Congruence Subgroups of Groups Commensurable with PSL $(2, \mathbb{Z})$ of Genus 0 and 1

C. J. Cummins

CONTENTS

2000 AMS Subject Classification: Primary 11F03, 11F22; Secondary 30F35

Keywords: Congruence subgroups, moonshine, genus

Thompson has shown that up to conjugation there are only finitely many congruence subgroups of $\mathrm{PSL}(2,\mathbb{R})$ of fixed genus. For $\mathrm{PSL}(2,\mathbb{Z})$, Cox and Parry found an explicit bound for the level of a congruence subgroup in terms of its genus. This result was used by the author and Pauli to compute the congruence subgroups of $\mathrm{PSL}(2,\mathbb{Z})$ of genus less than or equal to 24. However, the bound of Cox and Parry applies only to $\mathrm{PSL}(2,\mathbb{Z})$. In this paper a result of Zograf is used to find a bound for the level of any congruence subgroup in terms of its genus. Using this result, a list of all congruence subgroups, up to conjugacy, of $\mathrm{PSL}(2,\mathbb{R})$ of genus 0 and 1 is found.

This tabulation is used to answer a question of Conway and Norton who asked for a complete list of genus 0 subgroups, $\overline{G}$, of $\mathrm{PSL}(2,\mathbb{R})$ such that

(i) $\overline{G}$ contains $\overline{\Gamma}_0(N)$ for some N.

(ii) $\overline{G}$ contains the translation $z \mapsto z + k$ iff k is an integer.

Thompson has also shown that for fixed genus there are only finitely many subgroups of $\mathrm{PSL}(2,\mathbb{R})$ which satisfy these conditions. We call these groups "moonshine groups." The list of genus 1 moonshine groups is also found. All computations were performed using Magma.

1. INTRODUCTION

Thompson has shown the following:

Theorem 1.1. [Thompson 80] *Up to conjugation there are only finitely many congruence subgroups of* $\mathrm{PSL}(2,\mathbb{R})$ *of fixed genus* g.

This result is a stronger version of a result originally conjectured by Rademacher, that there are only finitely many genus 0 congruence subgroups of $\mathrm{PSL}(2,\mathbb{Z})$. This problem was studied by Knopp and Newman [Knopp and Newman 65], McQuillen [McQuillan 66a, McQuillan 66b], and Dennin [Dennin 71, Dennin 72, Dennin 74]. Cox and

Parry [Cox and Parry 84a, Cox and Parry 84b], independently of Thompson, showed that there are only finitely many congruence subgroups of $\mathrm{PSL}(2,\mathbb{Z})$ of fixed genus. The work of Cox and Parry applies only to subgroups of $\mathrm{PSL}(2,\mathbb{Z})$, but for this case their results give explicit bounds which they used to find a list of all congruence subgroups of $\mathrm{PSL}(2,\mathbb{Z})$ of genus 0. These bounds formed the basis of the tabulation in [Cummins and Pauli 03] of all congruence subgroups of $\mathrm{PSL}(2,\mathbb{Z})$ of genus less than or equal to 24.

Thompson's result was motivated by a desire to study the groups which appear in "moonshine." Conway and Norton [Conway and Norton 79] conjectured that the appropriate groups are the genus 0 subgroups of $\mathrm{PSL}(2,\mathbb{R})$ such that

(i) $\overline{G}$ contains $\overline{\Gamma}_0(N)$ for some N.

(ii) $\overline{G}$ contains the translation $z \mapsto z+k$ iff k is an integer.

Thompson used Theorem 1.1 to show that for fixed genus g there are only finitely many groups which satisfy these properties. We will call such groups "moonshine groups" of genus g.[1]

The motivation for this paper was to extend the explicit bounds of Cox and Parry to the general case, then to use these results to find all congruence and moonshine groups of low genus—in this case genus 0 and 1. The list of all congruence subgroups (up to conjugacy) in $\mathrm{PSL}(2,\mathbb{R})$ is contained in Table 2 and the notation is explained in Section 6. All computations were performed using Magma [Bosma et al. 97].

Genus 0 moonshine groups are of particular interest. The study of the Hauptmoduls (or normalized generators) of the fields of automorphic functions of genus 0 groups has a long history—particularly the "j-function" which is the generator of the field of automorphic functions of $\mathrm{PSL}(2,\mathbb{Z})$. The discovery of moonshine [McKay 78, Thompson 79, Conway and Norton 79, Borcherds 92] generated additional interest in this study. Computations [Conway and Norton 79, Alexander et al. 92, Norton 82] have extended the list of known Hauptmoduls, but whether or not this list was complete was not known. For the rational case we find there are 616 groups which correspond to the list of 616 rational Hauptmoduls found by Norton [Norton 97]—so this list is complete. We find that there are 5,870 irrational Hauptmoduls. However, as described in Section 3, there is an action of $\mathbb{Z}/24\mathbb{Z}$ on these groups and also Galois conjugation. There are 6,486 genus 0 moonshine groups, but only 371 equivalence classes under the corresponding equivalence relation. Of these, 310 have a rational representative and the remaining 61 are irrational. The list of these representative groups is contained in Table 3. See Tables 5 and 7 for detailed summaries and Section 6 for notation. Tables 4, 6, and 8 contain the corresponding information for the genus 1 moonshine groups. There is some overlap between these results and those of the paper of Chua and Lang [Chua and Lang 03]. This is discussed in more detail in Section 7. **Note:** All tables can be found at http://www.expmath.org/expmath/volumes/13/13.3/cumminstables.pdf.

[1] A better term might be "moonshine type groups," since it is not know if all these groups are involved in moonshine.

2. LEVEL BOUNDS

The aim of this section is to find a bound on the level of a congruence subgroup in terms of its genus. As part of this analysis we will find generalizations of the results of Larcher and Wohlfahrt.

If $\overline{G}$ is a discrete subgroup of $\mathrm{PSL}(2,\mathbb{R})$ which is commensurable with $\overline{\Gamma} = \mathrm{PSL}(2,\mathbb{Z}) = \mathrm{SL}(2,\mathbb{Z})/\{\pm 1\}$ (i.e., if $\overline{G} \cap \mathrm{PSL}(2,\mathbb{Z})$, has finite index in both $\overline{G}$ and $\mathrm{PSL}(2,\mathbb{Z})$), then $\overline{G}$ acts on the extended upper half plane $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$ by fractional linear transformations and the genus of $\overline{G}$ is defined to be the genus of the corresponding Riemann surface $\mathcal{H}^*/\overline{G}$. Where convenient we identify $\overline{G}$ with the corresponding group of fractional linear transformations.

From a computational point of view, it is easier to work with subgroups of $\Gamma = \mathrm{SL}(2,\mathbb{Z})$ and $\mathrm{SL}(2,\mathbb{R})$, rather than $\overline{\Gamma}$ and $\mathrm{PSL}(2,\mathbb{R})$. There is a one-to-one correspondence between the subgroups of $\mathrm{PSL}(2,\mathbb{R})$ and the subgroups of $\mathrm{SL}(2,\mathbb{R})$ which contain -1. Thus in this paper we shall mostly deal with subgroups of $\mathrm{SL}(2,\mathbb{R})$ and, where appropriate, we shall assume that these subgroups contain -1. If G is a subgroup of $SL(2,\mathbb{R})$ and we need to refer to its image in $\mathrm{PSL}(2,\mathbb{R})$, then this will be denoted by $\overline{G}$. When we refer to geometric invariants such as the genus or cusp number of G we mean the corresponding invariants of $\overline{G}$. Another important computational point is that in any subgroup of $\mathrm{SL}(2,\mathbb{R})$ which is commensurable with $\mathrm{SL}(2,\mathbb{Z})$ every element is a multiple of some matrix with integer entries and positive determinant. Thus any such subgroup is isomorphic to a subgroup of $\mathrm{PGL}(2,\mathbb{Q})^+$ and so is the image of a subgroup of $GL(2,\mathbb{Q})^+$. The discussions in this paper, for the most part, are stated in terms of subgroups of $SL(2,\mathbb{R})$, but

for writing the Magma programs it was easier to translate the results into $GL(2,\mathbb{Q})^+$ and work with multiples of integer matrices.

The key result in the study of the commensurability class of Γ in $\mathrm{SL}(2,\mathbb{R})$ is the following:

Definition 2.1.

$$\Gamma_0(f)^+ = \{e^{-1/2}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{R}) \;\Big|\; a,b,c,d,e \in \mathbb{Z}, \\ e|f, e|a, e|d, f|c, ad-bc = e\}.$$

Theorem 2.2. [Helling 66] *If G is a subgroup of $SL(2,\mathbb{R})$ which is commensurable with Γ, then G is conjugate to a subgroup of $\Gamma_0(f)^+$ for some squarefree f.*

Thus the study of groups commensurable with Γ is essentially the study of subgroups of the groups $\Gamma_0(f)^+$, f a squarefree integer. Amongst these groups are the congruence subgroups. In the case of $\mathrm{SL}(2,\mathbb{Z})$ a subgroup is said to be a congruence subgroup if it contains a principal congruence subgroup, where a principal congruence subgroup of level N is defined as

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \;\Big|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N \right\}.$$

The level of G is the smallest N such that $\Gamma(N) \subset G$. A subgroup of $\overline{\Gamma}$ is said to be a congruence subgroup if it is the image of a congruence subgroup of Γ.

It is possible, as we shall see shortly, to use the same definition of a congruence subgroup for subgroups of $\Gamma_0(f)^+$. However, it turns out to be more convenient to first introduce, following Thompson, the appropriate generalization of $\Gamma(N)$:

Definition 2.3. $G(n,f) = \Gamma_0(nf) \cap \Gamma(n)$.

Definition 2.4. Call a subgroup G of $\Gamma_0(f)^+$ a congruence subgroup if $G(n,f) \subset G$ for some n. If G is a congruence subgroup of $\Gamma_0(f)^+$, then let $n = n(G,f)$ be the smallest positive integer such that $G(n,f) \subset G$. We call $n(G,f)$ the level of G.

It is possible that G lies in more than one $\Gamma_0(f)^+$ and so the level will depend on a choice of f. We often work in some fixed $\Gamma_0(f)^+$ and then just refer to the level of G. The two definitions of congruence subgroup are equivalent:

Lemma 2.5. *Let G be a subgroup of $\Gamma_0(f)^+$. Then G contains $G(n,f)$ for some n iff G contains $\Gamma(m)$ for some m.*

Proof: Since $\Gamma(nf) \subset G(n,f) \subset \Gamma(n)$, if G is a congruence group with $G(n,f) \subset G$, then $\Gamma(nf) \subset G$ and conversely if $\Gamma(n) \subset G$, then $G(n,f) \subset G$ and so G is a congruence subgroup. □

The reasons for introducing the groups $G(n,f)$ are firstly that they are normal in $\Gamma_0(f)^+$ so that the generalizations of $\mathrm{SL}(2,\mathbb{Z}/m\mathbb{Z}) = \mathrm{SL}(2,\mathbb{Z})/\Gamma(m)$ are the groups $\Gamma_0(f)^+/G(n,f)$. These groups will be discussed in more detail later and their construction is a necessary step in finding the list of all congruence subgroups of a given genus. The second reason for introducing the $G(n,f)$ is that the level $n(G,f)$ is usually not the same as the smallest m such that $\Gamma(m)$ is contained in G, although they are related. This relationship will be used later when deriving a bound for $n(G,f)$ in terms of the genus of G and f. To make the distinction clear we make the following definition:

Definition 2.6. If G is a congruence subgroup, then the Γ-level, ℓ, of G is the smallest positive integer ℓ such that $\Gamma(\ell) \subset G$.

Several properties of the groups $G(n,f)$ will be needed. We first introduce a somewhat larger collection of subgroups of $\mathrm{SL}(2,\mathbb{Z})$:

Definition 2.7. Let p, q, and r be positive integers such that p divides qr, then define:

$$H(p,q,r) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid a \equiv d \equiv 1 \pmod{p}, \\ b \equiv 0 \pmod{q}, c \equiv 0 \pmod{r} \right\}. \quad (2\text{–}1)$$

It is easy to verify that $H(p,q,r)$ is a subgroup of $\mathrm{SL}(2,\mathbb{Z})$. Many of the standard congruence groups arise as special cases of these groups. For example $\Gamma_0(N) = H(1,1,N)$, $\Gamma_1(N) = H(N,1,N)$, $\Gamma(N) = H(N,N,N)$, $G(n,f) = H(n,n,nf)$. It is thus convenient to prove results, such as index formulas, in the general setting of the $H(p,q,r)$ groups.

We first recall a standard isomorphism theorem:

Lemma 2.8. *If A is a subgroup and B is a normal subgroup of a group G, then $AB/B \cong A/(A \cap B)$.*

Proposition 2.9. *Let a, b, c, p, q, and r be positive integers.*

1. *If $p|qr$ and $ap|bcqr$, then $H(ap, bq, cr)$ is a subgroup of $H(p, q, r)$.*
2. *If $a|bc$ and $p|qr$, then $H(a, b, c) \cap H(p, q, r) = H([a, p], [b, q], [c, r])$, where $[x, y] = \operatorname{lcm}(x, y)$.*
3. *If $p|qr$, then*

$$I(p,q,r) := \operatorname{Index}(\mathrm{SL}(2,\mathbb{Z}) : H(p,q,r)) = pqr \prod_{\substack{\ell \mid qr \\ \ell \text{ prime}}} (1+\frac{1}{\ell}) \prod_{\substack{\ell \mid p \\ \ell \text{ prime}}} (1-\frac{1}{\ell}) = \phi(p)\psi(qr).$$

Proof:

1. The congruence conditions which define $H(ap, bq, cr)$ imply those of $H(p, q, r)$ and so $H(ap, bq, cr)$ is a subgroup of $H(p, q, r)$.

2. First note that $a|bc$ and $p|qr$ implies that $[a, p]|[b, q][c, r]$, so that the group $H([a, p], [b, q], [c, r])$ exists. Since $[a, p], [b, q]$, and $[c, r]$ are multiples of a, b, and c, respectively, by (1) $H([a, p], [b, q], [c, r])$ is a subgroup of $H(a, b, c)$ and similarly it is a subgroup of $H(p, q, r)$ and hence of their intersection. Conversely if

$$\begin{pmatrix} u & v \\ w & x \end{pmatrix} \in H(a,b,c) \cap H(p,q,r),$$

then $u \equiv 1 \pmod{a}$ and $u \equiv 1 \pmod{p}$, so $a \equiv 1 \pmod{[a, p]}$ and similarly for the other congruence conditions. Hence $H(a, b, c) \cap H(p, q, r) \subset H([a, p], [b, q], [c, r])$ and the result follows.

3. By (1) $\Gamma(qr) = H(qr, qr, qr)$ is a subgroup of $H(p, q, r)$. So to find the index of $H(p, q, r)$ in $\mathrm{SL}(2, \mathbb{Z})$ it is sufficient to find the order of the quotient group $G = H(p, q, r)/\Gamma(qr)$. However, every element

$$\begin{pmatrix} u & v \\ w & x \end{pmatrix} \Gamma(qr)$$

of G has a unique decomposition:

$$\begin{pmatrix} u & v \\ w & x \end{pmatrix} \Gamma(qr) = \begin{pmatrix} 1 & 0 \\ xw & 1 \end{pmatrix} \begin{pmatrix} u & 0 \\ 0 & x \end{pmatrix} \begin{pmatrix} 1 & xv \\ 0 & 1 \end{pmatrix} \Gamma(qr),$$

as can be easily verified by noting that $ux \equiv 1 \pmod{qr}$ and $vw \equiv 0 \pmod{qr}$. Counting these elements shows that the order of G is $qrs_1s_2 \prod_{\ell | s_2} (1 - \frac{1}{\ell})$, ℓ prime, where $qr/p = s_1s_2$ with $s_1|p^\infty$ and $(s_2, p) = 1$. The notation $s|p^\infty$ means that s divides some power of p. This follows from the observation that $\#\{x \in (\mathbb{Z}/ps\mathbb{Z})^* \mid x \equiv 1 \pmod{p}\} = s_1\phi(s_2)$, where $s = s_1s_2$ with $s_1|p^\infty$ and $(s_2, p) = 1$. The order of G thus simplifies to $\frac{q^2r^2}{p} \prod_{\substack{\ell | qr \\ \ell \nmid p}} (1 - \frac{1}{\ell})$, ℓ prime. But the index of $\Gamma(qr)$ in $\mathrm{SL}(2, \mathbb{Z})$ is $q^3r^3 \prod_{\ell | qr} (1 - \frac{1}{\ell^2})$, ℓ prime, and then dividing and simplifying gives the required result. □

We now record some properties of $G(n, f)$.

Lemma 2.10. *Fix a positive squarefree integer f and let $G(n) = G(n, f)$.*

1. *$G(n)$ is a normal subgroup of $\Gamma_0(f)^+$.*
2. $$\operatorname{Index}(\mathrm{SL}(2,\mathbb{Z}) : G(n)) = n^3 f \prod_{\substack{p \mid nf \\ p \text{ prime}}} (1+\frac{1}{p}) \prod_{\substack{p \mid n \\ p \text{ prime}}} (1-\frac{1}{p}).$$
3. *If n divides m, then $G(m)$ is a subgroup of $G(n)$.*
4. *$G(m) \cap G(n) = G([m, n])$, where $[m, n] = \operatorname{lcm}(m, n)$.*
5. *If f is a positive squarefree integer, n is a positive integer, and $a|bcf$, then $H(a, b, cf)G(n, f) = H((a, n), (b, n), (c, n)f)$, where $(a, n) = \gcd(a, n)$.*
6. *$G(m)G(n) = G((m, n))$.*
7. *$G(1)/G(n) \cong G(1)/G(p_1^{e_1}) \times \cdots \times G(1)/G(p_k^{e_k})$, $n = p_1^{e_1}p_2^{e_2} \cdots p_k^{e_k}$.*

Proof:

1. If $m \in G(n, f) = \Gamma_0(nf) \cap \Gamma(n)$, then

$$m = \begin{pmatrix} \alpha & \beta \\ nf\gamma & \delta \end{pmatrix}$$

for integers α, β, γ, and δ such that $\alpha\delta - nf\gamma\beta = 1$. For any $g \in \Gamma_0(f)^+$ we have

$$g = e^{-1/2} \begin{pmatrix} ae & b \\ fc & de \end{pmatrix}$$

for integers a, b, c, d, e where $ade^2 - bfc = e$, and e is an exact divisor of f. A direct computation of $g^{-1}mg$ then shows that $g^{-1}mg \in \Gamma_0(nf) \cap \Gamma(n)$, so $G(n, f)$ is normal in $\Gamma_0(f)^+$.

2. This follows from Proposition 2.9 (3) since $G(n, f) = H(n, n, nf)$.

3. Similarly this follows from Proposition 2.9 (1).

4. Similarly this follows from Proposition 2.9 (2).

5. First note that $H(a,b,cf)$ and $G(n,f)$ are both subgroups of $\Gamma_0(f)^+$ and by (1), $G(n,f)$ is a normal subgroup. Thus by Lemma 2.8,

$$H(a,b,cf)G(n,f)/G(n,f) \cong H(a,b,cf)/(H(a,b,cf) \cap H(n,n,nf))$$

and by (2) of Proposition 2.9,

$$H(a,b,cf) \cap H(n,n,nf) = H([a,n],[b,n],[c,n]f).$$

If $a|bcf$, then $(a,n)|(b,n)(c,n)f$, so that the group $H((a,n),(b,n),(c,n)f)$ exists. Then we have

$$H(a,b,cf) \subset H((a,n),(b,n),(c,n)f)$$

and

$$H(n,n,nf) \subset H((a,n),(b,n),(c,n)f)$$

so that

$$H(a,b,cf)G(n,f) \subset H((a,n),(b,n),(c,n)f)$$

and so

$$\frac{H(a,b,cf)G(n,f)}{G(n,f)} \subset \frac{H((a,n),(b,n),(c,n)f)}{G(n,f)}.$$

The order of

$$H(a,b,cf)G(n,f)/G(n,f)$$

is the order of

$$H(a,b,cf)/H([a,n],[b,n],[c,n]f)$$

which is

$$I([a,n],[b,n],[c,n]f)/I(a,b,cf)$$

and the order of

$$H((a,n),(b,n),(c,n)f)/G(n,f)$$

is

$$I(n,n,nf)/I((a,n),(b,n),(c,n)f).$$

From the formula for $I(p,q,r)$ in (3) of Proposition 2.9, we find that

$$I(a,b,cf)I(n,n,nf) = I((a,n),(b,n),(c,n)f)I([a,n],[b,n],[c,n]f),$$

so that the orders of the groups

$$H(a,b,cf)G(n,f)/G(n,f)$$

and

$$H((a,n),(b,n),(c,n)f)/G(n,f)$$

are equal. Thus the index of $H(a,b,cf)G(n,f)$ in $H((a,n),(b,n),(c,n)f)$ is 1, and the result follows.

6. This follows from (5).

7. Let $n_i = n/p_i^{e_i}$, $= 1,\ldots,k$. Consider the homomorphism

$$\alpha : G(n_1)/G(n) \times G(n_2)/G(n) \times \ldots \times G(n_k)/G(n) \to G(1)/G(n)$$

defined by

$$\alpha(a_1G(n), a_2G(n), \ldots, a_kG(n)) = a_1a_2\ldots a_kG(n).$$

This is surjective since, by (6),

$$G(1) = G(n_1)G(n_2)\ldots G(n_k).$$

Suppose that $a_1a_2\ldots a_n \in G(n)$. Then

$$a_i \in G(n_1)G(n_2)\ldots G(n_{i-1})G(_{i+1})\ldots G(n_k)G(n).$$

So, again by (6), we have $a_i \in G(p_i^{e_i})$. But $a_i \in G(n_i)$ and so by (4), $a_i \in G(n)$. Hence α is also injective. By Lemma 2.8,

$$\begin{aligned} G(n_i)/G(n) &= G(n_i)/G(n_i) \cap G(p_i^{e_i}) \\ &\cong G(n_i)G(p^{e_i})/G(p_i^{e_i}) \\ &= G(1)/G(p_i^{e_i}) \end{aligned}$$

and so the result follows. □

Before proving the main results of this section, we first derive some basic properties of the level and Γ-level of congruence subgroups. Let

$$F_f = \begin{pmatrix} 0 & -1/\sqrt{f} \\ \sqrt{f} & 0 \end{pmatrix}$$

be the Fricke involution. So $F_f \in \Gamma_0(f)^+$.

Lemma 2.11. $G(n,f) = \Gamma(n) \cap F_f^{-1}\Gamma(n)F_f$.

Proof: If

$$m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(n) \cap F_f^{-1}\Gamma(n)F_f,$$

then $a-1 \equiv d-1 \equiv b \equiv 0 \pmod{n}$ since $m \in \Gamma(n)$ and $c \equiv 0 \pmod{nf}$ since $m \in F_f^{-1}\Gamma(n)F_f$ and so

$$\Gamma(n) \cap F_f^{-1}\Gamma(n)F_f \subset G(n,f).$$

Conversely

$$G(n,f) = \Gamma_0(nf) \cap \Gamma(n) \subset \Gamma(n)$$

and $G(n,f)$ is normal in $\Gamma_0(f)^+$, so

$$G(n,f) = F_f^{-1}G(n,f)F_f \subset F_f^{-1}\Gamma(n)F_f$$

and so

$$G(n,f) \subset \Gamma(n) \cap F_f^{-1}\Gamma(n)F_f.$$

Hence

$$G(n,f) = \Gamma(n) \cap F_f^{-1}\Gamma(n)F_f$$

as required. □

Lemma 2.12. *If G has level n and $G(n',f) \subset G$, then n divides n'. Also if ℓ is the Γ-level of G, then ℓ divides nf.*

Proof: By Proposition 2.10 (6), G contains

$$G(n)G(n') = G(\gcd(n,n')).$$

But from Definition 2.4 we must have $\gcd(n,n') \geq n$, so that $n = \gcd(n,n')$ and so n divides n'. By Proposition 2.9 (1) we have

$$\Gamma(nf) = H(nf,nf,nf) \subset H(n,n,nf) = G(n,f) \subset G.$$

Also $\Gamma(\ell) \subset G$, and ℓ is the smallest such ℓ. By Proposition 2.9 (6), with $f=1$, $\Gamma(\ell)\Gamma(nf) = \Gamma(\gcd(\ell,nf))$ and so, repeating the previous argument, ℓ divides nf. □

Proposition 2.13. *Let G be a congruence subgroup of $\Gamma_0(f)^+$ and let $n = n(G,f)$ be the level of G and $\ell = \ell(G)$ be the Γ-level of G. Then $n|\ell$, $\ell|nf$ (so in particular $n \leq \ell \leq nf$) and $f|\ell$.*

Proof: That ℓ divides nf was shown in Lemma 2.12. For any subgroup H of $\Gamma_0(f)^+$ we will use the notation $H_F = H \cap F_f^{-1}HF_f$. So if $\Gamma(\ell) \subset G$, then, by Lemma 2.11, $G(\ell,f) = \Gamma(\ell)_F \subset G_F$. But $G(n,f) = G(n,f)_F$ since $G(n,f)$ is normal, hence $G(n,f) \subset G_F$. So if n' is the level of G_F, then $n' \leq n$. But $G(n',f) \subset G_F \subset G$, so $n \leq n'$ and hence $n' = n$. As we have shown that $G(\ell,f) \subset G_F$ this gives $n|\ell$. Finally if $\Gamma(\ell) \subset \Gamma_0(f)^+$, then $\Gamma(\ell) \subset \Gamma_0(f)^+ \cap \mathrm{SL}(2,\mathbb{Z}) = \Gamma_0(f)$, so $f|\ell$. □

We now turn to the proof of the main result bounding the level of a congruence subgroup. Let G be a discrete subgroup of $\mathrm{SL}(2,\mathbb{R})$. We will assume that $-1 \in G$ and in the rest of this section we restrict to congruence subgroups containing -1 even if this condition is not explicitly stated. Let $\chi(G)$ and $g(G)$ be the Euler characteristic and genus of $\overline{G}$. Recall that

$$\chi(G) = 2(g(G)-1) + m + \sum_{i=1}^{k}(1 - \frac{1}{e_i}),$$

where m is the number of cusps of $\overline{G}$, k is the number of inequivalent elliptic points of $\overline{G}$ and e_i, $i = 1,\ldots,k$ the orders of these points. In particular $\chi(\mathrm{SL}(2,\mathbb{Z})) = \frac{1}{6}$.

Theorem 2.14. [Zograf 91]) *For any congruence subgroup K of G we have*

$$g(K) + 1 > \frac{3}{64}\ \chi(G)\ \mathrm{Index}(G:K).$$

As a corollary to this result Zograf notes that it implies Theorem 1.1 as follows: let $G = K = \Gamma_0(f)^+$, with f squarefree. Recall $\mathrm{Area}(G) = 2\pi\chi(G)$, so

$$\chi(\Gamma_0(f)^+) = \frac{1}{6}\prod_{p|f}\frac{1+p}{2}, \quad p \text{ prime}.$$

Then, writing g for $g(\Gamma_0(f)^+)$, we have

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

This bounds the possible f for a given genus. For example, if k is the number of prime factors of f, then

$$2^{k-2} < f/2^k < \prod_{p|f}\frac{1+p}{2} < 128(g+1), \quad p \text{ prime},$$

which bounds k and hence f. Thus the set

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

is finite. By Theorem 2.2 any congruence subgroup which is commensurable with Γ and of genus g is conjugate to a subgroup of at least one of the groups in $H(g)$. But by Proposition 2.14 there are only finitely many such subgroups and hence Theorem 1.1 follows.

The bound on f, and the following formula of Helling for the genus of $\Gamma_0(f)^+$, yield Table 1 which gives the maximum f such that $\Gamma_0(f)^+$ has genus g for $0 \leq g \leq 100$.

Theorem 2.15. [Helling 70] *Let f be a squarefree integer, $g_0^+(f)$ be the genus of $\Gamma_0^+(f)$, and $\pi(f)$ be the number of prime factors of f. Then*

$$g_0^+(f) = 2^{-\pi(f)}(g_0(f) - 1 - \frac{1}{2}W(f)) + 1,$$

where for p prime

$$g_0(f) = 1 - 2^{\pi(f)-1} + \frac{1}{12}\prod_{p|f}(p+1) - \frac{1}{4}\prod_{p|f}(1+\left(\frac{-4}{p}\right)) - \frac{1}{3}\prod_{p|f}(1+\left(\frac{-3}{p}\right))$$

is the genus of $\Gamma_0(f)$ and for $f \equiv 1 \pmod 2$

$$W(f) = \sum_D h(D) \prod_{\substack{p|f \\ p \text{ prime}}} (1+\left(\frac{D}{p}\right)),$$

where the sum is over $D < 0$, $D|4f$, $D \equiv 0$ or $1 \bmod 4$, $D \neq -4$. While for $f \equiv 0 \pmod 2$, $W(f) = W_0(f) + W_1(f)$ with

$$W_0(f) = \sum_D h(D) \prod_{\substack{p|(f/2) \\ p \text{ prime}}} (1+\left(\frac{D}{p}\right))$$

with $D < 0$, $D|4f$, $D \equiv 0 \bmod 4$, or $D = -3$.

$$W_1(f) = 3\sum_D h(D) \prod_{\substack{p|(f/2) \\ p \text{ prime}}} (1+\left(\frac{D}{p}\right))$$

with $D < 0$, $D|4f$, $D \equiv 1 \bmod 4$, $D \neq -3$.

For a given genus g, Table 1 tells us which groups $\Gamma_0(f)^+$ we have to consider to find all the congruence subgroups of genus g. In principle it is then possible to calculate all congruence subgroups of genus g, as Zograf's result bounds the index. However, in practice the bound appears to be too large for practical computation. Another approach is to construct permutation representations of the groups $\Gamma_0(f)^+/G(n,f)$, but this requires that we first bound the level of a congruence subgroup in terms of g and f. Although the bound we find appears not to be optimal, it leads to a feasible calculation, at least for small genus.

Recall first the following results of Larcher concerning the Γ-level of subgroups of $\mathrm{SL}(2,\mathbb{Z})$:

Theorem 2.16. [Larcher 82, Larcher 84] *Let H be a congruence subgroup of $\mathrm{SL}(2,Z)$ of level ℓ, then*

1. *$\ell \leq \mathrm{Index}(\mathrm{SL}(2,Z) : H)$.*
2. *if ℓ is squarefree, then the set of cusp widths of H is the set of all multiples of the smallest cusp width which divide ℓ.*
3. *H has a cusp of width ℓ.*

Using Larcher's Theorem and Zograf's bound we can find the required bound.[2]

Theorem 2.17. *Let K be a congruence subgroup of $\Gamma_0(f)^+$, with f squarefree. Let $n(K,f)$ be the level of K, $g(K)$ be the genus of K, and $\pi(f)$ be the number of prime factors of f. Then*

$$n < 2^{\pi(f)}128(g+1) \prod_{\substack{p|f \\ p \text{ prime}}} (1+\frac{1}{p})^{-1}.$$

Proof: Consider the following diagram of subgroups:

$$\begin{array}{ccc} \mathrm{SL}(2,\mathbb{Z}) & & \Gamma_0(f)^+ \\ | & & | \\ \Gamma_0(f) & \text{———} & \Gamma_0(f)K \\ | & & | \\ \Gamma_0(f)\cap K & \text{———} & K. \end{array}$$

Since $\Gamma_0(f)$ is normal in $\Gamma_0(f)^+$ we have

$$\Gamma_0(f)K/\Gamma_0(f) \cong K/\Gamma_0(f)\cap K$$

by Lemma 2.8. Thus

$$\begin{aligned}\mathrm{Index}(\Gamma_0(f) : \Gamma_0(f)\cap K) &= \mathrm{Index}(\Gamma_0(f)K : K) \\ &\leq \mathrm{Index}(\Gamma_0(f)^+ : K).\end{aligned}$$

Using Zograf's bound this yields

$$\mathrm{Index}(\Gamma_0(f) : \Gamma_0(f)\cap K) < \frac{64}{3\chi(\Gamma_0(f)^+)}(g(K)+1).$$

But, for p prime,

$$\chi(\Gamma_0(f)^+) = \frac{1}{2^{\pi(f)}6}\prod_{p|f}(1+p).$$

This yields, for p prime,

$$\mathrm{Index}(\Gamma_0(f) : \Gamma_0(f)\cap K) < 2^{\pi(f)}128(g(K)+1)\prod_{p|f}(1+p)^{-1}.$$

[2] After submitting this paper, I received a preprint from M. L. Lang [Lang 03] which contains a bound on the Γ-level of a group. The proof of his result is essentially the same as that of Theorem 2.17.

Now $\Gamma_0(f) = \mathrm{SL}(2,\mathbb{Z}) \cap \Gamma_0(f)^+$. So $\Gamma(n) \subset K$, iff $\Gamma(n) \subset \Gamma_0(f) \cap K$. Thus if ℓ is the Γ-level of K, then ℓ is also the Γ-level (and so the "usual" level) of $\Gamma_0(f) \cap K$. So we can apply Proposition 2.16 (3) to conclude that $\Gamma_0(f) \cap K$ has a cusp c of width ℓ inside $\mathrm{SL}(2,\mathbb{Z})$. In other words we have the following inclusions of parabolic subgroups fixing c:

$$\begin{array}{c} P_1 \subset \mathrm{SL}(2,\mathbb{Z}) \\ | \\ P_f \subset \Gamma_0(f) \\ | \\ P_K \subset \Gamma_0(f) \cap K \end{array} .$$

By Proposition 2.16 (2) $\mathrm{Index}(P_1 : P_f) = d$ for some divisor d of f and as already noted $\ell = \mathrm{Index}(P_1 : P_K)$. Thus $\ell/d = \mathrm{Index}(P_f : P_K) \leq \mathrm{Index}(\Gamma_0(f) : \Gamma_0(f) \cap K)$. Combining this with the inequality found earlier gives

$$\begin{aligned} \ell &< d2^{\pi(f)}128(g(K)+1) \prod_{\substack{p|f \\ p \text{ prime}}} (1+p)^{-1} \\ &\leq 2^{\pi(f)}128(g(K)+1) \prod_{\substack{p|f \\ p \text{ prime}}} (1+\frac{1}{p})^{-1}, \end{aligned}$$

using $d \leq f$ and the fact that f is squarefree. But $n \leq \ell$, by Proposition 2.13, and so the result follows. □

As part of the proof of Theorem 2.17 we proved the following generalization of Larcher's first result:

Corollary 2.18. *If K is a congruence subgroup of $\Gamma_0(f)^+$ with f squarefree and n is the level of K, then $n \leq f \times \mathrm{Index}(\Gamma_0(f)^+ : K)$.*

For completeness we now prove a generalization of Wohlfahrt's Theorem [Wohlfart 64].

Definition 2.19. Let G be a subgroup of finite index in $\Gamma_0(f)^+$ with f squarefree, $-1 \in G$, and K a subgroup of G of finite index with $-1 \in K$. Then define $C(G,K)$ to be the set of cusp widths of K measured relative to G, that is

$$C(G,K) = \{\mathrm{Index}(P_G(x) : P_K(x)) \mid x \in \mathbb{Q} \cup \{\infty\}\}$$

where $P_G(x) = \{g \in G \mid g(x) = x\}$.

Note that this is well-defined, as G has only finitely many cusps and the set of indices is finite since K has finite index in G.

Lemma 2.20. *With G and K as in the last definition and $\Gamma = \mathrm{SL}(2,\mathbb{Z})$, we have $C(G,K) = C(G \cap \Gamma, K \cap \Gamma)$.*

Proof: By [Shimura 71, Proposition 1.17], the groups $\overline{P}_G(x)$ are cyclic and generated by parabolic elements. But from the form of the elements of $\Gamma_0(f)^+$ given in Definition 2.1, if

$$e^{-1/2}\begin{pmatrix} ae & b \\ cf & de \end{pmatrix}$$

is parabolic, then $e^{1/2}(a+d) = \pm 2$. This forces $e = 1$ and so every parabolic element of $\Gamma_0(f)^+$ lies in Γ. Thus for all $x \in \mathbb{Q} \cup \{\infty\}$, $P_G(x) = P_G(x) \cap \Gamma$ and $P_H(x) = P_H(x) \cap \Gamma$ and so the result follows. □

Remark 2.21. The argument to show that parabolic elements of $\Gamma_0(f)^+$ lie in Γ is taken from [Sebbar 01, Theorem 4.1].

Wohlfahrt's theorem is the case $f = 1$ of the following:

Theorem 2.22. *Let K be a congruence subgroup of $\Gamma_0(f)^+$ with f squarefree. Let $n = n(K,f)$ be the level of K. Then $\mathrm{lcm}(C(\Gamma_0(f)^+, K))|n$ and $n|\big(f \times \mathrm{lcm}(C(\Gamma_0(f)^+, K))\big)$.*

Proof: We first show that $\mathrm{lcm}(C(\Gamma_0(f)^+, K))$ divides n. Consider the subgroups:

$$\begin{array}{c} \Gamma_0(f)^+ \\ | \\ K \\ | \\ \pm G(n,f) \end{array} .$$

Then for any $x \in \mathbb{Q} \cup \{\infty\}$ we have the inclusions of fixing groups:

$$\begin{array}{c} P_f(x) \subset \Gamma_0(f)^+ \\ | \\ P_K(x) \subset K \\ | \\ P_n(x) \subset \pm G(n,f) \end{array} .$$

If we consider the fixing groups of ∞ we see that $\pm G(n,f)$ has cusp width n at ∞, and since it is normal in $\Gamma_0(f)^+$ every cusp width of $\pm G(n,f)$ is n. Thus $\mathrm{Index}(P_f(x) : P_n(x)) = n$ and so $\mathrm{Index}(P_f(x) : P_K(x))$ divides n for all x and hence $\mathrm{lcm}(C(\Gamma_0(f)^+ : K))$ divides n.

To show that n divides $f \times \mathrm{lcm}(C(\Gamma_0(f)^+, K))$ we start with the inclusions

$$\begin{array}{c} \mathrm{SL}(2,\mathbb{Z}) \\ | \\ \Gamma_0(f) \\ | \\ \Gamma_0(f)\cap K\ , \end{array}$$

and for any x in $\mathbb{Q}\cup\{\infty\}$ the inclusions of fixing groups,

$$\begin{array}{c} P_1(x)\subset \mathrm{SL}(2,\mathbb{Z}) \\ | \\ P_f(x)\subset \Gamma_0(f) \\ | \\ P_K(x)\subset \Gamma_0(f)\cap K \quad . \end{array}$$

As noted previously $\mathrm{Index}(P_1(x) : P_f(x)) = d(x)$ for some divisor $d(x)$ of f. Let $\mathrm{Index}(P_1(x) : P_K(x)) = i(x)$ and $\mathrm{Index}(P_f(x) : P_K(x)) = j(x)$. As in the proof of Theorem 2.17, the Γ-level, ℓ, of K is equal to the Γ-level of $K\cap\Gamma_0(f)$. So by Wohlfahrt's Theorem,

$$\ell = \mathrm{lcm}(\{i(x) \mid x\in\mathbb{Q}\cup\{\infty\}\}).$$

Also, by Lemma 2.20,

$$\mathrm{lcm}(C(\Gamma_0(f)^+, K)) = \mathrm{lcm}(\{j(x) \mid x\in\mathbb{Q}\cup\{\infty\}\}).$$

Now, for all x, $i(x) = d(x)j(x)$ hence $i(x)$ divides $fj(x)$ and so $\mathrm{lcm}(\{i(x) \mid x\in\mathbb{Q}\cup\{\infty\}\}$ divides $f\times\mathrm{lcm}(\{j(x) \mid x\in\mathbb{Q}\cup\{\infty\}\})$. Hence ℓ divides f $\mathrm{lcm}(C(\Gamma_0(f)^+, K))$ and since from Proposition 2.13, $n(K, f)$ divides ℓ the result follows. □

3. MOONSHINE GROUPS

As described in the introduction, we define a moonshine group to be a discrete subgroup $\overline{G}$ of $\mathrm{PSL}(2,\mathbb{R})$ such that

(i) $\overline{G}$ contains some $\overline{\Gamma}_0(N)$.

(ii) $\overline{G}$ contains the translation $z\mapsto z+k$ iff k is an integer.

We call a subgroup G of $\mathrm{SL}(2,\mathbb{R})$ a moonshine group if $-1\in G$ and $\overline{G}$ is a moonshine group. As noted in the introduction it is easier computationally to consider subgroups of $\mathrm{SL}(2,\mathbb{R})$ rather than $\mathrm{PSL}(2,\mathbb{R})$. Thompson's proof that there are only finitely many moonshine groups of a given genus uses the following two results:

Lemma 3.1.

$$\gcd\{a-d \mid \begin{pmatrix} a & b \\ cN & d\end{pmatrix}\in\Gamma_0(N)\} \text{ divides } \gcd(N,24).$$

Proof: Let g be the gcd. Since

$$\begin{pmatrix} 1+N & 1 \\ N & 1\end{pmatrix}\in\Gamma_0(N),$$

g divides N. Then for all a such that $\gcd(a,g)=1$ we can find a' such that $a\equiv a' \pmod g$ with $\gcd(a',N)=1$ and so we can find a matrix

$$\begin{pmatrix} a' & b' \\ N & d'\end{pmatrix}\in\Gamma_0(N).$$

Thus $a'd'\equiv 1 \pmod g$ and, by the definition of g, $a'-d'\equiv 0 \pmod g$ which implies $a^2\equiv 1 \pmod g$ for all a coprime to g. The only integers with this property are the divisors of 24 and so g divides $\gcd(N,24)$ as required. □

Proposition 3.2. *Suppose G is a discrete subgroup of $\mathrm{SL}(2,\mathbb{R})$ such that G contains $\Gamma_0(N)$ for some N and the stabilizer of ∞ is generated by*

$$\pm\begin{pmatrix} 1 & 1 \\ 0 & 1\end{pmatrix}.$$

Then there is a matrix

$$\rho = \begin{pmatrix} p & q \\ 0 & ph\end{pmatrix}$$

$p, q, h\in\mathbb{Z}$, such that $\gcd(p,q)=1$, $h>0$, $0\le q<p$, p divides $\gcd(N,24)$, p^2h divides N, and

$$G^\rho = \rho^{-1}G\rho\subset\Gamma_0(f)^+$$

for some squarefree integer f. If the level of G^ρ is $n = n(G^\rho, f)$, then h divides n.

Proof: By Theorem 2.2, G is conjugate to a subgroup of $\Gamma_0(f)^+$ for some squarefree integer f: $\sigma^{-1}G\sigma\subset\Gamma_0(f)^+$, $\sigma\in SL(2,\mathbb{R})$. Since G and $\Gamma_0(f)^+$ are commensurable they have the same cusps and from this it follows that $\sigma:\mathbb{Q}\to\mathbb{Q}$, which implies $\lambda\sigma\in\mathrm{GL}(2,\mathbb{Q})^+$ for some nonzero $\lambda\in\mathbb{R}$. After multiplying by a suitable scalar, we can take

$$\sigma = \begin{pmatrix} a & b \\ c & d\end{pmatrix}$$

with $c, d\in\mathbb{Z}$, and $\gcd(c,d)=1$. Then

$$L = \begin{pmatrix} de & \beta \\ -ce & \gamma e\end{pmatrix}\in\Gamma_0(f)^+,$$

where $e = f/\gcd(f,c)$, so that $\gcd(e,c)=1$, and the integers γ,β are chosen so that $de\gamma + c\beta = 1$. Then

$$G^\rho = \rho^{-1}G\rho\subset\Gamma_0(f)^+,$$

where

$$\rho = \sigma L = \begin{pmatrix} p & q \\ 0 & r \end{pmatrix}.$$

Again multiplying by a suitable scalar if necessary, we may assume that $\gcd(p,q,r) = 1$, that $p, r > 0$, and, since

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_0(f)^+,$$

after a suitable conjugation, that $0 \le q < p$. We have

$$\begin{pmatrix} 1 & r/p \\ 0 & 1 \end{pmatrix} = \rho^{-1} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rho \in \Gamma_0(f)^+$$

so that p divides r. Write $r = hp$. Then since $\gcd(p,q,r) = 1$, we must have $\gcd(p,q) = 1$. Now,

$$\rho^{-1} \begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix} \rho = \begin{pmatrix} * & -q^2N/(p^2h) \\ N/h & * \end{pmatrix}$$

and since $\gcd(p,q) = 1$ this implies that h divides N and p^2h divides N.

Then for all $\begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma_0(N)$ we have

$$\rho^{-1} \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \rho = \begin{pmatrix} * & q(a-d)/p \pmod{\mathbb{Z}} \\ * & * \end{pmatrix}$$

so that p divides $a - d$ for all a and d such that

$$\begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma_0(N).$$

By the previous lemma this implies that p is a divisor of $\gcd(24, N)$.

If the level of G^ρ is n, then

$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in G^\rho.$$

So

$$\rho \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \rho^{-1} = \begin{pmatrix} 1 & n/h \\ 0 & 1 \end{pmatrix} \in G$$

and hence h divides n. □

Remark 3.3.

(i) The proof of the last proposition shows that if w is the smallest positive integer such that

$$\begin{pmatrix} 1 & w \\ 0 & 1 \end{pmatrix} \in G^\rho$$

and the stabilizer of infinity in G is generated by

$$\pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

then $h = w$.

(ii) Thompson's proof that there are only finitely many moonshine groups of genus g is as follows: by Theorem 1.1, for a fixed genus g, there are only finitely many possibilities for G^ρ and hence there is some bound $n_0(g)$ for n. This bounds the possible values of h and since $0 \le q < p \le 24$ it follows that the number of genus g moonshine groups is finite.

In our calculations of moonshine groups we will first compute the congruence subgroups of $\Gamma_0(f)^+$ of genus g. Then Proposition 3.2 tells us which conjugations of these groups we have to consider, but we need a test to determine which conjugations are moonshine groups. This is provided by the next three results.

Theorem 3.4. [Newman 55] *If $\Gamma_0(N) \subset G \subset \mathrm{SL}(2,Z)$, then $G = \Gamma_0(M)$ for some divisor M of N.*

Lemma 3.5. *Suppose $\Gamma_0(N) \subset G$ for some N and that N is minimal. Then $N = \ell$ where ℓ is the Γ-level of G.*

Proof: We have $\Gamma(\ell) \subset G$ and $\Gamma_0(N) \subset G$. Then G contains $< \Gamma(\ell), \Gamma_0(N) >$ which by Newman's Theorem and the minimality of N is equal to $\Gamma_0(N)$. Then $\Gamma(\ell) \subset \Gamma_0(N)$ so N divides ℓ. But $\Gamma(N) \subset G$ and so ℓ divides N since ℓ is the Γ-level of G. Hence $N = \ell$ as required. □

Proposition 3.6. *Suppose K is a congruence subgroup of level n of $\Gamma_0(f)^+$ for some squarefree f and let*

$$\rho = \begin{pmatrix} p & q \\ 0 & ph \end{pmatrix}$$

for integers p, q, and h with $\gcd(p,q) = 1$. Then $\rho K \rho^{-1}$ contains $\Gamma_0(N)$ for some N, N minimal, iff $\rho K \rho^{-1}$ contains C, where C is a set of coset representatives for $\Gamma_0(M)$ over $\Gamma(M)$ where $M = fnp^2h$.

Proof: First note that by a straightforward calculation, $\Gamma(M)^\rho \subset G(n,f)$. Now suppose $G = \rho K \rho^{-1}$ contains $\Gamma_0(N)$ with N minimal. By Lemma 3.5, N is the Γ-level of G. But $\Gamma(M) \subset \rho G(n,f) \rho^{-1} \subset \rho K \rho^{-1} = G$. So M is a multiple of N. Thus G contains $\Gamma_0(M)$ and hence it contains C so that $C^\rho \subset K$.

Conversely, if $C^\rho \subset K$, then, since, $\Gamma(M)^\rho \subset K$, we have $\Gamma_0(M)^\rho \subset K$. So $\rho K \rho^{-1}$ contains $\Gamma_0(M)$ and so contains $\Gamma_0(N)$ where N is minimal. □

Once we know that a conjugation is a moonshine group we need to find its Γ-level. The following lemma provides the necessary result:

Lemma 3.7. *Let*

$$\rho = \begin{pmatrix} p & q \\ 0 & ph \end{pmatrix},$$

where p, q, and h are integers such that $\gcd(p,q) = 1$. *Then the smallest positive integer N such that*

$$\rho^{-1} \begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix} \rho \in \Gamma_0(f)^+,$$

where f is squarefree, is $N = N_0 = fhp^2/\gcd(p^2, f)$. Moreover, any other value of N such that

$$\rho^{-1} \begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix} \rho \in \Gamma_0(f)^+$$

is a multiple of N_0.

Proof: For any positive integer N we have

$$\rho^{-1} \begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix} \rho = \begin{pmatrix} 1 - \frac{Nq}{ph} & -\frac{q^2 N}{p^2 h} \\ \frac{N}{h} & 1 + \frac{Nq}{ph} \end{pmatrix}.$$

For this matrix to be in $\Gamma_0(f)^+$ it must have integral entries and the lower-left entry must be divisible by f. Thus $N = hfk$ for some integer k. Using the fact that p is coprime to q this gives the condition $p^2 | kf$. Thus k is a multiple of $p^2/\gcd(p^2, f)$. So N is a multiple of $N_0 = hfp^2/\gcd(p^2, f)$. Moreover substituting $N = N_0$ in the above equation we find that

$$\rho^{-1} \begin{pmatrix} 1 & 0 \\ N_0 & 1 \end{pmatrix} \rho$$

is an element of $\Gamma_0(f)$. Thus the smallest value of N is N_0 as required. □

Remark 3.8. Suppose G is a moonshine group with $K = G^\rho$ as above. If

$$w = \begin{pmatrix} 1 & 0 \\ N_0 & 1 \end{pmatrix}^\rho$$

and w^s is the smallest power of w which lies in K, then by Theorem 3.4, $N = sN_0$ is the smallest N such that $\Gamma_0(N)^\rho$ is in K.

Once we know that $\Gamma_0(N)^\rho \subset K$ the next step is to construct the cosets of K over $\Gamma_0(N)^\rho$. If the level of K is n, then we know the cosets of K over $G(n, f)$. The following lemma is useful since it provides a large known subgroup of $\Gamma_0(N)^\rho$.

Lemma 3.9. *Let*

$$\rho = \begin{pmatrix} p & q \\ 0 & ph \end{pmatrix}$$

with integers p, q, and h such that $\gcd(p,q) = 1$ *and $p^2 h$ divides N. Then $H(ph, h, N) \subset \Gamma_0(N)^\rho$.*

Proof: If

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H(ph, h, N),$$

then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 + uph & vh \\ wN & 1 + xph \end{pmatrix},$$

for some integers u, v, w, and x. This gives

$$\rho \begin{pmatrix} a & b \\ c & d \end{pmatrix} \rho^{-1} =$$
$$\begin{pmatrix} a + qw(N/p) & q(x-u) + v + q^2(N/p^2 h) \\ hwN & d - qw(N/p) \end{pmatrix} \in \Gamma_0(N)$$

since $p^2 h | N$. So $\rho H(ph, h, N) \rho^{-1} \subset \Gamma_0(N)$ as required. □

Remark 3.10. Thus $G(n, f) \cap H(ph, h, N)$ is a common subgroup of K and $\Gamma_0(N)^\rho$. We can find cosets of $G(n, f)$ over $G(n, f) \cap H(ph, h, N)$ and hence of K over $G(n, f) \cap H(ph, h, N)$. From these we can find a subset which are the cosets of K over $\Gamma_0(N)^\rho$.

The following proposition is due to Norton:

Proposition 3.11. *Let W be the set of all discrete subgroups G of $SL(2, \mathbb{R})$ such that $\Gamma_0(N) \subset G$ for some N and such that the stabilizer of infinity in G is generated by*

$$\pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

For x in $\mathbb{Z}/M\mathbb{Z}$, define $t(x) \in \mathrm{SL}(2, \mathbb{R})$ by

$$t(x) = \begin{pmatrix} 1 & \overline{x}/M \\ 0 & 1 \end{pmatrix}$$

where $0 \le \overline{x} < M$ and the class of $\overline{x}$ in $\mathbb{Z}/M\mathbb{Z}$ is Mx. Then there is a group action of $\mathbb{Z}/24\mathbb{Z}$ on W given by $x : G \mapsto t(x)^{-1} G t(x)$.

Proof: If $G \in W$, then $\Gamma_0(N) \subset G$ for some N. Fix y, $0 \le y < 24$, and set

$$t = \begin{pmatrix} 1 & y/24 \\ 0 & 1 \end{pmatrix}.$$

Then for any

$$g = \begin{pmatrix} a & b \\ 24^2 cN & d \end{pmatrix} \in \Gamma_0(24^2 N)$$

we have

$$tgt^{-1} = \begin{pmatrix} a + 24yNc & \frac{y}{24}(d-a) + b - y^2 Nc \\ 24^2 Nc & d - 24yNc \end{pmatrix}.$$

However, since $g \in \Gamma_0(24^2N)$ we have $ab - 24^2Ncb = 1$, so $ad \equiv 1 \pmod{24}$. Hence $a - d \equiv 0 \pmod{24}$. Thus $tgt^{-1} \in \Gamma_0(N)$ and hence $t^{-1}Gt$ contains $\Gamma_0(24^2N)$. Moreover, the stabilizer of infinity in G commutes with t and so the stabilizer of infinity in $t^{-1}Gt$ is also generated by

$$\pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Thus $t^{-1}Gt$ is in W and so each element of $\mathbb{Z}/24\mathbb{Z}$ has a well-defined action on W. Since

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in G$$

it follows that

$$t(y)^{-1}t(x)^{-1}Gt(x)t(y) = t(x+y)^{-1}Gt(x+y)$$

and so the action is a group action. □

Remark 3.12.

(i) Since conjugation preserves the genus, there is also a group action of $\mathbb{Z}/24\mathbb{Z}$ on

$$W(g) = \{G \in W \mid \text{genus}(G) = g\}.$$

(ii) This result is useful since it means that we need only list one moonshine group from each $\mathbb{Z}/24\mathbb{Z}$ orbit.

When computing moonshine groups it is necessary to have a method to determine when two such groups are identical. A necessary condition is that they have the same Γ-level. If this is the case, then we have to verify that they have the same cosets over $\Gamma_0(N)$. A convenient way to do this is to find a canonical representative for each $\Gamma_0(N)$ coset and then to check that these canonical coset representatives are identical. One possible canonical form is given in the next proposition. The complicating factor is that the determinants of the coset representatives may have prime factors which divide N.

Proposition 3.13. *Let*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2, \mathbb{Z})$$

with $\gcd(a, b, c, d) = 1$ *and let* $\det(A) = D$ *with* $D \neq 0$. *Then in* $\Gamma_0(N)A$ *there is a unique element*

$$\begin{pmatrix} \lambda\alpha & \beta \\ \epsilon\alpha & \phi \end{pmatrix}$$

with $\alpha = \gcd(a, c)$, $\epsilon\alpha = \gcd(aN, c)$, $0 \leq \lambda < \epsilon$, *and*

$$\phi = \min\{x \in \mathbb{Z}^{>0} \mid \begin{pmatrix} * & * \\ \gcd(aN, c) & x \end{pmatrix} = yA,$$

for some $y \in \Gamma_0(N)\}$.

Proof: First we show that there is some $y \in \Gamma_0(N)$ such that yA has the given properties. Let $g = \gcd(aN, c)$. Since $\det(A) \neq 0$, either $a \neq 0$ or $c \neq 0$, so g is a positive integer. Also there are integers p and q such that $qaN + pc = g$. There is a unique decomposition $N = rs$ where $\gcd(r, p) = 1$ and $s|p^\infty$ (i.e., every prime which divides s also divides p). Set $k = r(1 + \gcd(aN, p))$ and define $p_1 = p - kaN/g$ and $q_1 = q + kc/g$. Then we have $q_1aN + p_1c = g$; note that this means that q_1 and p_1 are coprime. Moreover, we can show that $\gcd(N, p_1) = 1$ as follows: if a prime ℓ divides N, but does not divide p, then ℓ divides r and hence k. So ℓ does not divide $p - kaN/g$. If a prime ℓ divides N and also divides p, then it divides $\gcd(aN, p)$ and so ℓ does not divide k. But ℓ also does not divide aN/g, since $\gcd(aN/g, p) = 1$. So again ℓ does not divide $p - kaN/g$. Thus none of the primes dividing N divide p_1 and so $\gcd(N, p_1) = 1$. As already noted, q_1 and p_1 are coprime and so we can find integers u_1 and v_1 such that $u_1p_1 - v_1q_1N = 1$. So

$$t_1 = \begin{pmatrix} u_1 & v_1 \\ q_1N & p_1 \end{pmatrix}$$

is an element of $\Gamma_0(N)$ and

$$t_1A = \begin{pmatrix} a' & b' \\ g & d' \end{pmatrix}.$$

We can show that the parameter ϕ is well-defined as follows. For any integer r, the two integers rg^2N and $1 - ra'gN$ are coprime and so there are integers u_2 and v_2 such that

$$t_2 = \begin{pmatrix} u_2 & v_2 \\ rg^2N & 1 - ra'gN \end{pmatrix}$$

is an element of $\Gamma_0(N)$. A calculation shows that

$$t_2t_1A = \begin{pmatrix} * & * \\ g & d' + rgN(b'g - d'a') \end{pmatrix} = \begin{pmatrix} * & * \\ g & d' - rgND \end{pmatrix}$$

and for a suitable choice of r, we have $d' - rgND > 0$. So the set

$$\{x \in \mathbb{Z}^{>0} \mid \begin{pmatrix} * & * \\ \gcd(aN, c) & x \end{pmatrix} = yA, \text{ for some } y \in \Gamma_0(N)\}$$

is not empty and so ϕ is well-defined.

Let $\alpha = \gcd(a, c)$ and $\epsilon = g/\alpha$. Then we have shown that there is some y in $\Gamma_0(N)$ such that

$$yA = \begin{pmatrix} \lambda\alpha & \beta \\ \epsilon\alpha & \phi \end{pmatrix}$$

where the condition that $0 \le \lambda < \epsilon$ can be arranged by multiplication by a matrix of the form

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}.$$

To show that this element is unique, suppose

$$y'A = \begin{pmatrix} \lambda'\alpha' & \beta' \\ \epsilon'\alpha' & \phi' \end{pmatrix}.$$

Then we immediately have $\alpha' = \gcd(a, c) = \alpha$ and hence also $\epsilon' = g/\alpha = \epsilon$. Also from the definition, $\phi' = \phi$. Thus

$$y'A = \begin{pmatrix} \lambda'\alpha & \beta' \\ \epsilon\alpha & \phi \end{pmatrix}.$$

A computation shows that

$$yA(y'A)^{-1} = \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}.$$

But we also have $yA(y'A)^{-1} \in \Gamma_0(N)$ and so we must have

$$yA = \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} y'A.$$

Finally the condition $0 \le \lambda, \lambda' < \epsilon$ forces $z = 0$ and so $y'A = yA$ as required. □

Corollary 3.14. *The parameters $\lambda\alpha$, $\epsilon\alpha$, β, and ϕ uniquely fix the coset $\Gamma_0(N)A$.*

Remark 3.15.

(i) The parameters ϵ and α can be found using the method described in the proof of Proposition 3.13. A slight refinement of the proof also yields a method of finding ϕ, and hence λ, as follows. Given

$$t_1A = \begin{pmatrix} a' & b' \\ g & d' \end{pmatrix},$$

the most general matrix $t_2 \in \Gamma_0(N)$ such that

$$t_2t_1A = \begin{pmatrix} * & * \\ g & * \end{pmatrix}$$

has the form

$$t_2 = \begin{pmatrix} u & v \\ -rN & 1 + ra'N/g \end{pmatrix}.$$

So

$$t_2t_1A = \begin{pmatrix} * & *c \\ g & rND/g + d' \end{pmatrix}.$$

Thus ϕ is bounded below by $d_0 = d' \pmod{ND/g}$. This bound is not necessarily achieved as the corresponding value $r = r_0 = (d_0 - d')g/(ND)$ may have $\gcd(1 + r_0a'N/g, N) \ne 1$. However, r is bounded above, for example, by $r_1 = (d'^2 + 1)g^2$ and so a finite search gives the value of ϕ.

(ii) In practice, the index of $\Gamma_0(N)$ can be large so that storing all the coset representatives becomes a significant constraint on the calculation. This problem can be avoided, at the cost of extra computation, by finding a subset of "reduced canonical coset representatives" which generate the full set (by right multiplication). As we shall see in the next section, given two congruence subgroups G and H, it is straightforward to compute the "virtual index" of H in G, which is the index if H is a subgroup of G. So, if moonshine groups G and H have the same level, the virtual index of H in G is 1, and the reduced canonical coset representatives of H are contained in the canonical coset representatives of G, then $G = H$. The point here is that we do not have to compute the reduced canonical coset representatives of G, which would often involve significantly more computation.

4. MORE RESULTS NEEDED FOR THE COMPUTATIONS

In this section we record other results needed in the computations. In order to find the list of congruence subgroups we will need an explicit description of the quotient groups $\Gamma_0(f)^+/G(n, f)$.

If m is an element of $\mathrm{SL}(2, \mathbb{R})$ and m is such that $m = \lambda m'$ for some $\lambda \in \mathbb{R}$, $\lambda \ne 0$,

$$m' = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2, \mathbb{Z}),$$

$\gcd(a, b, c, d) = 1$, then we write $|m| = ad - bc$. This is well-defined since m' is unique up to a sign if it exists.

Lemma 4.1. *Let f be a squarefree integer. Define $E = \{e \in \mathbb{Z}^{>0} \mid e \text{ divides } f\}$ and a binary operation on E by $e_1 \cdot e_2 = e_1e_2/\gcd(e_1, e_2)^2$. Then with this operation E is a group and if $m_1, m_2 \in \Gamma_0(f)^+$, then $|m_1m_2| = |m_1| \cdot |m_2|$.*

Proof: That the set E, together with the given binary operation, forms a group is a straightforward exercise. To show that $|m_1m_2| = |m_1|\cdot|m_2|$, note that from Definition 2.1 we have $m_i = e_i^{-1/2}m_i'$, $i = 1, 2$, where m_i' is an integer matrix of determinant e_i, and so $|m_i| = e_i$, $i = 1, 2$. Then using the form of m_1 and m_2 given in Definition 2.1, it is easy to verify that $m_3 = \gcd(e_1, e_2)^{-1}m_1'm_2'$ is a matrix with integer entries and determinant $e_1 \cdot e_2$. Since the determinant is squarefree, the entries of m_3 are coprime. Moreover, m_3 is a multiple of m_1m_2, so that $|m_1m_2| = \det(m_3) = e_1 \cdot e_2 = |m_1| \cdot |m_2|$. □

Remark 4.2. We will use the notation $m \cdot e$ for $|m| \cdot e$.

Proposition 4.3. *Let f be a squarefree integer and n be a positive integer. Let K be a set and ψ a homomorphism of $\mathrm{SL}(2,\mathbb{Z})$ into $Sym(K)$ (the group of permutations of K) such that the kernel of ψ is $\Gamma(n)$. For convenience we write xm for $(x)\psi(m)$, $m \in \mathrm{SL}(2,\mathbb{Z})$, $x \in K$ (actions are from the right, as this is the Magma convention). Define*

$$\sigma : E \times \Gamma_0(n)^+ \to \mathrm{SL}(2,\mathbb{Z})$$

by $\sigma(e, m)$ $=QmP$, where

$$P = P(e,m) = \begin{pmatrix} \sqrt{e}\sqrt{e\cdot m}/f & 0 \\ 0 & \sqrt{e}/\sqrt{e\cdot m} \end{pmatrix}$$

and

$$Q = Q(e) = \begin{pmatrix} f/e & 0 \\ 0 & 1 \end{pmatrix}.$$

Define

$$\phi(m) : E \times K \to E \times K$$

by $(e, x)\phi(m) = (e \cdot m, x\sigma(e, m))$. Then $\phi : \Gamma_0(n)^+ \to Aut(E\times K)$ is a group homomorphism with kernel $G(n, f)$ (where $Aut(E \times K)$ is the group of permutations of the set $E \times K$).

Proof: We have

$$\begin{aligned}(e,x)\phi(m_1)\phi(m_2) &= (e\cdot m_1, x\sigma(e,m_1))\phi(m_2)\\ &= (e\cdot m_1\cdot m_2, x\sigma(e,m_1)\sigma(e\cdot m_1, m_2)).\end{aligned}$$

Thus to show that ϕ is a homomorphism it is sufficient to show that $\sigma(e, m_1)\sigma(e \cdot m_1, m_2) = \sigma(e, m_1m_2)$. From the definition of σ we have

$$\begin{aligned}&\sigma(e,m_1)\sigma(e\cdot m_1, m_2) =\\ &\qquad Q(e)m_1P(e,m_1)Q(e\cdot m_1)m_2P(e\cdot m_1, m_2).\end{aligned}$$

But $P(e, m_1)Q(e \cdot m_1) = (\sqrt{e}/\sqrt{e \cdot m_1})1_2$. So

$$\begin{aligned}\sigma(e,m_1)\sigma(e\cdot m_1, m_2) &= (\sqrt{e}/\sqrt{e\cdot m_1})Q(e)m_1m_2\\ &\qquad \times P(e\cdot m_1, m_2)\\ &= Q(e)m_1m_2P(e, m_1m_2)\\ &= \sigma(e, m_1m_2)\end{aligned}$$

as required.

Next we show that the kernel is $G(n, f)$. If

$$m = \begin{pmatrix} a & b \\ fc & d \end{pmatrix} \in G(n,f),$$

then

$$a - 1 \equiv d - 1 \equiv b \equiv c \equiv 0 \pmod{n}$$

and $|m| = 1$. Hence for any $e \in E$ we have

$$\sigma(e,m) = \begin{pmatrix} a & bf/e \\ ce & d \end{pmatrix} \in \Gamma(n).$$

So $(e, x)\phi(m) = (e \cdot 1, x\sigma(e, m)) = (e, x)$ for all $(e, x) \in E \times K$. Thus $G(n, f) \subset \mathrm{kernel}(\phi)$. Conversely, if $(e, x)\phi(m) = (e, x)$ for all $(e, x) \in E \times K$, then $|m| \cdot 1 = 1$ and so $|m| = 1$. Also $(1, x)\phi(m) = (1, x)$ implies

$$\begin{pmatrix} a & bf \\ c & d \end{pmatrix} \in \Gamma(n).$$

Hence $a-1 \equiv d-1 \equiv c \equiv 0 \pmod{n}$. Also $(f, x)\phi(m) = (f, x)$ implies

$$\begin{pmatrix} a & b \\ cf & d \end{pmatrix} \in \Gamma(n)$$

and hence $b \equiv 0 \pmod{n}$ and so $m \in G(n, f)$. □

Remark 4.4.

(i) If $m = \in \Gamma_0(f)^+$ with

$$m = |m|^{-1/2}\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

$a, b, c, d \in \mathbb{Z}$, then

$$\sigma(e,m) = \begin{pmatrix} a/g & bfg/(e|m|) \\ ce/fg & dg/|m| \end{pmatrix},$$

where $g = \gcd(e, |m|)$.

(ii) In particular if we take $K = (\mathbb{Z}/n\mathbb{Z})^2$, then the action of m on (e, x) is given by

$$\begin{aligned}\phi(m) : e &\mapsto e\cdot m\\ x_1 &\mapsto (a/g)x_1 + (ce/fg)x_2 \pmod{n}\\ x_2 &\mapsto (bfg/e|m|)x_1 + (dg/|m|)x_2 \pmod{n}\end{aligned}$$

where $g = \gcd(e, |m|)$.

(iii) In (ii), since $\sigma(e,m) \in \mathrm{SL}(2,\mathbb{Z})$, ϕ preserves $\gcd(x_1,x_2,n)$ and so we can restrict the representation to $\{x=(x_1,x_2) \mid \gcd(x_1,x_2,n)=1\}$.

When computing the congruence subgroups of $\Gamma_0(f)^+$ it is possible that the same group may appear for more than one value of f. Given a congruence subgroup G of $\Gamma_0(f)^+$, the following proposition tells us which other $\Gamma_0(F)^+$ contain G as a subgroup. This proposition was used in Table 2 to calculate the groups in the "Equal" column.

Proposition 4.5. *Let G be a level n congruence subgroup of $\Gamma_0(f)^+$ where f is squarefree. Let $G=\cup_{i=1}^{I} G(n,f)\gamma_i$ be a coset decomposition of G over $G(n,f)$, where*

$$\gamma_i = e_i^{-1/2}\begin{pmatrix} e_i a_i & b_i \\ f c_i & e_i d_i \end{pmatrix},$$

$a_i,b_i,c_i,d_i \in \mathbb{Z}$, e_i is an exact divisor of f, $\det(\gamma_i)=e_i$, and $\gcd(e_ia_i,b_i,fc_i,e_id_i)=1$, $1\le i\le I$. Define $f_{min}=\mathrm{lcm}(e_1,e_2,\ldots,e_I)$ and $C=\gcd(n,c_1,c_2,\ldots,c_I)$. Then G is a subgroup of $\Gamma_0(F)^+$ for F squarefree iff f_{min} divides F and F divides Cf. Also if $\{\gamma_{i_1},\ldots,\gamma_{i_s}\}$ is a subset of coset representatives which generate G over $G(n,f)$, then $C=\gcd(n,c_{i_1},\ldots,c_{i_s})$.

Proof: First note that since all the elements of $G(n,f)$ have determinant 1, the value of f_{min} is independent of the choice of coset representatives. The value of $\gcd(c_1,\ldots,c_I)$ depends of the choice of cosets, but different values are congruent modulo n so that C is independent of the choice of cosets.

Suppose G has level $n=n(G,f)$ and is a subgroup of $\Gamma_0(f)^+$ with invariants f_{min} and Cf and suppose also that G is a subgroup of $\Gamma_0(F)^+$; we show that f_{min} divides F and F divides Cf. Fix a coset decomposition of G, $G=\cup_{i=1}^{I} G(n,f)\gamma_i$. Then $\gamma_i\in\Gamma_0(F)^+$, $i=1,\ldots I$. Since the possible determinants of elements of $\Gamma_0(F)^+$ (when scaled to be integral with no common factor) are the divisors of F, we have $e_i|F$, $i=1,\ldots I$, so $f_{min}|F$. Since $G(n,f)\subset G\subset\Gamma_0(F)^+$ we have

$$\begin{pmatrix} 1 & 0 \\ nf & 1 \end{pmatrix} \in \Gamma_0(F)^+,$$

so $F|nf$. Also $\gamma_i\in\Gamma_0(F)^+$ implies that $F|fc_i$, $i=1,\ldots,I$, and hence $F|Cf$.

Conversely, suppose G is a level n subgroup of $\Gamma_0(f)^+$ and that F is a squarefree integer such that f_{min} divides F and F divides Cf. Then we have to show that G is a subgroup of $\Gamma_0(F)^+$. As before, let $G=\cup_{i=1}^{I} G(n,f)\gamma_i$, $i=1,\ldots,I$ be a coset decomposition of G over $G(n,f)$. We will show that $G(n,f)$ and all the coset representatives are in $\Gamma_0(F)^+$. An element m of $G(n,f)$ has the form

$$m=\begin{pmatrix} * & * \\ *nf & * \end{pmatrix}$$

and since F divides Cf it also divides nf and hence $m\in\Gamma_0(F)\subset\Gamma_0(F)^+$. Let

$$\gamma_i = e_i^{-1/2}\begin{pmatrix} e_i a_i & b_i \\ f c_i & e_i d_i \end{pmatrix}$$

be a coset representative of G over $G(n,f)$. Then e_i divides F, since e_i divides f_{min}. Also F divides Cf which divides c_if. Let $c_if=c_i'F$. Thus

$$\gamma_i = e_i^{-1/2}\begin{pmatrix} e_i a_i & b_i \\ c_i' F & e_i d_i \end{pmatrix},$$

where $e_ia_i,b_i,c_i'F,e_id_i\in\mathbb{Z}$, $\gcd(e_ia_i,b_i,Fc_i',e_id_i)=1$, and e_i divides F. So $\gamma_i\in\Gamma_0(F)^+$. Thus $G\subset\Gamma_0(F)^+$ as required.

For the last part of the proposition, let

$$\gamma = e^{-1/2}\begin{pmatrix} ea & b \\ fc & ed \end{pmatrix}$$

and

$$\gamma' = e'^{-1/2}\begin{pmatrix} e'a' & b \\ f'c' & e'd' \end{pmatrix}$$

be two coset representatives. Then we observe that

$$\gamma\gamma' = (ee')^{1/2} g\begin{pmatrix} * & * \\ (\frac{a'}{g}c+\frac{d}{g}c')f & * \end{pmatrix} = (e\cdot e')^{-1/2}\gamma'',$$

where $g=\gcd(e,e')$ and γ'' is a matrix with coprime entries and with determinant $e\cdot e'=ee'/g^2$. Similarly pre- or post-multiplying γ by an element of $G(n,f)$ gives a matrix with coprime entries and determinant e of the form

$$e^{-1/2}\begin{pmatrix} * & * \\ (rc+sn)f & * \end{pmatrix}.$$

Thus every element

$$\begin{pmatrix} * & * \\ cf & * \end{pmatrix} \in G$$

has c divisible by $C'=\gcd(n,c_{i_1},\ldots,c_{i_s})$. So C' divides C. But the cosets $\{\gamma_1,\ldots,\gamma_I\}$ also generate G over $G(n,f)$, so applying the same argument we have that C divides C' and so $C=C'$. □

Remark 4.6.

(i) Note that groups which are conjugate in $\Gamma_0(f)^+$ may give rise to subgroups of $\Gamma_0(F)^+$ which are not conjugate. For example, the groups $\Gamma_0(4)$ and $\Gamma(2)$ are conjugate in $\Gamma_0(2)^+$, but are not conjugate in $\Gamma(1)$. Thus in Table 2 we list the subgroups G of $\Gamma_0(f)^+$ up to conjugacy in $\Gamma_0(f)^+$ and in the "Equal" column give a list of subgroups G' of $\Gamma_0(F)^+$ up to conjugacy in $\Gamma_0(F)^+$, $F \neq f$, such that at least one conjugate of G in $\Gamma_0(f)^+$ is equal to at least one conjugate of G' in $\Gamma_0(F)^+$.

(ii) Although f_{min} is invariant under conjugation in $\Gamma_0(f)^+$ (since the corresponding determinants are invariant), it is not true that C is invariant under conjugation. For example, $\Gamma_1(3)$ is a level 3 congruence subgroup of $\Gamma(1)$ and possible coset representatives over $\Gamma(3)$ are

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \quad \text{and} \quad \begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}.$$

This gives $f_{min} = 1$, $C = 3$, and $Cf = 3$. So the proposition says that $\Gamma_1(3)$ is a congruence subgroup of $\Gamma(1)$ and $\Gamma_0(3)^+$, as expected. The conjugate $\Gamma^1(3)$, which is $\Gamma_1(3)$ conjugated by

$$\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix},$$

is also a level 3 congruence subgroup of $\Gamma(1)$ and possible coset representatives are

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}, \quad \text{and} \quad \begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix}.$$

So in this case $f_{min} = 1$ (as before), but now $C = 1$ and $Cf = 1$. Hence the proposition states that $\Gamma^1(3)$ is a congruence subgroup only of $\Gamma(1)$. This is, of course, a consequence of the fact that in Theorem 2.2 we have selected particular conjugates of the $\Gamma_0(f)^+$. For example, taking $\Gamma^0(f)^+$, the conjugate of $\Gamma_0(f)^+$ by

$$\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix},$$

we exchange the roles of $\Gamma_1(3)$ and $\Gamma^1(3)$ in this example.

We now give some results which provide a formula for the "virtual index" of one congruence group in another. Recall (see, for example, [Shimura 71, Chapter 3]) that subgroups A and B of a group G are said to be commensurable iff there is a subgroup H which has finite index in both A and B. If A and B are commensurable, then we write $A \sim B$. Commensurability is an equivalence relation, and the equivalence class of A is written $\mathrm{Cl}(A)$. The set $\mathrm{Com}(A) = \{g \in G \mid A^g \sim A\}$ is a subgroup of G and $\mathrm{Com}(A) = \mathrm{Com}(B)$ if $A \sim B$. $\mathrm{Com}(A)$ is called the commensurator of A. Also if $A \sim B$, then $A^g \sim B^g$ for any $g \in G$, where $A^g = g^{-1}Ag$.

Definition 4.7. Let G be a group and A be a subgroup of G. For any group B in $\mathrm{Cl}(A)$ and for any common subgroup H of finite index in A and B define

$$VI(A, B; H) = \frac{\mathrm{Index}(A : H)}{\mathrm{Index}(B : H)}.$$

Lemma 4.8. *Suppose A, B, and C are in the same commensurability class, then*

1. *$VI(A, B : H)$ is independent of the choice of H. Denote this common value by $VI(A, B)$.*
2. *$VI(A, B)VI(B, C) = VI(A, C)$. In particular, $VI(A, B) = 1/VI(B, A)$.*
3. *if A and B are subgroups of $\mathrm{PSL}(2, \mathbb{R})$ which are commensurable with $\mathrm{SL}(2, \mathbb{Z})$ and $g \in \mathrm{Com}(\mathrm{SL}(2, \mathbb{Z}))$, then $VI(A^g, B) = VI(A, B)$.*

Proof:

1. Suppose H and H' are two subgroups of finite index in both A and B. Then $H \sim A$ and $A \sim H'$, so $H \sim H'$ so there is a subgroup H'' of finite index in both H and H'. Then

$$\begin{aligned} VI(A, B; H') &= \frac{\mathrm{Index}(A : H')\mathrm{Index}(H' : H'')}{\mathrm{Index}(B : H')\mathrm{Index}(H' : H'')} \\ &= \frac{\mathrm{Index}(A : H)\mathrm{Index}(H : H'')}{\mathrm{Index}(B : H)\mathrm{Index}(H : H'')} \\ &= \frac{\mathrm{Index}(A : H)}{\mathrm{Index}(B : H)} \\ &= VI(A, B; H). \end{aligned}$$

2. There is a subgroup H_1 of finite index in both A and B and a subgroup H_2 of finite index in both B and C. H_1 is commensurable with H_2 since $H_1 \sim B$ and $B \sim H_2$. So there is a subgroup H_3 which has finite index in A, B, and C. Then from Defintion 4.7 we find $VI(A, B; H_3)VI(B, C; H_3) = VI(A, B, H_3)$

and so the result follows from (1). The second part follows by setting $A = C$ and noting that $VI(A,B) > 0$, so the inverse is defined.

3. For groups which are commensurable with $\mathrm{SL}(2,\mathbb{Z})$ we have $VI(A,B) = \mathrm{Area}(B)/\mathrm{Area}(A)$. Since A^g is commensurable with $SL(2,\mathbb{Z})$, $VI(A^g,B)$ is defined. Then

$$\begin{aligned} VI(A^g,B) &= \mathrm{Area}(B)/\mathrm{Area}(A^g) \\ &= \mathrm{Area}(B)/\mathrm{Area}(A) = VI(A,B). \end{aligned}$$ □

Remark 4.9. (3) is not true in general. For example, take $G = \mathrm{SL}(2,\mathbb{R})$ and

$$A = \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle.$$

Then A is conjugate in G to

$$B = \langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \rangle,$$

but $VI(A,B) = 2$. It is an easy exercise to show for $g \in \mathrm{Com}(A)$ that $VI(B^g,C) = VI(B,C)$ for all $B,C \in \mathrm{Cl}(A)$ iff $VI(D^g,D) = 1$ for some $D \in \mathrm{Cl}(A)$.

Corollary 4.10. *If K_i is a subgroup of $\Gamma_0(f_i)^+$ of level n_i and* $\mathrm{Index}(K_i, G(n_i,f_i)) = k_i$, *$i = 1,2$. Then*

$$VI(K_1,K_2) = \frac{k_1 n_2^3 \prod\limits_{\substack{\ell \mid n_2 f_2 \\ \ell \text{ prime}}} (1+\frac{1}{\ell}) \prod\limits_{\substack{\ell \mid n_2 \\ \ell \text{ prime}}} (1-\frac{1}{\ell})}{k_2 n_1^3 \prod\limits_{\substack{\ell \mid n_1 f_1 \\ \ell \text{ prime}}} (1+\frac{1}{\ell}) \prod\limits_{\substack{\ell \mid n_1 \\ \ell \text{ prime}}} (1-\frac{1}{\ell})}.$$

Proof: We have

$$\begin{aligned} VI(K_1,K_2) &= VI\big(G_1, G(n_1,f_1)\big) VI\big(G(n_1,f_1), \\ &\qquad G(n_2,f_2)\big) VI\big(G(n_2,f_2), G_2\big) \\ &= \frac{k_1}{k_2} VI\big(H(n_1,n_1,n_1f_1), H(n_2,n_2,n_2f_2)\big) \\ &= \frac{k_1}{k_2} \frac{VI\big(H(1,1,1), H(n_2,n_2,n_2f_2)\big)}{VI\big(H(1,1,1), H(n_1,n_1,n_1f_1)\big)}. \end{aligned}$$

Applying Proposition 2.9 (3) gives the result. □

Remark 4.11.

(i) A particular case of Corollary 4.10 is the following: if K is a subgroup of $\Gamma_0(f)^+$ of level n and $\mathrm{Index}(K : G(n,f)) = i$, then

$$VI(K,\Gamma_0(N)) = \frac{iN \prod\limits_{\substack{\ell \mid N \\ \ell \text{ prime}}} (1+\frac{1}{\ell})}{n^3 f \prod\limits_{\substack{\ell \mid nf \\ \ell \text{ prime}}} (1+\frac{1}{\ell}) \prod\limits_{\substack{\ell \mid n \\ \ell \text{ prime}}} (1-\frac{1}{\ell})}.$$

(ii) Corollary 4.10 together with Lemma 4.8 (3) gives a useful necessary condition for H to be a subgroup of some conjugate of G, namely that $VI(G,H)$ has to be an integer. In particular, (i) was used in the search for moonshine groups to check that $VI(K,\Gamma_0(N))$ was an integer before any of the detailed computations were performed.

The following three propositions provide a method for identifying $GL(2,\mathbb{Q})^+$ conjugates inside $\Gamma_0(f)^+$. This information was not included in the tables.

Proposition 4.12. *Suppose G and H are congruence subgroups of $\Gamma_0(f)^+$, with f squarefree, which are conjugate in* $\mathrm{SL}(2,\mathbb{R})$. *Then H is conjugate in $\Gamma_0(f)^+$ to $m^{-1}Gm$ where*

$$m = \begin{pmatrix} p & q \\ 0 & r \end{pmatrix}$$

with $p,r > 0$, $0 \le q < p$, $\gcd(p,q,r) = 1$, *$p \mid n$, $r \mid (n/p)\gcd(f,p)$ where n is the level of G. Also, the level of H divides* $\gcd(pr,n)n$.

Proof: By assumption $H = m'^{-1}Gm'$ with $m' \in \mathrm{SL}(2,\mathbb{R})$. As in Proposition 3.2, we can conjugate by a suitable element of $\Gamma_0(f)^+$ and multiply m by a suitable scalar so that $H' = m^{-1}Gm$ with

$$m = \begin{pmatrix} p & q \\ 0 & r \end{pmatrix},$$

$p,q,r \in \mathbb{Z}$, $p,r > 0$, $\gcd(p,q,r) = 1$, and H' is conjugate to H in $\Gamma_0(f)^+$. By conjugating by a suitable power of

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

we can also arrange that $0 \le q < p$. If G has level n, then

$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ nf & 1 \end{pmatrix}$$

are elements of G. Using the fact that the conjugates of these two elements by m have squarefree determinant, and hence must be contained in $\Gamma_0(f)$, we find that

$$p \mid nr,\ pr \mid nfq^2,\ r \mid nfq \text{ and } r \mid np.$$

Let $p = p_1p_2$ where $p_1 = \gcd(p, n)$. So $p_1|n$ and

$$\gcd(p_2, n/p_1) = 1.$$

Then $p_1p_2|nr$ gives $p_2|(n/p_1)r$, so $p_2|r$. So let $r = hp_2$. Since $\gcd(p, q, r) = 1$ this implies $\gcd(p_2, q) = 1$. Then $pr|nfq^2$ gives $p_1p_2^2h|nfq^2$, so in particular $p_1p_2^2|nfq^2$ and hence $p_2^2|(n/p_1)q^2f$. But p_2 is coprime to $(n/p_1)q^2$ and so $p_2^2|f$. Since f is squarefree this is only possible if $p_2 = 1$. Hence $p = p_1$ and so $p|n$.

To show that

$$r|(n/p)\gcd(n, f),$$

note that since $p|n$ we have

$$r|(n/p)fq^2.$$

Also $r|(n/p)p^2$. Thus

$$r|(n/p)\gcd(fq^2, p^2).$$

But

$$\gcd(fq^2, p^2)|\gcd(f, p^2)\gcd(q^2, p^2)$$

so that

$$r|(n/p)\gcd(f, p^2)\gcd(q^2, p^2).$$

But f is squarefree so $\gcd(f, p^2) = \gcd(f, p)$ and $\gcd(p, r, q) = 1$ so r is coprime to $\gcd(q^2, p^2)$. Thus $r|(n/p)\gcd(f, p)$ as required. (Note that this implies that $r|n$ and $pr|nf$.)

To show the condition on the level, a direct computation shows that $mG(prn, f)m^{-1} \subset G(n, f)$ and since $G(n, f) \subset G$ this gives $G(prn, f) \subset m^{-1}Gm$ and so, by Lemma 2.12, the level of $m^{-1}Gm$ divides prn. A similar calculation, using $p|n$, $r|n$, and $pr|nf$, shows that $G(n^2, f) \subset m^{-1}Gm$ and so that level also divides n^2. Hence the level of $m^{-1}Gm$ divides $\gcd(pr, n)n$. Now H is conjugate in $\Gamma_0(f)^+$ to $m^{-1}Gm$ and conjugacy in $\Gamma_0(f)^+$ preserves the level. Hence the level of H divides $\gcd(pr, n)n$ as required. □

Corollary 4.13. *If G and H are related as in the last proposition, then for all primes p, p divides the level of G if and only if p divides the level of H.*

Proof: Let n_G be the level of G and n_H be the level of H. By the last proposition n_H divides n_G^2. So if p divides n_H, then p also divides the n_G. Similarly, $n_G|n_H^2$ and so if p divides n_G it also divides n_H as required. □

Remark 4.14. Using Proposition 4.12 we can identify $\mathrm{SL}(2, \mathbb{R})$ conjugates as follows. Given $G \subset \Gamma_0(f)^+$, suppose $\gamma_1, \ldots, \gamma_k$ generate G. Then for each

$$m = \begin{pmatrix} p & q \\ 0 & r \end{pmatrix}$$

satisfying the constraints given in Proposition 4.12, and for each level n_H which divides $\gcd(pr, n)n$, we test

$$W(G, m, n_H) = \langle \gamma_1^m G(n_H, f), \ldots, \gamma_k^m G(n_H, f) \rangle$$

in $\Gamma_0(f)^+/G(n_H, f)$ for equality with the images in $\Gamma_0(f)^+/G(n, f)$ of all the conjugates of all the subgroups of $\Gamma_0(f)^+$ of level n_H and the same genus as G. It is possible that the pre-image, H, of $W(G, m, n_H)$ in $\Gamma_0(f)^+$ is strictly larger than G^m, but these cases can be identified by computing the virtual index of G in H.

5. OUTLINE OF THE ALGORITHMS

Implementing the algorithms given in the previous sections is a nontrivial task. The resulting Magma code is several thousand lines long and a detailed listing would not be practical. Thus this section gives only an outline of how the previous results are used in the computation of the tables.

Step 1: To use Proposition 4.3 to construct faithful permutation representations we first need to construct faithful permutation representations of the groups $\mathrm{SL}(2, \mathbb{Z}/p^n\mathbb{Z}) \cong \mathrm{SL}(2, \mathbb{Z})/\Gamma(p^n)$ for primes p and then apply the standard decomposition Lemma 2.10 (7) to construct $\mathrm{SL}(2, \mathbb{Z})/\Gamma(N)$. This calculation was done for all primes p and positive integers n such that $p^n < 2^{13}$ using ad hoc methods. The aim is to find representations of small degree. The only difficult case is when $p = 2$, since the centre of the group is enlarged.

Step 2: Next, generators and representatives of the torsion classes of $\Gamma_0(f)^+$ were computed for all squarefree f such that $f \leq 3000$ and for all f such that the genus of $\Gamma_0(f)^+$ is less than or equal to 24. This was done by constructing a fundamental domain for these groups bounded by principal circles, as described for example by Ford [F]. The details of this computation will appear elsewhere [Cummins and Pauli 03].

Step 3: For each fixed genus g (in this paper g=0 or 1) the list of all $\Gamma_0(f)^+$ with genus less than or equal to g was found, as described in Section 2. Then the list of possible levels was computed using Theorem 2.17. From this list the maximal levels, i.e., levels which are not divisors

of other possible levels, were found. For each maximal level, n, the group $\Gamma_0(f)^+/G(n,f)$ was constructed using Proposition 4.3 and the generators found in Step 2. The subgroup tree was then searched using the Magma routine MaximalSubgroups, starting with the full group. The genus of each subgroup was computed using the torsion classes found in Step 2 and the Riemann-Hurwitz formula. The stopping criteria applied were: Theorem 2.14, the fact that the genus is nondecreasing on each chain of subgroups, and the restriction that we require each subgroup to contain -1. Groups were identified up to conjugacy in $\Gamma_0(f)^+$. The results of this calculation for genus 0 and 1 are in Table 2. The notation is described in the next section.

Step 4: To find the list of moonshine groups, Proposition 3.6 was applied to each conjugate of each group found in Step 3 (note: before applying this test we first compute the virtual index of $\Gamma_0(fnp^2h)$ which, by Proposition 3.6, must be an integer). The level was then found using Lemma 3.7. Finally the cosets over $\Gamma_0(N)$ were computed as described in Section 3 (see Lemma 3.9). Identical groups were found using the methods described in Section 3 (see comments after Corollary 3.14). The results are in Tables 3 and 4.

Additional data was then computed which is described in the next section.

6. THE TABLES

The tables are described in this section. Again, all tables can be found at http://www.expmath.org/expmath/volumes/13/13.3/cumminstables.pdf.

6.1 Table 1

The maximum squarefree f such that $\Gamma_0(f)^+$ has genus g for $0 \le g \le 100$. The calculation of this table was explained in Section 2.

6.2 Table 2

This is the main table. It contains the list of congruence subgroups of genus 0 and 1. The first column is a label for (the conjugacy class of) the group G. It has the form $n(Label)_f^g$ where $n = n(G,f)$ is the level of G, g is the genus of G, f is a squarefree integer such that G is a subgroup of $\Gamma_0(f)^+$, and *Label* is a label used to distinguish groups with the same values of n, g, and f. The next column identifies the group, where appropriate, as a subgroup of the involutive normalizer of $\Gamma_0(m)$ for some m (not always the level). The notation is that of Conway and Norton [Conway and Norton 79]. So $m-$ is $\Gamma_0(m)$ and $m+$ is $\Gamma_0(m)^+$. The notation $m + a_1, a_2, \ldots$ identifies subgroups between $m+$ and $m-$ as described in [Conway and Norton 79] (see also [Atkin and Lehner 70]). Column I is the index of G in $\Gamma_0(f)^+$. Column N is the normalizer of G in $\Gamma_0(f)^+$ (which is not always the full normalizer in $\mathrm{SL}(2,\mathbb{R})$). Column L is the number of conjugates of G in $\Gamma_0(f)^+$. Column E identifies the conjugacy class of subgroups G' of $\Gamma_0(F)$ with $F \neq f$ such that at least one group in the conjugacy class of G in $\Gamma_0(f)^+$ is equal to at least one of the conjugates of G' in $\Gamma_0(F)^+$. This column was calculated using the method described in Proposition 4.5. Note that the restriction that the conjugations be in $\Gamma_0(f)^+$ and $\Gamma_0(F)^+$ means that this relation need not be transitive. For example, one of the conjugates of $4G_1^0$ in Γ is equal to one of the conjugates of $4J_2^0$ in $\Gamma_0(2)^+$. Also one of the conjugates of $8H_1^0$ in Γ is equal to one of the conjugates of $4J_2^0$ in $\Gamma_0(2)^+$. This means that $4G_1^0$ is conjugate to $8H_1^0$ in $\mathrm{SL}(2,\mathbb{R})$, but they are not conjugate in Γ. Column T describes the structure of the conjugacy classes of torsion elements of $\overline{G} = G/\{\pm 1\}$ written in partition notation. So, for example, $3^1 2^2$ means that $\overline{G}$ contains one conjugacy class of elements of order 3 and two conjugacy classes of elements of order 2. Column S gives a list of the conjugacy classes of minimal super-groups H of G in $\Gamma_0(f)^+$, in other words, G is conjugate to a subgroup K of H such that there is no group L with $K \subset L \subset H$, with the inclusions being proper and all groups contained in $\Gamma_0(f)^+$.

6.3 Table 3

This is the list of moonshine groups of genus 0. As described in Proposition 3.11, there is an action of $\mathbb{Z}/24\mathbb{Z}$ on these groups. We call the elements of the $\mathbb{Z}/24\mathbb{Z}$ orbit the translations of G. Also, for any group G which contains $\Gamma(N)$ there is an action of the Galois group $(\mathbb{Z}/N\mathbb{Z})^*$ [Shimura 71, Chapter 6] (see also, for example, [Norton 93] and [Cummins and Gannon 97, Section 6]). In particular, if G contains $\Gamma_0(N)$, then the Galois group has exponent 2 and so its fixed field has the form $\mathbb{Q}(\sqrt{\pm p_1}, \sqrt{\pm p_2}, \ldots, \sqrt{\pm p_k})$ where p_i, $i = 1, \ldots k$, is either 1 or a prime and $p_1 < p_2 < \cdots < p_k$. The Galois action can be calculated once the cosets over $\Gamma(N)$ (or $\Gamma_0(N)$) are known. If f is an automorphic function of G all of whose q coefficients lie in $\mathbb{Q}(\zeta_N)$, then there is a q expansion of f such that the Galois action corresponds to Galois conjugation of the coefficients of f. To reduce the size of this table only one representative is given for each orbit under the group generated by translations by

1/24 and Galois automorphisms. The representative is selected to:

1. minimize the degree of the fixed field of the Galois group.

2. then minimize the cyclotomic level of the fixed field of the Galois group. (The cyclotomic level of a field K with abelian Galois group over $\mathbb{Q}$ is the smallest m such that K is contained in $\mathbb{Q}(\zeta_m)$.)

3. then maximize the intersection of the Galois and translation subgroups.

4. then minimize the Γ-level of the group.

If these are equal, then the groups are sorted using the ordering of the groups in Table 2 to which they are conjugate. The Γ-level and fixed field listed in the table are for this minimal representative and will not necessarily be the same for other groups in the equivalence class. In fact although it turns out to be possible to find a representative which simultaneously minimizes both the degree and cyclotomic level of the Galois groups, this representative does not, in general, maximize the size of the intersection of the Galois and translation subgroups, nor minimize the Γ-level.

The first column in Table 3 has the form $N(Label)^g$ where N is the Γ-level of G (which by Lemma 3.5 is the smallest N such that $\Gamma_0(N)$ is a subgroup of G) and g is the genus of G. Where appropriate, the columns labeled L give the labels given to the groups in [Conway and Norton 79] and [Norton 97]. All the groups with entries in the L column are genus 0 and rational (fixed by all Galois automorphisms); at most two groups in each equivalence class can be rational. Column P gives the period p which is defined to be $p = 24/s$ where s is the number of orbits of G under translations by 1/24. If G has normalized Hauptmodul f, then f has a q expansion of the form $1/q + \sum_{n>0} a_{pn-1} q^{pn-1}$. Column G lists the number of Galois conjugates of G. Column GT lists the number of Galois conjugates which are also translations of G. Column Irr lists the minimal p_i, $i = 1, \ldots, k$ as described above. The notation is that $\overline{x}, \overline{y}, i, \ldots, a, b$ is the field $\mathbb{Q}(\sqrt{-x}, \sqrt{-y}, i, \ldots, \sqrt{a}, \sqrt{b})$. So, for example, $\overline{15}$ is the field $Q(\sqrt{-15})$ and i 2 is $\mathbb{Q}(i, \sqrt{2})$. Column C lists the conjugacy classes of groups G' from Table 2 such that at least one of the elements of the equivalence class of G is conjugate in $\mathrm{SL}(2, \mathbb{R})$ to at least one of the elements of the conjugacy class of G' in $\Gamma_0(f)^+$.

6.4 Table 4

This is a list of moonshine groups of genus 1. The notation is the same as that in Table 3.

6.5 Table 5

A summary of the number of genus 0 moonshine groups by coefficient field. Each column is the minimal coefficient field as described above. The first column lists the number of rational groups. The number of groups is up to Galois conjugations and translations.

6.6 Table 6

The summary of the number of genus 1 moonshine groups by coefficient field. The notation is the same as Table 5.

6.7 Table 7

Summary of the total number of moonshine groups of genus 0 by Γ-level. The first entry gives the number of groups of each Γ-level N, where $N = mh^2$ with h the largest divisor of 24 such that h^2 divides N. The second entry is the number of groups which contain $\Gamma_0(N)$ normally and the last is the number of groups which contain some $\Gamma_0(N)$ normally, but for which N is not necessarily the Γ-level (see Section 7 for a discussion of this point).

6.8 Table 8

Summary of the total number of moonshine groups of genus 1 by Γ-level. The notation is as in Table 7.

7. COMMENTS ON OTHER RESULTS

This section has been added to comment on the relationship between this paper and that of Chua and Lang [Chua and Lang 03]. In their paper, Chua and Lang compute all the groups of genus 0 between some $\Gamma_0(M)$ and its normalizer. Thus there is some overlap with the genus 0 moonshine groups computed here in Table 3. The main differences are that Chua and Lang do not impose the restriction that G contains $z \mapsto z + k$ iff k is an integer (the "cusp width one at infinity" condition), while in this paper the restriction that G contain some $\Gamma_0(N)$ normally is not imposed. The strategy of the calculations is also different. Chua and Lang work directly in the quotient Normalizer$(\Gamma_0(N))/\Gamma_0(N)$, while in this paper the moonshine groups are found as conjugates of the congruence subgroups of $\Gamma_0(f)^+$, f a squarefree integer.

Thus to compare our results, the groups of Chua and Lang must be restricted to have width one at infinity and the groups found here must be restricted to contain some $\Gamma_0(N')$ normally. It is possible that $\Gamma_0(N') \subset \Gamma_0(N) \subset$

G, where N is the Γ-level of G, $\Gamma_0(N')$ is normal in G, and $\Gamma_0(N)$ is not normal in G. However, in this case, $\Gamma_0(N')$ is normal in $\Gamma_0(N)$ and so the following proposition gives a finite list of possibilities for N' given the Γ-level N.

Proposition 7.1. *Suppose* $\Gamma_0(N') \subset \Gamma_0(N)$. *Then the inclusion is normal iff* N'/N *divides* $\gcd(N, 24)$.

Proof: Note first if $\Gamma_0(N') \subset \Gamma_0(N)$, then by Proposition 2.9 (2) N divides N'. By Theorem 3.4, $\Gamma_0(N)$ is generated by

$$\Gamma_0(N') \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix}.$$

So $\Gamma_0(N')$ is normal in $\Gamma_0(N)$ iff

$$\begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix}$$

normalizes $\Gamma_0(N')$. From the description of the normalizer of $\Gamma_0(N')$ in [CN] it follows that

$$\begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix}$$

normalizes $\Gamma_0(N')$ iff $\frac{N'}{h}$ divides N, where h is the largest divisor of 24 such that h^2 divides N'. So we have to show that $\frac{N'}{h}$ divides N iff N'/N divides $\gcd(N, 24)$. Let $N' = kN$. Suppose first that $N = c\frac{N'}{h}$, then $h = ck$ so k divides 24. Also $N' = mh^2$ and so $N = c^2mk$ and hence k divides N and so divides $\gcd(N, 24)$. Conversely, suppose k divides $\gcd(N, 24)$. Then $N = kN''$ and so $k^2N'' = N'$. Hence k^2 divides N' and k divides 24 so that k divides h. Writing $h = ck$ gives $hN = ckN = cN'$ so that $N = c\frac{N'}{h}$ as required. □

Thus if G contains $\Gamma_0(N)$ then to test if G contains some $\Gamma_0(N')$ normally it suffices to check for each k dividing $\gcd(N, 24)$ that each of the generators of G over $\Gamma_0(N)$ normalizes $\Gamma_0(kN)$. The results of this calculation for genus 0 are contained in Table 7 and are in agreement with the results of Chua and Lang [Chua and Lang 03].

ACKNOWLEDGMENTS

I would like to thank John McKay and Simon Norton for helpful comments on the first version of this paper.The author's work was partly supported by NSERC.

REFERENCES

[Alexander et al. 92] D. Alexander, C. J. Cummins, J. McKay, and C. Simons. "Completely Replicable Functions." In *Groups, Combinatorics & Geometry*, pp. 87–98, London Math. Soc. Lecture Note Ser. 165. Cambridge, UK: Cambridge Univ. Press, 1992.

[Atkin and Lehner 70] A. O. L. Atkin, J. Lehner. "Hecke Operators for $\Gamma_0(m)$ " *Math. Ann.* 185 (1970), 134–160.

[Borcherds 92] R. E. Borcherds. "Monstrous Moonshine and Monstrous Lie Superalgebras." *Invent. Math.* 109 (1992), 405–444.

[Bosma et al. 97] W. Bosma, J. J. Cannon, and C. Playoust. "The Magma Algebra System I: The User Language." *J. Symb. Comp.* 40 (1997), 235–265.

[Chua and Lang 03] K. S. Chua and M. L. Lang. "Congruence Subgroups Associated to the Monster." *Exper. Math.* 13:3 (2004), 343–360.

[Conway and Norton 79] J. H. Conway and S. P. Norton. "Monstrous Moonshine." *Bull. Lond. Math. Soc.* 11 (1979), 308–339.

[Cox and Parry 84a] D. A. Cox and W. R. Parry. "Genera of Congruence Subgroups in Q-Quaternion Algebras." *J. Reine Angew. Math.* 351 (1984), 66–112.

[Cox and Parry 84b] D. A. Cox and W. R. Parry. "Genera of Congruence Subgroups in Q-Quaternion Algebras." Unabridged version, 1984.

[Cummins and Gannon 97] C. J. Cummins and T. Gannon. "Modular Equations and the Genus Zero Property of Moonshine Functions." *Invent. Math.* 129 (1997), 413–443.

[Cummins and Pauli 03] C. J. Cummins and S. Pauli. "Congruence Subgroups of PSL$(2,\mathbb{Z})$ of Genus Less than or Equal to 24." *Exper. Math.* 12:2 (2003), 243–255.

[Cummins and Pauli 04] C. J. Cummins and S. Pauli. "Fundamental Domains of Discrete Subgroups of PSL$(2,\mathbb{R})$." In preparation, 2004.

[Dennin 71] J. B. Dennin Jr. "Fields of Modular Functions of Genus 0." *Illinois J. Math.* 15 (1971), 442–455.

[Dennin 72] J. B. Dennin Jr. "Subfields of $K(2^n)$ of Genus 0." *Illinois J. Math.* 16 (1972), 502–518.

[Dennin 74] J. B. Dennin Jr. "The Genus of Subfields of $K(p^n)$." *Illinois J. Math.* 18 (1974), 246–264.

[Helling 66] H. Helling. "Bestimmung der Kommensurabilittsklasse der Hilbertschen Modulgruppe." *Math. Z.* 92 (1966), 269–280.

[Helling 70] H. Helling. "On the Commensurability Class of the Rational Modular Group." *J. London Math. Soc. (2)* 2 (1970), 67–72.

[Knopp and Newman 65] M. I. Knopp and M. Newman. "Congruence Subgroups of Positive Genus in the Modular Group." *Illinois J. Math* 9 (1965), 577–583.

[Lang 03] M. L. Lang. "On Thompson's Finiteness Theorem." Preprint, 2003.

[Larcher 82] H. Larcher. "The Cusp Amplitudes of the Congruence Subgroups of the Classical Modular Group." *Illinois J. Math.* 26:1 (1982), 164–172.

[Larcher 84] H. Larcher. "The Cusp Amplitudes of the Congruence Subgroups of the Classical Modular Group. II. *Illinois J. Math.* 28:2 (1984), 312–338.

[McKay 78] J. McKay. Unpublished letter to J. Thompson, 1978.

[McQuillan 66a] D. L. McQuillan. "Some Results on the Linear Fractional Group." *Illinois J. Math.* 10 (1966), 24–38.

[McQuillan 66b] D. L. McQuillan. "On the Genus of Fields of Elliptic Modular Functions." *Illinois J. Math.* 10 (1966), 479–487.

[Newman 55] M. Newman. "Structure Theorems for Modular Subgroups." *Duke Math. J.* 22 (1955), 25–32.

[Norton 82] S. P. Norton and S. P. Norton. "More on Moonshine." In *Computational Group Theory,* pp. 185–193. London: Academic Press, 1984.

[Norton 93] S. P. Norton. "Non-Monstrous Moonshine." In *Groups, Difference Sets, and the Monster,* pp. 433–441, Ohio State Univ. Math. Res. Inst. Publ. 4. Berlin: de Gruyter, 1996.

[Norton 97] S. P. Norton. Unpublished tables, 1997.

[Sebbar 01] A. Sebbar. "Classification of Torsion-Free Genus Zero Congruence Groups." *Proc. Amer. Math. Soc.* 129:9 (2001), 2517–2527 (electronic).

[Shimura 71] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions.* Princeton, NJ: Princeton University Press, 1971.

[Thompson 79] J. G. Thompson. "Some Numerology between the Fischer-Griess Monster and the Elliptic Modular Function." *Bull. London Math. Soc.* 11:3 (1979), 352–353.

[Thompson 80] J. G. Thompson. "A Finiteness Theorem for Subgroups of $PSL(2,\mathbb{R})$ Which Are Commensurable with $PSL(2,\mathbb{Z})$." In *Proc. Sym. Pure. Math.* 37, pp. 533–555. Providence, RI: Amer. Math. Soc., 1980.

[Wohlfart 64] K. Wohlfahrt. "An Extension of F. Klein's Level Concept." *Illinois J. Math.* 8 (1964), 529–535.

[Zograf 91] P. Zograf. "A Spectral Proof of Rademacher's Conjecture for Congruence Subgroups of the Modular Group." *J. Reine Angew. Math.* 414 (1991), 113–116.

Chris Cummins, Department of Mathematics and Statistics, Concordia University, Montreal, Québec H3G 1M8, Canada (cummins@mathstat.concordia.ca)

Received September 23, 2003, accepted March 19, 2004.