv) Each vertex lies on exactly two sides and is a common endpoint of each of the two sides.

(v) If two sides have non-empty intersection, then they meet in a vertex, which is a common endpoint of the two sides.

(vi) The map  $\phi : P(D) \rightarrow S(D)$  defined by  $\phi(g) = \tilde{D} \cap g\tilde{D}$  is a bijection.

(vii) The elements of  $P(D)$  generate  $G$ .

*Proof.* See Beardon [1, Sections 9.3 and 10.1]. □

The sets  $\{g, g^{-1}\}$ , for  $g$  in  $P(D)$ , partition  $P(D)$  into subsets of size 1 or size 2, with the size being 1 precisely when  $g$  has order 2. The map  $\phi$  then yields a corresponding partition of the sides of  $D$ . If  $\{s, s'\}$  is the image of  $\{g, g^{-1}\}$ , then  $s = \tilde{D} \cap g\tilde{D}$  and  $s' = \tilde{D} \cap g^{-1}\tilde{D}$ . Moreover,  $g(s') = s$  and  $g^{-1}(s) = s'$ . We thus have a pairing of the sides of  $D$  by elements from  $P(D)$ , which constitute what we shall call the set of pairing transformations. We include the possibility that a side may be ‘self-paired’ by an element  $g$  of order 2.

There are different approaches to constructing convex, locally finite, fundamental domains. We shall find it convenient to use a method first introduced by Ford [13]. To define a Ford fundamental domain, we first need to define the isometric circles of the group  $G$ .

**DEFINITION 3.5.** Suppose  $c \neq 0$ . The isometric circle  $I_g$  of the matrix  $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{R})$  is the circle in the complex plane with centre  $-d/c$  and radius  $1/|c|$ ; that is,  $I_g = \{z \in \mathbb{C} \mid |cz + d| = 1\}$ . If  $G$  is a subgroup of  $\text{SL}(2, \mathbb{R})$  and  $g \in G$ , then we say that  $I_g$  is an isometric circle of  $G$ . We also define  $\text{Ext}(I_g) = \{z \in \mathbb{C} \mid |cz + d| > 1\}$  and  $\text{Int}(I_g) = \{z \in \mathbb{C} \mid |cz + d| < 1\}$ .

We shall use isometric circles to construct a fundamental domain for  $G$ . The key properties of the isometric circle  $I_g$  that we shall use are as follows.

**LEMMA 3.6.** Let  $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  be an element of  $\text{SL}(2, \mathbb{R})$  such that  $c \neq 0$ .

(i) The transformation of  $\mathbb{C}$  given by  $z \mapsto g(z) = (az + b)/(cz + d)$  is the transformation obtained by performing an inversion in  $I_g$  followed by a reflection in the perpendicular bisector of the line from the centre of  $I_g$  to the centre of  $I_{g^{-1}}$ . If  $I_g = I_{g^{-1}}$ , then the reflection is in the line through the centre of  $I_g$  parallel to the imaginary axis.

(ii) The transformation  $z \mapsto g(z)$  maps  $\text{Ext}(I_g) \cup \{\infty\}$  bijectively to  $\text{Int}(I_{g^{-1}})$ .

*Proof.* Statement (i) follows from a direct calculation. Statement (ii) follows from statement (i). □

For any element  $g$  in  $\text{SL}(2, \mathbb{R})$ , let  $c_g$  be the lower left entry of  $g$ . Let  $G_\infty$  be the subgroup of  $G$  that stabilizes  $\infty$ . Then  $g \in G_\infty$  if and only if  $c_g = 0$ . Thus  $g$  has an isometric circle if and only if  $g \in G - G_\infty$ . We shall assume from this point on that  $G_\infty$  is equal to  $\{\pm \begin{pmatrix} 1 & kT \\ 0 & 1 \end{pmatrix} \mid k \in \mathbb{Z}\}$  for some  $T > 0$ . This is the case for all the groups we wish to consider.

We next define some subsets of  $\mathcal{H}$ .

**DEFINITION 3.7.**

$$\begin{aligned}
 R_\infty(G) &= \{z \in \mathcal{H} \mid 0 < \Re(z) < T\}, \\
 R_1(G) &= \mathcal{H} \cap \bigcap_{g \in G - G_\infty} \text{Ext}(I_g), \\
 R_2(G) &= \mathcal{H} \cap \bigcup_{g \in G - G_\infty} \text{Int}(I_g), \\
 R_3(G) &= \{z \in \mathcal{H} \mid \exists g \in G - G_\infty \text{ such that } z \in I_g \text{ and } z \notin R_2(G)\}, \\
 R(G) &= R_\infty \cap R_1(G).
 \end{aligned}
 \tag{3.1}$$

We shall show that  $R(G)$  is a convex, locally finite, fundamental domain for  $G$ . This type of fundamental domain was originally introduced by Ford, so we shall call  $R(G)$  the Ford fundamental domain of  $G$ . As most references give a full treatment only for the case where  $G_\infty$  is trivial, we shall provide a detailed discussion.

The image of an isometric circle of a group  $G$  upon transformation by an element  $h$  of  $SL(2, \mathbb{R})$  is not necessarily an isometric circle of the group obtained by conjugating  $G$  by  $h$ . It follows that a conjugated Ford fundamental domain of  $G$  is not necessarily a Ford fundamental domain of the group obtained by conjugating  $G$ , even though it is a fundamental domain for this group. See [1, Section 7.36] for a more detailed discussion of this point.

For an isometric circle  $I$  of the group  $G$ , let  $\langle I \rangle$  be the set of circles obtained upon translating  $I$  by the transformations corresponding to the elements of  $G_\infty$ . Let  $S = \{\langle I_g \rangle \mid g \in G - G_\infty\}$ .

LEMMA 3.8. *The map  $\varphi : G_\infty(G - G_\infty)G_\infty \rightarrow S$  given by  $\varphi(G_\infty g G_\infty) = \langle I_g \rangle$  is a bijection.*

*Proof.* That  $\varphi$  is well-defined on the double cosets is easily verified. Clearly,  $\varphi$  is surjective. If  $\varphi(G_\infty g G_\infty) = \varphi(G_\infty g' G_\infty)$ , then  $I_g = t_1(I_{g'})$  for some  $t_1 \in G_\infty$ , and so  $I_g = I_{g't_1}$ . This implies that  $g = t_2 g' t_1$  for some  $t_2 \in G_\infty$ , and so the two double cosets are equal, as required.  $\square$

Let  $r(\langle I \rangle)$  be the (Euclidean) radius of  $I$ . This is well-defined, since each circle in  $\langle I \rangle$  has the same radius.

LEMMA 3.9.

(i) *With  $G$  as above, there is some  $M > 0$ , depending only on  $G$ , such that  $r(\langle I \rangle) \leq M$  for all  $\langle I \rangle \in S$ .*

(ii) *For all  $N > 0$ , the set  $\{\langle I \rangle \in S \mid N \leq r(\langle I \rangle) \leq M\}$  is finite.*

*Proof.* By using Lemma 3.8, both assertions follow from [26, Lemmas 1.24 and 1.25].  $\square$

PROPOSITION 3.10. *Let  $C$  be any compact subset of  $\mathcal{H}$ . Then there are only finitely many isometric circles of  $G$  that meet  $C$ . Moreover, there are only finitely many isometric circles whose interiors meet  $C$ .*

*Proof.* Let  $z$  be any point of  $\mathcal{H}$ . The hyperbolic distance from  $z$  to  $C$  is bounded, and thus  $C$  lies inside some hyperbolic disc centred on  $z$ , which is a Euclidean circle  $E$  contained in  $\mathcal{H}$ . In particular,  $C$  is bounded away from the real axis in the Euclidean metric. It follows from Lemma 3.9(ii) that there are only finitely many equivalence classes  $\langle I \rangle$  such that some isometric circle in  $\langle I \rangle$  meets  $C$ . Furthermore, if  $I$  meets  $E$ , then there are only finitely many circles in  $\langle I \rangle$  that meet  $E$  and hence finitely many that meet  $C$ . We conclude that only finitely many isometric circles meet  $C$ , as required. A similar argument shows that there are only finitely many isometric circles whose interiors meet  $C$ .  $\square$

COROLLARY 3.11. *If  $z$  is a point in  $\mathcal{H}$ , then  $z$  has a neighborhood that meets only finitely many isometric circles of  $G$ .*

*Proof.* As every neighborhood of  $z$  contains a closed hyperbolic disc, which lies in  $\mathcal{H}$ , this result follows from Proposition 3.10.  $\square$

PROPOSITION 3.12.

(i) *The three sets  $R_1(G)$ ,  $R_2(G)$  and  $R_3(G)$  form a partition of  $\mathcal{H}$ , and each set is invariant under the group  $G_\infty$ .*

(ii)  *$R_1(G)$  and  $R_2(G)$  are open sets.*

- (iii)  $R_1(G) \cup R_3(G)$  is the closure of  $R_1(G)$  in  $\mathcal{H}$  and  $R_3(G) = \partial R_1(G)$ .
- (iv) The closure of  $R(G)$  in  $\mathcal{H}$  is  $(R_3(G) \cap \widetilde{R_\infty(G)}) \cup (R_1(G) \cap \widetilde{R_\infty(G)})$ .
- (v) The boundary of  $R(G)$  is the disjoint union of  $L_0 \cap R_1(G)$ ,  $L_T \cap R_1(G)$  and  $R_3(G) \cap \widetilde{R_\infty(G)}$ , where  $L_x = \{z \in \mathcal{H} \mid \Re(z) = x\}$ .

*Proof.*

(i) That the three sets are disjoint follows immediately from their definitions. If  $z$  is not in either  $R_1(G)$  or  $R_2(G)$ , then there is at least one isometric circle  $I$  such that  $z$  is not in either  $\text{Ext}(I)$  or  $\text{Int}(I)$ . So  $z$  is in  $R_3(G)$  and therefore  $R_3(G)$  is the complement of  $R_1(G) \cup R_2(G)$  in  $\mathcal{H}$ . As the set of isometric circles is invariant under translations in  $G_\infty$ , it follows that  $R_1(G)$  and  $R_2(G)$  are invariant under translations in  $G_\infty$ . As  $R_3(G)$  is the complement of  $R_1(G) \cup R_2(G)$  in  $\mathcal{H}$  and  $\mathcal{H}$  is invariant under translations in  $G_\infty$ , it follows that  $R_3(G)$  is also invariant.

(ii) The set  $R_2(G)$  is open, since it is the intersection of a union of open sets with  $\mathcal{H}$ . To show that  $R_1$  is open, suppose  $z \in R_1$ . Then, by Corollary 3.11,  $z$  has a neighborhood that meets only finitely many isometric circles. However, as  $z$  lies in the exterior of every isometric circle, it cannot lie on an isometric circle. Thus, there is some open hyperbolic disc centred on  $z$  that meets no isometric circles. As this disc is connected and meets no isometric circles, it is in either the interior or the exterior of each isometric circle. But it cannot be in any interior, as that would imply that  $z$  is not a point of  $R_1$ . So the disc must be contained in the exterior of every isometric circle and hence contained in  $R_1$ . Thus  $R_1$  is open as required.

(iii) Since  $R_1(G)$  and  $R_2(G)$  are open, it follows that  $\partial R_1(G)$  is a subset of  $R_3(G)$ . So we need to show that every point of  $R_3(G)$  is in the closure of  $R_1(G)$ . Suppose  $z \in R_3(G)$  and let  $r = \{z + iy \in \mathcal{H} \mid y > 0\}$  be the vertical ray with endpoint  $z$ . Suppose  $z' = z + iy' \in r$ ,  $z' \in r$  and  $z' \notin R_1(G)$ . Then  $z' \in R_3(G) \cup R_2(G)$ , and so  $z'$  lies on or inside some isometric circle. But then  $z$  lies inside the same isometric circle and is therefore in  $R_2(G)$ , which is a contradiction. Thus,  $z' \in R_1(G)$  for all  $z' \in r$  and so  $z$  is in the closure of  $R_1(G)$ , as required.

(iv) Note first that  $R_1(G) \cap R_\infty(G) \subseteq \widetilde{R_1(G) \cap R_\infty(G)}$ . By part (iii),  $R_1(G)$  is the disjoint union of  $\widetilde{R_1(G)}$  and  $R_3(G)$ . It follows that  $\widetilde{R_1(G) \cap R_\infty(G)}$  is equal to the disjoint union  $(R_3(G) \cap \widetilde{R_\infty(G)}) \cup (\widetilde{R_1(G) \cap R_\infty(G)})$ . Thus the proof will be complete once we show that every element of this disjoint union is a limit point of  $R_1(G) \cap R_\infty(G)$ . Now,  $\widetilde{R_\infty(G)}$  is the disjoint union of  $R_\infty(G)$  and the two lines  $L_0$  and  $L_T$ . Thus  $\widetilde{R_1(G) \cap R_\infty(G)}$  is the disjoint union of  $R_1(G) \cap R_\infty(G)$ ,  $R_1(G) \cap L_0$  and  $R_1(G) \cap L_T$ . If  $z \in R_1(G) \cap L_0$ , then every sufficiently small neighborhood of  $z$  is contained in  $R_1(G)$  and contains points with positive real parts, which are therefore in  $R_1(G) \cap R_\infty(G)$ . Hence  $\widetilde{R_1(G) \cap L_0}$  is in the closure of  $R_1(G) \cap R_\infty(G)$  and, similarly, so is  $\widetilde{R_1(G) \cap L_T}$ . Thus  $\widetilde{R_1(G) \cap R_\infty(G)}$  is in the closure of  $R_1(G) \cap R_\infty(G)$ . Next, consider  $R_3(G) \cap \widetilde{R_\infty(G)}$ . Once again, this set decomposes into the disjoint union of three sets,  $A$ ,  $A_0$  and  $A_T$ , say. The set  $A$  consists of those points of  $R_3(G)$  whose real parts are strictly between 0 and  $T$ ;  $A_0$  consists of the points of  $R_3(G)$  with real parts equal to 0; and  $A_T$  consists of those points with real parts equal to  $T$ . By the same argument as in part (iii),  $A$  consists of points in the closure of  $R_1(G) \cap R_\infty(G)$ . It is possible that  $A_0$  and  $A_T$  are empty, in which case we are done. Since  $R_3(G)$  is invariant under translations in  $G_\infty$ , if  $A_0$  is non-empty, then so is  $A_T$ . Suppose that  $A_0$  is not empty. Then it consists of exactly one point, because if not, it would contain two points  $z_1$  and  $z_2$  with  $\Re(z_1) = \Re(z_2)$ ,  $\Im(z_1) < \Im(z_2)$  and  $z_2 \in I$  for some isometric circle  $I$ ; but then  $z_1 \in \text{Int}(I)$ , which is a contradiction. Let  $A_0 = \{iy_0\}$ . As before, the ray  $r = \{z \in \mathcal{H} \mid z = iy, y > y_0\}$  is contained in  $R_1(G)$ . Take a sequence of points  $r_1, r_2, r_3, \dots$  of  $r$  that converge to  $iy_0$ . Since  $R_1(G)$  is open, there is a sequence of positive numbers  $\epsilon_1, \epsilon_2, \dots$  converging to zero such that the  $\epsilon_i$ -neighborhood of each  $r_i$  is contained in  $R_1(G)$ . Each such neighborhood contains points of  $R_1(G) \cap R_\infty(G)$ , so we obtain a sequence

of points of  $R_1(G) \cap R_\infty(G)$  that converges to  $iy_0$ , as required. A similar argument shows that if  $A_T$  is non-empty, then it is in the closure of  $R_1(G) \cap R_\infty(G)$ .

(v) This follows from the proof of part (iv). □

**COROLLARY 3.13.** *The set  $R(G)$  is a convex domain.*

*Proof.* If  $R(G)$  is convex, then it is connected, so we need to show that  $R(G)$  is convex and open. It is sufficient to show that  $R_1(G)$  is convex and open, since  $R_\infty(G)$  is convex and open. But this is clearly true:  $R_1(G)$  is convex because it is the intersection of convex sets, and it is open by the previous proposition. □

The following proposition is based on Lehner [20, p. 57].

**PROPOSITION 3.14.**  *$R(G)$  is a fundamental domain of  $G$ .*

*Proof.* By Proposition 3.12(v), the boundary of  $R(G)$  has zero hyperbolic area. If  $z$  is in  $R(G)$ , then any translation in  $G$  takes  $z$  out of  $R(G)$ . If  $g$  is not a translation, then  $g(z) \in \text{Int}(I_g) \subset R_2(G)$  and so, again,  $g(z)$  is not in  $R(G)$ . Thus each orbit of  $G$  intersects  $R(G)$  at most once, and so  $R(G)$  is contained in some fundamental set of  $G$ . It remains to show that every orbit of  $G$  has non-empty intersection with  $\widetilde{R(G)}$ . We first show that if  $z$  is not in  $\widetilde{R_1(G)}$ , then there is some  $g \in G$  such that  $g(z)$  is in  $\widetilde{R_1(G)}$ . By Proposition 3.12, if  $z_0 \notin \widetilde{R_1(G)}$ , then  $z_0$  is in  $R_2(G)$ . Let  $z_0 = x_0 + iy_0$ . There is some  $g_0$  such that  $z_0$  is inside  $I_{g_0}$ . Let  $z_1 = g_0(z_0)$  and  $z_1 = x_1 + iy_1$ . Since the action of  $g_0$  is an inversion in  $I_{g_0}$  followed by reflection in a line parallel to the imaginary axis, it follows that  $y_1 > y_0$ . Continuing in this way, either we find some  $z_i$  that is in  $\widetilde{R_1(G)}$ , or we have a sequence of distinct points  $z_0, z_1, z_2, \dots$  that are all on the same  $G$ -orbit and all elements of  $R_2(G)$ . Their imaginary parts are thus bounded above by the bound  $M$  from Lemma 3.9(i) and bounded below by  $y_0$ . These points may be translated by appropriate elements of  $G_\infty$  so that they are in  $\widetilde{R_\infty(G)}$ . The resulting points are still distinct as their imaginary parts are unchanged. This yields an accumulation point of an orbit of  $G$  that is  $\mathcal{H}$ , but this is impossible since  $G$  is discrete.

We conclude that the orbit of  $z_0$  must intersect  $\widetilde{R_1(G)}$ . So, by applying a translation in  $G_\infty$  if necessary, we obtain a point in  $\widetilde{R_\infty(G)}$  and hence in  $\widetilde{R(G)}$ , as required. □

**PROPOSITION 3.15.**  *$R(G)$  is locally finite.*

*Proof.* We have to show that every compact subset of  $\mathcal{H}$  meets only finitely many  $G$ -images of  $R(G)$ . Suppose not; then we can find some compact subset  $C$ , a sequence of points  $z_0, z_1, \dots$  in  $R(G)$  and a sequence of distinct elements  $g_0, g_1, \dots$  in  $G$  such that  $g_i(z_i)$  is in  $C$  for  $i = 1, 2, 3, \dots$ . Since  $C$  is bounded in the hyperbolic metric, it is contained in some hyperbolic disc of finite radius, which is some Euclidean disc contained in  $\mathcal{H}$ . It follows that there are only finitely many translations  $t$  in  $G$  such that  $t(R(G))$  has non-empty intersection with  $C$ .

Thus, by passing to a subsequence if necessary, we can assume that each term of the sequence  $g_1, g_2, \dots$  has an isometric circle. By Proposition 3.10, there are only finitely many isometric circles whose interiors meet  $C$ . Thus, again, by passing to a subsequence if necessary, we can assume that we have an infinite sequence of distinct group elements  $g_0, g_1, g_2, \dots$  such that  $I_{g_i} = I_{g_j}$  for all  $i, j \geq 1$ . (Recall that by Lemma 3.6(ii),  $g_i(z_i)$  is a point in  $\text{Int}(I_{g_i})$ .) This implies that for  $i = 1, 2, 3, \dots$ ,  $g_i = g_0 t_i$  for some translation  $t_i \in G_\infty$ . As the  $g_i$  are all distinct, the translations  $t_i$  are all distinct. It follows that  $|\Re(t_i(z_i))| \rightarrow \infty$  as  $i \rightarrow \infty$ . But then  $\Im(g_i(z_i)) = \Im(g_0(t_i(z_i))) \rightarrow 0$  as  $i \rightarrow \infty$ , and this is a contradiction since  $C$  is bounded away from the real axis. □



We have now shown that  $R(G)$  is a convex, locally finite, fundamental domain of  $G$ . We next investigate the structure of the boundary of  $R(G)$  in more detail. Following Beardon [1, p. 218], we shall call the maximal geodesic segments of the boundary of  $R(G)$  the *edges* of  $R(G)$ . Although an edge of  $R(G)$  is not necessarily a side of  $R(G)$ , we shall see later (in Proposition 3.26) that this is usually the case. We start by finding the decomposition of  $R_3(G) \cap \widetilde{R_\infty(G)}$  into edges of  $R(G)$ .

**LEMMA 3.16.** *There are finitely many distinct isometric circles  $I_1, I_2, \dots, I_k$  such that  $R_3(G) \cap \widetilde{R_\infty(G)}$  is the union  $\gamma_1 \cup \gamma_2 \cup \dots \cup \gamma_k$  where  $\gamma_i = I_i \cap R_3(G) \cap \widetilde{R_\infty(G)}$  for  $i = 1, \dots, k$ . Each  $\gamma_i$  is an edge of  $R(G)$ . If an endpoint of  $\gamma_i$  is in  $\mathcal{H}$ , then  $\gamma_i$  includes this endpoint. If  $i \neq j$ , then the intersection  $\gamma_i \cap \gamma_j$  is empty, except possibly when  $j = i + 1$ . When  $j = i + 1$ , then either the intersection is empty, in which case the circles  $I_i$  and  $I_j$  meet in a single point on the real line, or the intersection  $\gamma_i \cap \gamma_j$  consists of a single point, which is then the common endpoint of  $\gamma_i$  and  $\gamma_{i+1}$  in  $\mathcal{H}$ . Each side of  $R(G)$  is either  $L_0 \cap \widetilde{R_1(G)}$ ,  $L_T \cap \widetilde{R_1(G)}$  or a sub-geodesic segment of some  $\gamma_i$ . Each  $\gamma_i$  contains only finitely many sides of  $R(G)$ .*

*Proof.* First, we observe that if  $t$  is the translation  $z \mapsto z + T$ , then

$$\begin{aligned} t(\widetilde{R(G)}) \cap \widetilde{R(G)} &= t(\widetilde{R_1(G)} \cap \widetilde{R_\infty(G)}) \cap \widetilde{R(G)} \\ &= \widetilde{R_1(G)} \cap t(\widetilde{R_\infty(G)}) \cap \widetilde{R(G)} \\ &= \widetilde{R_1(G)} \cap L_T = (L_T \cap R_1(G)) \cup (L_T \cap R_3(G)). \end{aligned}$$

Let  $s_T = (L_T \cap R_1(G)) \cup (L_T \cap R_3(G))$ . Then  $s_T$  and  $s_0 = (L_0 \cap R_1(G)) \cup (L_0 \cap R_3(G))$  are sides of  $R(G)$ , which are paired by  $t$  and  $t^{-1}$ .

Now consider the part of the boundary of  $R(G)$  consisting of  $R_3(G) \cap \widetilde{R_\infty(G)}$ ; call this  $\beta$ . Since  $R(G)$  is a locally finite, fundamental domain, by Theorem 3.4 we have  $\beta = \bigcup_{j=1}^n s_j$  where the  $s_j$ ,  $j = 1, \dots, n$ , are sides of  $R(G)$ . Let  $s$  be one of these sides, and let  $z$  be a point of  $s$  that is not an endpoint. As  $z$  is in  $R_3(G)$ , there is some isometric circle  $I$  such that  $z \in I$ . If  $s$  is not a subset of  $I$ , then as both  $s$  and  $I \cap \mathcal{H}$  are geodesics, they must meet at  $z$  and at no other points of  $\mathcal{H}$ . But then there must be points of  $s$  that are in  $\text{Int}(I)$  and hence are not points of  $\beta$ , which is a contradiction. It follows that  $s$  is a subset of  $I$ . Thus there are finitely many isometric circles  $I_i$ ,  $i = 1, \dots, k$ , such that  $\beta = \bigcup_{j=1}^n s_j = \bigcup_{i=1}^k \beta \cap I_i$ . For  $i = 1, \dots, k$ , let  $\gamma_i = \beta \cap I_i$ , so that each  $\gamma_i$  is a union of finitely many sides of  $R(G)$ .

Now let  $I$  be any one of the isometric circles  $I_1, \dots, I_k$ . If  $z_1$  and  $z_2$  are distinct points of  $I \cap \beta$  and  $z$  lies on the geodesic segment between  $z_1$  and  $z_2$ , then  $z$  cannot be in  $R_2(G)$  since this would imply that either  $z_1$  or  $z_2$  also lies in  $R_2(G)$ . So  $\gamma = I \cap \beta$  is a convex set and hence an edge of  $R(G)$ . We thus have the required decomposition of  $\beta$  into edges of  $R(G)$ .

Two of these edges intersect in at most one point, which, if it exists, must be a common endpoint, since otherwise points of one of the edges would be in the interior of the isometric circle corresponding to the other edge.

If  $\gamma$  is an edge contained in  $\beta$ , then its projection onto  $\mathbb{R}$  is an interval  $\text{Proj}_\gamma$ . If  $\gamma'$  is another edge contained in  $\beta$ , then  $\text{Proj}_\gamma$  and  $\text{Proj}_{\gamma'}$  intersect in at most one point, since otherwise there would be points on one edge that lie in the interior of the isometric circle corresponding to the other edge. Thus, we can reorder the edges by, say, the midpoints of the corresponding intervals. If two consecutive projected intervals did not meet at a common endpoint, then the hyperbolic area of  $R(G)$  would be infinite, which is a contradiction. So, either two consecutive edges meet in  $\mathcal{H}$ , or their closures in  $\mathbb{C}$  meet at a point on the real line. Thus, the decomposition of  $\beta$  into a union of edges has the required intersection properties. □

Some authors adopt a convention in which every elliptic fixed point of order 2 on the boundary of  $R(G)$  is considered to be a vertex. In this convention, the single ‘self-paired’

side  $s$  is considered as two sides meeting at the fixed point. We do not follow this convention here. It is, however, useful to keep track of these points. To do so, we shall call a fixed point of order 2 on a ‘self-paired’ side a *pseudo-vertex*.

We have now established all of the standard properties, as given in Theorem 3.4, for the Ford fundamental domain  $R(G)$ . In order to develop an algorithm for finding the Ford fundamental domain of a group  $G$ , it will be helpful to record some additional properties. We start with a lemma concerning the orbit of a vertex.

LEMMA 3.17. *If  $v$  is a vertex of  $R(G)$  and  $g$  is an element of  $G$  such that  $g(v)$  is also a vertex of  $R(G)$ , then there is some sequence of side-pairing elements  $g_1, g_2, \dots, g_w \in P$  such that  $g = g_w g_{w-1} \dots g_2 g_1$ . Moreover, for  $j = 2, \dots, w$ , the two sides  $\phi(g_j^{-1})$  and  $\phi(g_{j-1})$  have a common endpoint  $g_{j-1} g_{j-2} \dots g_2 g_1(v)$ . Also,  $v$  is an endpoint of  $\phi(g_1^{-1})$ .*

*Proof.* This follows from Beardon [1, Theorem 9.3.3]. See also Ford [13, Section 26] for an extended discussion. □

The cycle of a vertex  $V$  is defined to be the intersection of the orbit  $G(v)$  with  $\widetilde{R(G)}$ . By Lemma 3.17, the cycle of a vertex can be calculated using only the action of the pairing transformations on the sides of  $R(G)$ .

The sum of the angles subtended by  $R(G)$  at each vertex of a cycle is related to the order of the stabilizer of any vertex in the cycle, as described in the following lemma.

LEMMA 3.18. *Let  $O = O(v) = \{v_1, v_2, \dots, v_n\}$  be the cycle of the vertex  $v$ , where  $v_1 = v$ , and for  $i = 1, \dots, n$  let  $\theta_i$  be the angle subtended by  $R(G)$  at  $v_i$ . Let  $\text{Ord}(v)$  be the order of the subgroup of  $\widetilde{G} = G/\{\pm 1_2\} \cap G$  that stabilizes  $v$ ; this is finite and equal to the order of the stabilizer of any element of  $O(v)$ . Then  $\theta_1 + \theta_2 + \dots + \theta_n = 2\pi/\text{Ord}(v)$ .*

*Proof.* See Beardon [1, Theorem 9.3.5]. □

Note that, as explained in [13, Section 26], Lemma 3.17 can be used to find a generator for the stabilizer of  $v$ . We do not discuss the details of this computation, as it is not used in the algorithm given below for finding the Ford fundamental domain. These generators were, however, computed and are included in the data files.

The points of  $\mathbb{R}$  which are in the closure of  $R(G)$  in  $\mathbb{C}$ , together with the point  $\infty$ , are called the vertices at infinity of  $R(G)$ . By Lemma 3.16, there are finitely many vertices at infinity of  $R(G)$ . In the terminology of [1, Definition 9.3.7], these points are *proper vertices at infinity* of  $R(G)$ ; that is, they are common endpoints ‘at infinity’ of two sides of  $R(G)$ . In general, a Fuchsian group may have vertices at infinity which are *improper*; see, for example, [1, p. 223] for a discussion. The results given above for vertices of  $R(G)$  hold, with minimal modifications, for vertices at infinity of  $R(G)$ . If  $v$  is a vertex at infinity of  $R(G)$ , then let the cycle of  $v$  be the intersection of  $G(v)$  with the set of vertices at infinity of  $R(G)$ .

LEMMA 3.19. *Let  $v$  be a vertex at infinity of  $R(G)$ , where  $G$  is a finitely generated Fuchsian group of the first kind.*

- (i) *The cycle of  $v$  is finite.*
- (ii) *The subgroup of  $G$  that stabilizes  $v$  is a parabolic subgroup.*
- (iii) *If  $g$  is an element of  $G$  such that  $g(v)$  is also a vertex at infinity of  $R(G)$ , then there is some sequence of side-pairing elements  $g_1, g_2, \dots, g_w \in P$  such that  $g = g_w g_{w-1} \dots g_2 g_1$ . Moreover, for  $j = 2, \dots, w$ , the two sides  $\phi(g_j^{-1})$  and  $\phi(g_{j-1})$  have a common endpoint in  $E$ , namely  $g_{j-1} g_{j-2} \dots g_2 g_1(v)$ . Also,  $v$  is an endpoint of  $\phi(g_1^{-1})$ .*

*Proof.* The finiteness of the cycle of  $v$  follows from Lemma 3.16. That the stabilizer of  $v$  is parabolic follows from [1, Theorem 9.3.8], which says that the stabilizer is either parabolic or trivial, and [20, Theorem 2, Section 41], which tells us that the stabilizer cannot be trivial if the fundamental domain has finitely many sides. (This section of [20] concerns Dirichlet fundamental domains, but the proof of that particular theorem applies more generally.) The proof of the last part of the lemma is essentially identical to the proof in the case where  $v$  is a vertex.  $\square$

As we shall see in Section 5, we make use of the cycles of the vertices of  $R(G)$  in the calculation of the hyperbolic area of  $R(G)$ . To find the cycles, we need an efficient method of finding the pairing transformations. The following lemma supplies this method, provided that we know the isometric circles and sides which appear in Lemma 3.16.

LEMMA 3.20. *Suppose that  $s$  is a side of  $R(G)$  contained in an isometric circle  $I$ . Suppose that  $g \in G$  pairs  $s$  with the side  $s'$ . Then  $I = I_g$ .*

*Proof.* Suppose not; that is, suppose  $I_g$  and  $I$  are distinct. As their intersections with  $\mathcal{H}$  are hyperbolic geodesics, they intersect in at most one point in  $\mathcal{H}$ . Since no points of  $s$  are in  $R_2(G)$ , with the exception of at most one point,  $s$  must be contained in  $\text{Ext}(I_g)$ . It follows that, except for perhaps one point,  $g(s)$  is contained in  $\text{Int}(I_{g^{-1}})$ . But then  $s'$  cannot be a side of  $R(G)$ , which is a contradiction.  $\square$

Lemma 3.20 determines  $g$  up to a translation. But, as  $s$  and  $s'$  lie between 0 and  $T$ , this translation is easily found and so we have a simple algorithm for finding the pairing transformations, given the isometric circles and sides bounding  $R(G)$ .

In order to implement the algorithms of the next sections, we shall need a more precise description of the relationship between the sides and edges of  $R(G)$  than that given in Lemma 3.16.

We start with some preliminary lemmas.

LEMMA 3.21. *Suppose that  $g = e^{-1/2} \begin{pmatrix} ae & b \\ cf & de \end{pmatrix}$  is an element of  $\Gamma_0(f)^+$ , where  $c \neq 0$ . Let  $L_x = \{z \in \mathcal{H} \mid \Re(z) = x\}$ . Then, for each integer  $i$ , either  $I_g \cap L_i$  is empty or the centre of  $I_g$  lies on  $L_i$ .*

*Proof.* By translating by an integer if necessary, we can assume  $x = 0$ . The circle  $I_g$  has centre  $-de/cf$  and radius  $\sqrt{e}/f|c|$ . If  $-de/cf < 0$ , then  $I_g$  intersects  $L_0$  if and only if  $-de/cf + \sqrt{e}/f|c| > 0$ . (Note that by definition  $L_0$  does not contain the origin.) This implies that  $d^2e < 1$ , and, as  $d$  and  $e$  are integers and  $e > 0$ , we must have  $d = 0$ , which is a contradiction.

A similar argument in the case where  $-de/cf > 0$  also leads to a contradiction. We conclude that  $d = 0$ , and so if  $I_g \cap L_0$  is not empty, then the centre of  $I_g$  is on the line  $L_0$ .  $\square$

This lemma is useful in two ways. As we shall see below, it allows us to simplify the classification of the sides of  $R(G)$ , since with our choices the edges of  $R(G)$  are the sides of  $R(G)$ , with at most one exception.

It also tells us that we need only consider those isometric circles whose centres are in the interval  $[0, T]$ , as follows.

COROLLARY 3.22. *Suppose that  $G$  is a subgroup of  $\Gamma_0(f)^+$  and  $I_g$  is an isometric circle of  $G$ . If  $I_g \cap R_\infty(G)$  is not empty, then the centre of  $I_g$  lies in the interval  $[0, T]$ .*

*Proof.* If the centre of  $I_g$  does not lie in the interval  $[0, T]$  but  $I_g$  has non-trivial intersection with  $R_\infty(G)$ , then  $I_g$  meets either  $L_0$  or  $L_T$ . In either case we obtain a contradiction.  $\square$

LEMMA 3.23. *If  $z \in R_3(G)$  and  $g \in G - G_\infty$  is such that  $g(z) \in R_3(G)$ , then  $z \in I_g$ .*

*Proof.* Since  $z$  is in  $R_3(G)$ , there is some isometric circle  $I$  such that  $z \in I$ . If  $I = I_g$ , then we are done. So suppose  $I \neq I_g$ . Since the intersections of  $I$  and  $I_g$  are geodesics,  $I \cap I_g \cap \mathcal{H}$  consists of at most one point. If this point is  $z$ , again we are done; so suppose not. Then, since  $z$  is not in  $R_2(G)$ , we must have  $z \in \text{Ext}(I_g)$ . But then  $g(z) \in \text{Int}(I_{g^{-1}}) \subseteq R_2(G)$ , which is a contradiction. So  $z \in I_g$  as required.  $\square$

LEMMA 3.24. *If  $z_1$  and  $z_2$  are in  $R_3(G)$  and  $z_2 = g(z_1)$  for some  $g$  in  $G$ , then  $\Im(z_1) = \Im(z_2)$ .*

*Proof.* If  $g$  is an element of  $G_\infty$ , then  $g$  acts as a translation and so the imaginary parts of  $z_1$  and  $z_2$  are equal. Otherwise, we can apply Lemma 3.23 to conclude that  $z_1 \in I_g$ , so the action of  $g$  is to reflect  $z_1$  in a line parallel to the imaginary axis; thus  $z_1$  and  $z_2$  again have the same imaginary part.  $\square$

As in Lemma 3.16, a maximal geodesic segment of positive length contained in  $R_3(G)$  will be called an edge of  $R_3(G)$ . Note that in Lemma 3.16, the segments  $\gamma_2, \dots, \gamma_{k-1}$  are edges of both  $R(G)$  and  $R_3(G)$ . Although  $\gamma_1$  and  $\gamma_k$  are edges of  $R(G)$ , they may or may not be edges of  $R_3(G)$ .

Thus an edge of  $R_3(G)$  is not necessarily an edge of  $R(G)$ , but, as we now show, they are closely related.

LEMMA 3.25. *Suppose that  $\gamma \subseteq R_3(G)$  is a geodesic segment of positive length. Let  $z_1$  and  $z_2$  be distinct points in  $\gamma$ . If  $g$  is an element of  $G$  such that  $g(z_1) \in R_3(G)$  and  $g(z_2) \in R_3(G)$ , then  $g(\gamma) \subseteq R_3(G)$ . In particular, if  $\gamma$  is an edge of  $R_3(G)$  and  $g(\gamma)$  intersects  $R_3(G)$  in at least two points, then  $g(\gamma)$  is an edge of  $R_3(G)$ .*

*Proof.* First, if  $g$  is a translation, then since  $R_3(G)$  is invariant under translations it follows that  $g(\gamma) \subseteq R_3(G)$ . Suppose next that  $g$  is not a translation. Then, by Lemma 3.23, we have  $z_1 \in I_g$  and  $z_2 \in I_g$ . Since  $I_g \cap \mathcal{H}$  is a geodesic and  $I_g \cap \gamma$  contains the distinct points  $z_1$  and  $z_2$ , it follows that we must have  $\gamma \subseteq I_g$ . Suppose there is some point  $s \in \gamma$  such that  $g(s)$  is not in  $R_3(G)$ . We will show that this leads to a contradiction. Since  $g(s) \in I_{g^{-1}}$ , we have that  $g(s)$  is not in  $R_1(G)$  and so  $g(s)$  is in  $R_2(G)$ . Hence there is some  $g'$  such that  $g(s) \in \text{Int}(I_{g'})$ , and then  $\Im(g'(g(s))) > \Im(s)$ . Continuing in this way, we obtain a sequence of points with strictly increasing imaginary parts. As in Proposition 3.15, if all these points are in  $R_2(G)$ , then we obtain an accumulation point of an orbit of  $G$ , which gives a contradiction. Otherwise, after a finite number of steps, we obtain a point  $w$  that is in either  $R_1(G)$  or  $R_3(G)$ . By Lemma 3.24,  $w$  cannot be in  $R_3(G)$  and so must be in  $R_1(G)$ . But  $R_1(G)$  is invariant under translations, and the image of a point of  $R_1(G)$  by an element of  $G$  that is not a translation is in  $R_2(G)$ ; so there are no points of  $R_1(G)$  that are images of points in  $R_3(G)$ , and hence  $w$  is not an element of  $R_1(G)$ . This is a contradiction. Therefore, for every point  $s$  of  $\gamma$ ,  $g(s)$  is in  $R_3(G)$  as required.

Finally, if  $\gamma$  is an edge of  $R_3(G)$  and  $g(\gamma)$  intersects  $R_3(G)$  in at least two points, then, as we have just shown,  $g(\gamma)$  is contained in  $R_3(G)$  and hence is contained in some edge  $\gamma'$  of  $R_3(G)$ . But then  $g^{-1}(\gamma')$  contains  $\gamma$  and so must be equal to  $\gamma$ , since  $\gamma$  is an edge of  $R_3(G)$ . Thus  $g(\gamma) = \gamma'$ , as required.  $\square$

Roughly speaking, Lemma 3.25 says that the sides of  $R_3(G)$  are the edges of  $R_3(G)$ . We will use this result, together with Lemma 3.21, to show that the edges of  $R(G)$  are sides, with

one possible exception. This assumes our choice of  $R_\infty(G)$  and that  $G$  is a subgroup of some  $\Gamma_0(f)^+$ . First, we require some notation. The reader may find it helpful at this point to look at the example in Section 6.

If there is some edge  $\mathcal{E}$  of  $R_3(G)$  such that  $\mathcal{E} \cap L_0$  is not empty, then the translate of  $\mathcal{E}$  by  $T$  meets  $L_T$  in  $\mathcal{H}$  also. In this case, we let  $\mathcal{E}_l$  be the part of  $\mathcal{E}$  whose points have non-negative real parts and let  $\mathcal{E}_r$  be the part of the translate of  $\mathcal{E}$  by  $T$  whose points have real parts less than or equal to  $T$ . This is illustrated in Figure 1 (see Section 6). In this example, side 2 is  $\mathcal{E}_l$  for this fundamental domain while side 8 is  $\mathcal{E}_r$ .

We next describe the sides of  $R(G)$ . Recall the notation  $A_0$  and  $A_T$  from the proof of Proposition 3.12(iv).

PROPOSITION 3.26. *The sides of  $R(G)$  are as follows:*

- (i)  $s_0 = (L_0 \cap R_1(G)) \cup A_0$ ;
- (ii)  $s_T = (L_T \cap R_1(G)) \cup A_T$ ;
- (iii)  $\mathcal{E}_l$ , if it exists;
- (iv)  $\mathcal{E}_r$ , if it exists;
- (v) all the edges of  $R_3(G)$  that are contained in  $R_\infty(G)$ , with at most one exception, which is described below.
- (vi) The exception occurs if there is some edge  $\gamma$  of  $R_3(G)$  that is contained in  $R_\infty(G)$  and for which there exists some pairing transformation  $g$  with  $g(\gamma) \cap L_0$  not empty. In this case, let  $x_0$  be the centre of the isometric circle that contains  $\gamma$ . Then  $L_{x_0}$  intersects  $\gamma$ , and the point of intersection is a vertex of  $R(G)$ . The edge  $\gamma$  consists of two sides which meet at this common vertex. These two sides are paired with  $\mathcal{E}_l$  and  $\mathcal{E}_r$ . If this exception does not occur, and if  $\mathcal{E}_l$  and  $\mathcal{E}_r$  exist, then  $\mathcal{E}_l$  and  $\mathcal{E}_r$  are paired.

*Proof.* That the union of these sets form the boundary of  $R(G)$  follows from Proposition 3.12. By Proposition 3.12(v) and Lemma 3.16,  $s_0$  and  $s_T$  are sides and edges of  $R(G)$  paired by the translation  $z \mapsto z + T$  and its inverse.

Suppose that  $\gamma$  is an edge of  $R(G)$ , other than  $s_0$  or  $s_T$ , which contains a side  $s$ . Suppose also that  $s$  is paired with the side  $s'$  by  $g$  and that  $s'$  is contained in an edge  $\gamma'$  of  $R(G)$ . So  $\gamma'$  is also neither  $s_0$  nor  $s_T$ .

If  $\gamma$  is an edge of  $R_3(G)$ , then by Lemma 3.25  $g(\gamma)$  is also an edge of  $R_3(G)$ . If  $g(\gamma)$  is contained in  $R_\infty(G)$ , then by Lemma 3.16 it is an edge of  $R(G)$ ; but then it must also be a side of  $R(G)$ , since it is contained in the side  $\widetilde{R(G)} \cap g\widetilde{R(G)}$ . So we have that  $s = \gamma$  and  $s' = \gamma'$ . Since  $g(\gamma)$  contains  $\gamma'$ , if  $g(\gamma)$  is not contained in  $R_\infty(G)$ , then  $\gamma'$  is not an edge of  $R_3(G)$ .

Thus it remains to consider the cases where either  $\gamma$  or  $\gamma'$  is not an edge of  $R_3(G)$ . Without loss of generality we can assume it is  $\gamma$  that is not an edge of  $R_3(G)$ . So  $\gamma$  is contained in some edge  $\delta$  of  $R_3(G)$ . Again, by Lemma 3.16, if  $\delta$  is contained in  $R_\infty(G)$ , then it is an edge of  $R(G)$ . This implies  $\gamma = \delta$ , which is a contradiction, and so  $\delta$  contains either  $\mathcal{E}_l$  or  $\mathcal{E}_r$ . Suppose that  $\delta$  contains  $\mathcal{E}_l$  (the case where  $\delta$  contains  $\mathcal{E}_r$  is similar). In particular, the side  $s$  of  $R(G)$  is contained in  $\mathcal{E}_l$ . The image  $g(\gamma)$  is contained in some edge  $\delta'$  of  $R_3(G)$  such that  $g(\delta) = \delta'$ . One possibility is that  $\delta'$  is contained in  $R_\infty(G)$  and hence is an edge of  $R(G)$ . In this case, we have  $g^{-1}\delta' = \delta$  and so  $g^{-1}\delta' \cap \widetilde{R(G)} = \mathcal{E}_l$ . This implies that  $\mathcal{E}_l$  is a side of  $R(G)$  and so  $s = \mathcal{E}_l$ . Similarly,  $\mathcal{E}_r$  is a side of  $R(G)$  which is paired with a subsegment of  $\delta'$  via a translation by  $-T$  followed by the transformation  $g$ . As  $\delta$  is the union of  $\mathcal{E}_l$  and the translation of  $\mathcal{E}_r$  by  $-T$  and  $\delta'$  is the image of  $\delta$  by  $g$ , we see that  $\delta'$  consists of two sides, one of which is paired with  $\mathcal{E}_l$  and the other with  $\mathcal{E}_r$ . By Lemma 3.24, the common vertex of these two sides is on the vertical line passing through the centre of the isometric circle  $I$  that contains  $\delta'$ .

The other possibility is that  $\delta'$  is not contained in  $R_\infty(G)$ . In this case, part of  $\delta'$  is  $\mathcal{E}_r$ . (It cannot contain  $\mathcal{E}_l$  by Lemmas 3.21 and 3.24.) Thus the side  $s$  is contained in  $\mathcal{E}_l$  and is paired

with the side  $s'$ , which is contained in  $\mathcal{E}_r$ , by some  $g$  in  $G$ . It again follows that  $g(\delta) = \delta'$ , and so if  $t$  is the translation  $z \mapsto z - T$ , we have that  $tg(\delta) = \delta$  by Lemma 3.25. Thus  $h = tg$  is an element of projective order 2 and  $\delta$  is contained in  $I_h = I_{h^{-1}}$ . It follows that the imaginary axis is an axis of symmetry of  $\delta$ . So  $g = t^{-1}h$  maps  $\mathcal{E}_l$  to  $\mathcal{E}_r$ . Thus, in this case also,  $\mathcal{E}_l$  and  $\mathcal{E}_r$  are sides of  $R(G)$ . □

We emphasize again that the simple form of the sides of  $R(G)$  in the previous proposition depends on the fact that  $G$  is a subgroup of some  $\Gamma_0(f)^+$  and also on the choice of  $R_\infty(G)$ .

Finally, we record the following technical lemma, which will be needed in the next section.

LEMMA 3.27. *Let  $C$  be a finite set of isometric circles. Let  $I_1, I_2$  and  $J$  be isometric circles with centres  $x_1, x_2$  and  $x_J$ , respectively, where  $x_1 < x_J < x_2$ . For  $i = 1, 2$ , let  $D_i = C \cup \{I_i\}$  and  $D = D_1 \cup D_2$ ; also let  $\rho_i = \bigcap_{I \in D_i} \text{Ext}(I) \cap \mathcal{H}$  and  $\rho = \rho_1 \cap \rho_2$ . Suppose that for any  $I$  in  $C$  with centre  $x_I$ , we have  $x_I \notin [x_1, x_2]$ . Suppose also that there are geodesic segments  $\gamma_1$  and  $\gamma_2$  in  $\mathcal{H}$  of positive length such that  $\gamma_1 \in I_1 \cap \rho_2$  and  $\gamma_2 \in I_2 \cap \rho_1$ . Then there is a geodesic segment  $\gamma$  in  $\mathcal{H}$  of positive length such that  $\gamma \subseteq J \cap \rho$  if and only if  $I_1 \cap I_2 \subseteq \text{Int}(J)$ ,  $J \not\subseteq I_1 \cup \text{Int}(I_1)$  and  $J \not\subseteq I_2 \cup \text{Int}(I_2)$ .*

*Proof.* We consider the three cases of  $I_1 \cap I_2 = \emptyset$ ,  $I_1 \cap I_2 = \{p\}$  (with  $p \in \mathbb{R}$ ) and  $I_1 \cap I_2 = \{p, \bar{p}\}$  with  $p \in \mathcal{H}$ . In the case where the intersection is empty, let  $S$  be the subinterval of  $[x_1, x_2]$  consisting of the points exterior to both circles together with the two endpoints. Suppose  $S = [a, b]$ . Then no circle in  $C$  can meet the region  $K = \{z \in \mathbb{C} \mid a \leq \Re(z) \leq b\}$ , since any such circle would contain either  $I_1$  or  $I_2$ . But this contradicts the assumption of the existence of the geodesics  $\gamma_1$  and  $\gamma_2$ . Now, if  $J \subseteq I_1 \cup \text{Int}(I_1)$  or  $J \subseteq I_2 \cup \text{Int}(I_2)$ , then it follows that no points of  $J$  are external to both  $I_1$  and  $I_2$  and so there is no  $\gamma$  contained in  $J \cap \rho$ . Conversely, if  $J \not\subseteq I_1 \cup \text{Int}(I_1)$  and  $J \not\subseteq I_2 \cup \text{Int}(I_2)$ , then  $J$  must meet the interior of  $K$ . Taking  $\gamma = J \cap K \cap \mathcal{H}$ , we have that  $\gamma$  is external to both  $I_1$  and  $I_2$  and, by the argument above, external to the circles of  $C$ ; hence it is contained in  $J \cap \rho$  as required.

If  $I_1 \cap I_2 = \{p\}$ , let  $r$  be the ray  $z = p + iy, y > 0$ . As in the first case, the circles in  $C$  cannot meet  $r$ , owing to the assumption of the existence of  $\gamma_1$  and  $\gamma_2$ . Now, if  $\{p\} \not\subseteq \text{Int}(J)$ , then necessarily either  $J \subseteq \text{Int}(I_1)$  or  $J \subseteq \text{Int}(I_2)$ , and once again there is no  $\gamma$ . Conversely, if  $p$  is in  $\text{Int}(J)$  (and hence also  $J \not\subseteq I_1 \cup \text{Int}(I_1)$  and  $J \not\subseteq I_2 \cup \text{Int}(I_2)$ ), then  $J$  meets  $r$  at some point, say  $z$ . Thus there is some open neighborhood  $N$  of  $z$  that is contained in  $\rho$ , and so  $N \cap J$  is the required geodesic  $\gamma$ .

Finally, suppose  $I_1 \cap I_2 = \{p, \bar{p}\}$  with  $p \in \mathcal{H}$ . Let  $r$  be the ray  $p + iy, y > 0$ . Suppose that  $I$  is a circle in  $C$  with centre  $x_I$  such that  $x_2 < x_I$ . If  $I$  meets  $r$ , then the points of  $I_2 \cap \mathcal{H}$  with real parts greater than or equal to the real part of  $p$  are contained in  $I$ . It is possible that  $I$  meets  $I_2$  in  $\mathcal{H}$ , but the point of intersection has real part less than the real part of  $p$ , so the points of  $I_2$  that are external to  $I$  are inside  $I_1$ . Thus, no part of  $I_2$  is in  $\rho_1$ , which contradicts the existence of  $\gamma_2$ . A similar argument for when the centre of  $I$  is less than  $x_1$  shows that no circle in  $C$  meets  $r$ . Now, let  $W$  be the complement of  $\text{Int}(I_1) \cup \text{Int}(I_2)$  in  $\mathbb{C}$ . The set  $W$  is closed, and so the Euclidean distance  $d(z, x_J)$  from  $x_J$  to  $z \in W$  has a minimum value. A calculation in elementary geometry shows that the minimum is attained at  $p$  and  $\bar{p}$ . Thus, if  $p$  is in  $\text{Ext}(J) \cup J$ , then there is no geodesic segment of  $J$  of positive length that is in  $\rho$ . Conversely, if  $p$  is in the interior of  $J$  (so that necessarily  $J \not\subseteq I_1 \cup \text{Int}(I_1)$  and  $J \not\subseteq I_2 \cup \text{Int}(I_2)$ ), then  $J$  meets  $r$ . Again, there is a neighborhood  $N$  of this intersection point that is contained in  $\rho$ . So  $J \cap N$  yields the required geodesic segment. □

#### 4. The algorithm

In this section, we describe an algorithm for computing the Ford fundamental domains for the groups described in Section 2.

Fix a discrete subgroup  $G$  of  $\mathrm{SL}(2, \mathbb{R})$  and assume that  $G$  contains  $-1_2$ . Then  $G$  is countable, since any discrete subgroup of  $\mathrm{SL}(2, \mathbb{R})$  is countable. So the set of isometric circles of  $G$  is a countable set. Thus we can select some sequence  $S$  consisting of all the isometric circles of  $G$ . It will be explained shortly how to generate such a sequence given a decision procedure for membership of  $G$ . For simplicity, however, we present the algorithm in a form for which it is more straightforward to verify correctness.

As explained in Section 2, we will assume that  $G$  is a subgroup of  $\Gamma_0(f)^+$  for some square-free, positive integer  $f$ .

ALGORITHM FOR COMPUTING THE FUNDAMENTAL DOMAIN

*Input:* a decision procedure to determine whether an element of  $\Gamma_0(f)^+$  is in the subgroup  $G$ ; the index of  $G$  in  $\Gamma_0(f)^+$ ; a sequence  $S = I_1, I_2, \dots$  containing every isometric circle of  $G$ .

*Output:* a finite set  $C$  of isometric circles of  $G$  which, together with  $L_0$  and  $L_T$ , bound a fundamental domain  $R(G)$  of  $G$ .

---

```

 $C \leftarrow \{\}$ 

 $T \leftarrow$  the smallest positive integer  $T$  such that  $\begin{pmatrix} 1 & T \\ 0 & 1 \end{pmatrix}$  is in  $G$ 

 $R_\infty \leftarrow \{x + iy \in \mathbb{C} \mid y > 0, 0 < x < T\}$ 

while  $\mathrm{Area}(C) \neq \mathrm{Index}(\Gamma_0(f)^+ : G) \times \mathrm{Area}(\Gamma_0(f)^+)$ 

   $I \leftarrow$  next isometric circle from  $S$ 

  if  $I$  contains a geodesic segment of positive length that is contained in  $R_\infty$ 
    and is external to all the circles of  $C$ , then

     $C \leftarrow C \cup \{I\}$ 
    remove any circles whose geodesic segments in  $R_\infty$  external to the other circles in  $C$ 
    are now contained in  $I \cup \mathrm{Int}(I)$ 

  end if

end while

return  $C$ 

```

---

The procedure  $\mathrm{Area}(C)$  is any procedure that returns either  $-1$  or the hyperbolic area of the region  $R(C) = R_\infty \cap \bigcap_{I \in C} \mathrm{Ext}(I)$ , with the restriction that it must return the hyperbolic area if  $R(C) = R(G)$ . A specific choice of such a procedure is given in the next section. The details of the inner if loop will be explained in more detail shortly.

**PROPOSITION 4.1.** *The algorithm terminates and returns a set of isometric circles that, together with  $L_0$  and  $L_T$ , bound a Ford fundamental domain of  $G$ .*

*Proof.* By the results of Section 3, the Ford fundamental domain  $R(G)$  is bounded by (segments of) finitely many isometric circles of  $G$  and (segments of)  $L_0$  and  $L_T$ . So for the sequence  $S$ , there is a smallest integer  $N$  such that all the isometric circles bounding  $R(G)$  occur in the first  $N$  terms of  $S$ . We will show that the algorithm terminates after exactly  $N$  iterations.

Let  $C_i, i \geq 1$ , be the set of isometric circles after the  $i$ th iteration of the while loop. If  $C_i$  contains one of the circles that bounds  $R(G)$ , then this circle will never be removed, since it contains some geodesic segment of positive length that is external to all the other isometric circles of  $G$ . Moreover,  $C_N$  will contain no circle  $I$  that is not a bounding circle, since such an  $I$  would have to contain a geodesic segment of positive length contained in  $R_1(G)$ , which is impossible. Thus  $C_N$  consists of precisely the isometric circles that bound  $R(G)$ . So  $\text{Area}(R(C_N))$  returns  $\text{Area}(G)$ , and the algorithm terminates after at most  $N$  iterations.

The algorithm cannot terminate before  $N$  iterations. If  $\text{Area}(R(C_i))$  is infinite, then the algorithm does not terminate at the  $i$ th iteration. If the hyperbolic area of  $R(C_i)$  is finite for  $i < N$ , then its hyperbolic area is strictly larger than the hyperbolic area of  $R(G)$ , since a circle is added only if it contains points external to the circles of  $C_i$ , which would produce a region with strictly smaller hyperbolic area. □

The algorithm terminates correctly for any choice of sequence  $S$ . However, it is clearly desirable to make an efficient choice. By Corollary 3.22, for a subgroup  $G$  of some  $\Gamma_0(f)^+$ , if  $I$  is an isometric circle of  $G$ , then  $I$  meets  $R_\infty(G)$  if and only if the centre of  $I$  lies in the interval  $[0, T]$ . Thus we need only consider such circles. To generate all the isometric circles  $I$  of  $G$  such that the radius of  $I$  lies in the interval  $(r_1, r_2]$ , for  $0 < r_1 < r_2$ , while the centre of  $I$  lies in the interval  $[0, T]$ , we proceed as follows.

If  $m = e^{-1/2} \begin{pmatrix} ae & b \\ cf & de \end{pmatrix}$ , the constraints on the radius and centre of  $I_m$  yield a finite set of values for  $e, c$  and  $d$  as follows. As  $e$  is a divisor of  $f$ , there are only finitely many choices for  $e$ . The radius of  $I_m$  is  $e^{1/2}/|c|f$ , and  $c$  is an integer, so the bounds on the radius of  $I_m$  are satisfied by only finitely many values of  $c$ . Finally, the centre of  $I_m$  is at  $-de/cf$  and so, given  $c$  and  $e$ , since  $d$  is an integer there can only be finitely many values of  $d$  such that the centre of  $I_m$  is in the interval  $[0, T]$ . Given the values of  $e, c$  and  $d$ , we can then find some choice for  $m$  by finding some solution to the determinant equation  $ade^2 - bcf = e$  for  $a$  and  $d$ . The other elements of  $\Gamma_0(f)^+$  with the same isometric circle are  $\pm t^i m$ , where  $i \in \mathbb{Z}$  and  $t$  is the translation  $z \mapsto z + 1$ . Thus,  $I_m$  is an isometric circle of  $G$  if and only if  $t^i m \in G$  for some  $i \in \{0, 1, 2, \dots, T - 1\}$ . This we can easily test, since we assume that we have a decision procedure to test membership of  $G$ . Thus, we can generate all the isometric circles of  $G$  that satisfy the given constraints. The maximum radius of an isometric circle in any  $\Gamma_0(f)^+$  is 1; therefore, if we choose the intervals  $(r_1, r_2]$  so that they partition  $(0, 1]$ , then this procedure will generate all of the isometric circles of  $G$  whose centres lie in the interval  $[0, T]$ , as required.

The main algorithm requires a procedure for ‘refining’ a collection of isometric circles. This is provided by the following algorithm. More specifically, given  $C = C_i$  and the next isometric circle  $I$ , this algorithm determines whether or not  $I$  contains a geodesic segment of positive length that is external to all the circles in  $C_i$  and contained in  $R_\infty$ . If so,  $I$  is added to  $C$ , and any circles with geodesic segments that were originally contained in  $R_\infty$  and external to the other circles in  $C$  but which are now contained in  $I \cup \text{Int}(I)$  are removed. If  $I$  fails the test, then the algorithm just returns  $C$ . The algorithm assumes that the set  $C$  is presented as a list, sorted by the positions of the centres of the circles in  $C$ . The algorithm returns a list that is again sorted by the positions of the centres of the circles.

ALGORITHM TO ACCEPT OR REJECT THE NEXT CIRCLE

*Input:* a list  $C$  of isometric circles of  $G$  ordered by the positions of their centres; an isometric circle  $I$  of  $G$ .

*Output:* if  $I$  contains a geodesic segment of positive length that is external to all the circles in  $C_i$  and lies in  $R_\infty$ , then return a new ordered list of isometric circles including  $I$  but excluding any circles of  $C$  whose geodesic segments exterior to the other circles of  $C$  are now inside or on  $I$ ; otherwise, return  $C$ .



---

```

i ← Position(C, I)

n ← Card(C)

if n = 0 then
    return a list containing only I
end if

if i = 1 then
    if I ⊆ I1 ∪ Int(I1) then
        return(C)
    else
        return(Insert(C, I))
    end if
elif i = n + 1 then
    if I ⊆ In ∪ Int(In) then
        return(C)
    else
        return(Insert(C, I))
    end if
else
    if I ⊆ Ii-1 ∪ Int(Ii-1) or I ⊆ Ii ∪ Int(Ii) or Ii-1 ∩ Ii ⊄ Int(I) then
        return(C)
    else
        return(Insert(C, I))
    end if
end if

```

---

*Notes.*

(1) The function Position(*C*, *I*) is defined as follows. Suppose  $C = [I_1, I_2, \dots, I_n]$ , where the centre of the circle  $I_i$  is  $x_i$ , with  $x_1 < x_2 < x_3 < \dots < x_n$ . If  $x$  is the centre of  $I$ , then Position(*C*, *I*) is either the smallest  $i$  such that  $x \leq x_i$ , or  $n + 1$  if  $x > x_n$ .

(2) The function Insert(*C*, *I*) inserts  $I$  into the list  $C$ , keeping the ordering by centres; it then removes any circle with a geodesic segment that was inside  $R_\infty$  and external to the circles of  $C$  but which is now contained in  $I \cup \text{Int}(I)$ .

(3) The algorithm depends on  $n$  through the functions Position and Insert. In the particular implementation in Appendix 1, Position was implemented as a binary search with a run-time of  $O(\log(n))$ , but Insert was implemented as a simple linear calculation with a run-time of  $O(n)$ . This was sufficiently fast for our particular application.

(4) The correctness of the cases where  $i$  is not equal to 1 or  $n$  follows from Lemma 3.27. The correctness at the endpoints follows from a similar, but easier, argument using Lemma 3.21, which we omit.

(5) These procedures involve only computations in  $\text{Quad} = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots)$ . More specifically, the procedures can be written so that the only numerical computations are tests

of whether a given number in Quad is positive, negative or zero. We shall return to this point below.

5. *The procedure Area(C)*

The procedure Area(C) attempts to compute the hyperbolic area of the domain bounded by the circles of C and the vertical lines  $\Re(z) = 0$  and  $\Re(z) = T$ , using the Gauss–Bonnet formula. This area may be infinite, for example when there is some subinterval of  $[0, T]$  that is not inside any of the circles in C. In this case, Area(C) returns  $-1$ . However, there are other cases where the hyperbolic area is finite but for which it is convenient to have Area(C) return  $-1$ , as we shall discuss below.

As described in Lemmas 3.17 and 3.18, the set of vertices V of  $R(G)$  is partitioned into cycles under the action of G. The sum of the angles subtended by  $R(G)$  at each vertex of a cycle results in an angle of  $2\pi/m$ , where m is the order of the stabilizer in  $\overline{G}$  of each vertex. By Lemma 3.19, this result also applies to vertices at infinity, where the sum is zero and the stabilizer is a parabolic subgroup of G (and  $\overline{G}$ ).

By Proposition 3.26, with possibly one exception the sides of  $R(G)$  are the edges of  $R(G)$ . The exception, if it exists, can be found by testing the edges of  $R_3(G)$  that meet  $L_0$  and  $L_T$  and adding an extra vertex to one of the edges of  $R_3(G)$  contained in  $R_\infty(G)$ , if necessary. Thus, the algorithm for computing Area(C) proceeds by first attempting to find a pairing of the sides of  $R(G)$  by elements of G using Lemma 3.20. If a complete set of pairing transformations is found, then the algorithm tries to compute the induced partition of the vertices and vertices at infinity using Lemmas 3.17 and 3.19. If C is not a set of bounding circles of the Ford fundamental domain, then it is possible that these computations will fail. If this happens, then the procedure returns  $-1$ .

If a partitioning of the vertices is found, then for each cycle the sum  $\theta$  is computed. By considering possible traces of elements of  $\Gamma_0(f)^+$ , it is not difficult to show that the only possible (projective) orders of elliptic elements of  $\Gamma_0(f)^+$  are 1, 2, 3, 4 and 6. So if  $\theta$  is not equal to  $2\pi/m$  for  $m = 1, 2, 3, 4$  or 6, then the bounding circles cannot bound a fundamental domain and  $-1$  is returned.

If all of the resulting angles for vertices in the upper half-plane are  $2\pi/m$  for  $m = 1, 2, 3, 4$  or 6, then the hyperbolic area is computed using the Gauss–Bonnet formula. The area and the other computed data are then returned. Note that the partitioning of the vertices at infinity is not required for the computation of the area, since the sum of the angles subtended at these vertices is zero. This information is, however, still useful; for example, the number of equivalence classes of vertices at infinity is the cusp number of G.

It might seem that the computation of the angle  $\theta$  requires calculations outside the field Quad. However, it is a simple matter to verify that the sine and cosine of the angle formed by the intersection of two circles or of a line and a circle are in Quad. Thus, using the angle addition formulas, the sine and cosine of the sum of angles in a cycle are also in Quad. Hence, the whole algorithm can be performed using only arithmetic and order relations in Quad. These operations were implemented without using floating-point approximations.

ALGORITHM FOR COMPUTING AREA

*Input:* a decision procedure to determine whether an element of  $\Gamma_0(f)^+$  is in a subgroup G which is assumed to contain  $-1_2$ ; a set C of isometric circles of G.

*Output:* if a pairing of the sides of  $R(C)$ , the induced partitioning of the vertex set V, a set of angles associated with each cycle of vertices and Area( $R(C)$ ) are found, then return this data; otherwise, return  $-1$ .

---

If there is some subinterval  $[a, b]$  of  $[0, T]$ , with  $0 \leq a < b \leq T$ , such that  $[a, b]$  is not contained in any of the circles in  $C$ , then return  $-1$ .

For each edge of  $R(C)$ , starting with the edge that meets  $L_0$  (if it exists)

if the edge can be mapped to another edge then  
 record the pairing and group element (the two edges are sides);  
 for the exceptional case, where the initial edge meets  $L_0$  and is mapped to a subset of some other edge  $\gamma$  with  $\gamma$  contained in  $R_\infty$ ,  $\gamma$  is divided into two sides with a common endpoint at the apex of  $\gamma$   
 else if no pairing exists then  
 return  $-1$   
 end if

end for

From the pairing of the sides, compute the induced partitioning of the vertices.

For each cycle of vertices

compute the sine and cosine of the sum of the angles at each vertex

if the corresponding sum of angles is  $2\pi/m$  for  $m = 1, 2, 3, 4$  or  $6$   
 or the angle is zero then  
 record the angle  
 else  
 return  $-1$   
 end if

end for

Compute the hyperbolic area using the Gauss–Bonnet formula.

Return the area and all computed data.

---

In practice, it seems to be more efficient to avoid invoking this area algorithm after the addition of a single circle to  $C$ . A better strategy appears to be to add a set of circles, for example all the circles whose radii are in some interval, using the accept/reject algorithm. The resulting set  $C$  is then tested with the area algorithm. This approach will usually mean some unnecessary attempts to add circles after the fundamental domain has been found but not yet tested. In practice, however, since the area algorithm involves more computation, the ‘delayed evaluation’ strategy seems faster, and this is what is used in the code given in Appendix 1.

Note that the algorithm does not require that the subgroup  $G$  be a congruence subgroup. Appendix 4 contains a procedure that takes a permutation representation of  $\text{PSL}(2, \mathbb{Z})$  on the cosets of a subgroup  $G$  and returns the fundamental domain data for  $G$ . An example for a non-congruence group of index 7 is included.

## 6. An example

It is straightforward to use the data in Appendix 2 to create a decision procedure for determining whether or not a given element of  $\Gamma_0(f)^+$  is in  $G$ , where  $G$  is a congruence subgroup of genus zero or genus one, as follows. The data gives the image of  $G$  as a subgroup

$H$  of  $\Gamma_0(f)^+/G(n, f)$ , where  $n$  is the level of  $G$ . So an element  $\Gamma_0(f)^+$  is in  $G$  if and only if its image in  $\Gamma_0(f)^+/G(n, f)$  is in  $H$ . For efficient computations, these groups were constructed as permutation groups; see [8] and the data files for more details. Applying the algorithms of Section 2 then gives the fundamental domain of  $G$ , together with generating elements, side pairings, vertices corresponding to the classes of elliptic elements and vertices at infinity corresponding to the classes of parabolic fixed points. The output data is presented in Appendix 3 in the following format.

**i, j, level, label, genus, f, index:** the  $i$  and  $j$  labels are internal labels used to identify the groups in the data computed in [8]. The level, genus and  $f$  values are the level and genus of the group  $G$  and the value of  $f$  corresponding to the maximal discrete subgroup  $\Gamma_0(f)^+$  that contains  $G$ . Together with the label value, these give the corresponding entry in [8, Table 2], where the (conjugacy class of) the group  $G$  is labeled using the notation  $(\text{level})(\text{label})_f^{\text{genus}}$ .

**Cover:** the bounding circles of the fundamental domain. The notation  $[x, y, z]$  means a circle with centre  $-y/x$  and radius  $1/(x\sqrt{z})$

**ram\_classes:** information on the set of parabolic and elliptic elements stabilizing (some of) the vertices of the fundamental domain. Each entry is a pair. The second entry of the pair is a list of integers  $[a, b, c, d]$  such that the elliptic or parabolic element is  $g = e^{-1/2} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ , where  $e = ad - bc$ . The first entry of the pair is the smallest vertex label in the cycle of the fixed point of  $g$ , or 0 if  $g$  stabilizes  $\infty$ . Also included in this list is the case where the cycle corresponds to an ordinary point (that is,  $m = 1$ ); in this case, the group element is given by the list  $[1, 0, 0, 1]$ . If a bounding circle is ‘self-paired’ by an elliptic element of (projective) order 2, then we call the fixed point of this element a pseudo-vertex; it is labeled by the half-integer between the integers labeling the endpoints of the corresponding side. The first pair in **ram\_classes** always contains as its second entry a parabolic element stabilizing  $\infty$ . The vertex  $\infty$  is always labeled by  $\bar{0}$ . Here we use  $\bar{i}$  to denote the  $i$ th vertex and  $i$  to denote the  $i$ th side. In the data file, the over-bars are omitted. The vertices are labeled counterclockwise in such a way that the side  $i$  is bounded by vertices  $\bar{i} - 1$  and  $\bar{i}$ . By convention, we do not distinguish between vertices and vertices at infinity in this labeling scheme.

**Pairs:** the pairing of the sides of the fundamental domain. The numbering starts at 1 on the imaginary axis and then runs counterclockwise. A side mapped to itself by an elliptic element of order 2 is included as a ‘self-paired’ side, rather than being split into two sides.

**pairing\_mats:** the matrices of the group that pair the sides. These generate the group.

**intersection\_matrices:** if a vertex is at the intersection of two consecutive circles, a matrix obtained by inversion in first one circle and then the other is listed. For a pseudo-vertex, the matrix is  $[1, 0, 0, 1]$  by convention. The ordering of circles, vertices and pseudo-vertices is as given above.

**intersection\_points:** the coordinates of the vertices, vertices at infinity and pseudo-vertices. The notation is that  $[x, y_1, y_2]$  is the point  $x + iy_1(-y_2)^{1/2}$  with  $y_2$  square-free.

**v:** the cycles of the vertices and vertices at infinity of the fundamental domain. Pseudo-vertices, which are labeled by half-integers, are not included in this list, since they always form cycles consisting of one point.

The following example was selected as it illustrates the conventions and phenomena mentioned above. A picture of the fundamental domain is given in Figure 1. The entry  $5A_1^0$  in [8, Table 2] is the first conjugacy class (hence the label A) of level-5, genus-zero subgroups of  $SL(2, \mathbb{Z}) = \Gamma_0(1)^+$ . This conjugacy class contains five conjugate subgroups of  $SL(2, \mathbb{Z})$ , each of index 5. They are cycloidal subgroups; that is, they have cusp number equal to one. Each of these subgroups is conjugate to a ‘rational non-monstrous moonshine group’ containing  $\Gamma_0(25)$

$\bar{0}$

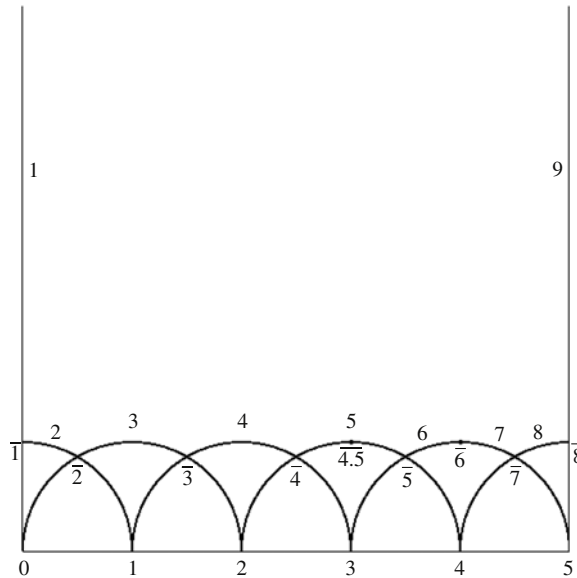


FIGURE 1. Fundamental domain for  $5A_1^0$ . Sides are labeled by integers, and vertices are labeled by integers with an over-bar. There is one pseudo-vertex labeled by  $\bar{4.5}$ . By convention,  $\infty$  is labeled by  $\bar{0}$ .

and labeled by  $25A^0$  in [8] and by  $5a$  in [14]. For the particular choice of subgroup given here, the conjugating element is  $\begin{pmatrix} 1 & 2 \\ 0 & 5 \end{pmatrix}$ .

The corresponding entry containing the information on the fundamental domain for this group is as follows.

[\* 1,22, 5,"A",0,1, 5,

[ [ 1,0,1 ],  
 [ 1,-1,1 ],  
 [ 1,-2,1 ],  
 [ 1,-3,1 ],  
 [ 1,-4,1 ],  
 [ 1,-4,1 ],  
 [ 1,-5,1 ] ],

[ [\* 0, [ 1,5,0,1 ] \*],  
 [\* 1, [ 1,0,0,1 ] \*],  
 [\* 2, [ 1,0,0,1 ] \*],  
 [\* 3, [ 1,-3,1,-2 ] \*],  
 [\* 9/2, [ 3,-10,1,-3 ] \*],  
 [\* 7, [ 4,-21,1,-5 ] \*] ],

[ [ 1,9 ],  
 [ 2,6 ],  
 [ 3,4 ],

```

[ 5,5 ],
[ 7,8 ] ],

[ [ 1,5,0,1 ],
  [ 4,-1,1,0 ],
  [ 2,-3,1,-1 ],
  [ 3,-10,1,-3 ],
  [ 5,-21,1,-4 ] ],

[ [ 0,1,-1,0 ],
  [ 1,-1,1,0 ],
  [ 2,-3,1,-1 ],
  [ 3,-7,1,-2 ],
  [ 4,-13,1,-3 ],
  [ 1,0,0,1 ],
  [ 5,-21,1,-4 ],
  [ -5,26,-1,5 ] ],

[ [ 0,1,-1 ],
  [ 1/2,1/2,-3 ],
  [ 3/2,1/2,-3 ],
  [ 5/2,1/2,-3 ],
  [ 7/2,1/2,-3 ],
  [ 4,1,-1 ],
  [ 9/2,1/2,-3 ],
  [ 5,1,-1 ] ],

[ [ 1,6,8 ],
  [ 2,4,5 ],
  [ 3 ],
  [ 7 ] ] *]

```

Thus, the group is labeled by the pair  $[1, 22]$  in the raw data file from [8] and by  $5A_1^0$  in [8, Table 2]. The group has index 5 in  $SL(2, \mathbb{Z})$ .

There are six circles bounding the fundamental domain. The fifth circle is included twice in the list. Its intersection with itself is, by convention, vertex 6, which is a vertex with angle  $\pi$ . This vertex is required for closure of the cycle containing the vertices 1 and 8. The three vertices 1, 6 and 8 form a cycle corresponding to an ordinary point (the sum of the angles is  $2\pi$ ). This corresponds to the entry  $[* 1, [1, 0, 0, 1] *]$  in the list **ram\_classes**. The cycle consisting of the vertices 2, 4 and 5 also corresponds to an ordinary point. Vertices 3 and 7 each form cycles with one element and are fixed points of elements of (projective) order 3.

The side 5 is paired with itself and so there is an additional pseudo-vertex with angle  $\pi$ . This is labeled by  $9/2$ , since it is between the vertices 4 and 5. This pseudo-vertex is stabilized by an element of (projective) order 2, and the corresponding cycle contains only this pseudo-vertex.

### 7. The appendices

The electronic appendices available with this paper contain external data and code files.

**Appendix 1.** These files contain complete MAGMA source code implementing the algorithm.

**Appendix 2.** These files contain input data used to compute the fundamental domains.

**Appendix 3.** These files contain output data giving the fundamental domains for a representative of each conjugacy class of congruence subgroups of genus zero or genus one, as described in Section 4.

**Appendix 4.** These files contain example code for computing the fundamental domain of a non-congruence subgroup.

*Acknowledgement.* I thank the referee for many helpful comments.

### References

1. A. F. BEARDON, *The geometry of discrete groups*, Graduate Texts in Mathematics 91 (Springer, New York, 1983).
2. R. E. BORCHERDS, ‘Monstrous moonshine and monstrous Lie superalgebras’, *Invent. Math.* 109 (1992) no. 2, 405–444.
3. W. BOSMA, J. CANNON and C. PLAYOUST, ‘The Magma algebra system. I. The user language’, *J. Symbolic Comput.* 24 (1997) no. 3–4, 235–265. Computational Algebra and Number Theory (London, 1993).
4. J. H. CONWAY, ‘Understanding groups like  $\Gamma_0(N)$ ’, *Groups, difference sets, and the monster (Columbus, OH, 1993)*, Ohio State University Mathematical Research Institute Publications 4 (de Gruyter, Berlin, 1996) 327–343.
5. J. H. CONWAY and S. P. NORTON, ‘Monstrous moonshine’, *Bull. London Math. Soc.* 11 (1979) no. 3, 308–339.
6. D. A. COX and W. R. PARRY, ‘Genera of congruence subgroups in  $\mathbf{Q}$ -quaternion algebras’, *J. Reine Angew. Math.* 351 (1984) 66–112.
7. D. A. COX and W. R. PARRY, ‘Genera of congruence subgroups in  $\mathbf{Q}$ -quaternion algebras’, Preprint (unabridged version of [6]), 1984.
8. C. J. CUMMINS, ‘Congruence subgroups of groups commensurable with  $\mathrm{PSL}(2, \mathbb{Z})$  of genus 0 and 1’, *Experiment. Math.* 13 (2004) no. 3, 361–382.
9. C. J. CUMMINS, ‘On conjugacy classes of congruence subgroups of  $\mathrm{PSL}(2, \mathbb{R})$ ’, *LMS J. Comput. Math.* 12 (2009) 264–274.
10. J. B. DENNIN Jr, ‘Fields of modular functions of genus 0’, *Illinois J. Math.* 15 (1971) 442–455.
11. J. B. DENNIN Jr, ‘Subfields of  $K(2^n)$  of genus 0’, *Illinois J. Math.* 16 (1972) 502–518.
12. J. B. DENNIN Jr, ‘The genus of subfields of  $K(p^n)$ ’, *Illinois J. Math.* 18 (1974) 246–264.
13. L. R. FORD, *Automorphic functions*, 2nd edn (Chelsea Publishing Company, New York, 1951) reprinted by AMS Chelsea Publishing, American Mathematical Society, Providence, RI, 2004.
14. D. FORD, J. MCKAY and S. NORTON, ‘More on replicable functions’, *Comm. Algebra* 22 (1994) no. 13, 5175–5193.
15. I. FRENKEL, J. LEPOWSKY and A. MEURMAN, *Vertex operator algebras and the monster*, Pure and Applied Mathematics 134 (Academic Press, Boston, MA, 1988).
16. H. HELLING, ‘Bestimmung der Kommensurabilitätsklasse der Hilbertschen Modulgruppe’, *Math. Z.* 92 (1966) 269–280.
17. H. HELLING, ‘On the commensurability class of the rational modular group’, *J. London Math. Soc.* (2) 2 (1970) 67–72.
18. G. A. JONES, ‘Congruence and noncongruence subgroups of the modular group: a survey’, *Proceedings of groups—St Andrews 1985*, London Mathematical Society Lecture Note Series 121 (Cambridge University Press, Cambridge, 1986) 223–234.
19. M. I. KNOPP and M. NEWMAN, ‘Congruence subgroups of positive genus of the modular group’, *Illinois J. Math.* 9 (1965) 577–583.
20. J. LEHNER, *A short course in automorphic functions* (Holt, Rinehart and Winston, New York, 1966).
21. J. MCKAY, Unpublished letter to J. Thompson (1978).
22. D. L. MCQUILLAN, ‘On the genus of fields of elliptic modular functions’, *Illinois J. Math.* 10 (1966) 479–487.
23. D. L. MCQUILLAN, ‘Some results on the linear fractional group’, *Illinois J. Math.* 10 (1966) 24–38.
24. S. P. NORTON, ‘More on moonshine’, *Computational group theory (Durham, 1982)* (Academic Press, London, 1984) 185–193.
25. S. P. NORTON, ‘Non-monstrous moonshine’, *Groups, difference sets, and the monster (Columbus, OH, 1993)*, Ohio State University Mathematical Research Institute Publications 4 (de Gruyter, Berlin, 1996) 433–441.
26. G. SHIMURA, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan 11 (Iwanami Shoten, Tokyo, 1971) Kanô Memorial Lectures 1.
27. J. G. THOMPSON, ‘Some numerology between the Fischer–Griess Monster and the elliptic modular function’, *Bull. London Math. Soc.* 11 (1979) no. 3, 352–353.

28. J. G. THOMPSON, 'A finiteness theorem for subgroups of  $\mathrm{PSL}(2, \mathbf{R})$  which are commensurable with  $\mathrm{PSL}(2, \mathbf{Z})$ ', *The Santa Cruz conference on finite groups (University of California, Santa Cruz, 1979)*, Proceedings of Symposia in Pure Mathematics 37 (American Mathematical Society, Providence, RI, 1980) 533–555.
29. P. ZOGRAF, 'A spectral proof of Rademacher's conjecture for congruence subgroups of the modular group', *J. Reine Angew. Math.* 414 (1991) 113–116.

*C. J. Cummins*

*Department of Mathematics*

*and Statistics*

*Concordia University*

*Montréal, Québec H3G 1M8*

*Canada*

[cummins@mathstat.concordia.ca](mailto:cummins@mathstat.concordia.ca)